UNIVERSIDADE FEDERAL DE PERNAMBUCO
CIn – CENTRO DE INFORMÁTICA
PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Moisés Neves Camêlo

G-PRIV: um guia para especificação de requisitos de privacidade em conformidade com a LGPD

Recife
2022

Moisés Neves Camêlo

G-PRIV: um guia para especificação de requisitos de privacidade em conformidade com a LGPD

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestre em Ciência da Computação: Área de concentração: Engenharia de Software e Linguagens de Programação.

Orientador(a): Profa. Dra. Carina Frota Alves

Recife
2022

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

C181g Camêlo, Moisés Neves
G-PRIV: um guia para especificação de requisitos de privacidade em conformidade com a LGPD / Moisés Neves Camêlo. – 2022.
146 f.: il., fig., tab.

Orientadora: Carina Frota Alves.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2022.
Inclui referências e apêndices.

1. Engenharia de software. 2. Engenharia de requisitos. I. Alves, Carina Frota (orientadora). II. Título.

005.1 CDD (23. ed.) UFPE - CCEN 2022 – 57

Moisés Neves Camêlo

“G-Priv: um guia para especificação de requisitos de privacidade em conformidade com a LGPD”

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Engenharia de Software e Linguagens de Programação.

Aprovado em: 22/02/2022.

BANCA EXAMINADORA

_____

Profa. Dra. Jéssyka Flavyanne Ferreira Vilela
Centro de Informática / UFPE

_____

Profa. Dra. Edna Dias Canedo
Departamento de Ciência da Computação / UnB

_____

Profa. Dra. Carina Frota Alves
Centro de Informática / UFPE
(**Orientadora**)

AGRADECIMENTOS

Agradeço a Deus, por ter me dado o dom da vida, por sempre estar comigo guiando os meus caminhos, dando-me força e sabedoria para superar as adversidades, e levar-me a fazer o que for de melhor e correto. A Ele também sou grato por me dar condições de realizar este sonho, que até então era tão distante, e por ter me presenteado com muita saúde, paz de espírito, muitos amigos e uma família espetacular.

Agradeço a toda minha família, que é minha fortaleza onde sempre encontrei apoio, inspiração, união, carinho e amor. E aos amigos que a vida me deu, que me ajudaram para a concepção e a conclusão dessa pesquisa.

Em especial, agradeço e dedico este mestrado a minha esposa Raquel, as minhas filhas Catarina e Heloísa, a minha mãe, a professora Socorro Neves (UFPB), que sempre me apoiaram nessa jornada, dando todo o suporte necessário na vida acadêmica, profissional e familiar, e por toda compreensão nos momentos de angústia ou ausência. Amo todos vocês!

À minha orientadora, PhD. Carina Frota Alves, pela oportunidade de me tornar um aluno do Centro de Informática da UFPE, por toda dedicação, orientação, profissionalismo, compreensão nas dificuldades em conciliar trabalho, família, mestrado e pandemia, e a confiança na pesquisa desenvolvida.

À professora Eugênia Carvalho, da UFPB, pelo primoroso trabalho de revisão ortográfica, gramatical e linguística desta dissertação.

A todos os professores do CIn/UFPE, pela dedicação e entusiasmo no ensino de qualidade. A todos servidores, alunos e funcionários da UFPE, com quem tive o prazer de conviver como aluno, pesquisador, ou colega de turma.

Agradeço a todos, muito obrigado!

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) visa proteger os dados pessoais, inclusive nos meios digitais, processado por pessoa natural ou por pessoa jurídica de direito público ou privado. Atualmente, as organizações precisam implementar várias medidas para garantir que seus sistemas de software estejam em conformidade com a lei. No entanto, a LGPD, assim como outras legislações é de difícil entendimento por parte dos profissionais de TI, principalmente para extrair e operacionalizar requisitos legais. Dessa forma, essa pesquisa visa auxiliar analistas de requisitos na especificação dos requisitos de privacidade para garantir sua conformidade com a LGPD. Para atingir esse objetivo, foram realizadas entrevistas exploratórias, com o intuito de investigar o ponto de vista de analistas de requisitos, ressaltando possíveis desafios enfrentados na especificação de requisitos de privacidade. As entrevistas revelaram os principais achados classificados em cinco categorias: Conceitos de Privacidade, Processo de Conformidade, Obstáculos na Conformidade, *Tradeoff* entre Privacidade e Transparência, Rotina de Trabalho. A partir da análise dos dados coletados nas entrevistas, foi elaborado um guia chamado G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. O guia proposto possui atividades bem definidas, *templates* e um catálogo com padrões de requisitos de privacidade. Ao final da pesquisa, executamos um *survey* com 18 participantes com o objetivo de avaliar a aceitação do G-Priv e dos artefatos propostos no guia. O *survey* foi conduzido através de um questionário utilizado no formulário no Google Forms, como também foi disponibilizada uma documentação detalhada do guia, apresentando de forma sistemática as suas etapas, interações entre os atores e os *templates* disponibilizados. Com base na avaliação, o G-Priv foi considerado de fácil entendimento, principalmente na definição dos papéis e responsabilidades dos atores envolvidos nas quatro etapas do guia. Os participantes do *survey* também ressaltaram a agilidade de utilização do guia. Sendo assim, consideramos que o guia proposto pode auxiliar os analistas de requisitos na especificação dos requisitos de privacidade em conformidade com a LGPD.

Palavras-chaves: engenharia de requisitos; requisitos de privacidade; Lei Geral de Proteção de Dados (LGPD); padrões de privacidade.

ABSTRACT

The General Data Protection Law (LGPD) aims to protect personal data, included in digital media, by a natural person or by a legal entity governed by public or private law. Organizations currently need to implement several measures to ensure their software systems are in compliance with the law. However, the LGPD as well as other legislations are difficult for IT professionals to understand, mainly to extract and operationalize legal requirements. Thus, this research aims to assist requirements analysts in specifying privacy requirements to ensure their compliance with the LGPD. To achieve this objective, exploratory interviews were carried out, with the aim of investigating the point of view of requirements analysts, highlighting possible challenges faced in the specification of privacy requirements. The interviews revealed the main findings classified into five categories: Privacy Concepts, Compliance Process, Obstacles to Compliance, Tradeoff between Privacy and Transparency, Work Routine. From the analysis of the data collected in the interviews, a guide called G-Priv was created to support the specification of privacy requirements in accordance with the LGPD. The proposed guide has well-defined activities, templates, and a catalog with standards of privacy requirements. At the end of the research, we carried out a survey with 18 participants in order to assess the acceptance of G-Priv and the artifacts proposed in the guide. The survey was conducted through a questionnaire used in the form of Google Forms, as well as detailed documentation of the guide, systematically presenting its steps, interactions between the actors, and the templates available. Based on the assessment, the G-Priv was considered to be easy to understand, especially in defining the roles and responsibilities of the actors involved in the four stages of the guide. Survey participants also highlighted the agility of using the guide. Therefore, we consider that the proposed guide can assist requirements analysts in specifying the privacy requirements in accordance with the LGPD.

Keywords: requirements engineering; privacy requirements; General Data Protection Law (LGPD); privacy patterns.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Recentemente, inúmeros casos de vazamento de dados foram reportados na mídia. Como exemplo, destacamos o caso em que o Ministério Público do Distrito Federal e Território acusa a empresa de telefonia Vivo de vender indevidamente dados de 73 milhões de usuários, principalmente dados de geolocalização para comercializar publicidade (MPAVVDU, 2019). Outro caso, que foi considerado um dos maiores vazamentos no país, revelou dados pessoais de cerca de 223 milhões de brasileiros, sendo expostos dados biométricos, faixa salarial, informações sobre *score* de crédito de consumidores, dados de imposto de renda, perfis de redes sociais e fotografias (MVD, 2021). Essas situações reforçam a fragilidade dos sistemas de software em relação a aspectos de privacidade, conforme ilustrado na Figura 1 com os principais vazamentos de dados no Brasil. A privacidade tornou-se uma das principais preocupações no desenvolvimento de software, principalmente devido às incidências sobre a exploração não autorizada de dados, uso indevido de informações armazenadas em aplicativos de mídias sociais e divulgação de informações pessoais para terceiros sem o consentimento dos titulares (KALLONIATIS, 2017).

Figura 1 - Principais vazamentos e incidentes de segurança do Brasil.

Fonte: TFVD (2021).

Os sistemas e serviços de software contemporâneos exigem uma conectividade entre indivíduos e entidades corporativas, sejam elas públicas ou privadas, que resultam em atividades de coletar, processar ou divulgar regularmente grandes volumes de dados. É importante salientar que a falta de conformidade com políticas de privacidade pode causar consequências sérias com possíveis danos individuais e sociais (ANTHONYSAMY ET AL., 2017). Os dados dos sistemas de software, geralmente revelam uma grande quantidade de informações pessoais e que podem ser utilizadas para outra finalidade que não seja a demanda de origem. A divulgação de tais informações de forma não autorizada gera inúmeros problemas de privacidade para as organizações, essas divulgações não autorizadas foram afirmado por ANTHONYSAMY ET AL. (2017), naquela oportunidade o autor apresentou que as preocupações sobre privacidade mudaram substancialmente pós-Snowden, principalmente pelo fato que o WhatsApp garantia que os dados dos usuários não seriam compartilhados com terceiros, mas essa garantia foi relaxada após a aquisição pelo Facebook.

Como forma de proteger a privacidade de usuários, diversos países elaboraram legislações para governar o uso de dados pessoais, tais como a *General Data Protection Regulation* (GDPR) na União Europeia (EU, 2016) e a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil (BRASIL, 2018). Em particular, a LGPD trata de aspectos de privacidade de dados valendo-se do princípio da finalidade, pois exige que o tratamento de dados tenha propósitos legítimos, específicos, explícitos e informados ao titular sem a possibilidade posterior de forma incompatível com as finalidades (BRASIL, 2018). Apesar dos avanços na legislação a fim de garantir a privacidade de dados dos usuários, o desenvolvimento de sistemas de software em conformidade com tais leis ainda enfrenta diversos desafios. Em particular, vários autores reforçam a necessidade de especificar privacidade durante as fases iniciais do desenvolvimento, ou seja, durante a fase de engenharia de requisitos (AYALA-RIVERA ET AL., 2018; HADAR ET AL., 2018; GHARIB ET AL., 2020; PEIXOTO ET AL., 2020).

Considerando que a LGPD entrou em vigor recentemente, empresas de diferentes setores e órgãos públicos ainda estão enfrentando desafios para adequarem seus sistemas de software em conformidade com a legislação vigente. Garantir a conformidade legal visa evitar que sanções administrativas sejam aplicadas pela autoridade nacional de proteção de dados. As infrações à LGPD vão desde advertência até a imposição de sanções de natureza pecuniária que podem chegar a 2% do faturamento da empresa, limitadas a R$50 milhões por infração (BRASIL, 2018).

1.1 MOTIVAÇÃO

A importância em proteger a privacidade dos dados pessoais vem crescendo diariamente e tem o objetivo de proporcionar aos titulares dos dados integral controle e entendimento sobre o que está sendo realizado com seus dados pessoais em todo o seu ciclo de vida, que se inicia com a coleta, passando pelo uso, compartilhamento, armazenamento e encerrando-se com sua exclusão, sem que isso impacte negativamente os novos modelos de negócio e os legados (MALDONADO, 2018).

Essa importância está cada vez mais evidente, pois as pessoas e as corporações estão cada vez mais conectadas, em consequência disso, cada vez mais os dados são coletados, compartilhados, transferidos e processados. Dessa forma, o conjunto de dados pessoais possuem informações que agregam valores e podem traçar perfis que dizem respeito a cada indivíduo. No entanto, essas novas exigências significam grandes oportunidades para uma enorme gama de profissionais de várias áreas de atuação. Profissionais que antes mantinham suas atuações restritas a uma determinada área precisarão interagir com outros *experts* para que, juntos, consigam dar sentido e empreender conformidade no que se refere ao conjunto de regras de proteção de dados (MALDONADO, 2019). A exemplo do analista de requisitos, que não poderá seguir suas atividades sem trilhar de forma muito próxima de um especialista jurídico para auxiliá-lo em suas atividades cotidianas em perfeito regramento legal.

A preocupação desses profissionais é decorrente das consequências financeiras envolvendo suas instituições, com penalidades que variam de simples advertências administrativas a multas que equivalem a 2% do seu faturamento total, podendo chegar à importância de R$50.000,00 (cinquenta milhões de reais) por infração (BRASIL, 2021). Além dessas sansões, a organização penalizada pode ter seus serviços suspensos parcial ou totalmente do banco de dados, por um período máximo de seis meses, podendo estender-se até a sua regularização do banco (BRASIL, 2021). Com isso, causando não apenas perdas financeiras, mas também credibilidade impactando a imagem da organização perante a sociedade.

Assim, a motivação dessa pesquisa considerou a relevância em auxiliar os analistas de requisitos na especificação dos requisitos de privacidade, como um fator crítico de sucesso para a implantação da conformidade legal nos sistemas de softwares. Também foi observado na literatura que esses profissionais não possuem conhecimento suficiente em legislações de privacidade para garantir a conformidade legal dos sistemas

e necessitam de uma abordagem sistemática para especificar requisitos (HADAR ET AL., 2018; CANEDO ET AL., 2020).

1.2 QUESTÕES DE PESQUISA

A partir da motivação dessa pesquisa, foi percebida a necessidade de investigar como auxiliar os analistas de requisitos para apoiar a especificação de requisitos de privacidade e proteção de dados em conformidade com a LGPD.

Assim, essa pesquisa buscou identificar as percepções dos analistas de requisitos em relação à privacidade, como também otimizar, de forma ágil e prática, as especificações de requisitos de privacidade de dados. Diante do que foi considerado no contexto e os desafios apresentados, elaboramos as seguintes questões de pesquisa:

QP1. "Quais são as percepções de analistas de requisitos em relação à privacidade e proteção de dados?"

QP2." Como auxiliar os analistas de requisitos na especificação de requisitos de privacidade em conformidade com a LGPD?"

1.3 OBJETIVOS

A fim de responder às questões de pesquisa, foram propostos um guia de privacidade e um catálogo de padrões de privacidade, com o objetivo geral de auxiliar os analistas de requisitos, em relação à atividade de especificar os requisitos de privacidade em conformidade com a Lei Geral de Proteção de Dados Pessoais.

A pesquisa apresenta inicialmente resultados de entrevistas exploratórias realizadas com cinco analistas de requisitos da uma organização pública do poder judiciário. As entrevistas revelaram desafios enfrentados por esses profissionais para especificar requisitos de privacidade em conformidade com a LGPD. Em particular, eles relataram dificuldades no processo de interpretar a lei e na mudança de paradigma da rotina de trabalho, a fim de adequar os novos sistemas e os sistemas legados com a legislação vigente.

Os resultados das entrevistas exploratórias com os analistas de requisitos serviram de *insights* para elaborar o guia de privacidade e o catálogo de padrões de privacidade, os quais têm o objetivo de auxiliar os analistas de requisitos e de alinhar o entendimento das necessidades dos *stakeholders*, entendimento do problema e suas possíveis limitações aos requisitos de privacidade impostos pela LGPD. Diante disso, a pesquisa visa direcionar

de maneira prática a especificação dos requisitos de privacidade em conformidade com a LGPD, em uma proposta de guia modelado como um fluxo de etapas, artefatos em formato de *templates* de simples e atores com responsabilidades bem definidas.

Com o objetivo de obter um diagnóstico da utilização do guia, a pesquisa conta com um *survey* para avaliar o G-Priv (guia de privacidade) em relação a sua utilidade e facilidade de uso para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD, sob a perspectiva de analistas de requisitos de vários segmentos e atividades, como também outros profissionais. Com os resultados obtidos no *survey*, foi possível identificar os benefícios no processo de padronizar a especificação de requisitos de privacidade, como também uma série de ações ou iniciativas, com algumas delas já em execução, como a preocupação em especificar requisitos de privacidade e a busca de um mecanismo para atuar como facilitador para os analistas de requisitos na conformidade com a LGPD.

1.4 ESTRUTURA DA DISSERTAÇÃO

O documento está estruturado da seguinte forma:

- O Capítulo 2 apresenta o *background* de referencial teórico sobre o processo de engenharia de requisitos, requisitos de privacidade, Lei Geral de Proteção de Dados Pessoais, *Privacy by Design* e ABNT ISO NBR 27701.
- O Capítulo 3 descreve a metodologia de pesquisa, que apresenta as etapas do trabalho envolvendo as entrevistas exploratórias, concepção na elaboração do guia de privacidade, catálogo de padrão de privacidade e avaliação do guia proposto através de um *survey*, a partir do ponto de vista de profissionais de organizações privadas e públicas, que atuam nas áreas de engenharia de requisitos, análise de sistemas, privacidade de dados, segurança da informação, desenvolvimento de software.
- O Capítulo 4 registra os resultados das entrevistas exploratórias.
- O Capítulo 5 apresenta um guia de privacidade e uma proposta de catálogo de padrões de privacidade para apoiar a conformidade na especificação de requisitos de privacidade com a LGPD, que podem ser utilizados em diferentes contextos organizacionais e com objetivo de otimizar a

especificação dos requisitos de privacidade em conformidade com a legislação de privacidade de dados pessoais.

- O Capítulo 6 aborda a avaliação do G-Priv e o catálogo de padrão de privacidade, que foi executado um *survey* com 18 (dezoito) participantes de diversos seguimentos da indústria de software.
- O Capítulo 7 finaliza essa dissertação, apresentando as considerações finais, conclusões, limitações da pesquisa e perspectivas para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta uma visão geral dos principais conceitos sobre Engenharia de Requisitos, Requisitos de Privacidade e a Lei Geral de Proteção de Dados Pessoais, com ênfase em aspectos importantes para uma melhor compreensão do problema abordado nessa dissertação. A seção 2.1 descreve os conceitos e definições sobre engenharia de requisitos, requisitos funcionais, requisitos não funcionais, ciclo do processo e abordagens usadas em cada fase. A seção 2.2 descreve os conceitos básicos de requisitos de privacidade, bem como alguns fatores práticos para sua implantação. Na seção 2.3, são apresentadas as principais legislações de privacidade, onde são abordados as definições, conceitos, princípios, sanções e requisitos para o tratamento de dados exigidos pela Lei Geral de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados. A seção 2.4 aborda a Norma ISO 27701, com seus controles e diretrizes de privacidade. Por fim, na seção 2.5, apresenta-se o resumo do capítulo e considerações finais.

2.1 ENGENHARIA DE REQUISITOS

A principal medida de sucesso de um sistema de software é o grau que atende ao propósito para o qual foi pretendido. Em termos gerais, a engenharia de requisitos é o processo de descobrir esse propósito, identificando as partes interessadas e suas necessidades, e documentá-los de uma forma que seja passível de análise, comunicação e posterior implementação (NUSEIBEH e EASTERBROOK, 2000).

A engenharia de requisitos fornece um conjunto de abordagens apropriadas para entender aquilo que o cliente deseja, analisando as necessidades, avaliando a viabilidade, negociando uma solução razoável, especificando uma solução sem ambiguidades, validando a especificação e gerenciando as necessidades que são transformadas em um software (PRESSMAN, 2011). Nesse contexto, a disciplina de engenharia de requisitos é uma atividade multidisciplinar, implantando uma variedade de técnicas e ferramentas em diferentes estágios de desenvolvimento e para diferentes tipos de domínios de aplicativo (NUSEIBEH e EASTERBROOK, 2000). Segundo Fernández et al. (2016), a engenharia de requisitos tem por objetivo a elicitação, análise e especificação de requisitos que refletem inequivocamente a finalidade pretendida de um sistema de software, considerando e alinhando o ponto de vista de todas as partes interessadas e relevantes.

Assim, podemos considerar que antes de iniciar o processo de desenvolvimento, é necessário entender a relevância do uso sistemático e repetitivo de técnicas que envolve a disciplina de engenharia de requisitos, visando sempre identificar os principais *stakeholders*, suas necessidades e alinhar o conjunto de requisitos às regras de negócio.

Os principais problemas associados às especificações de requisitos são: os requisitos que não refletem as reais necessidades do usuário; os requisitos que são inconsistentes, incompletos ou ambíguos, que sofrem problemas de comunicação e habilidades inadequadas; a dispendiosa atividade de fazer mudanças após os requisitos terem sidos acordados e implementados; e a existência de diferenças de interpretações entre clientes e equipe de desenvolvimento (KARLSSON ET AL., 2002; NUSEIBEH e EASTERBROOK, 2000; FERNÁDEZ ET AL., 2016).

Tais problemas surgem principalmente devido às dificuldades relacionadas à comunicação com os usuários. Estudos mostram que os principais problemas associados ao insucesso dos projetos de software estão relacionados com a engenharia de requisitos (RC, 2014). Segundo o estudo do *Project Smart* (RC, 2014), cinco dos onze principais fatores de falhas em projetos de software têm relação direta com requisitos, conforme exposto na Tabela 1, nas linhas "1, 2, 4, 6 e 8".

Tabela 1 - Principais causas de falhas em projetos de software.

ID	Problema	%
1	Requisitos incompletos	13,1%
2	Falta de envolvimento do usuário	12.4%
3	Falta de recursos	10,6%
4	Expectativa não realista	9,9%
5	Falta de apoio executivo	9,3%
6	Mudança nos requisitos	8,7%
7	Falta de planejamento	8,1%
8	Requisitos desnecessários	7,5%
9	Falta de gerenciamento de TI	6,2%
10	Analfabetismo de TI	4,3%
11	Outros	9,9%

Fonte: RC (2014).

Outro ponto importante é que quanto mais tarde os problemas com requisitos são detectados no processo de desenvolvimento, maior será o custo para corrigi-los. O sucesso das etapas posteriores do processo de desenvolvimento depende da especificação

de requisitos gerada (NUSEIBEH e EASTERBROOK, 2000). Por essas razões, a disciplina de Engenharia de Requisitos é classificada como uma das fases mais críticas no desenvolvimento de software.

2.1.1 Tipos de Requisitos

A Engenharia de Requisitos corresponde à atividade de entendimento das necessidades do usuário no contexto do problema a ser resolvido, bem como das limitações impostas na solução (SOMMERVILLE, 2011). Esses requisitos refletem as necessidades dos clientes no sistema com uma finalidade determinada, que, no seu desenvolvimento de software, são descritos as suas restrições e o seu funcionamento, tais como, cadastrar os dados pessoais e armazenar numa base de dados (KONTNYA e SOMMERVILLE, 1998).

Segundo Sommerville (2011), os requisitos de software são frequentemente classificados como requisitos funcionais e não funcionais. Os requisitos não funcionais são conhecidos como requisitos de qualidade e, ao contrário dos requisitos funcionais, os não funcionais estabelecem restrições ao sistema, bem como noções particulares de qualidades que um sistema pode ter. Por isso, podemos dizer que enquanto os requisitos funcionais determinam "o que" o sistema deve fazer, descrevendo o que é de valor para o usuário, os não funcionais restringem "como" o sistema deve realizar "o que", descrevendo as condições sob as quais as funcionalidades fornecidas sejam realmente uteis (CYSNEIROS e YU, 2004; KOPCZYNSKA ET AL., 2018).

- Os **requisitos funcionais** de um sistema descrevem o que ele deve fazer, como deve reagir às entradas específicas e como se comportar em determinadas situações, esses requisitos são reflexos do tipo de software a ser desenvolvido, de quem são os seus possíveis usuários e a abordagem geral adotada pela organização ao escrever os requisitos (SOMMERVILLE, 2011; SANTANDER, 2002). Cysneiros e Yu (2004) reforçam a ideia de que os requisitos funcionais devem descrever como o sistema irá reagir perante as entradas e qual será o seu comportamento em determinadas situações, portanto abordam problemas específicos implementados através de módulos ou componentes;
- Enquanto isso, os requisitos **não funcionais** são restrições aos serviços ou funções oferecidas pelo sistema, que estão relacionados às propriedades

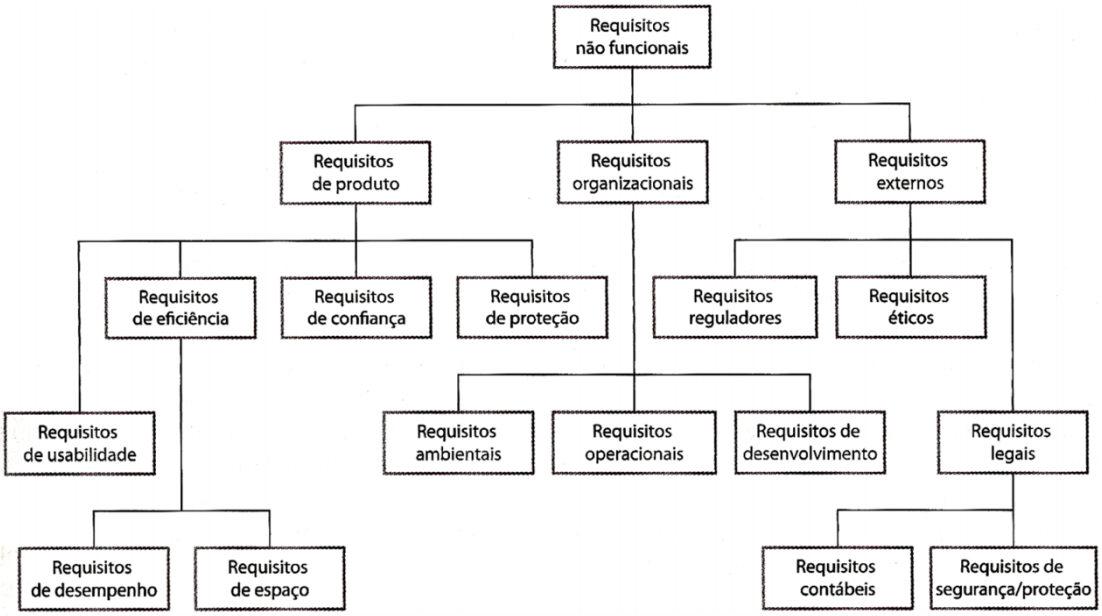
> do mesmo, como confiabilidade, tempo de resposta, ocupação de área ou disponibilidade (SOMMERVILLE, 2011). Segundo Nuseibeh e Easterbrook (2000), os não funcionais geralmente são difíceis de expressar e mensurar, assim tornando-os mais difíceis de analisar. Muitas vezes negligenciados, especialmente aqueles que são difíceis de escrever e aparentemente óbvios, e isso é um fator de risco importante, pois, em muitos casos, uma falha de projeto pode ser rastreada, entre outros, a uma gestão inadequada dos requisitos (KOPCZYNSKA ET AL., 2018).

Os requisitos podem afetar a arquitetura geral de um sistema, ou até definir característica de um produto ou organização. A exemplo disso, podemos citar a situação de quando os requisitos de segurança são contemplados, e, hipoteticamente, se há a necessidade de organizar e fundamentar as instruções de conformidade das regras de negócio, com legislações, regulamentos, normas e políticas de segurança.

Outra característica importante para atender a diferentes requisitos não funcionais pode levar a conflitos que precisam ser tratados (CYSNEIROS e YU, 2004). Por exemplo, para abordar preocupações de segurança e privacidade, um sistema coleta dados pessoais de um usuário, dentre eles a biometria, mas coletar a biometria pode gerar um conflito de finalidade e um conflito com preocupações de custo.

Conforme Sommerville (2011), podemos ilustrar os requisitos não funcionais provenientes das características requeridas para um software na Figura 2.

Figura 2 - Classificação dos requisitos não funcionais.



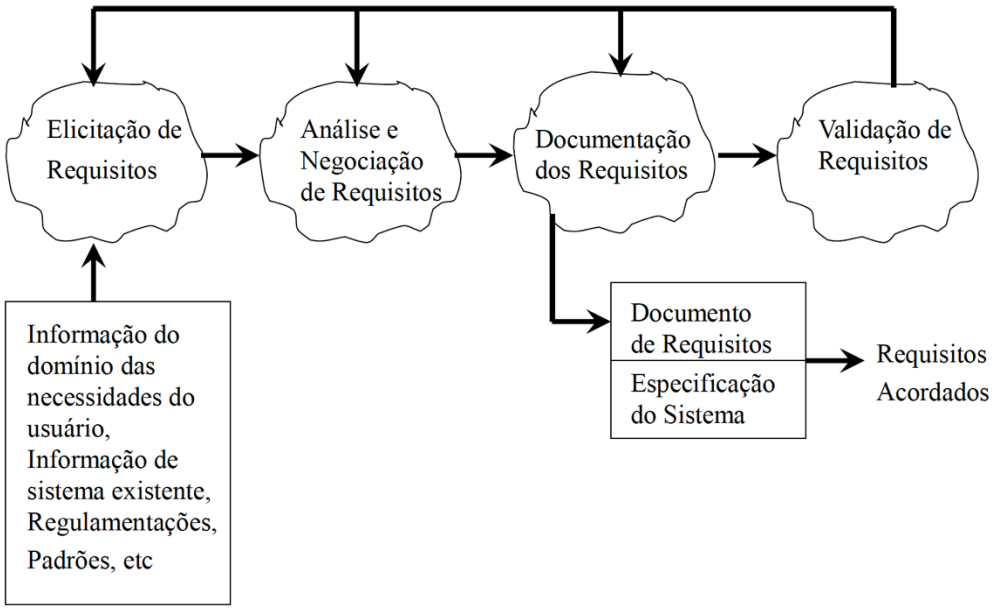
Fonte: Sommerville (2011)

- **Requisitos de produto** - especificam ou restringem o comportamento do software, como desempenho, confiabilidade, usabilidade, eficiência e espaço de armazenamento. (SOMMERVILLE, 2011), (KONTNYA e SOMMERVILLE, 1998).
- **Requisitos organizacionais** - são requisitos gerais de sistemas derivados das políticas e procedimentos da organização do cliente e desenvolvedor, como, por exemplo, o processo de desenvolvimento na especificação na linguagem de programação, tipo de banco de dados e sistema operacional. (SOMMERVILLE, 2011), (KONTNYA e SOMMERVILLE, 1998).
- **Requisitos externos** – descrevem os fatores externos ao sistema e ao seu processo de desenvolvimento, como requisitos regulatórios, legais e éticos (SOMMERVILLE, 2011), (KONTNYA e SOMMERVILLE, 1998).

2.1.2 Processo Da Engenharia de Requisitos

O processo de descobrir, analisar, documentar e verificar esses serviços e restrições é definido como um conjunto de atividades que compõem o Processo de Engenharia de Requisitos. Segundo Kotonya e Sommerville (1998) e Sommerville (2011), o processo de Engenharia de Requisitos inclui quatro atividades de alto nível: avaliar se o sistema é útil para o negócio (estudo de viabilidade), realizar a descoberta de requisitos (elicitação e análise), converter os requisitos em um formato padrão (especificação), e verificar se os requisitos, realmente, definem o sistema que o cliente deseja (validação). Esse processo é ilustrado na Figura 3.

Figura 3 - Modelo de atividade de alto nível do processo de engenharia de requisitos.



Fonte: Kotonya e Sommerville (1998).

2.1.3 Elicitação de Requisitos

A complexidade da Engenharia de Requisitos está justamente na elicitação dos requisitos do cliente, ou seja, no levantamento das necessidades dos usuários dentro do domínio do problema. Segundo Nuseibeh e Easterbrook (2000), um dos objetivos mais importantes da **elicitação** é descobrir qual problema precisa ser resolvido, portanto devem-se identificar os limites do sistema. E esses limites em alto nível definem como o sistema será entregue e se encaixará no ambiente operacional. Existem várias técnicas que podem ser usadas durante o processo de elicitação de requisitos, a sua escolha depende do tempo de recursos disponíveis e o tipo de informação que precisa ser extraída.

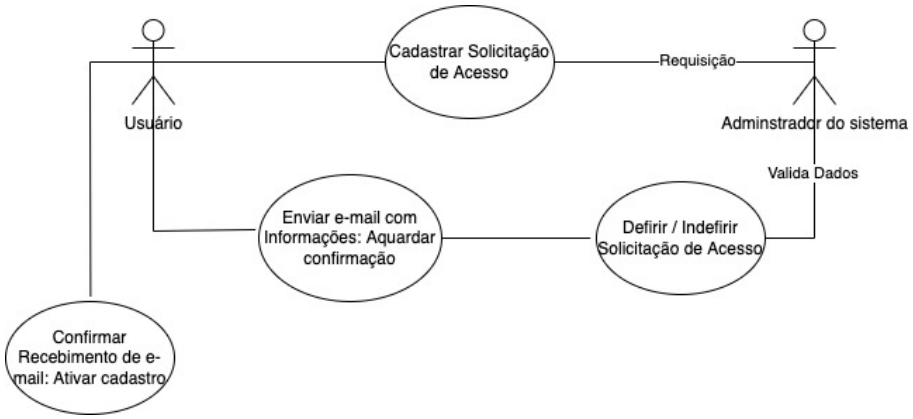
A **elicitação** é uma etapa importante no processo de engenharia de requisitos, pois compreende as atividades relacionadas ao entendimento das metas e objetivos da construção do sistema proposto (CHENG e ATLEE, 2007). Como entendimento do domínio da aplicação, entendimento do problema, entendimento do negócio e as necessidades e limitações dos *stakeholders*. Portanto, a elicitação de requisitos está intimamente relacionada a outras atividades de Engenharia de Requisitos.

Para facilitar o procedimento de elicitação de requisitos, são utilizadas técnicas de levantamento e descoberta dos requisitos, e essas técnicas dependem do tempo dos recursos disponíveis para o analista de requisitos, e claro, o tipo de informação a ser extraída:

a) **Entrevista**: entrevistas formais ou informais fazem parte da maioria dos processos de engenharia de requisitos, em que são formuladas perguntas aos *stakeholders* sobre o sistema que utilizam e o futuro sistema que será desenvolvido. Segundo Kontnya e Sommerville (1998), existem basicamente dois tipos de entrevista:
    a. Entrevistas fechadas – neste caso os *stakeholders* respondem a um conjunto predefinido de perguntas;
    b. Entrevistas abertas – aqui não há agenda predefinida e discute-se, de modo aberto, o que os *stakeholders* esperam do sistema.

b) **Técnicas baseadas em Modelos/Cenário**: consiste na elaboração de cenários, incluindo fatos previsíveis inseridos no dia a dia dos usuários, assim podem ser descritos como histórias que explicam como o sistema é utilizado, sendo úteis, inicialmente, para agregar detalhes em uma descrição resumida de requisitos. Uma das técnicas mais conhecidas que utiliza cenários é os casos de uso (PRESSMAN, 2011; NUSEIBEH e EASTERBROOK, 2000).
    a. **Casos de uso** – é uma técnica baseada em cenários para obtenção de requisitos e que se tornou uma característica fundamental da notação em UML, para descrever modelos de sistemas orientados a objetos (SOMMERVILLE, 2011). A Figura 4 representa um caso de uso, em que cada ator é representado por uma figura de traços e cada classe de interação é definida por um nome na elipse.

Figura 4 - Exemplo de Caso de uso.



Fonte: O autor (2022).

c) **Etnografia**: é uma técnica de observação que pode ser usada para compreender os processos operacionais e ajudar a extrair os requisitos de apoio para esses processos (SOMMERVILLE, 2011). Nesse caso, o analista de requisitos fica imerso no ambiente de trabalho no qual o sistema será utilizado, observando a rotina de trabalho, analisando as atividades nas quais os usuários estão envolvidos.
d) **Prototipagem**: corresponde a uma versão do sistema que está disponível no início do projeto, quando o usuário pode simular as situações e realizar testes (NUSEIBEH e EASTERBROOK, 2000). De acordo com Boar (1984), a prototipação implementa parte dos requisitos do sistema por meio da construção de um protótipo que executa o comportamento real do sistema. A prototipação para desenvolvimento de software é dividida nas seguintes abordagens:
e) **Técnicas de elicitação em grupo:** visam fomentar o acordo e aceitação das partes interessadas, enquanto explora a dinâmica da equipe para obter uma compressão mais rica das necessidades. Aqui, incluem-se grupos focais, *workshops* e *brainstorming*, que é uma técnica de geração de ideias bastante utilizada para promover a interação entre um pequeno grupo, a fim de se obter a resolução para um determinado problema. Essa técnica possui três fases: exposição de abertura, exposição de ideias e fase de escrutínio (NUSEIBEH e EASTERBROOK, 2000).
f) **Técnicas tradicionais:** consiste numa ampla gama de dados coletados, isso inclui questionários, entrevistas e análise de documentação existentes, tais como organogramas, modelos, padrões de processos e manuais de sistemas e usuários existentes (NUSEIBEH e EASTERBROOK, 2000).

2.1.4 Análise e Negociação de Requisitos

A **análise e negociação de requisitos** consiste na análise detalhada dos requisitos, de acordo com cada uma das origens de requisitos, de forma a decidir quais serão aceitos. Segundo Sommerville (2011), essa etapa é necessária, pois existirão conflitos entre os requisitos e suas respectivas origens, tanto por haver requisitos incompletos ou incompatíveis, seja do ponto de vista financeiro ou técnico. Como também analisar se todos os requisitos que foram elicitados são realmente necessários para a implementação, assim evitando problemas, como erros relacionados à ambiguidade, inconsistência e incoerência (CHENG e ATLEE, 2007).

A fase de análise revela possíveis dificuldades de entendimentos dos requisitos ou questionamentos que retornariam para a fase de elicitação. Para isso, a análise de requisitos possui técnicas, tais como: análise de risco e análise de impacto, que podem ajudar melhor a entender os requisitos, seus relacionamentos e suas consequências potenciais, de modo que os analistas de requisitos possam tomar decisões mais embasadas (CHENG e ATLEE, 2007), Sessões de *Joint Application Development* (JAD), que é uma dinâmica de grupo em que um líder neutro orienta usuários através de um processo interativo e flexível para se obter consenso sobre o assunto.

2.1.5 Documentação de requisitos

A **documentação dos requisitos ou especificação de requisitos** é uma etapa após a análise e negociação, que é necessário modelar e documentar os requisitos em um nível no qual todos os utilizadores do sistema entendam, onde são geralmente utilizadas linguagens escritas e gráficas para melhor entendimento das partes envolvidas, e que tem por finalidade formalizar os requisitos que serão utilizados como referência para as outras fases do ciclo de vida do software (SOMMERVILLE, 2011).

O objetivo da documentação de requisitos é comunicar os requisitos entre os desenvolvedores e *stakeholders* do sistema com a finalidade de validação. Nessa fase, o analista de requisitos especifica os requisitos de maneira que todos os *stakeholders* possam entender, utilizando maneiras de representação, entre elas a linguagem formal, semiformal e informal, representações gráficas e simbólicas (SOMMERVILLE, 2011). Lembrando que, em alguns casos, a especificação dos requisitos pode fazer parte do contrato do projeto.

Segundo Leite et al. (2000), existem diversas propostas na literatura sobre as formas de documentar requisitos, geralmente são usados modelos em forma de cenários, que descrevem o comportamento detalhado do futuro sistema. A principal vantagem do uso de modelos na Engenharia de Requisitos está na melhoria da comunicação entre os *stakeholders*. O foco da utilização dos modelos está na representação dos requisitos, de modo que os usuários possam compreender o sistema proposto e os desenvolvedores implementarem o futuro software a partir da representação.

2.1.6 Validação de Requisitos

A **validação dos requisitos** é a etapa onde os requisitos são cuidadosamente analisados pelos envolvidos no projeto, para verificar se há coerência entre os requisitos e se existe alguma falha ou item que não foi descrito (SOMMERVILLE, 2011). Além da análise dos envolvidos no projeto, é preciso envolver os *stakeholders*, principalmente para oficializar todas as informações coletadas até o momento (CHENG e ATLEE, 2007). Segundo Nuseibeh e Easterbrook (2000), a **validação** de requisitos é difícil por dois motivos. A primeira razão é de natureza filosófica e diz respeito à questão da verdade e do que é conhecível. A segunda razão é social e diz respeito à dificuldade de chegar a um acordo entre diferentes partes interessadas com objetivos conflitantes.

A forma mais tradicional de simulação é através do uso de protótipos (PRESSMAN, 2011), no entanto outras formas alternativas existem, tais como: *StoryBoard*, Diagramas de Afinidade, *Card Sorting* e Prototipação em papel (MAGUIRE, 2001). O processo é usualmente iterativo dado que, durante a validação, os usuários podem requisitar ou pedir alterações nos requisitos, levando a um novo ciclo de atividades.

2.1.7 Gerenciamento de Requisitos

Nessa etapa, o objetivo é capturar, armazenar, disseminar e gerenciar informações. O gerenciamento de requisitos inclui todas as atividades preocupadas com mudanças, controle de versão e rastreamento de requisitos. E, paralelamente, dá apoio a todas as atividades citadas no processo de requisitos.

Autores como Nuseibeh e Easterbrook (2000), reconhecem que que essa fase é crucial para o sucesso, pois requer uma habilidade, não apenas de escrever requisitos, mas também de fazê-los de forma legível e rastreável por muitos, a fim de gerenciar sua evolução ao longo do tempo.

2.2 REQUISITOS LEGAIS DE PRIVACIDADE

Privacidade é um conceito amplamente investigado em diferentes áreas, tais como direito, filosofia e sociologia. Recentemente, privacidade tem sido um tema de crescente interesse da comunidade de engenharia de requisitos. Requisitos de privacidade são difíceis de quantificar e especificar com precisão (AYALA-RIVERA e PASQUALE, 2018; WEBSTER e IVANOVA, 2005). Martin e Kung (2018) seguem o mesmo

raciocínio afirmando que engenheiros de software estão habituados a pensar em termos de modelos de dados e arquiteturas. Todavia, eles se sentem perdidos para traduzir questões regulatórias nas suas atividades de desenvolvimento.

Segundo Kalloniatis et al. (2008), privacidade é o direito em determinar quando, como e em que condições é permitido compartilhar informações pessoais e transmitir tais informações para terceiros. A partir de um mapeamento sistemático conduzido por Anthonysamy et al. (2017), requisitos de privacidade podem ser classificados em quatro categorias de acordo com a compreensão sobre a natureza e a perspectiva do usuário, são elas: conformidade, controle de acesso, verificação e usabilidade. A seguir, descrevemos cada uma dessas categorias.

A privacidade na perspectiva de **conformidade** opera com base em requisitos de privacidade decorrentes da legislação de proteção de dados, tendo como foco a obtenção e análise de requisitos necessários para desenvolver sistemas. O foco dessa visão é a obtenção e análise de requisitos necessários para desenvolver sistemas de software. Essa perspectiva faz o uso de referenciais teóricos fornecidos por juristas e estruturas de padrões de segurança e privacidade para eliciar requisitos de privacidade.

A privacidade na perspectiva do **controle de acesso** é conhecida por ser uma tarefa difícil e problemática para usuários em diversas áreas de segurança, como autenticação, autorização etc. Essa categoria foca na definição de mecanismos de controle de acesso em relação às informações divulgadas ao usuário.

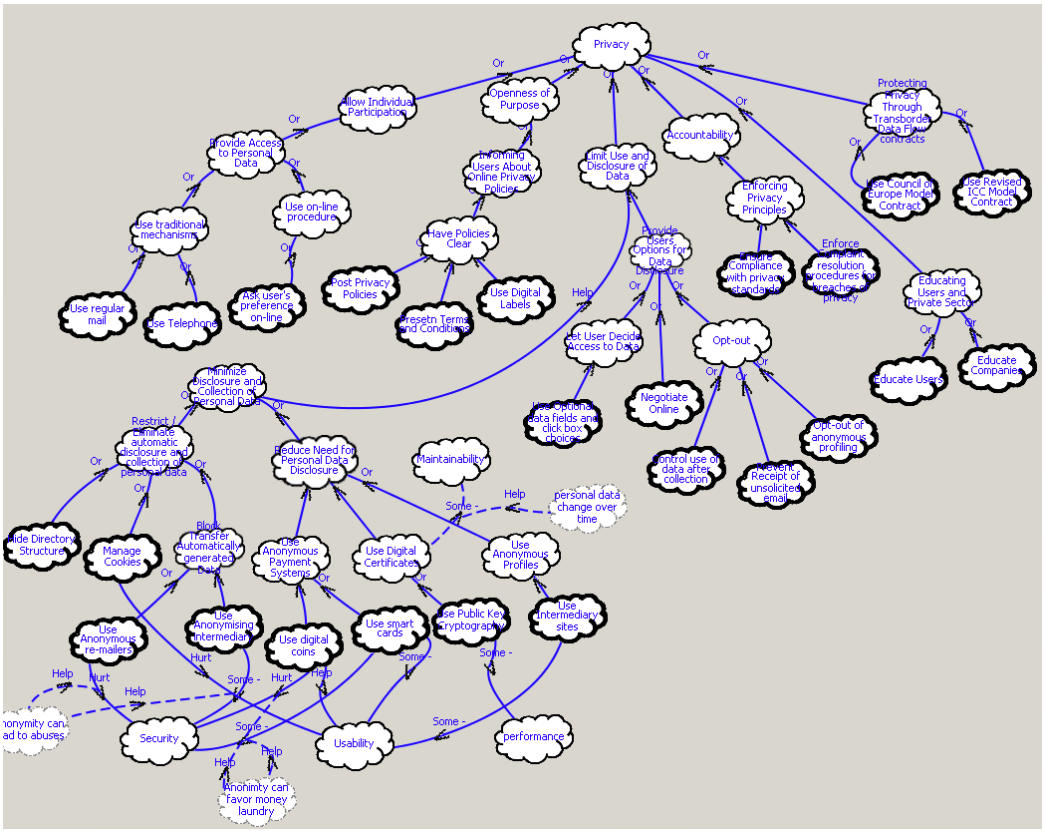
A privacidade na perspectiva de **verificação e correção** de sistemas de software tem como objetivo a aplicação de métodos formais para verificação de requisitos de segurança e privacidade a fim de aumentar a confiabilidade dos sistemas de software.

A privacidade sob a perspectiva de **usabilidade** concentra-se na avaliação de comportamentos, necessidades e motivações dos usuários através de técnicas de observação e análise de problemas de usabilidade para aplicar em soluções que garantam a privacidade dos usuários. Essa perspectiva cobre um amplo espectro que inclui estudos centrados nos usuários sobre suas percepções de privacidade, violações de privacidade nas mídias sociais e melhoria da conscientização e comportamentos dos usuários.

Hadar et al. (2018) reforçam a necessidade de abordagens sistemáticas para especificar requisitos de privacidade, pois muitos profissionais da área não possuem conhecimento e compreensão suficientes sobre conceitos de privacidade. Nessa mesma direção, Canedo et al. (2020) consideram que engenheiros de software possuem pouco conhecimento sobre como garantir que sistemas estejam em conformidade com

legislações que visam à proteção de dados de usuários. Com o objetivo de oferecer uma visão ampla sobre requisitos de privacidade, Peixoto et al. (2020) propuseram um modelo conceitual e um catálogo de conceitos relacionados a requisitos de privacidade (*Privacy Criteria Method - PCM*). O modelo conceitual apresenta diversos mecanismos de privacidade que podem ser úteis para guiar o desenvolvimento de sistemas de software aderentes a requisitos de privacidade. Na mesma direção, Gharib et al. (2020) desenvolveram uma ampla ontologia para modelar requisitos de privacidade, tais requisitos são refinados nos conceitos: confidencialidade, anonimização, pseudonimização, inobservidade, notificação, transparência, responsabilização. Cysneiros e Yu (2004) ilustraram um catálogo para privacidade, onde o objetivo é ter *softgoals* de privacidade refinados, que limitem o uso e a divulgação de dados, sendo assim decompondo a minimização, a divulgação e coleta de dados pessoais, entre outras opções, em reduzir a necessidade de dados pessoais, a Figura 5 mostra o catálogo para privacidade proposto por Cysneiros e Yu (2004).

Figura 5 - Catálogo de soluções alternativas de privacidade.



Fonte: Cysneiros e Yu (2004).

2.3 LEGISLAÇÕES DE PRIVACIDADE

A proteção da segurança da informação não é uma preocupação recente das empresas. Antes da criação e vigência de leis e regulamentos de privacidade e proteção de dados, como a GDPR e a LGPD, algumas normas já haviam sido criadas com o objetivo de implementar a privacidade dos dados e uma gestão de segurança da informação. Essas medidas podem ser encontradas com a família das Normas Técnicas ABNT NBR ISO 27000 (ABNT, 2019) e a Diretiva 95/46/CE (DIRECTIVA, 1995), que é a antecessora da GDPR.

2.3.1 Regulamento Geral De Proteção De Dados (GDPR)

No ano de 2016, foi lançada a proposta chamada de *General Data Protection Regulation* (GDPR) ou traduzindo para o português RGPD – Regulamento Geral de Proteção de Dados, Regulação 2016/679 (EU) (EU, 2016), que entrou em vigor no dia 25 de maio de 2018, substituindo a Diretiva 95/46/CE; diferente da Diretiva, a regulação é autoaplicável e não requer aprovação de leis nacionais compatíveis com suas determinações. Seu objetivo é eliminar inconsistências em leis nacionais, ampliar o escopo de proteção à privacidade e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, como aqueles decorrentes do advento da internet (MALDONADO e BLUM, 2019; EU, 2016).

A primeira proposta para a GDPR ocorreu em janeiro de 2012, e o fim das negociações se deu em dezembro de 2015, culminando na assinatura do regulamento em janeiro de 2016 (REBELO, 2019). As modificações perante a Diretiva 95 visam reajustar conceitos e incorporar as noções de *data controller* e *data processor*, reforçar princípios como o da proporcionalidade e da minimização do uso de dados; acrescentar disposição específica para regulamentação do consentimento do titular dos dados; alargar o catálogo de dados considerados sensíveis, reforçar as exigências em matéria de segurança e proteção de dados; atribuir novos direitos aos titulares dos dados e criar novas obrigações, segundo Rebelo (2019).

A GDPR é composta por duas grandes partes, a primeira contém 173 considerações que explicam a motivação do regulamento e seus objetivos, e a segunda

parte é composta por 99 artigos que representam as normativas a serem seguidas (MALDONADO e BLUM, 2018).

Diversas pesquisas têm sido realizadas para apoiar a aderência com a legislação da GDPR. Ayala-Rivera e Pasquale (2018) propõem uma abordagem sistemática organizada em um guia para apoiar a elicitação dos requisitos de software em conformidade com a GDPR. Seguindo a mesma linha de pesquisa, Martin e Kung (2018) afirmam que, para projetar a privacidade, engenheiros de requisitos devem ser efetivamente envolvidos e dotados de ferramentas metodológicas e tecnológicas da engenharia para se atingir a definição de engenharia de privacidade, como: gestão de riscos, engenharia de requisitos, *privacy by design*. Reforçando a ideia de se utilizarem métodos e modelos, Tom et al. (2018) apresentaram uma versão preliminar de um modelo, que visa fornecer uma visão geral mais simples e visual da GDPR. O modelo tem o objetivo de explicar como a conformidade com a regulamentação pode ser alcançada usando-se uma abordagem baseada em modelo com suporte de ferramenta, assim auxiliando na implementação e na compreensão das associações entre diferentes entidades na GDPR (MATULEVICIUS ET AL., 2020).

2.3.2 Lei Geral De Proteção De Dados (LGPD)

A LGPD entrou em vigor no dia 18 de setembro de 2020, mantendo a linha da GDPR, possibilitando as relações entre Brasil e a União Europeia com segurança de dados equivalentes. A LGPD serve de eixo para o sistema normativo brasileiro de proteção de dados pessoais (MALDONADO e BLUM, 2019). A lei determina o que pode e não pode ser feito em relação à coleta de dados no país, prevendo punições para as empresas que desrespeitarem os seus dispositivos. A LGPD regula as operações de tratamento de dados pessoais realizadas por agentes públicos e privados, ou seja, regula o acesso, coleta, armazenamento, processamento e compartilhamento de dados pessoais.

A LGPD possui 65 artigos distribuídos em definições, conceitos, princípios, sanções e requisitos para tratamento de dados (BRASIL, 2021). Dentre os principais conceitos, destacamos os tipos de dados:

- **Dado pessoal** – é a informação relacionada à pessoa natural identificada ou identificável, ou seja, qualquer informação que possa identificar uma pessoa, tais como: nomes, números, códigos de identificação, endereços;

- **Dado pessoal sensível** – trata de um dado pessoal sobre origem racial, religião, saúde, opção sexual, opinião pública, dado genético ou biométrico quando vinculado a uma pessoa;
- **Dado anonimizado** –refere-se ao dado relativo ao titular que não possa ser identificável;
- **Dado pseudonimização** – é o tratamento para perder associação ou link direto ou indireto do indivíduo, mas com possibilidade de recuperar a origem;
- **Autoridade nacional** – é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo território nacional;
- **Titular** – é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Controlador** – é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referente ao tratamento de dados pessoais;
- **Operador** – é a pessoa que realiza o tratamento de dados em nome do controlador e pode ser uma pessoa física ou jurídica de direito público ou privado;
- **Encarregado** – é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares e a autoridade nacional;
- **Tratamento** – é toda operação realizada com dado pessoal, por exemplo, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.

Dentro da LGPD, o tratamento dos dados pessoais de um indivíduo apenas pode ser tratado a partir de princípios estabelecidos que impõem novas diretrizes e limites sobre o tratamento dos dados pessoais (BRASIL, 2021), são eles:

- **Finalidade** – o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias;

- **Adequação –** o tratamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular de acordo com o contexto do tratamento;
- **Necessidade** – o tratamento dos dados pessoais deve ser no mínimo necessário para realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação a finalidades do tratamento de dados;
- **Livre acesso** – trata da consulta garantida aos titulares de maneira facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos dados** – garantia aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência –** é garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais;
- **Segurança –** devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção –** devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação –** impossibilidade de realização do tratamento para fins discriminatórios ilícios ou abusivos;
- **Responsabilização e prestação de contas –** demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O desafio enfrentado para garantir a conformidade legal aos sistemas de software, as organizações têm o objetivo de evitar que sanções administrativas sejam aplicadas pela autoridade nacional de proteção de dados. As infrações à LGPD vão desde advertência até a imposição de sanções de natureza pecuniária que podem chegar a 2% do faturamento da empresa, ou limitadas a R$50 milhões por infração (BRASIL, 2018).

Diante do exposto e além dos problemas causados com vazamento de dados conforme já discutimos na introdução dessa dissertação, surge também um aparente conflito normativo, em que de um lado, temos a LGPD, destacando as suas medidas de prevenção de segurança, sigilo das informações e retenção de documentos. E, de outro lado, temos a Lei de Acesso à Informação que regula e determina o acesso às informações públicas brasileiras, a partir de transparência ativa e passiva, sendo a lei mais abrangente em significância vigente no Brasil sobre transparência.

A LAI, como é conhecida na sua forma sintetizada, determina, por exemplo, em seu Artigo 3º, I: "observância da publicidade como preceito geral e do sigilo como exceção" (Brasil, 2011). E no Art. 6º, VI, a lei determina e assegura a proteção da informação sigilosa e da informação pessoal, observada sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. nº 12.527, LAI (BRASIL, 2011). Com isso, destacamos como é difícil, para um analista ou engenheiro de requisitos, entender o limiar entre o público e o privado, ou o transparente e o sigiloso.

Diversas pesquisas têm sido realizadas para apoiar a aderência com a Lei Geral de Proteção de Dados Pessoais. Canedo et al. (2020) realizaram uma revisão sistemática da literatura para identificar trabalhos relacionados com privacidade de software, requisitos de privacidade, as metodologias e técnicas usadas para especificá-los. E os resultados revelaram que os profissionais de tecnologia da informação não têm um conhecimento abrangente de privacidade de software, requisitos de privacidade e a LGPD. Compartilhando dos mesmos resultados, Peixoto et al. (2020) afirmam, na sua pesquisa, que desenvolvedores têm conhecimento empírico de privacidade, pois a maioria deles não sabe como interpretar adequadamente os requisitos de privacidade, assim como muitos deles desconhecem a própria lei (LGPD). Como também, na falta de uma abordagem para orientar as empresas a avaliar e alcançar a conformidade com a LGPD em seus processos, Araújo et al. (2021), propuseram o método LGPD4BP (LGPD for Business Process). Por fim, Carvalho et al. (2019) abordaram os possíveis desafios entre transparência (LAI) e privacidade (LGPD) nos aspectos de TI em sistemas da informação.

2.3.3 *Privacy By Design*

O *Privacy by Desing* é um conceito que tem sua origem atribuída a Ann Cavoukian, que era comissária de informação e privacidade em Ontário, no Canadá. De acordo com o documento publicado pela autora em 2010, "*Privacy by Desing*: os 7

princípios fundamentais", adotado pela *International Assembly of Privacy commissioners na data Protection Authorities* e difundido no mundo todo, o termo *privacy by desing* que também pode ser referido com a sigla "PbD", significando a metodologia que visa proteger a privacidade do usuário desde a concepção de qualquer sistema de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano e as liberdades fundamentais (CAVOUKIAN, 2010).

Os sete princípios são definidos e expostos na prática conforme o seu documento oficial (Cavoukian, 2010), em que destaca que o PbD deve permear por toda tecnologia, processos, culturas e governança das empresas e instituições:

I – Proativo e não reativo, preventivo e não corretivo: a abordagem PbD é caracterizada por medidas proativas e não reativas, pois antecipa e evita os eventos invasivos de privacidade antes que eles aconteçam, ou melhor, que sejam identificados e corrigidos na fase de planejamento, antes do desenvolvimento e lançamento do produto;

II – Privacidade com padrão (*by default*): este princípio busca oferecer o nível máximo de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema ou negócio de TI, se o indivíduo não faz nada, sua privacidade ainda permanece intacta, pois nenhuma ação é necessária por parte do indivíduo, a privacidade já está embutida no sistema por padrão;

III – Privacidade Incorporada ao *design*: esse princípio define que a privacidade deve ser incorporada nas tecnologias e nas práticas de negócio de maneira holística, tornando-se um componente essencial e não um mero complemento;

IV – Funcionalidade Total – soma positiva, não soma zero: esse princípio busca acomodar todos os objetivos e interesses legítimos de uma maneira positiva, com ganhos em dobro para os indivíduos e a sociedade, evitando abordagens duvidosas ou antiquadas que possam colocar a privacidade como um cálculo de resultado zero;

V – Segurança de ponta-a-ponta e proteção durante todo o ciclo de vida dos dados: o PbD tendo sido incorporado ao sistema antes do primeiro elemento de informação ser coletado estende-se com segurança por todo o ciclo de vida dos dados envolvidos, isso garante que os dados sejam retidos com segurança e, em seguida, com segurança destruído no final do processo, em tempo hábil, assim garantindo a confidencialidade, integridade e disponibilidade dos dados pessoais em todo o ciclo de vida;

VI – Visibilidade e Transparência: esse princípio visa garantir a todos os interessados que independentemente da prática ou tecnologia comercial envolvida estejam operando de acordo com as promessas e objetivos declarados, destacando que as promessas estão sujeitas à verificação. Documentar, disponibilizar as políticas e procedimentos relacionados à privacidade e disponibilizar canal de comunicação podem ser uma medida organizacional para atender o princípio;

VII – Respeito pela privacidade do usuário – mantenha o foco no usuário: acima de tudo, o PbD exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro lugar, oferecendo medidas com fortes padrões de privacidade, aviso apropriado, capacitando a facilidade de uso, e, o mais importante, que o usuário mantenha o controle sobre os seus dados pessoais. Uma medida organizacional adotada é capacitar os titulares dos dados a gerenciar ativamente os seus dados pessoais, evitando abuso e uso indevido de seus dados;

Seguindo o raciocínio de Ann Cavoukian ao concluir que somente as leis não garantem a privacidade, necessita-se de uma metodologia de apoio; diante desse pensamento, as legislações adotadas no continente europeu e a publicada no Brasil preveem explicitamente os conceitos de *Privacy by Design* e *Privacy by Default* na sua redação como metodologia de apoio à privacidade e proteção de dados.

Diante disso, temos o Artigo 25º da *General Data Protection Regulation,* conforme extração do texto em destaque, que prevê expressamente os conceitos citados no parágrafo anterior, inclusive dando enfoque na titulação do dispositivo legal com a seguinte nomenclatura "Proteção de dados por *design* e por padrão" (Regulamento (UE) 2016/679):

> **Artigo 25º Proteção de dados por *design* e por padrão:**
>
> 1. Levando em conta o estado da arte, o custo de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como os riscos de probabilidade e severidade variáveis dos direitos e liberdades das pessoas singulares representadas pelo processamento, o responsável pelo tratamento deve, no momento da determinação dos meios de processamento e no próprio momento do processamento, implementar medidas técnicas e organizacionais apropriadas, como a pseudonimização, projetadas para implementar princípios de proteção de dados, como minimização de dados, e de forma eficaz e integrar as

> salvaguardas necessárias ao tratamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos dos titulares dos dados.
>
> 2. O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do processamento sejam processados. Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão de seu processamento, ao período de seu armazenamento e à sua acessibilidade. Em particular, essas medidas devem garantir que, por padrão, os dados pessoais não sejam acessíveis sem a intervenção do indivíduo a um número indefinido de pessoas físicas.
>
> 3. Um mecanismo de certificação aprovado nos termos do Artigo 42, que pode ser utilizado como um elemento para demonstrar a conformidade com os requisitos estabelecidos nos parágrafos 1 e 2 do presente artigo."

Essa tendência foi refletida no Brasil com a Lei Geral de Proteção de Dados Pessoais no seu Artigo 46, §1º e 2º, que também adotou os conceitos de *privacy by design e privacy by default* no corpo da sua redação (BRASIL, 2018):

> **Art. 46**. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."

2.4 ABNT NBR ISO 27701:2019

A proteção da privacidade no contexto do tratamento de dados pessoais é uma necessidade da sociedade, bem como um tópico da Lei Geral de Proteção de Dados. A Norma Técnica ABNT NBR ISO/IEC 27701:2019 foi criada com a proposta de ser uma **extensão** das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para gestão da privacidade da informação, com requisitos e diretrizes.

A Norma Técnica 27001 tem o objetivo de garantir a confidencialidade, integridade e disponibilidade de um sistema de segurança, isso significa, a proteção da informação se faz necessário para qualquer tipo de organização que tem o objetivo de **definir especificamente os requisitos de privacidade** e prover um modelo para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). E a Norma Técnica 27002 trata de uma norma estrutural de gestão de segurança da informação que define o **catálogo de controles**, com o objetivo de orientar quais elementos devem ser considerados essenciais para garantir a conformidade da privacidade de dados.

Diante desses conceitos, essa pesquisa de mestrado utilizou a Norma 27701 como fonte de inspiração para estruturar os requisitos de privacidade, elaborar um catálogo de padrões de privacidade e conectar de forma prática os controles de privacidade com os artigos da Lei Geral de Proteção de Dados. Com isso, essa Norma nos auxiliou na elaboração do catálogo de padrões de privacidade, com o objetivo de direcionar as recomendações e soluções existentes na norma, para lacunas de privacidade de dados pessoais encontradas no contexto do sistema de software. Essas propostas estão inseridas no contexto do processo de atingir a conformidade legal dos sistemas de software, proposto pelo guia de privacidade elaborado na pesquisa.

2.5 CONSIDERAÇÕES FINAIS

A visão geral apresentada nesse capítulo permite uma compreensão dos conceitos básicos relacionados à Engenharia de Requisitos, as definições de requisitos funcionais e não funcionais, o ciclo do processo e as abordagens utilizadas em cada fase. Além disso, os conceitos de requisitos de privacidade foram retratados, bem como sua relação com a legislação. Também foram apresentados os conceitos, definições, princípios, sanções e requisitos de leis e regulações vigentes, como a LGPD e a GDPR. Como também os

conceitos da metodologia que visa proteger a privacidade desde a concepção. E as Normas Técnicas da Família 27000 sobre gestão de segurança da informação, controles e diretrizes sobre proteção e privacidade de dados.

3 MÉTODO DE PESQUISA

Esse capítulo apresenta a abordagem metodológica selecionada para essa pesquisa, que tem o objetivo de especificar requisitos de privacidades em conformidade com a LGPD, por parte dos analistas de requisitos, com o propósito de propor um modelo que auxilie de forma prática a operacionalização dessa atividade.

Nesse capítulo, apresentamos o método de pesquisa adotado nessa dissertação. A seção 3.1 descreve o planejamento de estudo de pesquisa. A seção 3.2 detalha a condução das entrevistas exploratórias. Na seção 3.3, são apresentadas a elaboração do guia de privacidade e o catálogo de padrões de privacidade. A seção 3.4 relata o método para avaliar o guia de privacidade e do catálogo de padrões de privacidade. A seção 3.5 apresenta as considerações éticas inerentes ao estudo. Por fim, a seção 3.6 apresenta um resumo do capítulo.

As limitações e as ameaças à validade da pesquisa serão tratadas na seção 7.1 do capítulo da conclusão da pesquisa.

3.1 PLANEJAMENTO DO ESTUDO

Essa seção tem o objetivo de apresentar o conjunto de estratégias e procedimentos utilizados nesse trabalho de pesquisa, a fim de alcançar os objetivos definidos no Capítulo 1. As fases do método de pesquisa são apresentadas na Figura 6, que ilustra a condução do desenho da pesquisa, seguindo as 4 (quatro) etapas.

Figura 6 - Etapas da pesquisa.

Fonte: O autor (2022).

A atividade que antecipou a primeira fase dessa pesquisa foi a realização de uma revisão bibliográfica informal sobre os temas relacionados aos conceitos básicos de engenharia de requisitos, requisitos de privacidade, leis, regulamentos e normas de privacidades, como LGPD, GDPR, Família ISO 27000 e Diretiva 95/EU. Essa atividade teve o objetivo de obter um entendimento macro sobre as iniciativas da disciplina de

engenharia de requisitos e as legislações de privacidade de dados no meio acadêmico a fim de se identificarem os problemas e as lacunas para a pesquisa. Aqui foram considerados os artefatos de revisão, livros, artigos científicos, dissertações, teses, sites do governo e sites de notícias.

Inicialmente, no planejamento de pesquisa ocorreu a definição do problema de pesquisa, que teve o objetivo de investigar as lacunas para especificar os requisitos de privacidade em conformidade com a Lei Geral de Proteção de Dados. Nessa etapa, também foram definidos os objetivos e as questões de pesquisa.

Posteriormente, com o entendimento sobre o problema de pesquisa definido, a estratégia foi definir a condução do método de pesquisa. Segundo Yin (2003), é fundamental definir o caso e a unidade da análise, pois representam a estratégia preferida quando se colocam questões do tipo "como" e "porque", quando o pesquisador tem um pouco de controle sobre os eventos e quando o foco se encontra em fenômenos contemporâneos inseridos em algum contexto da vida real.

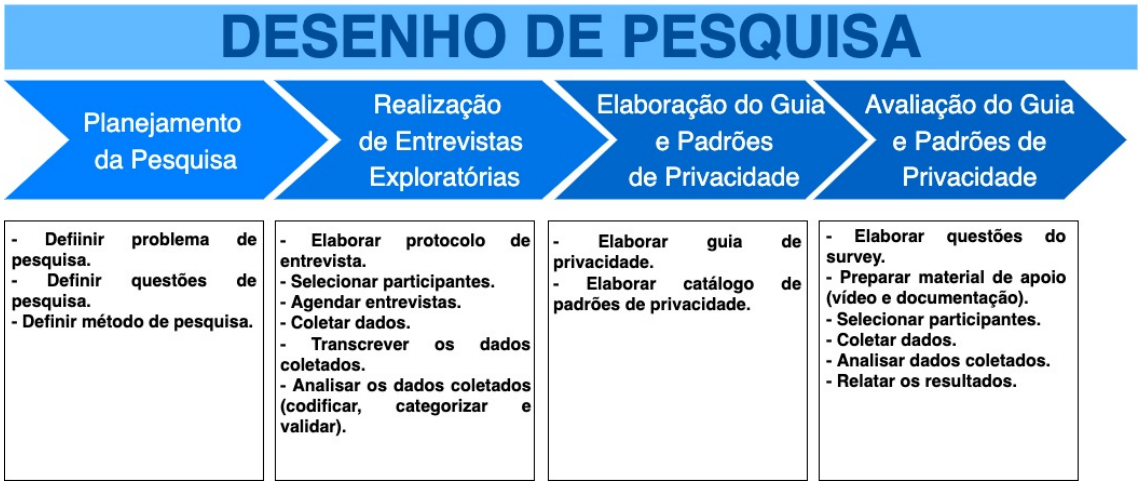
Diante disso, a estratégia foi executar entrevistas exploratórias focalizadas em um tema específico para um grupo de pessoas que estão inseridos naquele contexto. Em seguida, foi realizada a **preparação** para a coleta dos dados, com a elaboração do protocolo de entrevistas, a seleção dos participantes e os agendamentos das entrevistas. Durante a **coleta** de dados, ocorreram as entrevistas semiestruturadas, como também as transcrições dos áudios das entrevistas e as suas codificações. A **análise de dados** promoveu a transformação dos dados em informações, nessa etapa, os dados foram categorizados e organizados por temas superiores. A **síntese dos dados** apresenta os achados da pesquisa. E por fim, na etapa de **resultados**, foi gerado um diagnóstico dos aspectos mais relevantes sobre especificar requisitos de privacidade em conformidade com Lei Geral de Proteção de Dados.

Com os resultados obtidos na segunda fase da pesquisa, a terceira fase possibilitou a concepção de um catálogo de padrões de requisitos de privacidade e a iniciativa de propor um guia de privacidade que auxiliasse os analistas de requisitos durante a especificação dos requisitos de privacidade, trazendo os benefícios de ser uma proposta de ágil e de fácil entendimento.

Por fim, a última fase do planejamento do estudo foi a execução do *survey* com o objetivo de apresentar os resultados da avaliação do G-Priv, o guia para apoiar a conformidade na especificação de requisitos de privacidade com a LGPD. A avaliação foi realizada a partir do ponto de vista de profissionais de organizações privadas e

públicas que atuam nas áreas de engenharia de requisitos, análise de sistemas, privacidade de dados, segurança da informação, desenvolvimento de software. A Figura 7 resume os passos realizados para o desenvolvimento dessa pesquisa.

Figura 7 - Etapas da pesquisa detalhada.



Fonte: O autor (2022).

3.2 CONDUÇÃO DAS ENTREVISTAS

Essa seção tem o objetivo de descrever como foram realizadas as etapas das entrevistas exploratórias da pesquisa. Assim, para uma melhor compreensão, na seção 3.2.1, encontra-se o contexto sobre as entrevistas exploratórias da pesquisa. A seção 3.2.2 trata da preparação para a coleta de dados. Na seção 3.2.3, é apresentada a coleta de dados. Já na seção 3.2.4, descreve-se a fase de análise dos dados.

3.2.1 Contexto Das Entrevistas

As entrevistas podem ser informais, que são poucos estruturadas, quase uma conversa, mas com o objetivo de recolher dados. Essas entrevistas são focalizadas num tema específico cujos entrevistados fornecem informações livres ao discorrer sobre o assunto abordado. Como também seguem uma estrutura de perguntas preparadas pelo pesquisador, a que se submetem os entrevistados a fim de colher informações (MARCONI e LAKATOS, 2019). Segundo Flick (2009), o não direcionamento é obtido por meio de diversas formas de perguntas. A entrevista semiestruturada define o assunto concreto, deixando-se para o entrevistado a resposta em aberto, como por exemplo, “Na

sua opinião, como sua equipe entende o conceito de privacidade e proteção de dados pessoais, ao desenvolver um produto ou serviço?"

Na pesquisa, foi adotada a entrevista semiestruturada por possuir uma mistura de questões quase estruturadas. Segundo Yin (2001), esse tipo de entrevista tem como objetivo principal "compreender os significados que os entrevistados atribuem às questões e situações relativas aos temas de interesse". Dessa forma, pode-se investigar o ponto de vista dos analistas de requisitos a partir de suas afirmações e buscar compreender as percepções dos analistas de requisitos em relação à privacidade e proteção de dados, como também propor um padrão de requisito que os auxiliem na especificação de requisitos de privacidade em conformidade com a LGPD.

As entrevistas exploratórias foram conduzidas com o objetivo de responder a primeira questão de pesquisa (QP1 – Quais são as percepções de analistas de requisitos em relação à privacidade e proteção de dados?). A preparação para as entrevistas exploratórias iniciou-se com a elaboração de um protocolo de entrevistas semiestruturadas e a seleção de 5 (cinco) profissionais que atuam como analista de requisitos em um órgão público do poder judiciário; assim dimensionamos o que foi explorado, devido à necessidade de investigar o ponto de vista e a perspectiva desses profissionais em relação à especificação de requisitos de privacidade em conformidade a LGPD.

Os resultados dessas entrevistas apontam dados e *insights* concretos que foram analisados, utilizando os princípios técnicos da Teoria Fundamentada de Dados. Após as análises, identificamos *insights,* que nos possibilitaram definir características e necessidades dos analistas de requisitos durante a especificação dos requisitos de privacidade em conformidade com a LGPD, assim conseguimos revelar o propósito da exploração.

Colaborando para sustentar o propósito da exploração, fizemos uma análise e observações de um caso concreto de um sistema, que está funcionando no mesmo órgão público do poder judiciário estadual de Pernambuco, em que os analistas de requisitos entrevistados trabalham. A organização é o Tribunal de Justiça de Pernambuco, ao longo dos anos, a organização tem buscado inovar na área de TI. Ela tem participado ativamente na implantação do Processo Judicial Eletrônico (PJe). O objetivo principal é manter um sistema eletrônico capaz de permitir a prática de atos processuais em todos os ramos do Judiciário (Federal, Estadual e do Trabalho). Considerando a recente necessidade de adequação à LGPD, identificamos a oportunidade de contribuir com a melhoria do

processo de requisitos da organização. É importante ressaltar que o pesquisador desse estudo desempenhou durante muitos anos a função de analista de requisitos e hoje atua como gerente de projetos na organização estudada. Dessa forma, esse caso concreto serviu para investigar um problema real enfrentado pela organização.

O sistema Nísia (2021), que foi implementado pela equipe de TI da organização, é um aplicativo desenvolvido com o objetivo de possibilitar melhor acesso à informação de processos de medida protetiva. Com o aplicativo, a mulher ofendida pode acompanhar o andamento do processo pelo seu telefone celular sem precisar se deslocar até o órgão julgador onde tramita o processo. Nesse contexto, existe uma preocupação predominante de se preservar as mulheres, que são vítimas de violência doméstica independente de terem ou não processos tramitando no judiciário. O aplicativo pode ser acessado pela própria vítima de violência ou qualquer pessoa que sinta o desejo de ajudar uma mulher em situação de violência. Considerando o perfil dos usuários (i.e., mulheres que sofrem violência) e a natureza de dados sensíveis acessados pelo aplicativo Nísia, requisitos de privacidade são aspectos críticos que o sistema precisa satisfazer.

De uma forma geral, podemos considerar que a iniciativa de implantar a LGPD tem evoluído de forma satisfatória, uma vez que esta é lei, é uma exigência nacional e é patrocinada pela alta gestão. No entanto, identificamos diversos desafios e dificuldades que a organização precisa superar para garantir a conformidade legal dos seus sistemas. E um dos seus grandes desafios é alinhar os conhecimentos de privacidade com todos envolvidos, como também a mudança cultural dessas pessoas e consolidar um mecanismo sistemático para operacionalizar os seus processos internos e sistemas de software à legislação presente.

3.2.2 Coleta de Dados

Essa pesquisa utilizou como instrumento para realizar a coleta de dados entrevistas semiestruturadas, seguindo-se um protocolo disponível no APÊNDICE B. Conduzimos entrevistas semiestruturadas com 5 analistas de requisitos da organização. Todos os participantes possuem mais de dez anos de experiência e também acumulam cargos de gestão nas suas equipes, tais como: coordenação, chefia, direção e gerência. A Tabela 2 apresenta o perfil dos entrevistados.

Tabela 2 - Perfil dos entrevistados.

ID	Experiência profissional	Função	Formação acadêmica
E1	15 anos	Chefe do Núcleo de Gestão de Processos e Serviços de TI e Analista de requisitos	Possui curso superior e Mestrado em Ciência da Computação.
E2	18 anos	Gerente de arquitetura de negócios e Engenheiro de Software	Possui curso superior e pós-graduação em Ciência da Computação.
E3	20 anos	Analista de requisitos e Chefe do Núcleo de Gestão de Segurança da Informação	Possui curso superior em Ciência da Computação, Mestrado em Ciência da Computação e Especialização em Gestão de Segurança da Informação.
E4	13 anos	Diretor de Sistemas e Analista de requisitos	Possui curso superior e pós-graduação em Ciência da Computação.
E5	20 anos	Gerente de Projetos e Analista de requisitos	Possui curso superior em Ciência da Computação, Especialização em Gestão de Projetos e Mestrado em Ciência da Computação.

Fonte: O autor (2021).

Os participantes da pesquisa, previamente selecionados, foram contactados com antecedência em relação à realização das entrevistas por telefone, e-mail e mensagem instantânea, nos quais a pesquisa foi apresentada e feito o convite para a sua participação. As entrevistas foram conduzidas individualmente de maneira remota por vídeo conferência. No momento de cada entrevista, foi feita a apresentação da motivação e do objetivo de pesquisa, política de confidencialidade, objetivos e resultados esperados. Em cada entrevista, foi lido o TCLE (Apêndice A) e a coleta de autorização realizada previamente no formulário elaborado no Google Forms. Além disso, o pesquisador solicitou verbalmente a autorização para gravar a entrevista, e, se permitida, foi gravada.

3.2.3 Execução das Entrevistas

As entrevistas ocorreram no período de outubro a dezembro de 2020, e utilizamos a ferramenta Cisco Webex de videoconferência. O primeiro contato para agendamento de cada uma das entrevistas foi realizado pelo pesquisador, através de e-mail, contato telefônico, mensagem instantânea ou pessoalmente. Nesse momento, foi exposto um resumo sobre a pesquisa, a motivação e importância da conformidade dos sistemas de software às legislações de privacidade. Após a confirmação do participante, o pesquisador enviou uma mensagem e um e-mail solicitando a melhor data e horário para o entrevistado em um período predefinido. Com base nas respostas, foi enviado convite pela agenda do Google formalizando a data e hora da entrevista. Nenhum dos entrevistados contactados se recusou a participar das entrevistas.

O protocolo de entrevista possui 27 questões e está disponível no Apêndice B. Durante cada entrevista, foi utilizado como material de apoio um roteiro de entrevistas (Apêndice B) que foi projetado numa apresentação em *PowerPoint*.

No início de cada entrevista, foi feita uma apresentação da pesquisa que estava sendo elaborada, sua motivação e relevância, além da estimativa de seu tempo de duração. Também foi informada a política de privacidade de confidencialidade e a participação voluntária, após leitura do Termo de Consentimento Livre e Esclarecido (Apêndice A) e a ciência das demais informações descritas, os entrevistados informavam se estavam de acordo em prosseguir com a entrevista. Nesse momento, o pesquisador solicitava autorização verbal para gravação de áudio e, se permitida, as gravações eram registradas. Nenhum participante se recusou a prosseguir com a entrevista. As informações dos entrevistados estão disponíveis na Tabela 3 dessa pesquisa. Para cada participante, geramos um código aleatório com o proposito de manter a sua identidade em sigilo.

Todas as entrevistas foram gravadas e resultaram em cerca de seis horas e trinta minutos de gravação. Cada entrevista durou em torno de uma hora. Com exceção do entrevistado **E5** que durou 01 hora e 32 minutos, consistindo a entrevista mais longa. A entrevista mais curta foi a do participante **E1** que teve uma duração de 59 minutos.

Na transcrição das entrevistas, foram geradas 48 páginas de dados brutos. O processo de transcrição ocorreu em paralelo com a fase de entrevistas, assim sendo iniciado no mês de outubro de 2020 e finalizado em janeiro de 2021. As transcrições foram feitas na íntegra, escutando os áudios e transcrevendo num arquivo *Word*. Todas as transcrições foram realizadas pelo pesquisador.

Com os dados coletados nas entrevistas, foi possível investigar o ponto de vista dos analistas de requisitos, buscando compreender suas percepções durante a especificação de requisitos de privacidade e entender como a organização está trabalhando seus processos internos para garantir conformidade com a LGPD.

Assim como as observações, realizamos a análise de documentos durante a fase de coleta de dados da pesquisa, a documentação oficial do Sistema Nísia, como por exemplo, o manual do usuário e a política de privacidade. Essa técnica serviu para corroborar com as evidências identificadas como relevantes na pesquisa.

3.2.4 Análise de Dados

Essa etapa da análise possibilita que os dados sejam refinados e transformados em informações. Para analisar os dados, nós utilizamos técnicas baseadas nos procedimentos metodológicos da Teoria Fundamentada nos Dados (TFD), do inglês *Grounded Theory* (FLICK, 2009; STRAUSS e CORBIN, 2008; MERRIAM, 2009, CRUZES, 2014).

A teoria fundamentada nos dados tem o objetivo de criar uma teoria a partir dos dados coletados e analisados sistematicamente, e o processo central é a codificação que diz respeito ao processo de analisar dados segundo Strauss e Corbin (2008).

Segundo a linha proposta por Strauss, durante a codificação são identificados conceitos (ou códigos) e categorias. Um conceito (ou código) dá nome a um fenômeno de interesse para o pesquisador. Categorias são agrupamentos de conceitos unidos em um grau de abstração mais alto. O produto final da pesquisa na teoria fundamentada é uma série de conceitos fundamentados e integrados em torno de uma categoria ou questão central para formar um arcabouço teórico que explique como e porque as pessoas reagem a determinados acontecimentos, desafios ou problemáticas.

O processo de codificação apresenta as seguintes etapas: codificação aberta, codificação axial e codificação seletiva. Na codificação aberta, são realizadas a quebra, a análise, a comparação e a categorização dos dados. Segundo Merriam (2009), codificação aberta envolve etiquetar qualquer unidade de dados que possa ser relevante para o estudo. Para Flick (2009), a codificação aberta é o processo analítico pelo qual os conceitos são identificados e desenvolvidos em termos de suas propriedades e dimensões, em que se tem a finalidade de expressar dados e fenômenos na forma de conceitos e esses dados são primeiramente segmentadas e classificadas pela unidade de significados, em sequências curtas de palavras. Nas fases iniciais da codificação aberta, o pesquisador explora os

dados examinando minuciosamente aquilo que lhe parece relevante devido à leitura intensiva dos textos.

Na codificação axial, examina-se as relações entre as categorias que formam as proposições da teoria substantiva. Segundo Merriam (2009), a codificação axial é o processo de relacionar categorias e propriedades entre si, refinando o esquema de categorias. A codificação axial é um conjunto de procedimentos realizados após a codificação aberta em que os dados são colocados em uma nova forma, por meio das relações entre as categorias, isto é, realizado com o paradigma de codificação que envolve condições, contexto, estratégias de ação/interação e suas consequências (STRAUSS e CORBIN, 1990). Flick (2009) afirma que essas categorias axiais são enriquecidas na medida em que se ajustam à maior quantidade de trechos possível. Por fim, a codificação seletiva realiza o refinamento de todo o processo identificando a categoria central da teoria com a qual todas as outras estão relacionadas.

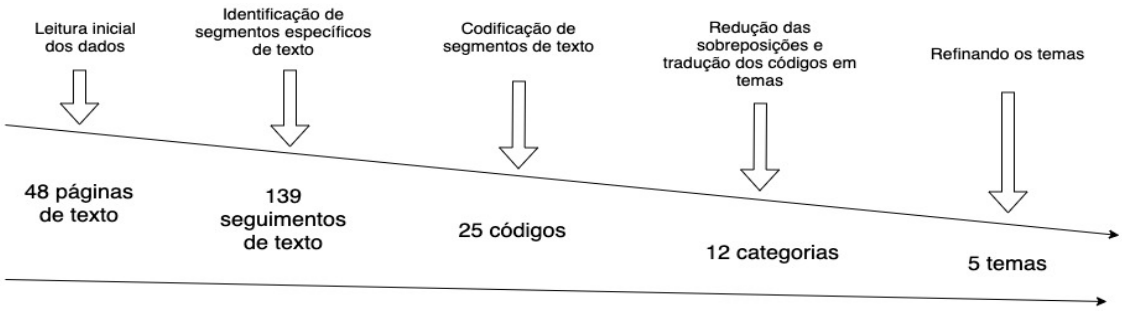
Segundo Cruzes (2014), a síntese temática é uma variação da análise de conteúdo, consiste em um método para identificar, analisar e registrar padrões (temas ou categorias) a partir dos dados. Que são divididas em cinco passos descritos na ilustração da Figura 8.

- **Extrair dados** – extrair dados das transcrições das entrevistas, visando aos objetivos da pesquisa, contexto e resultados, como também informações dos estudos primários, incluindo informações bibliográficas;
- **Codificar dados** – identificar e codificar conceitos relevantes, categorias, achados e organizar os resultados de forma sistemática numa base de dados;
- **Traduzir categorias** – traduzir e organizar em temas, subtemas e temas superiores;
- **Criar um modelo hierárquico de temas** – nesse passo, foi realizada a exploração de relacionamentos entre temas e criado um modelo com temas de ordem mais elevados;
- **Avaliar a confiabilidade da síntese –** avaliar e validar a confiabilidade da interpretação desde os dados básicos, até o resultado final com a síntese temática.

A partir da Figura 8 é possível identificar o processo de análise e refinamento dos dados, que se inicia com a leitura inicial das entrevistas transcritas, passando para a identificação de seguimentos específicos, seguindo para a codificação desses

seguimentos, que identificados possibilitam o agrupando de códigos em categorias, para, finalmente, permitir o refinamento dos temas.

Figura 8 - Processo de análise e refinamento de dados.



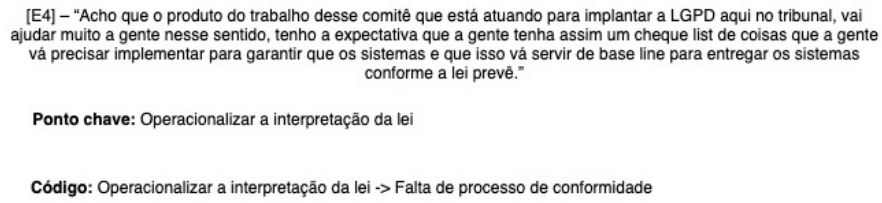
Fonte: O autor (2021).

I- Codificação

Durante a fase de análise, adotamos a abordagem de Teoria Fundamentada nos Dados (TFD), do inglês *Grounded Theory*, que envolveu as fases de codificação aberta, codificação axial e codificação seletiva. A TFD tem como objetivo criar uma teoria a partir dos dados coletados e analisados sistematicamente com o processo central de codificação dos dados.

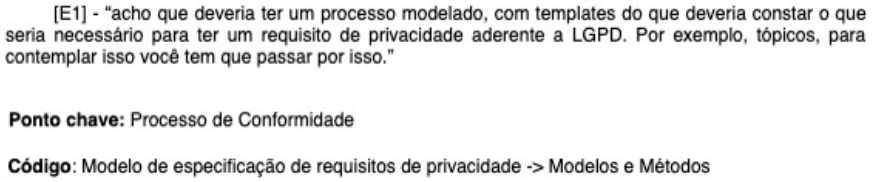
O processo de análise dos dados foi realizado da seguinte forma. Inicialmente, utilizamos a codificação aberta. Nesse momento, as entrevistas foram lidas e analisadas por um dos autores, realizando as codificações individuais com anotações, comentários e observações nas margens dos documentos transcritos. Esse procedimento ocorreu nas cinco entrevistas, com o objetivo de identificar dados de potencial relevância, com semelhanças e diferenças para descrever o fenômeno em estudo e responder às questões de pesquisa. Nessa etapa, várias interações de comparações foram realizadas para a seleção de códigos que indicavam relatos representativos em citações de cada entrevista. Na codificação aberta, a comparação e os questionamentos são dois procedimentos analíticos básicos que propiciam mais precisão e especificidade às características fundamentais aos conceitos (STRAUSS e CORBIN, 2008). Nas Figuras 9 e 10, apresentamos o exemplo de trechos de entrevista, com seu respectivo código.

Figura 9 - Evidência da entrevista, ponto chave e código.



Fonte: O autor (2021).

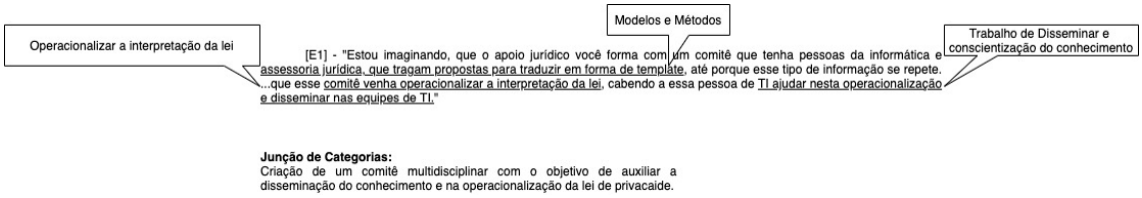
Figura 10 - Evidência da entrevista, ponto chave e código.



Fonte: O autor (2021).

Durante o processo de codificação axial, que consiste em aprimorar e diferenciar as categorias resultantes da codificação aberta, criamos os relacionamentos entre os códigos através das categorias em que elaboramos temas de ordem superior. Segundo Cruzes e Dyba (2011), categorias são conceitos unificadores recorrentes ou declarações sobre o assunto investigado, com o propósito de caracterizar evidências de estudos individuais em percepções mais gerais de um conjunto de dados. Na Figura 11, apresentamos o exemplo da construção das relações.

Figura 11 - Codificação Axial: Construindo relações.



Fonte: O autor (2021).

Finalmente, a codificação seletiva é a fase de refinamento da codificação axial em um nível superior de abstração, cujo objetivo é integrar e sintetizar categorias em um nível mais abstrato. Segundo Strauss e Corbin (2008), o fenômeno central é o coração do processo de integração. Nessa etapa, elaboramos a categoria central *especificação de requisitos em conformidade com a LGPD*, em torno da qual as outras categorias foram desenvolvidas e integradas. Na síntese dos dados, foi realizada uma classificação final das categorias, considerando como critério de definição das categorias, o grau de

relevância em relação aos aspectos de privacidade de dados na especificação de requisitos em conformidade legal.

II- Síntese Temática

Na síntese dos dados, foi realizada uma classificação final das categorias, considerando como critério de definição das categorias, o grau de relevância em relação aos aspectos de privacidade de dados na especificação de requisitos em conformidade legal. A Tabela 3 traz as categorias obtidas na síntese dos dados, e para cada categoria, apresentamos a frequência de ocorrências nas falas dos entrevistados.

Tabela 3 - Categorias da pesquisa.

Categorias da pesquisa	**Frequência**	**Percentual**
1. Processo de Conformidade	40	30,08%
2. Obstáculos na Conformidade	29	21,80%
3. Tradeoff entre Privacidade X Transparência	27	20,30%
4. Rotina de Trabalho	24	18,04%
5. Conceitos de Privacidade	13	9,77%
Total	**133**	**100%**

Fonte: O Autor (2021).

Ao final do procedimento de análise dos dados coletados (codificação, categorização e refinamento dos temas superiores), o pesquisador apresentava os resultados em formato de seminário para a professora orientadora, que estava inserida na pesquisa, em que tinha o objetivo de avaliar e validar os códigos, categorias e os achados de pesquisa extraídos nos trechos das entrevistas exploratórias.

3.3 ELABORAÇÃO DO GUIA DE PRIVACIDADE E O CATÁLOGO DE PADRÕES DE PRIVACIDADE

A elaboração do guia para apoiar a conformidade na especificação de requisitos de privacidade com a LGPD (G-Priv) e o catálogo de padrões de privacidade foram conduzidas com o objetivo de responder à segunda questão de pesquisa (QP2 – Como auxiliar analistas de requisitos na especificação de requisitos de privacidade em conformidade com a LGPD?).

A partir da análise das percepções dos entrevistados, identificamos a necessidade de uma abordagem para especificar requisitos de privacidade que seja ágil e forneça diretrizes simples. Diante disso, o G-Priv foi inspirado nos resultados das entrevistas

exploratórias conforme detalhado no capítulo 4, onde os entrevistados reforçam a necessidade de operacionalizar a adequação dos seus processos internos e sistemas de software à LGPD na sua rotina de trabalho. Este obstáculo na conformidade está diretamente conectado à ausência de um processo, modelo ou método que auxilie na especificação de requisitos de privacidade, como também a limitação de conhecimento sobre os princípios e conceitos de privacidade e proteção de dados.

O G-Priv teve também como fonte de inspiração, os conceitos de *Privacy by Desing*, conforme apresentado na seção 2.3.3 do capítulo 2 do referencial teórico, que tem o objetivo metodológico de proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação. Essa pesquisa de mestrado visa à privacidade dos dados pessoais a partir da especificação dos requisitos de privacidade.

O catálogo de padrões de privacidade foi elaborado para alinhar os objetivos de privacidade aos princípios da LGPD, com o objetivo de operacionalizar, facilitar a conformidade e a reutilização do conhecimento adquirido durante a especificação de requisitos de privacidade. Conforme as seções 2.2 e 2.3.2, que tratam dos requisitos de privacidade e os princípios da LGPD respectivamente.

A elaboração deste catálogo seguiu os conceitos e modelos de padrões de privacidade propostos na literatura, conforme apresentado nas seções 5.1 e 5.2. Como também serviu de inspiração, o catálogo de controles sugeridos pela Norma Técnica ISO 27701, que contém controles de privacidade mapeados pelos artigos da LGPD e suas respectivas diretrizes de privacidade, conforme exposto na seção 2.4 do capítulo 2.

3.4 SURVEY PARA AVALIAÇÃO DO GUIA

Segundo Kitchenham (2008), *survey* não é apenas o instrumento (o questionário ou lista de verificação) para coletar informações. *Survey* é um método abrangente de pesquisa para coletar informações para descrever, comparar ou explicar o conhecimento, atitudes e comportamentos. A principal forma de coletar informações é fazendo perguntas, cujas respostas constituem os dados a serem analisados. Geralmente, as informações devem ser coletadas apenas de uma fração da população estudada e não cada membro da população.

Nessa pesquisa de mestrado, foi elaborado e disponibilizado pelo pesquisador um questionário eletrônico do Google Forms, onde os dados foram coletados por meio das respostas dos participantes, conforme detalhado no capítulo 6 e no apêndice H. O

questionário foi acompanhado de várias informações administrativas, como explicação do objetivo do estudo, uma explicação realista do tempo necessário para preencher o questionário e informações sobre os pesquisadores.

Ao formular as perguntas, elaboramo-las de duas maneiras: questões fechadas e abertas. Nas questões fechadas, os respondentes são solicitados a escolher uma das respostas predefinidas, ou uma escala ordinal definida entre: discordo totalmente, discordo parcialmente, indiferente, concordo parcialmente e concordo totalmente. Nas questões abertas, os participantes são solicitados a enquadrar a sua própria resposta. Segundo Kitchenham (2008), as perguntas abertas podem deixar espaço para interpretações erradas e o fornecimento de uma reposta irrelevante ou confusa, sendo assim, as respostas abertas podem ser difíceis de codificar e analisar.

As perguntas foram colocadas em uma importante ordem, em que se recomenda que as perguntas sejam feitas em uma ordem lógica, começando com perguntas mais fáceis, como questões demográficas que descrevem o participante, assim encorajando para as perguntas de avaliação sobre o tema abordado. Em nossa pesquisa, utilizamos o TAM (*Technology Acceptance Model*), que foi projetado para compreender a relação casual entre variáveis externas de aceitação dos usuários e o uso real do computador, buscando entender o comportamento desses usuários através do conhecimento da utilidade e da facilidade de utilização percebida por eles (DAVIS, 1989).

Quanto à motivação e às taxas de respostas, primeiramente o pesquisador buscou na sua rede de relacionamento profissional, pessoas que se enquadravam no objetivo do estudo (Engenharia de requisitos, Privacidade de dados, Desenvolvimento de software, Segurança da Informação e Análise de Sistemas), em seguida justificando o contato, mostrando aos participantes que foram escolhidos por sua relevância e importância para a pesquisa, por fim garantido que a confidencialidade será preservada. Diante disso, segundo Kitchenham (2008), podemos concluir que nossa amostragem é do tipo não probabilísticos, termo criado para justificar quando respondentes são escolhidos porque são facilmente acessíveis ou o pesquisador tem alguma justificativa para acreditar que eles são representativos da população.

Uma consideração importante durante a construção do questionário é o impacto de nosso próprio viés. Então, tomamos o cuidado na forma de elaborar a pesquisa, assim evitando que nossas perguntas sejam de uma forma que é para confirmar o resultado desejado. Para isso, escrevemos instruções claras e imparciais, como também tentamos

desenvolver perguntas neutras que cobriam adequadamente o tópico, evitando a imparcialidade.

O objetivo principal do *survey* foi avaliar a facilidade de uso, o funcionamento sistemático das etapas, as interações entre os atores e a utilidade dos artefatos propostos no guia de privacidade (G-Priv) e no catálogo de padrões de privacidade, em um universo populacional de 18 participantes especialistas no tema de privacidade de dados e engenharia de requisitos.

3.5 CONSIDERAÇÕES ÉTICAS

Por utilizarmos pessoas como a nossa fonte de coleta de dados, tratamos de considerações éticas na pesquisa. Durante a realização das entrevistas, esclarecemos aos entrevistados sobre os objetivos do estudo. Também os conscientizamos sobre a voluntariedade de participação e informamos sobre a garantia do sigilo da identidade e do conteúdo das entrevistas, bem como asseguramos que as informações coletadas sobre eles não serão utilizadas por qualquer instituição contra os interesses do participante.

Para tal, utilizamos como base o Termo de Consentimento Livre e Esclarecido (TCLE), Resolução 196/96, estabelecido pelo Conselho Nacional de Saúde que tem o propósito de proteger pessoas envolvidas em pesquisas através do respeito à ética no desenvolvimento do trabalho.

No início de cada entrevista, lemos o Termo de Consentimento Livre e Esclarecido (Apêndice A) e aguardamos o consentimento verbal do participante para dar continuidade ao procedimento de coleta de dados, como também solicitamos a permissão para a gravação do vídeo e áudio. E segundo Merrian (2009), com esse procedimento reduziremos o risco de expor ou denigrir a imagem dos participantes, evitando violações éticas.

3.6 RESUMO DO CAPÍTULO

Esse capítulo apresentou a metodologia utilizada nessa pesquisa, citando o planejamento de estudo, a condução para as entrevistas semiestruturadas, execução das entrevistas, procedimento de coleta e análise dos dados, elaboração do guia de privacidade e o catálogo de padrões de privacidade, *survey* de pesquisa para avaliar o guia de privacidade e o catálogo de padrões de privacidade, as considerações éticas e as

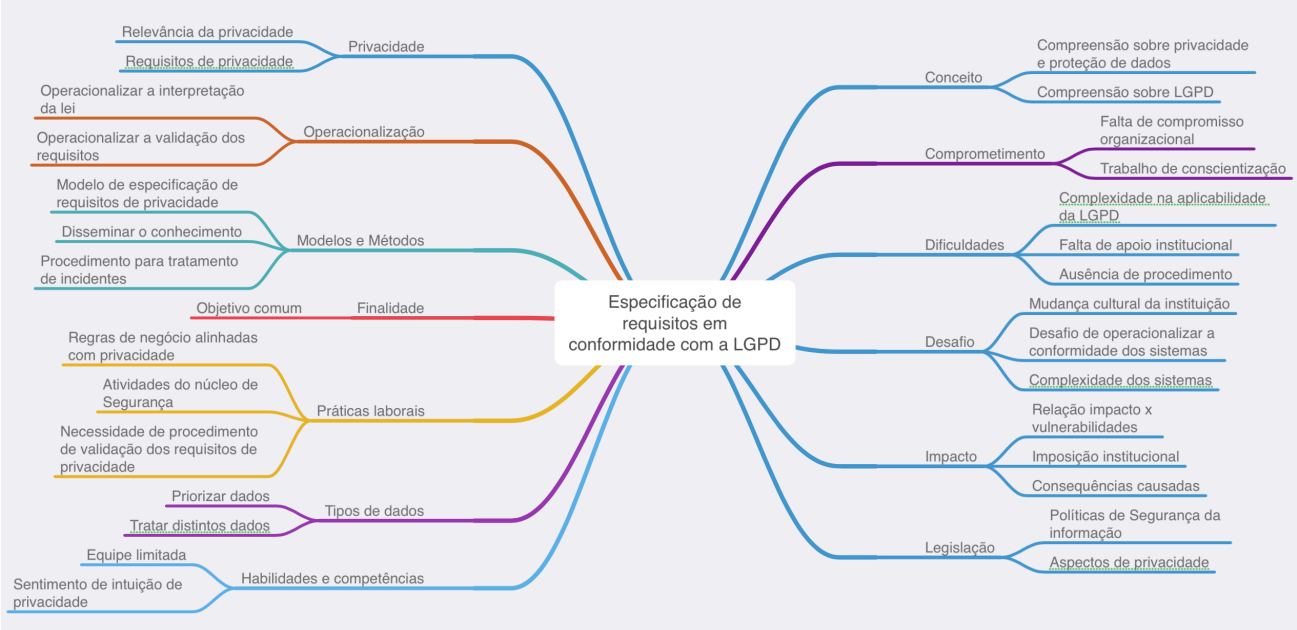
ameaças à validade. O próximo capítulo irá discorrer sobre os resultados das entrevistas exploratórias.

4 RESULTADOS DAS ENTREVISTAS EXPLORATÓRIAS

Nessa seção, apresentamos os resultados obtidos a partir das entrevistas realizadas. A seguir, discutimos os principais achados e trechos de falas dos entrevistados dentro de cinco categorias identificadas. A seção 4.1 tratará dos aspectos de limitação de conhecimento sobre privacidade e proteção de dados. A seção 4.2 descreverá a necessidade de um processo de conformidade, que seja sistemático e operacional. A seção 4.3 abordará a forma como a organização encara os obstáculos de conformidade. A seção 4.4 fará referência como a organização sofre influência das leis internas e externas, um *Tradeoff* entre privacidade e transparência. A seção 4.5 traçará um perfil de competências e atividades da rotina de trabalho. A seção 4.6 apresentará a síntese dos achados encontrados nas entrevistas exploratórias. A seção 4.7 tratará o resumo do trabalho.

Na Figura 12 apresentamos uma visão geral de todos os códigos, categorias e temas superiores em torno do tema central, que foram obtidos a partir das entrevistas realizadas.

Figura 12 - Códigos, Categorias, Temas Superiores e Fenômeno Central.



Fonte: O autor (2021)

4.1 CONCEITOS DE PRIVACIDADE

Essa categoria diz respeito à limitação de conhecimento sobre princípios e conceitos de privacidade e proteção de dados. É por meio do conhecimento apropriado

sobre a legislação vigente e como ela pode ser operacionalizada em requisitos de privacidade que os sistemas novos e legados estarão em conformidade com a LGPD. Identificamos, nos relatos dos entrevistados, que a falta de entendimento conceitual sobre privacidade de dados, traz como consequências a fragilidade de especificar requisitos de privacidade, assim como a falta de maturidade na operacionalidade das regras legais impacta o correto desenvolvimento de novos sistemas. A seguir, apresentamos evidências encontradas nas entrevistas:

[E1] "Eles (equipe de TI) têm total desconhecimento, até porque ***o requisito de segurança da informação que está ligado à LGPD como requisito não funcional, ele nunca foi uma prioridade*** *no desenvolvimento de sistemas."*

[E5] "Eu acho que a minha equipe entende o que é divulgado na mídia, mas ***não tem o entendimento profundo sobre esta questão. É o que está no dia a dia, na cultura ou mesmo por ética e valor da própria pessoa.****"*

Diante dessa preocupação, os entrevistados reforçaram que o primeiro passo necessário para garantir um conhecimento amplo sobre privacidade e proteção de dados envolve investimento em capacitação e conscientização sobre o tema. Isso pode ser evidenciado nos seguintes trechos:

[E2] "Quanto aos métodos ou modelos, penso que devemos trabalhar em cima das ***capacitações das pessoas, para elas entenderem o que são essas preocupações de privacidade*** *e elas embutem isso nas especificações que eles vão fazer."*

[E3] "Acho que existe um nível de preocupação, ***acho que esse conhecimento não está zerado, mas acho que é algo que precisa ser amadurecido diante dos requisitos atuais.*** *A realidade de agora exige uma preocupação mais reforçada do que vinha se tendo. Acho que nossa equipe precisa-se amadurecer para os requisitos de agora. O primeiro passo para esse amadurecimento vem com o* ***trabalho de conscientização****, que já iniciamos com cursos de capacitação."*

[E5] "Eles (equipe de TI) não fizeram cursos de proteção de dados e não foram capacitados formalmente para isso. (...) a quantidade de sistemas de informações disponibilizado para o público aumenta exponencialmente, então a gente precisa ter uma ***capacitação atualizada dessas questões de dados pessoais****."*

4.2 PROCESSO DE CONFORMIDADE

Essa categoria envolve o modo sistemático como a organização deseja operacionalizar a adequação dos seus processos internos e sistemas de software à

legislação vigente. Verificamos que a principal necessidade destacada pelos entrevistados é a operacionalização da interpretação da lei, isso é visto como um desejo unânime entre os entrevistados. A necessidade de garantir a conformidade com a legislação está diretamente ligada à ausência de um processo, modelo ou método que auxilie na especificação de requisitos de privacidade em conformidade com a LGPD. Esses aspectos podem ser evidenciados nos seguintes trechos de entrevistas:

[E1] "Estou imaginando um ***comitê que tenha pessoas da informática e assessoria jurídica****, que traga propostas para traduzir em forma de* ***template****, até porque esse tipo de informação se repete...que esse comitê venha operacionalizar a interpretação da lei, cabendo a essa pessoa de TI ajudar nessa operacionalização e disseminar conhecimento nas equipes de TI."*

[E1] ""acho que deveria ter um ***processo modelado, com templates do que deveria constar o que seria necessário para ter um requisito de privacidade*** *aderente à LGPD. Por exemplo, tópicos, para contemplar isso você tem que passar por isso."*

[E3] "O ideal que tivesse esse ***apoio jurídico para operacionalizar esta atividade****, mas já está em construção esse caminho que possa viabilizar uma expertise na área jurídica do tribunal, para que tenhamos esse apoio."*

[E4] "Acho que o produto do trabalho ***desse comitê, que está atuando para implantar a LGPD*** *aqui, vai ajudar muito a gente nesse sentido, tenho a expectativa que a gente tenha* ***um checklist de coisas que a gente vá precisar implementar para garantir que os sistemas*** *estejam em conformidade e que isso vá servir de baseline para entregar os sistemas conforme a lei prevê."*

[E4] "uma dessas lacunas que existe certamente é a ***adaptação do nosso processo de desenvolvimento para deixá-lo em conformidade*** *com esse novo contexto que a gente vive, onde a proteção dos dados é algo fundamental"*

[E4] "a cabeça de quem é de TI é meio cartesiana, ***eles querem modelos, parametrizar, digamos assim que tem que ser parametrizada****. E fora isso nós temos um volume grande de coisas para fazer, as demandas são muitas e precisamos de algo para dar vazão, que possam viabilizar a implantação dessas coisas mais produtiva"*

[E5] "Seria um ***template que operacionalizasse essa especificação dos requisitos*** *de privacidade com campos obrigatórios, acho isso iria ajudar muito."*

4.3 OBSTÁCULOS NA CONFORMIDADE

Essa categoria explora a forma como a organização encara os obstáculos para alinhar os seus sistemas, bases de dados, e a própria mentalidade das pessoas envolvidas em relação aos aspectos de privacidade em conformidade legal. Observamos, nos relatos dos entrevistados, que as maiores dificuldades são evidenciadas como a complexidade na aplicabilidade da LGPD, em que a principal preocupação dos analistas é satisfazer as regras de negócios. Além disso, os entrevistados relataram que a atual cultura organizacional é considerada um obstáculo, como também a complexidade dos sistemas e os dados. Esses achados podem ser evidenciados nos seguintes trechos das entrevistas:

*[E1] "**Não existe essa cultura de especificar de forma explícita os requisitos de privacidade**, (...) vai ser um grande desafio a LGPD porque de fato a coisa está muito embrionária."*

*[E1] "O grande desafio é operacionalizar tudo isso (Privacidade de dados), definir é muito fácil e bom, **mas na hora que operacionalizar e colocar como projeto estratégico e competir com as outras demandas**, aí que vou ver a seriedade da coisa"*

*[E2] "**Não existe essa preocupação com proteção e privacidade de dados, a preocupação é pela regra de negócio**. A preocupação é para deixar o sistema rodando em produção."*

*[E2] "A maior dificuldade que vamos encontrar está na **cultura da nossa organização**, (...) a nossa instituição a cada dois anos troca de gestão, quando muda a gestão muda as pessoas, mas existe um conjunto de comportamentos e culturas que permanecem e acho que **essa é a maior dificuldade que é uma cultura** independente das pessoas."*

*[E3] "Me parece que a alta gestão já tem um nível de sensibilidade para isto. O que me preocupa mais não é a alta gestão, mas a operação mesmo**, a gente descer para os níveis mais táticos e operacionais**."*

*[E3] "...o primeiro desafio é o **volume de sistemas e dados** que se trata no tribunal. O segundo desafio é dentre esses dados e sistemas uma grande parte são **dados não estruturados**, inclusive nosso principal sistema que é o PJE, onde se tem um misto de dados estruturados com um volume muito grande de dados não estruturados, esse é um desafio bem considerável para gente."*

*[E4] "Tenho até a impressão que antes desse tema (Privacidade de dados) vir à tona, **isso não era algo tão presente ou importante e não era levado em consideração**.*

Essa visão tenho em relação a mim e a outros colegas, enfim, na minha experiência profissional não se via uma preocupação relacionado a isso, talvez quando se fala em segurança da informação, se pensa numa maneira mais ampla, a segurança sempre aparecia e era presente nos requisitos, nos requisitos não funcionais dos aspectos de segurança e não nos aspectos de privacidade."

4.4 *TRADEOFF* ENTRE PRIVACIDADE E TRANSPARÊNCIA

Essa categoria refere-se ao modo como a organização sofre influência das leis internas e externas vigentes e o impacto das novas legislações nos seus sistemas e serviços prestados. Observamos que existe um verdadeiro dilema entre os entrevistados, na forma como tratar os diversos tipos de dados conforme a lei e a necessidade, ou melhor, alinhar os conceitos de privacidade com outras leis vigentes, como a Lei de Acesso à Informação (LAI). Esse é um desafio enfrentado por organizações públicas em geral. A equipe de TI precisa diferenciar como disponibilizar informações que são privadas daquelas que precisam ser públicas. Isso reflete um *tradeoff* entre privacidade e transparência e que pode ser confirmado nos seguintes trechos:

[E3] "O desafio que é o esclarecimento dos aspectos da lei geral de proteção de dados no âmbito do judiciário, que mostre a consonância da LGPD com as leis que já regem nosso funcionamento (códigos de processos, LAI), é um desafio grande a gente ***lidar com a lei de acesso à informação e a lei de privacidade de dados, que é transparência x privacidade****."*

*[E4] "Eu acho que devemos analisar caso a caso, e acho que sim, que podem surgir situações de conflito, a depender da informação que o cidadão deseja ter e isso pode entrar em conflito com a LGPD e gerar uma situação delicada****. Eu acredito que na maioria dos casos seja possível haver uma conciliação.*** *Essas informações requisitadas com base na LAI, geralmente, não têm um propósito de requisitar dados pessoais, geralmente chega solicitação para finalidade de pesquisas acadêmicas ou para matéria jornalística."*

[E5] "Se formos pecar por excesso, vamos colocar tudo como segredo de justiça, aí você pode estar prejudicando a população onde o processo tem que ser público(...) então ***esse limite entre o que tem que ser público e sigiloso não está bem definido, e esse limite que, muitas vezes, não é dado pela legislação****."*

Por outro lado, vimos que sistemas que tratam de casos em segredo de justiça já têm as caraterísticas inerentes de privacidade devido à relevância social, à situação delicada numa eventual exposição desses dados e à exigência de lei específica. Isso pode ser reforçado no seguinte trecho:

[E4] "São mulheres vítimas de violência doméstica. E como são pessoas que estão em situação de vulnerabilidade, (...) a gente sabe que ***se essas informações de alguma forma vazarem, as vítimas podem sofrer agressão*** *e até perder a vida. Então a gente se preocupa muito com isso."*

[E3] "Na regra geral os sistemas são desenvolvidos sem essas características de privacidade e proteção de dados. ***Tem casos que a segurança já é inerente ao tipo de sistema****, aí nesses casos passam com mais rigor no olhar de segurança da informação"*

4.5 ROTINA DE TRABALHO

Essa categoria refere-se ao modo como as equipes de TI da organização realizam seu trabalho, envolvendo suas competências e atividades do dia a dia. Segundo relatos dos entrevistados, muitas vezes, os aspectos de privacidade são tratados de maneira intuitiva pelas equipes envolvidas. Como não há uma estratégia ou processo bem definido, requisitos de privacidade são abordados de maneira *ad hoc*.

[E3] "A privacidade é tocada em soluções internas muito mais pelo feeling, e quando a gente tem outra legislação específica, por exemplo: dados sobre criança e adolescente, já uma questão que já tratamos e rebate no tema de privacidade… ***essas questões de privacidade às vezes são tratadas por intuição ou ad hoc.****"*

*[E5] "****Não tem processo formal, não tem ferramenta, método ou modelo que contemplem os aspectos de privacidade. Então vai mais pelo feeling do engenheiro de requisitos****, inclusive ele pode esquecer de contemplar os aspectos de privacidade, que isso já aconteceu, usuários tiveram acessos a fluxos do processo que não poderiam ver."*

Um ponto de fragilidade levantado pelos entrevistados é a limitação de recursos de pessoal. Diante disso, ficou claro que a prioridade é entregar o produto com agilidade, devido ao grande volume de sistemas e novas demandas. Os projetos possuem poucas pessoas, e nem todas que estão disponíveis são capacitadas. Essa questão pode ser evidenciada nos seguintes trechos das entrevistas:

*[E4] "****A cabeça de quem é de TI é meio cartesiana, eles querem modelos****, parametrizar, digamos assim que tem que ser parametrizada. (...) temos um volume*

grande de coisas para fazer, as demandas são muitas e precisamos de algo para dar vazão, que possa viabilizar a implantação dessas coisas mais produtiva."

*[E2] "**A equipe até tem o conhecimento, mas devido à celeridade da entrega dos sistemas o tratamento não é o adequado**. (...) Nós temos uma equipe limitada de recursos, de pessoas capacitadas para fazer esse tipo de levantamento de requisitos e são muitas coisas para fazer, então **eles vão fazer rápido para liberar logo**."*

*[E4] "Para mim **a dificuldade é de conciliar a mão de obra** mesmo, em função de outras demandas que temos. (...) para mim o trabalho maior será em fazer a adaptação desses sistemas legados, então acho que esse será o maior desafio."*

4.6 SÍNTESE DOS ACHADOS

A partir da análise das percepções dos entrevistados, destacamos a necessidade de **operacionalizar** a interpretação da Lei Geral de Proteção de Dados, com o objetivo de adequá-la aos sistemas de softwares na **atividade laboral de especificar os requisitos** de software. Segundo os entrevistados, essa necessidade é originada dos desafios e dificuldades a serem superadas, como a ausência de um processo formal que auxilie os analistas de requisitos durante a especificação de requisitos de privacidades, como também o **pouco ou a falta de conhecimento** sobre privacidade de dados, **conflitos** com outras leis vigentes e **mudança cultural das pessoas** envolvidas no processo de conformidade.

Diante disso, os achados possibilitaram a iniciativa de propor um guia de privacidade que auxiliasse os analistas de requisitos de maneira ágil, de fácil entendimento, atividades bem definidas, artefatos simples, com definição de atores e suas responsabilidades.

- **Atividades -** as atividades devem ser bem definidas com artefatos, atores e responsabilidades;
- **Artefatos simples** - artefatos objetivos e genéricos que possam ser utilizados por qualquer organização;
- **Atores e responsabilidades -** atores com suas respectivas responsabilidades bem definidas no contexto envolvido;
- **Modelo de padrão** - um guia modelado como um fluxo de etapas, com as atividades distribuídas nessas etapas, que geram diferentes artefatos que servirão de entradas e saídas de uma etapa para outra.

4.7 RESUMO DO CAPÍTULO

Esse capítulo apresentou os resultados das entrevistas exploratórias, identificando os aspectos, desafios, dificuldades e facilitadores para operacionalizar a interpretação das legislações de privacidade. O resultado do estudo proporcionou a elaboração de um modelo de padrão de requisito de privacidade. A seguir, é apresentada a proposta dessa dissertação para auxiliar os analistas de requisitos na especificação de requisitos de privacidade em conformidade com a LGPD.

5 UMA PROPOSTA PARA ESPECIFICAR REQUISITOS EM CONFORMIDADE COM A LGPD

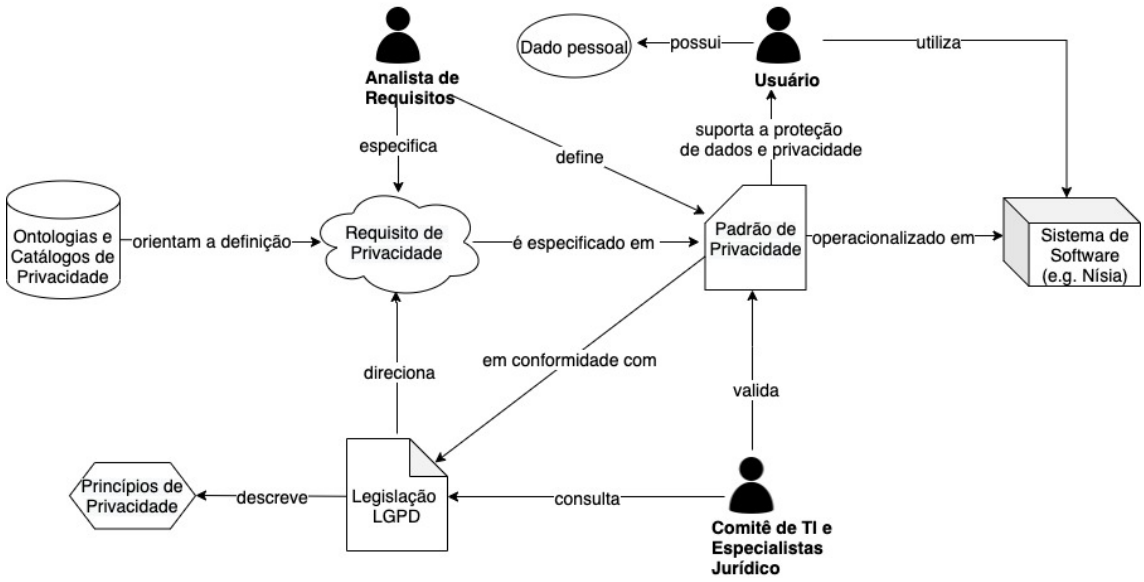
5.1 VISÃO GERAL

A partir da análise das percepções dos entrevistados da organização, identificamos que os analistas de requisitos necessitam de uma abordagem para especificar requisitos de privacidade de maneira ágil e que forneça diretrizes simples em formato de *templates* ou *checklists*. Além disso, em um primeiro momento, é recomendável realizar ações de conscientização e capacitação a fim de disseminar uma cultura alinhada com valores de privacidade. Dessa forma, a abordagem deve apresentar *guidelines* claros e boas práticas para garantir seu uso de forma fácil e rápida. Considerando tais necessidades, elaboramos uma proposta baseada em padrões de privacidade para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD.

Nossa motivação para a utilização de padrões é devido a sua ampla adoção pela comunidade de Engenharia de Software. Padrões fornecem uma estrutura simples para sistematizar e reusar conhecimento, e compartilhar boas práticas (FRANCH ET AL., 2010). Além disso, diferentes padrões de privacidade têm sido propostos por vários pesquisadores (LENHARD ET AL., 2017).

A Figura 13 apresenta uma visão geral da nossa abordagem. Partimos do pressuposto de que os padrões de privacidade serão definidos por analistas de requisitos e validados por um comitê multidisciplinar com profissionais de TI e especialistas jurídicos. Para garantir a disseminação de uma visão compartilhada sobre conceitos de privacidade e proteção de dados, adotamos ontologias (GARIB ET AL., 2020) e catálogos (PEIXOTO ET AL., 2020) como base de conhecimento na área. Tais bases de conhecimento têm como objetivo orientar a definição de requisitos que serão especificados no formato de padrões de privacidade. O objetivo do padrão de privacidade é definir de forma clara e simples como requisitos de privacidade em conformidade com a LGPD serão operacionalizados e implementados nos sistemas.

Figura 13 - Visão Geral da Proposta de Padrões de Privacidade.



Fonte: O autor (2021).

Nessa visão geral representada na Figura 13, destacamos os seguintes passos:

1º - O primeiro passo para se obter a conformidade legal dos requisitos de privacidade é necessário adquirir um conhecimento prévio dos termos e conceitos de privacidade de dados, para isso o analista de requisitos terá uma base com ontologias e catálogos de privacidade e os princípios descritos na LGPD, que servirão de orientação para as definições dos requisitos de privacidade;

2º - Em seguida, o analista de requisitos especifica o requisito de privacidade no artefato chamado de padrão de privacidade, que tem o objetivo de fornecer orientações conforme as regras vigentes da lei;

3º - O terceiro passo envolve a validação do padrão de privacidade pelo comitê gestor, que é composto por especialistas jurídicos e especialistas de TI, que devem auxiliar na validação do padrão de privacidade;

4º - Por fim, o artefato do padrão de privacidade segue para a operacionalização e implementação do sistema de software, conforme as orientações estabelecidas na lei vigente.

Para demonstrar o detalhamento na concepção do padrão de privacidade, a seção 5.2 apresenta de forma detalhada como os modelos de padrões de privacidade foram elaborados, os padrões de requisitos de privacidade têm o objetivo de alinhar os requisitos de privacidade com a Lei Geral de Proteção de Dados, conforme ilustrado na Figura 12.

Considerando a relevância em operacionalizar a interpretação da Lei Geral de Proteção de Dados, identificamos nos relatos dos entrevistados a necessidade de formalizar a operacionalização da interpretação da lei em um fluxo de atividades, que servirá de apoio para a especificação dos requisitos de privacidade e possibilitar a implementação de um sistema de software de maneira ágil e em conformidade com a legislações vigente.

Para garantir essa operacionalização da interpretação da LGPD nas atividades de desenvolvimento, correção e melhoria de software, o analista deverá conduzir o processo de conformidade em observância dos controles sobre os requisitos legais seguindo um conjunto de etapas. Primeiro, é necessário realizar um diagnóstico inicial da gestão dos dados, uma análise das lacunas de privacidade conforme a lei estabelece e um plano para especificar os requisitos de privacidade. Para demonstrar o detalhamento desse processo de conformidade, propomos o G-Priv para apoiar o processo de conformidade na especificação de requisitos de privacidade à LGPD, que visa obter esse diagnóstico dos dados pessoais tratados na especificação dos requisitos de privacidade.

5.2 CATÁLOGO DE PADRÕES DE REQUISITOS DE PRIVACIDADE

O catálogo de privacidade serve para alinhar os objetivos de privacidade aos princípios da LGPD. Ele é usado como orientação para reutilização dos controles de privacidade. Ele pode ser utilizado como base de conhecimento, tendo seus controles de privacidade sido construídos a partir da NBR ISO 27701, a fim de minimizar os riscos envolvidos com questões de privacidade durante a especificação dos requisitos de software.

Nessa pesquisa, apresentaremos um catálogo de requisitos de privacidade, sempre com o objetivo de operacionalizar e facilitar a conformidade e a reutilização do conhecimento adquirido durante a especificação de requisitos. Embora os controles de privacidade listados no catálogo forneçam um conjunto de mecanismos úteis, conforme especificado na extensão da norma brasileira de requisitos e diretrizes de privacidade, eles não são a única maneira de satisfazer o requisito de privacidade.

Para a elaboração desse catálogo, seguimos o seguinte processo: primeiro, extraímos os conceitos de privacidade na literatura (PEIXOTO ET AL., 2020), (GHARIB ET AL., 2020), (CYSNEIROS e YU, 2004) e a norma técnica da NBR ISO/IEC 27701:2018. Em seguida, criamos categorias correlatas, como por exemplo, agrupamos tudo que trata sobre o conceito de armazenamento de dados pessoais. Por fim, criamos a relação das

categorias conceituais de privacidade com os contextos, as diretrizes e as referências legais.

Os padrões de privacidade propostos nessa seção têm o objetivo de servir como modelo de referência para auxiliar o preenchimento do *template*, conforme exemplificado na atividade III da seção 5.3 e ilustrado no Apêndice F, os exemplos tratam das instanciações de padrões de requisitos de um sistema real em funcionamento no órgão público do poder judiciário de Pernambuco.

As Tabelas 5, 6, 7, 8 e 9 apresentam os catálogos de privacidade detalhados, conforme a seguir: **conceito de privacidade**, que são tipos de privacidade e seus respectivos objetivos; **contexto**, que exemplifica uma situação em que se enquadra o conceito de privacidade; **diretrizes**, as quais têm o objetivo de direcionar a melhor estratégia para atingir os requisitos de privacidade; e as **referências**, que servem para fundamentar cada elemento de privacidade conforme o regimento da lei e da norma.

A Tabela 4 faz referência ao catálogo de padrão de privacidade de acesso à informação, extraído da Norma Técnica 27701, esse catálogo tem o objetivo de contemplar os princípios da necessidade, finalidade, adequação, livre acesso, qualidade dos dados, transparência, responsabilização e prestação de contas, conforme apresentados na seção 2.3.2 da LGPD. A organização deve limitar o acesso à informação e aos recursos de processamento de dados.

Tabela 4 - Padrão de Privacidade – Acesso à Informação.

Conceito de Privacidade	**Objetivo**
Acesso	Limitar o acesso à informação e aos recursos de processamento da informação.
Contexto	REGISTRO E CANCELAMENTO DE USUÁRIO
Diretrizes	Procedimentos para registro e cancelamento de usuários que administrem ou operem sistemas e serviços, que tratam dados pessoais considerados em situação que o controle de acesso do usuário para aqueles usuários esteja comprometido, como a corrupção ou o comprometimento de senhas ou outros registros de dados de usuários (por exemplo, como um resultado de uma divulgação inadvertida). Convém que a organização não reemita aos usuários qualquer *login* expirado ou desativado dos sistemas e serviços que tratam dados pessoais.
Referências	NBR ISO/IEC 27701 6.6.2.1; Lei 13.709 – LGPD Art. 38º
Contexto	PROVISIONAMENTO PARA ACESSO DE USUÁRIO
Diretrizes	A organização deve manter um registro preciso e atualizado dos perfis dos usuários criados para os usuários que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos. Este perfil compreende um conjunto de dados sobre aquele usuário, incluindo o ID de usuário, necessário para implementar os controles técnicos identificados que fornecem acesso autorizado. A implementação dos ID individuais de acesso do

	usuário permite que sistemas configurados identifiquem adequadamente que acessou os dados pessoais e quais acréscimos, exclusões ou mudanças eles fizeram. Da mesma forma que a organização é protegida, os usuários são também protegidos, uma vez que eles podem identificar o que foi tratado e o que não foi tratado.
Referências	NBR ISO/IEC 27701 6.6.2.2; Lei 13.709 – LGPD Art. 46º e 49º
Contexto	PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA *(LOG-ON)*
Diretrizes	Convém que uma técnica de autenticação adequada seja escolhida para validar a identificação alegada de um usuário. A requerida verificação de identidade e uma forte autenticação, convém que métodos alternativos de autenticação para as senhas, como meios criptográficos, *smart cards, tokens* ou biometria, sejam usados. As senhas representam uma forma comum de prover identificação e autenticação com base no segredo de que somente o usuário é quem conhece, isto também pode ser obtido com protocolos criptográficos, então convém que a complexidade de autenticação do usuário seja apropriada para a classificação da informação a ser acessada.
Referências	NBR ISO/IEC 27701 6.6.4.2; Lei 13.709 – LGPD Art. 46º e 49º
Contexto	ACESSO, CORREÇÃO E/OU EXCLUSÃO
Diretrizes	Convém que a organização implemente políticas, procedimentos e/ou mecanismos para permitir aos titulares de dados pessoais obtenham acesso para corrigir e excluir os seus dados pessoais, quando solicitado e sem atraso indevido. Convém que a organização defina um tempo de resposta e que a solicitação seja tratada de acordo com isto. Quaisquer correções ou exclusões sejam disseminadas por todo o sistema e/ou para os usuários autorizados, e convém que sejam passadas para terceiros, para os quais o dado pessoal foi transferido. Convém que a organização implemente políticas, procedimentos e/ou mecanismos para uso quando puder existir uma disputa sobre a precisão ou correção do dado pelo titular de dados pessoais. Estas políticas, procedimentos e/ou mecanismos incluam informação do titular sobre quais as mudanças foram feitas, e as razões por que as correções não foram realizadas (quando este for o caso).
Referências	NBR ISO/IEC 27701 7.3.6; Lei 13.709 – LGPD Art. 9º

Fonte: O autor (2022).

A Tabela 5 apresenta o padrão de privacidade sobre coleta de dados pessoais, extraído da Norma Técnica 27701, esse catálogo tem o objetivo de contemplar os princípios da necessidade, finalidade, adequação, livre acesso, qualidade dos dados, transparência, responsabilização e prestação de contas, conforme apresentados na seção 2.3.2 da LGPD. A organização deve limitar a coleta de dados pessoais a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.

Tabela 5 - Padrão de Privacidade – Coleta de Dados Pessoais.

Conceito de Privacidade	**Objetivo**
Coleta de Dados Pessoais	A organização deve limitar a coleta de dados pessoais a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.
Contexto	DETERMINANDO QUANDO E COMO O CONSENTIMENTO DEVE SER OBTIDO
Diretrizes	Pode ser necessário o consentimento para o tratamento de dado pessoal, a menos que outros motivos legais se apliquem. A organização deve documentar claramente a necessidade de obtenção de consentimento e os requisitos para obter o consentimento. Pode ser útil correlacionar os propósitos para tratamento com as informações sobre se e como o consentimento é obtido.
Referências	NBR ISO/IEC 27701 7.2.3; Lei 13.709 – LGPD Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14º
Contexto	OBTENDO E REGISTRANDO O CONSENTIMENTO
Diretrizes	Convém que a organização obtenha e registre os consentimentos dos titulares de dados pessoais de forma que ela possa fornecer, sob solicitação, detalhes do consentimento fornecido (por exemplo, o tempo em que o consentimento foi fornecido, a identificação do titular de dados pessoal e a declaração de consentimento). O consentimento deve ser dado livremente, específico quanto ao propósito para o tratamento, e explícito.
Referências	NBR ISO/IEC 27701 7.2.4; Lei 13.709 – LGPD Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14º
Contexto	LIMITE DE COLETA
Diretrizes	Convém que a organização limite a coleta de dado pessoal para o que é adequado, relevante e necessário na relação para os propósitos identificados. Isto inclui limitar a quantidade de dado pessoal que a organização coleta indiretamente (por exemplo, por meio de logs da web, logs de sistemas etc).
Referências	NBR ISO/IEC 27701 7.4.1; Lei 13.709 – LGPD Art. 16º

Fonte: O autor (2022).

A Tabela 6 apresenta o padrão de privacidade sobre armazenamento de dados pessoais, extraído da Norma Técnica 27701, esse catálogo tem o objetivo de contemplar os princípios da necessidade, finalidade, adequação, livre acesso, qualidade dos dados, transparência, responsabilização e prestação de contas, conforme apresentados na seção 2.3.2 da LGPD. A organização deve determinar os elementos técnicos e procedimentais necessários para armazenar os dados pessoais tratados.

Tabela 6 - Padrão de Privacidade – Armazenamento.

Conceito de Privacidade	**Objetivo**
Armazenamento	A organização deve determinar os elementos que são necessários para armazenar os dados pessoais tratados.
Contexto	RETENÇÃO
Diretrizes	A organização deve desenvolver e manter esquemas de retenção para as informações que ela guarda, considerando o requisito para retenção de dados pessoais por um tempo não maior do que é necessário. Convém que estes esquemas considerem requisitos legais, regulamentares e de negócio. Onde ocorrem conflitos com estes requisitos, uma decisão de negócio precisa ser tomada (com base em uma avaliação de riscos) e documentada no esquema apropriado.
Referências	NBR ISO/IEC 27701 7.4.7; Lei 13.709 – LGPD Art. 16º
Contexto	DESCARTE
Diretrizes	A escolha das técnicas de descarte do DP depende de um número de fatores, uma vez que uma técnica de descarte difere nas suas propriedades e resultado (por exemplo, na granularidade da mídia física resultante, ou a capacidade para recuperar uma informação excluída de uma mídia eletrônica). Fatores a considerar ao escolher uma técnica de descarte apropriada incluem, porém não estão limitados a natureza e a abrangência do DP a ser descartado, se existe ou não um metadado associado ao DP, e as características físicas da mídia na qual o DP é armazenado.
Referências	NBR ISO/IEC 27701 7.4.8; Lei 13.709 – LGPD CAPÍTULO VII
Contexto	ARQUIVOS TEMPORÁRIOS
Diretrizes	Convém que a organização realize verificações periódicas de modo que arquivos temporários não usados sejam excluídos dentro de um período de tempo identificado. Sistemas de informação podem criar arquivos temporários no curso normal de suas operações. Estes arquivos são específicos para um sistema ou para aplicação, porém podem incluir sistemas de arquivos de reversão (rollback journals) e arquivos temporários associados à atualização das bases de dados e à operação de outras aplicações de software. Arquivos temporários não são necessários após a tarefa de tratamento da informação relacionada ter sido completada, porém existem circunstâncias nas quais não é possível que eles sejam excluídos. A extensão do tempo para o qual estes arquivos permanecem em uso não é sempre determinada, porém convém que um procedimento de liberação de espaço ocioso (garbarge collection) identifique os arquivos relevantes e determine por quanto tempo ele existe desde a última vez que foi usado.
Referências	NBR ISO/IEC 27701 7.4.6; Lei 13.709 – LGPD CAPÍTULO VII

Fonte: O autor (2022).

A Tabela 7 apresenta o padrão de privacidade sobre compartilhamento de dados pessoais, extraído da Norma Técnica 27701, esse catálogo tem o objetivo de contemplar os princípios da necessidade, finalidade, adequação, livre acesso, qualidade dos dados, transparência, responsabilização e prestação de contas, conforme apresentados na seção 2.3.2 da LGPD. A organização deve determinar os elementos técnicos e procedimentais necessários para compartilhamento dos dados pessoais tratados.

Tabela 7 - Padrão de Privacidade – Compartilhamento.

Conceito de Privacidade	**Objetivo**
Compartilhamento	A organização deve determinar os elementos que são necessários para o compartilhamento dos dados pessoais tratados.
Contexto	POLÍTICAS E PROCEDIMENTOS PARA TRANSFERÊNCIA DE INFORMAÇÕES
Diretrizes	Convém que a organização considere procedimentos para assegurar que regras relativas ao tratamento de DP são mandatórias por todo o sistema e fora dele, onde aplicável.
Referências	NBR ISO/IEC 27701 6.10.2.1; Lei 13.709 – LGPD Art. 46º
Contexto	CONTROLE DE TRANSMISSÃO DE DADOS PESSOAIS
Diretrizes	A transmissão de dados necessita ser controlada, basicamente para assegurar que somente pessoas autorizadas tenham acesso aos sistemas de transmissão, seguindo os processos apropriados (incluindo a retenção de logs de auditoria), para assegurar que o DP seja transmitido sem comprometimento para os destinatários corretos. A transmissão de dado pessoal precisa ser controlada, tipicamente para assegurar que somente pessoas autorizadas tenham acesso a sistemas de transmissão e sigam os processos apropriados (incluindo a retenção de dados de auditoria) para assegurar que dados pessoais sejam transmitidos sem comprometimento para os destinatários corretos. Requisitos para controles de transmissão podem ser incluídos no operador de dado pessoal – contrato com o cliente. Onde não existem implementados requisitos contratuais relativos à transmissão, pode ser apropriado obter aconselhamento do cliente, antes da transmissão.
Referências	NBR ISO/IEC 27701 7.4.9, 8.4.3; Lei 13.709 – LGPD CAPÍTULO VII
Contexto	IDENTIFICANDO AS BASES PARA TRANSFERÊNCIA DE DADOS PESSOAIS ENTRE JURIDIÇÕES
Diretrizes	Uma transferência de dado pessoal pode estar sujeita a uma legislação e/ou regulamentação dependendo da jurisdição ou da organização internacional para a qual os dados estão para serem transferidos (e de onde eles se originam). Convém que a organização documente o *compliance* com estes requisitos como a base para a transferência.
Referências	NBR ISO/IEC 27701 7.2.1; Lei 13.709 – LGPD Art. 7º; Art. 6º VII, VIII, Art. 37º e Art. 46º
Contexto	REGISTRO DE TRANSFERÊNCIA DE DADOS PESSOAIS
Diretrizes	Registros podem incluir transferências de terceiros de dado pessoal que tenham sido modificados como um resultado das suas obrigações no gerenciamento dos controladores, ou na transferência para terceiros para implementar solicitações legítimas dos titulares de dados pessoais, incluindo solicitações para exclusão do dado pessoal (por exemplo, após o consentimento do cancelamento).
Referências	NBR ISO/IEC 27701 7.5.3; Lei 13.709 – LGPD CAPÍTULO V

Fonte: O autor (2022).

A Tabela 8 apresenta o padrão de privacidade sobre anonimização e criptografia de dados pessoais, extraído da Norma Técnica 27701, esse catálogo tem o objetivo de contemplar os princípios da necessidade, finalidade, adequação, livre acesso, qualidade

dos dados, transparência, responsabilização e prestação de contas, conforme apresentados na seção 2.3.2 da LGPD. A organização deve determinar os elementos técnicos e procedimentais necessários para o uso de anonimização e criptografia dos dados pessoais tratados.

Tabela 8 - Padrão de Privacidade – Anonimização e Criptografia.

Conceito de Privacidade	**Objetivo**
Anonimização e Criptografia	A organização deve determinar os elementos que são necessários para o tratamento dos dados pessoais com uso de anonimização e criptografia.
Contexto	ANONIMIZAÇÃO E EXCLUSÃO DE DADO PESSOAL AO FINAL DO TRATAMENTO
Diretrizes	Convém que a organização tenha mecanismos para excluir o dado pessoal quando nenhum tratamento adicional for antecipado. Alternativamente, algumas técnicas de anonimização podem ser usadas uma vez que os resultados dos dados anonimizados não podem permitir, de forma razoável, a reidentificação dos titulares de dados pessoais.
Referências	NBR ISO/IEC 27701 7.4.5; Lei 13.709 – LGPD Art. 16º
Contexto	POLÍTICAS PARA O USO DE CONTROLES CRIPTOGRÁFICOS
Diretrizes	Convém que a organização forneça informações para o cliente em relação às circunstâncias em que ela usa a criptografia para proteger os dados pessoais que ela trata. E que a organização também forneça informações para o cliente sobre quaisquer capacidades que ela fornece, que possam atender ao cliente, aplicando sua própria proteção de criptografia.
Referências	NBR ISO/IEC 27701 6.7.1.1; Lei 13.709 – LGPD Art. 46º

Fonte: O autor (2022).

5.3 G-PRIV: GUIA PARA APOIAR A CONFORMIDADE NA ESPECIFICAÇÃO DE REQUISITOS DE PRIVACIDADE COM A LGPD

Com o objetivo de fazer um diagnóstico dos dados utilizados nos sistemas de software, para apoiar a especificação dos requisitos de privacidade com a LGPD, propomos um guia de privacidade. Esse guia auxiliará os analistas de requisitos, logo após a fase de elicitação dos requisitos no processo de software, quando há o entendimento do negócio, entendimento das necessidades dos *stakeholders*, entendimento do problema e suas possíveis limitações.

Nesse contexto de entendimento, os analistas de requisitos despertam para a necessidade de alinhar as regras de negócio com os requisitos de privacidade impostos pela LGPD. Diante disso, o nosso guia tem a proposta de direcionar, de maneira prática, a especificação dos requisitos de privacidade em conformidade com a LGPD.

O nosso guia foi inspirado no *GuideMe*, abordagem proposta por Ayala-Rivera e Pasquale (2018), que é uma abordagem sistemática, dividida em etapas, com o objetivo de apoiar a especificação de requisitos de privacidade em conformidade com a GDPR (*General Data Protection Regulation*). Na nossa pesquisa, adaptamos o *GuideMe* para o contexto da Lei de nº 13.709/2018, a Lei Geral de Proteção de Dados, vigente no Brasil.

O Art. 46, § 2º, do mencionado diploma legal, cita que as medidas de segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço, seguindo até a sua execução. Essa disposição legal se apresenta como um conceito fundamental para a proteção da privacidade dos dados pessoais, denominado **Privacidade desde a Concepção** (do inglês *Privacy by Design*).

A abordagem proposta está embasada na construção de uma perspectiva de conformidade com a LGPD, que se consolida com a elaboração de um Padrão de Privacidade. A partir desse padrão de privacidade, o analista de requisitos poderá assegurar a conformidade legal dos sistemas de TI, que contenham o tratamento de dados pessoais de acordo com os princípios da LGPD. Vale salientar que a checagem de conformidade é realizada de forma manual pelo analista de requisitos.

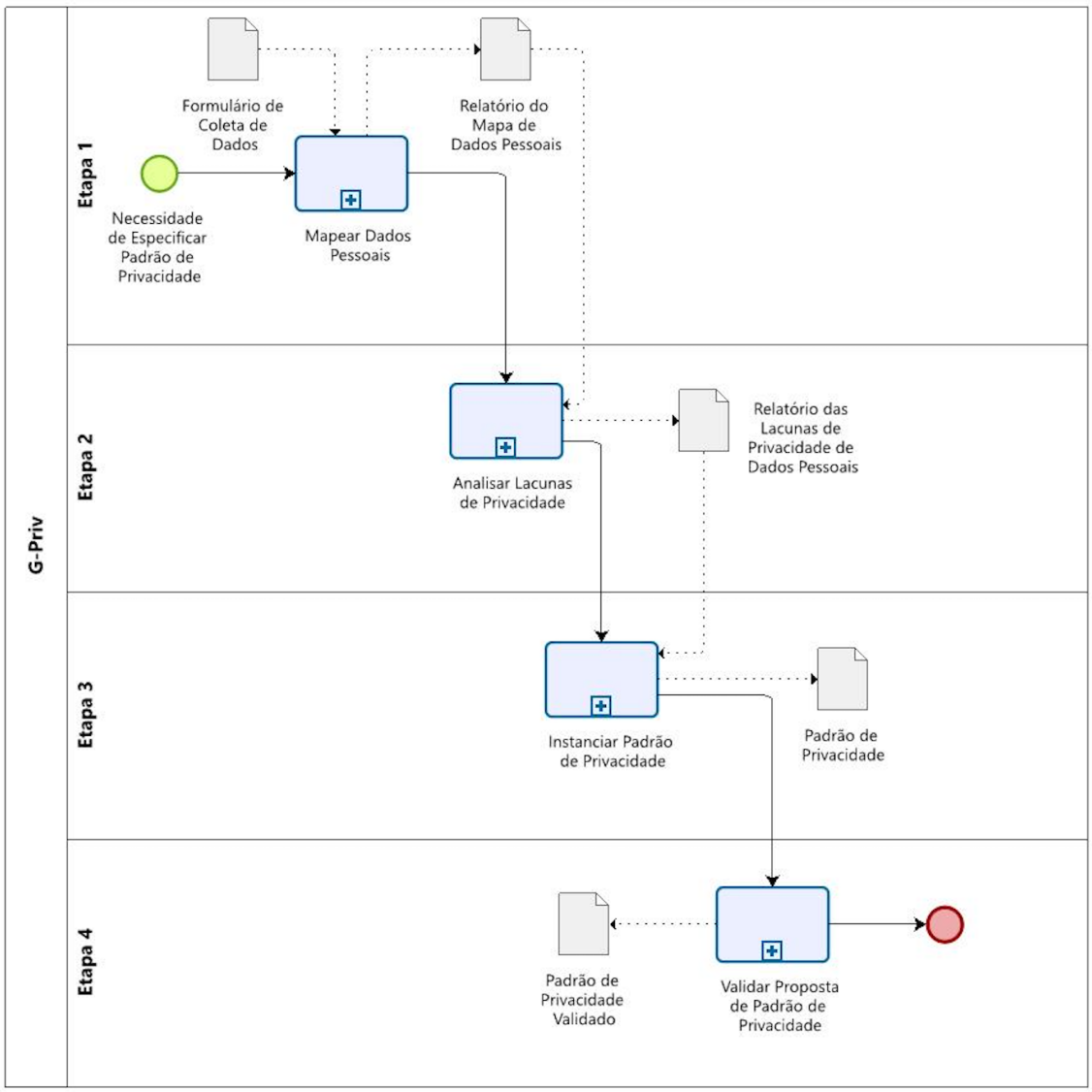
O guia para apoiar a conformidade na especificação de requisitos de privacidade com à LGPD, nomeamos, sinteticamente, de G-Priv. Ele é um guia composto por um fluxo de quatro etapas:

1. Mapear dados pessoais;
2. Analisar lacunas de privacidade;
3. Instanciar padrão de privacidade;
4. Validar proposta de padrão de privacidade;

O guia proposto foi modelado como um fluxo de etapas, a fim de orientar a especificação dos requisitos de privacidade e garantir que os sistemas de software estejam em conformidade com a Lei Geral de Proteção de Dados.

Com o guia G-Priv, as etapas geram diferentes artefatos que servirão de entradas e saídas de uma etapa para outra e, por fim, resultarão no padrão de privacidade para especificar os requisitos de privacidade. O fluxo dessas etapas é apresentado de forma geral na Figura 14.

Figura 14 - Visão geral do G-Priv.



Fonte: O autor (2022).

O guia G-priv está envolvido num escopo do processo de desenvolvimento de software: a especificação dos requisitos. Esse é o momento de modelar e documentar os requisitos de forma que todos os *stakeholders* do sistema tenham um entendimento compartilhado sobre os requisitos para o sistema de software. Nessa fase, geralmente, são utilizadas linguagens escritas e gráficas de melhor entendimento.

Esse guia disponibiliza artefatos que poderão ser utilizados pelas organizações, são eles: formulário de coleta de dados; relatório do mapa de dados pessoais; relatório das lacunas de privacidade; proposta de padrão de privacidade, padrão de privacidade, conforme descrito na Tabela 9. Esses artefatos estão disponíveis no Apêndice C.

Tabela 9 - Etapas, artefatos e objetivos.

Etapa	Artefato	Objetivo
Etapa 1: Mapear dados pessoais	Formulário de coleta de dados.	Com esse formulário, é possível mapear e ter um diagnóstico dos dados pessoais tratados no requisito de privacidade.
	Relatório do mapa de dados pessoais.	Este artefato tem o objetivo de obter um diagnóstico dos dados pessoais no contexto do sistema de software.
Etapa 2: Analisar lacunas de privacidade	Formulário de análise de lacunas de privacidade.	O preenchimento do formulário de análise de lacunas de privacidade, especialistas das áreas jurídicas e de privacidade analisam o resultado das respostas, emitem um relatório contendo um diagnóstico, apresentando os princípios que não estão em conformidade legal no contexto do sistema.
	Relatório das lacunas de privacidade.	O artefato contém as possíveis lacunas de privacidade dos dados pessoais envolvidos no contexto do sistema.
Etapa 3: Instanciar padrão de privacidade	Proposta de Padrão de Privacidade.	Propor padrão de privacidade conforme as

		lacunas de privacidade encontradas.
Etapa 4: Validar o plano proposto no padrão de privacidade	Padrão de Privacidade.	Validar o padrão de privacidade elaborado pelo analista de requisito.

Fonte: O autor (2021).

A Tabela 10 apresenta os atores e suas respectivas responsabilidades definidos no guia G-Priv, a fim de garantir uma definição clara das responsabilidades dos atores envolvidos no contexto desse guia.

Tabela 10 - Atores e responsabilidades.

Ator	**Responsabilidades**
Stakeholder	Responsável por solicitar o novo sistema de software, melhorias e/ou correção de erros nos sistemas de software já implantados.
Analista de requisitos	Responsável pelo levantamento de requisitos e especificações de projetos de TI, desenvolvendo soluções para processos, mapeamento e análise de negócio; Elabora a documentação técnica de especificação de requisitos de software e um relatório de acompanhamento para gestão de projetos.
Comitê gestor de privacidade de dados	Grupo responsável por garantir a conformidade legal de privacidade de dados nos sistemas de software; Identifica, analisa e define ações para os principais riscos, que possam impactar na conformidade legal durante a especificação dos requisitos para o desenvolvimento de software; Disponibiliza os artefatos utilizados no guia, como também faz a sua validação; Garante que a comunicação seja realizada adequadamente durante o processo de conformidade;

	Decide sobre a implementação ou rejeição dos requisitos de privacidade propostos pelos analistas de requisitos; Disponibiliza documentação que servirá para fins de capacitação e conscientização sobre privacidade de dados e conformidade com a LGPD.
Especialista jurídico	Responsável por acompanhar e dar suporte de conformidade à Lei Geral de Proteção de Dados e outras leis vigentes que podem interferir na privacidade dos dados.
Analista em privacidade de dados	Responsável por participar ativamente da adequação à LGPD na organização; Responsável por organizar dados e gerar relatórios para subsidiar processos de tomadas de decisão; Ajuda na organização e monitoramento de projetos ligados à segurança da informação e privacidade de dados; Atua no planejamento, execução, acompanhamento e controle de todas as atividades inerentes à privacidade e proteção de dados pessoais.
Equipe de desenvolvimento de software	Responsável por implementar os requisitos de privacidade nos sistemas de software da organização.

Fonte: Fonte: O autor (2021).

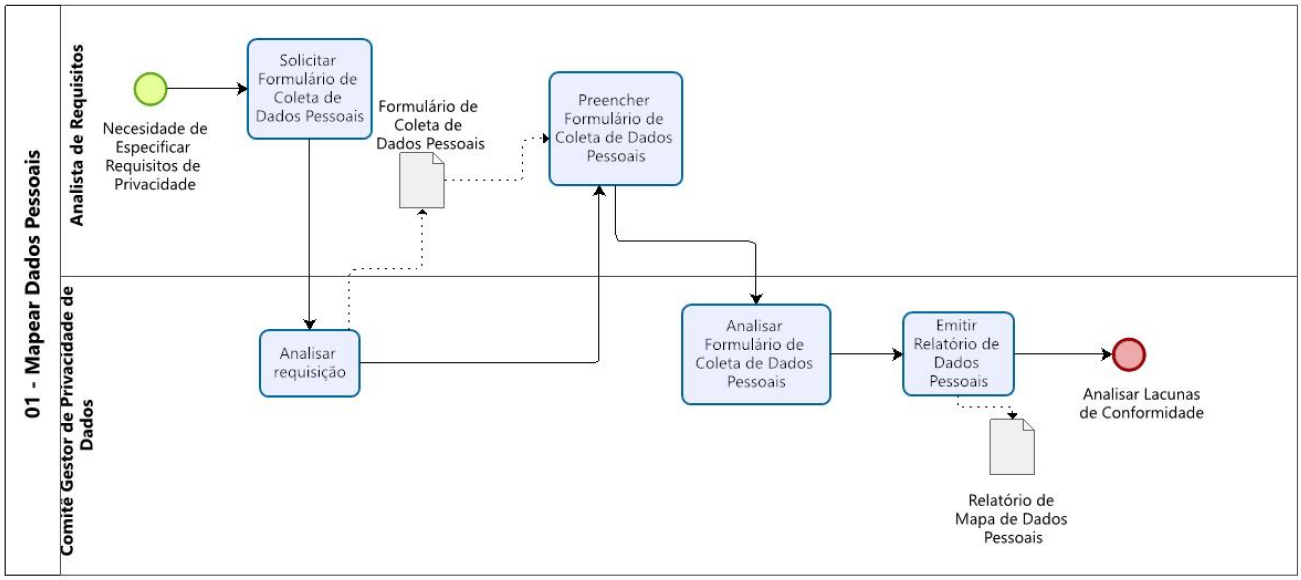
5.3.1 Etapa 1: Mapear Dados Pessoais

A primeira etapa do guia consiste no mapeamento dos dados pessoais no contexto do sistema de software que será desenvolvido. Essa etapa tem como objetivo elaborar um relatório de análise de dados, que se consolida com um diagnóstico dos dados pessoais tratados no sistema de software, possibilitando, assim, a demonstração dos tipos de dados e o nível de exposição aos riscos de não conformidade com a LGPD.

A proposta da primeira etapa é mapear os dados pessoais, identificando sua origem (quais dados são coletados? como são coletados? onde são armazenados?), a retenção (como são armazenados?), as credenciais (quem tem acesso? quais são os perfis?), e as saídas (esses dados são processados? esses dados são compartilhados?).

Para a execução dessa etapa, devem-se envolver atores com perfis de especialista em privacidade de dados (que pode ser figurado no analista em segurança da informação), especialista de TI (que pode ser o analista de requisitos) e os *stakeholders* do sistema de software. Além disso, é necessário elaborar um formulário de coleta, a fim de levantar informações para obter um diagnóstico inicial sobre o ciclo de vida dos dados no contexto do sistema e possibilitar uma visão abrangente do cenário e dos riscos que irão influenciar o processo de especificação dos requisitos de privacidade. A Figura 15 apresenta o detalhamento da etapa de "Mapear Dados Pessoais".

Figura 15 - Etapa 1: Mapear Dados Pessoais.



Fonte: O autor (2021).

A Tabela 11 apresenta o objetivo, as entradas e saídas da primeira etapa do G-Priv.

Tabela 11 - Etapa 1: Mapear Dados Pessoais.

Objetivo da Etapa 1	**Solicitar formulário de dados, analisar formulário de dados, preencher formulário de dados e emitir relatório de mapa de dados pessoais.**
Entradas	Documento de requisitos elicitados, Formulário de coleta de dados pessoais.
Saídas	Relatório do mapa de dados pessoais.

Fonte: O autor (2021).

Descrição das atividades da Etapa 1- Mapear Dados Pessoais

I. **Solicitar formulário de coleta de dados pessoais**: Toda especificação de requisitos de software deve ser solicitada para iniciar o processo de conformidade dos requisitos de privacidade à LGPD.

   a. O mapeamento dos dados pessoais pode ser registrado com o auxílio do *template* de formulário de mapeamento dos dados pessoais, fornecido pelo comitê gestor de privacidade de dados, disponibilizado no Apêndice C. Os elementos do formulário de mapeamento de dados pessoais devem ser preenchidos de acordo com a necessidade especificada nos requisitos de privacidade do sistema de software. Nesse formulário, é possível mapear e ter um diagnóstico dos dados pessoais tratados naquele requisito de privacidade, tais como: identificando suas origens, credenciais, retenção, saídas e descartes;

   b. A necessidade de especificar os requisitos de privacidade surge a partir da demanda das organizações para atender a conformidade legal de privacidade estabelecida no Brasil. E para aderir à conformidade da LGPD, é necessário se ter pleno conhecimento de como os dados pessoais são processados;

II. **Avaliar requisição de formulário de mapeamento de dados pessoais**: Nessa atividade, é realizada a análise da requisição do formulário de mapeamento de dados pessoais.

   a. O analista de privacidade de dados, em conjunto com o especialista de TI, analisa e verifica se a demanda é fidedigna. Se as pessoas que compõem o comitê gestor observarem alguma incoerência, essa solicitação será indeferida;

   b. O analista de privacidade identifica a possibilidade de efetuar o mapeamento dos dados pessoais naquele contexto do sistema de software e encaminha o *template* do formulário de mapeamento de dados pessoais para o analista de requisitos que solicitou o mapeamento;

III. **Preencher formulário de dados pessoais**: Nessa atividade, o analista de requisitos que solicitou o mapeamento dos dados pessoais deve preencher o formulário.

a. O analista de requisitos que solicitou o mapeamento dos dados pessoais deve preencher o formulário juntamente com o *stakeholder* ou setor demandante do sistema de software;
b. Após o preenchimento do formulário de mapeamento dos dados pessoais, o documento é encaminhado para o comitê gestor de privacidade de dados;

IV. **Analisar o formulário de dados pessoais**: Nessa atividade, o comitê gestor de privacidade de dados confere o preenchimento do formulário.
   a. O comitê gestor avalia o preenchimento do formulário com base nos critérios técnicos da descrição da atividade especificada. Como por exemplo, os dados pessoais utilizados no requisito para cadastro de usuário no sistema;
   b. O comitê gestor pode validar o formulário informando ao analista de requisitos que o formulário seguirá para emissão do relatório de mapeamento dos dados pessoais, caso contrário ele será refeito pelo analista de requisitos;

V. **Emitir relatório de dados pessoais**: O comitê gestor emitirá um relatório do mapeamento dos dados pessoais.
   a. O comitê gestor emitirá um relatório do mapeamento dos dados pessoais com o objetivo de obter um diagnóstico dos dados pessoais no contexto do sistema de software;
   b. O relatório de mapeamento dos dados pessoais servirá de entrada para avaliar as lacunas de conformidade legal;
   c. O analista de requisitos que solicitou o mapeamento dos dados pessoais aguardará o artefato com a proposta de possíveis soluções para atender os requisitos de privacidade.

Ao final dessa etapa, o comitê gestor de privacidade será capaz de emitir um relatório contendo um diagnóstico dos dados pessoais envolvidos no contexto do sistema, podendo seguir para a próxima etapa do guia que é a de analisar as lacunas de privacidade de dados existentes.

5.3.2 Etapa 2: Analisar Lacunas de Privacidade

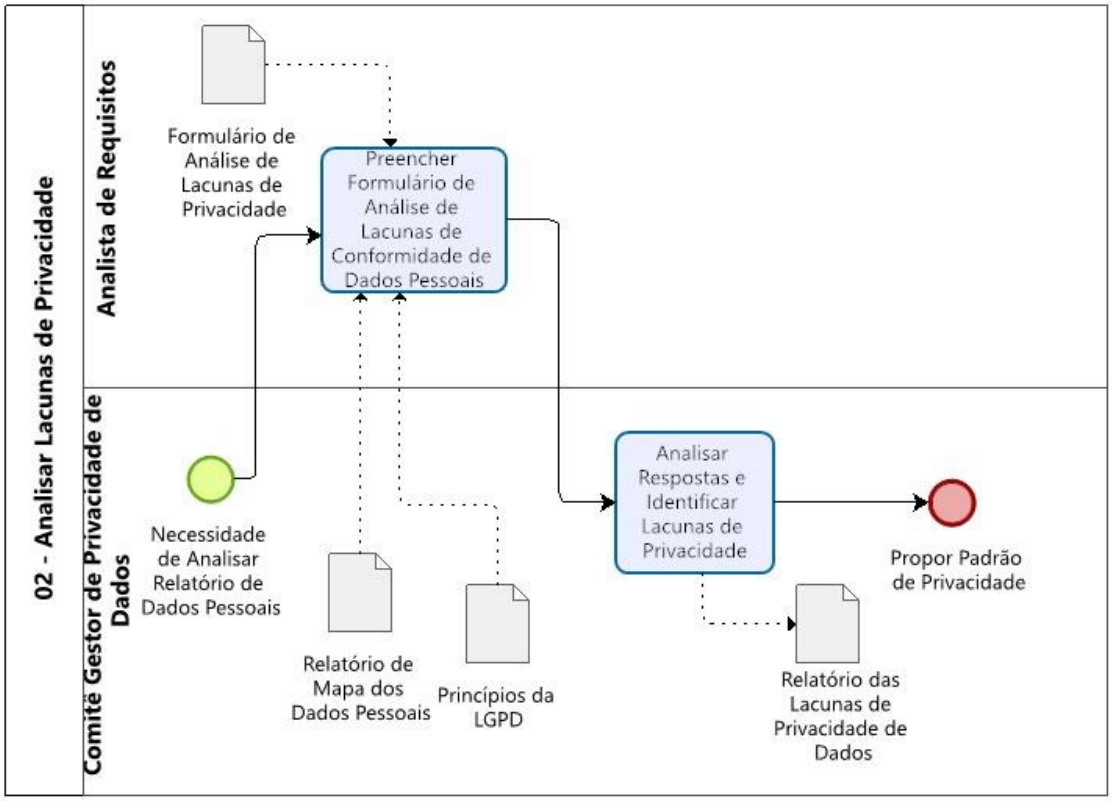
Após o mapeamento dos dados pessoais, a segunda etapa do guia tem o objetivo de auxiliar na análise e identificação dos *gaps*, que são lacunas que precisam ser preenchidas

com soluções, objetivando as correções, melhorias e novas implementações que contemplem o desenvolvimento de software, em conformidade com a base legal de privacidade de dados, atendendo as especificações expostas nos Arts. 6º e 7º da LGPD (Definição dos princípios e a base legal).

Nessa etapa, é produzido um relatório contendo descobertas, recomendações e cenários onde as medidas de privacidade de dados pessoais serão aplicadas para garantir a conformidade legal. Para contribuir com a execução dessa etapa, deve-se contar com a participação dos seguintes atores: analista de requisitos, especialista em privacidade de dados e especialista jurídico. O analista de requisitos deverá responder a um pequeno formulário, que permitirá identificar as lacunas de possíveis violações dos princípios da LGPD, que está disponibilizado no Apêndice D. As questões do formulário de lacunas de privacidade disponibilizado no Apêndice D foi inspirado nas questões da LGPD4BP dos autores Araújo et al. (2021).

Finalizado o preenchimento do formulário de análise de lacunas de privacidade dos dados, especialistas das áreas jurídicas e de privacidade analisam o resultado das respostas, emitem um relatório contendo um diagnóstico, apresentando os princípios da LGPD que não estão em conformidade legal no contexto do sistema. Nesse diagnóstico, a partir das questões que foram respondidas de maneira negativa, sendo, assim, possível apontar as lacunas existentes para a próxima etapa. A Figura 16 apresenta o detalhamento da etapa 2: “Analisar lacunas de privacidade”.

Figura 16 - Etapa 2: Analisar Lacunas de Privacidade.



Fonte: O autor (2021).

A Tabela 12 apresenta o objetivo, as entradas e saídas da segunda etapa do G-Priv.

Tabela 12 - Etapa 2: Analisar Lacunas de Privacidade.

Objetivo da etapa 2	**Solicitar formulário para identificar as lacunas de privacidade, analisar respostas e identificar lacunas de privacidade e emitir relatório das lacunas de privacidade dos dados pessoais.**
Entradas	Relatório de mapa dos dados pessoais.
Saídas	Relatório das lacunas de privacidade de dados.

Fonte: O autor (2021).

Descrição das atividades da Etapa 2 – Analisar Lacunas de Privacidade

I. **Preencher formulário das lacunas de privacidade de dados:** Nessa atividade, o analista de requisitos deverá responder a um pequeno formulário, sob a supervisão do comitê gestor de privacidade de dados, que assim permitirá identificar as lacunas de possíveis violações dos princípios da LGPD.

a. O formulário para identificar as lacunas de privacidade de dados pode ser registrado com o auxílio do *template* de formulário de lacuna de privacidade dos dados pessoais, fornecido pelo comitê gestor de privacidade de dados, disponibilizado no Apêndice D. Os elementos desse formulário devem ser preenchidos com base no relatório de mapeamento dos dados pessoais, como também de acordo com a necessidade especificada nos requisitos de privacidade do sistema de software, e com base na experiência do comitê gestor em relação ao sistema, será possível identificar as violações dos princípios de privacidade;
b. Nesse formulário, é possível analisar e identificar as lacunas de privacidade de dados pessoais tratados no requisito de software, tais como, por exemplo: na especificação de requisitos referentes ao cadastro de usuários do sistema, os princípios da finalidade e a necessidade não foram atendidos, com isso chega-se à conclusão de identificar as lacunas nesses princípios da LGPD;

II. **Analisar respostas e identificar lacunas de privacidade no formulário de análise de lacunas**: Nessa atividade, são realizadas a análise e a identificação das lacunas de privacidade de dados.
   a. O analista de privacidade e o especialista jurídico analisam e verificam a conformidade e completude das informações contidas no formulário;
   b. O analista de privacidade e o especialista jurídico identificam as possíveis lacunas de privacidade;
   c. Após a análise e identificação das lacunas de privacidade, o comitê gestor encaminha o relatório com as lacunas de privacidade para a etapa seguinte.

Ao final dessa etapa, o comitê gestor de privacidade será capaz de emitir um relatório contendo as possíveis lacunas de privacidade dos dados pessoais envolvidos no contexto do sistema, sendo, assim, seguir para a próxima etapa do guia que é a de instanciar o padrão de privacidade para sanar as lacunas de privacidade de dados existentes.

5.3.3 Etapa 3: Instanciar Padrão de Privacidade

A terceira etapa, que contempla a atividade de instanciar o padrão de privacidade, utiliza-se dos artefatos gerados nas etapas anteriores, que são: relatório de mapa de dados pessoais e relatório de lacunas de privacidade de dados.

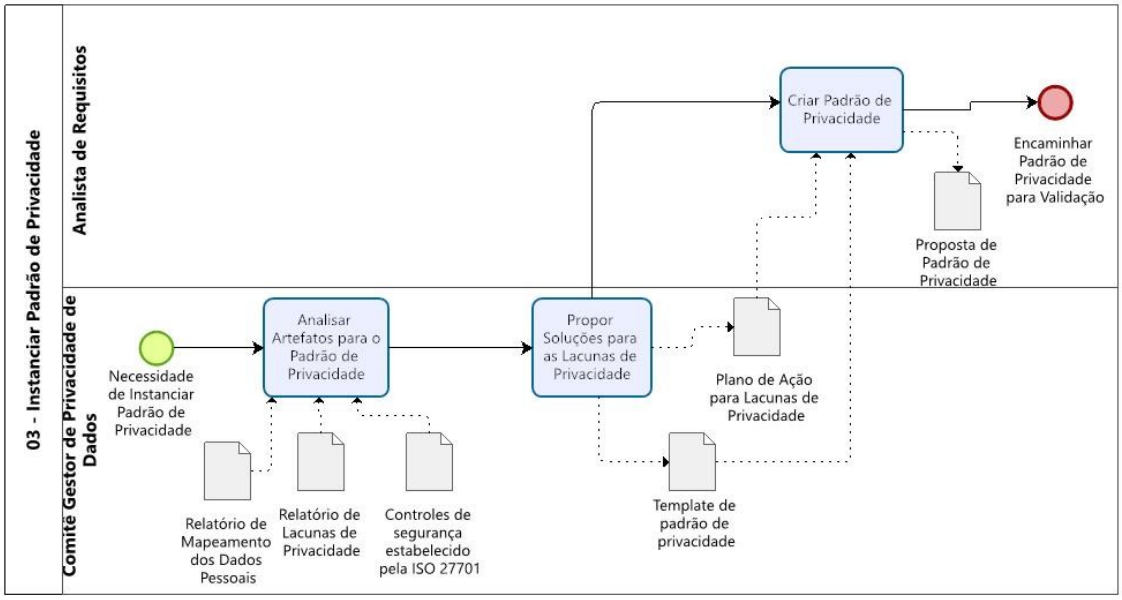
Nessa etapa, é produzida uma proposta de padrão de privacidade contendo descobertas, recomendações, soluções para as lacunas de privacidade de dados no contexto dos sistemas de software, de forma que essas medidas sejam aplicadas para garantir a conformidade legal. Aqui, podemos ter uma solução tecnológica para atingir os objetivos de privacidade, como, por exemplo, uso de anonimização, controle de acesso, políticas de privacidade, tipos de armazenamento etc.

Para identificar as lacunas e direcionar uma solução, utilizamos como fonte de inspiração o catálogo de controles sugeridos pela Norma ISO 27701. Essa norma contém os controles de privacidade mapeados pelos artigos da LGPD e suas respectivas diretrizes orientadoras para a conformidade legal. Os exemplos desses controles estão apresentados na segunda parte do *template* do Apêndice E do catálogo de controles de privacidade, que é o documento que contém os controles identificados a partir das lacunas, as suas diretrizes e os artigos da lei que os fundamentam.

O catálogo será utilizado como orientação para reutilização e base de conhecimento, para relacionar os objetivos de privacidade aos artigos e princípios da LGPD, auxiliando, dessa forma, de maneira ágil os analistas de requisitos durante a atividade de especificar os requisitos de privacidade.

Para exemplificar essa etapa, utilizamos a funcionalidade de cadastro dos usuários no Sistema Nísia do TJPE que se encontra no Apêndice F, no qual os dados fornecidos para o cadastro poderão ser compartilhados com outros órgãos públicos ou particulares envolvidos na demanda. Diante do cenário exposto, os atores do comitê gestor poderão identificar as lacunas mapeadas na etapa anterior, traçar um planejamento com soluções orientado pelas diretrizes de controles esboçadas na legislação, com o objetivo de evitar, por exemplo, que dados de uma mulher, vítima de violência sob medida protetiva, sejam acessados de forma indevida por pessoas/partes que não fazem parte do processo daquele contexto judicial ou informações e sejam expostos sem a devida autorização. No Apêndice E, o catálogo de controle de privacidade apresenta os controles e as respectivas diretrizes, conforme as lacunas identificadas. A Figura 17 apresenta o detalhamento da etapa 3: “Instanciar Padrão de Privacidade”.

Figura 17 - Etapa 3:Instanciar Padrão de Privacidade.



Fonte: O autor (2021).

A Tabela 13 apresenta o objetivo, as entradas e as saídas da terceira etapa do G-Priv.

Tabela 13 - Etapa 3: Instanciar Padrão de Privacidade.

Objetivo da Etapa 3	**Instanciar um padrão de privacidade com base nas lacunas de privacidade encontradas na etapa anterior, esta proposta deve atender as diretrizes definidas no catálogo de controle da ISO 27701, com o objetivo de suprir as necessidades encontradas nas lacunas de privacidade.**
Entradas	Relatório de mapeamento dos dados pessoais, Relatório das lacunas de privacidade de dados e Controles da ISO 27701.
Saídas	Proposta de padrão de privacidade.

Fonte: O autor (2021).

Descrição das atividades da Etapa 3 – Instanciar Padrão de Privacidade

I. **Analisar Artefatos para o Padrão de Privacidade:** Nessa atividade, o comitê gestor de privacidade deve analisar e identificar fraquezas, com base nos artefatos gerados nas etapas anteriores.

   a. O comitê gestor de privacidade deve analisar os artefatos concebidos nas etapas anteriores, identificar fraquezas e propor soluções para o padrão de

privacidade, tomando como referência o relatório com as lacunas de privacidade e as diretrizes no catálogo de controle de segurança da ISO 27701;

II. **Propor Soluções para as Lacunas de Privacidade**: O comitê gestor deve propor um plano de ação para as lacunas de privacidade identificadas.
   a. O comitê gestor de privacidade emite uma proposta de plano de ação, com as possíveis soluções para as lacunas de privacidade de dados. Essas soluções para as lacunas de privacidade podem ser diretrizes com soluções tecnológicas ou procedimentais, como, por exemplo, no caso de acesso ao sistema, convém que métodos alternativos de autenticação para as senhas, como meios criptográficos, *smart cards*, *tokens* ou biometria, sejam usados, caso contrário, à luz da lei, alguns princípios da LGPD não estarão em conformidade, como o princípio da segurança, prevenção e necessidade;
   b. O *template* de padrão de privacidade e o plano de ação para as lacunas de privacidade são encaminhados para o analista de requisitos, com a finalidade de criar o padrão de requisitos de privacidade.

III. **Criar Padrão de Privacidade**: O analista de requisitos deve criar o padrão de privacidade.
   a. O padrão de privacidade pode ser registrado com o auxílio do *template* padrão de privacidade, fornecido pelo comitê gestor de privacidade, disponibilizado no Apêndice F;
   b. Os elementos do padrão de privacidade devem ser preenchidos de acordo com as descrições nas linhas das tabelas no Apêndice F. No padrão, é preciso definir o ID do requisito, as vulnerabilidades, soluções, base legal, descrição legal e consequências;
   c. Após o preenchimento dos campos, o padrão de privacidade deve ser submetido à validação pelo comitê gestor de privacidade.

A nossa proposta de padrões de privacidade foi inspirada nos trabalhos (XUAN ET AL., 2014; FRANCH ET AL., 2010; SALIN e KANMANI, 2012; PP, 2021). No Apêndice F, apresentamos exemplos de padrões de privacidade, compostos por elementos que auxiliam o entendimento e operacionalização da LGPD. Os padrões ilustrativos

foram definidos de forma genérica. Eles podem ser reusados ou adaptados de forma padronizada em qualquer contexto de sistema de software.

O *template* de padrão de privacidade possui um **ID do requisito,** que pode ser indexado a outro sistema; citação da **Conformidade legal,** campo que conecta a base legal às funcionalidades do sistema, como também a sua **Descrição Legal**; **Objetivo de privacidade**, campo que aponta os princípios de privacidade conforme a lei; **Ativos**, campo que aponta os titulares dos dados; **Vulnerabilidades**, campo que indica as possíveis fraquezas sobre os dados pessoais; **Solução,** campo com solução proposta a partir das lacunas encontradas; **Consequências**, campo que indica os possíveis problemas caso a conformidade legal sugerida não seja atendida.

Ao final dessa etapa, o comitê gestor de privacidade será capaz de emitir uma proposta recomendando as possíveis soluções para as lacunas de privacidade dos dados pessoais envolvidos no contexto do sistema.

As recomendações para resolver as lacunas de privacidade são encaminhadas em conjunto com o *template* do padrão de privacidade para o analista de requisitos preencher. Após o preenchimento do *template* de padrão de privacidade, esse artefato é encaminhado para a próxima etapa do guia, que é a etapa de validar o padrão de privacidade conforme as sugestões de conformidade legal.

Lembrando que é sempre possível elaborar novos padrões de privacidade seguindo a mesma estrutura proposta, pois não exaurimos todas as possibilidades, nessa seção, exemplificamos cinco padrões de privacidade a partir das referências propostas nos catálogos de privacidade conforme apresentados no Apêndice F. Os padrões de privacidade precisam ser instanciados para atender as necessidades específicas de cada projeto.

5.3.4 Etapa 4: Validar Padrão de Privacidade

A validação do padrão de privacidade proposto consiste na revisão do artefato "Padrão de Privacidade". Nessa etapa, todos os atores que compõem o comitê de privacidade de dados revisam o plano de conformidade com a LGPD, sempre levando em consideração os efeitos colaterais que quaisquer alterações planejadas podem trazer ao negócio.

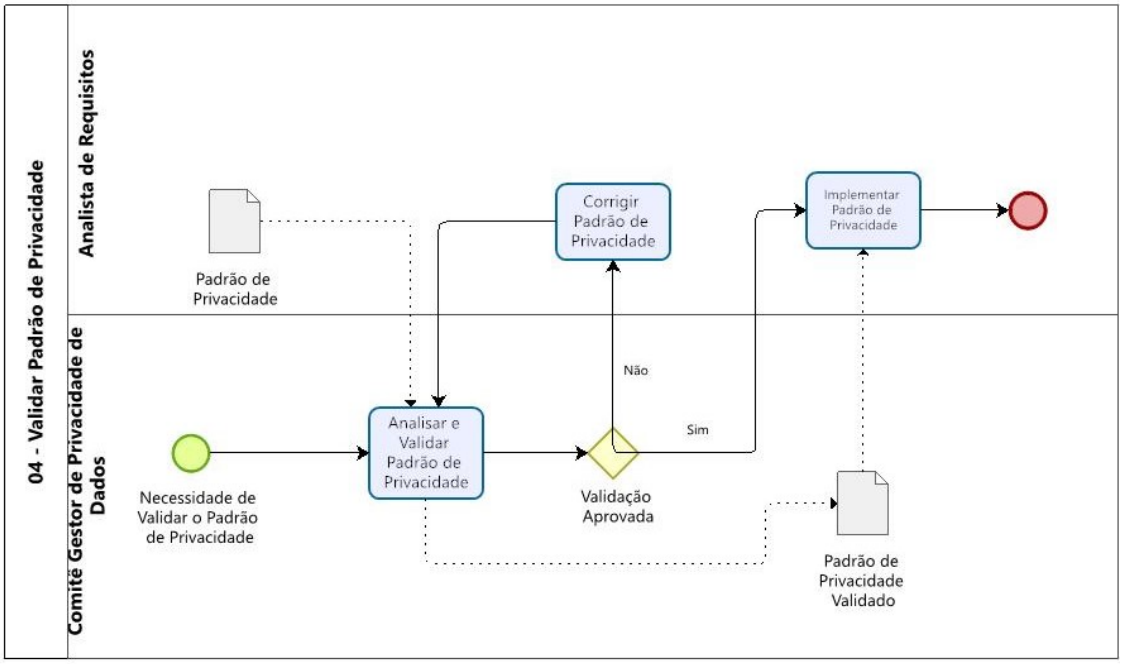
O comitê deve conduzir uma análise para avaliar os prós e os contras dos controles de privacidade sugeridos, avaliando vários fatores, como o escopo específico ou contexto

de domínio do sistema, custo da implementação, desempenho, esforço necessário, capacitação etc. Um exemplo de implementação que impactaria no desempenho seria implementar criptografia de dados nas bases de dados, tendo em vista que essa solução poderia tornar o desempenho do sistema complicado e insatisfatório.

Os atores dessa etapa são analistas de requisitos, especialistas em privacidade e especialistas jurídicos. Estes últimos atores têm o objetivo de tornar os princípios da LGPD de fácil entendimento para os analistas de requisitos e para a equipe de desenvolvimento de software.

A etapa de validar padrão de privacidade é finalizada com a análise do *template* do padrão de privacidade, que será encaminhado para a equipe de desenvolvimento de software, que a executará conforme especificado no padrão de privacidade. A Figura 18 apresenta o detalhamento da etapa de "Validar Padrão de Privacidade Proposto".

Figura 18 - Etapa 3: Validar Padrão de Privacidade.



Fonte: O autor (2021).

A Tabela 14 apresenta o objetivo, as entradas e saídas da etapa 4.

Tabela 14 - Etapa 4: Validar Padrão de Privacidade.

Objetivo da etapa 4	**Validar o preenchimento do padrão de privacidade; E encaminhar o padrão de privacidade para implementação.**
Entradas	Padrão elaborado pelo analista de requisitos.
Saídas	Validar o padrão de privacidade elaborado pelo analista de requisitos.

Fonte: O autor (2021).

Descrição das atividades da Etapa 4 – Validar Padrão de Privacidade

I. **Analisar e Validar Padrão de Privacidade**: O comitê gestor de privacidade deve avaliar os prós e os contras dos controles de privacidade no contexto do requisito especificado, conforme o preenchimento dos campos no *template* de padrão de privacidade, executado pelo analista de requisitos, conforme as soluções sugeridas na etapa anterior.

II. **Corrigir Padrão de Privacidade**: Após a análise do padrão de privacidade, o comitê gestor de privacidade têm a opção de aprovar ou revogar o padrão de privacidade.
   a. Identificando problemas na elaboração, o comitê gestor revoga e retorna o padrão de privacidade para o analista de requisitos, de forma que se deve implementar ações de correção;
   b. Em caso de aprovação do padrão de privacidade, este deve ser encaminhado para o analista de requisitos.

III. **Implementar padrão de privacidade**: O analista de requisitos deve encaminhar o padrão de privacidade para a equipe de desenvolvimento.

Ao final dessa etapa, o analista de requisitos encaminha o padrão de privacidade instanciado e validado para a equipe de desenvolvimento, com o objetivo de implementar os requisitos de privacidade conforme as orientações sugeridas pelo padrão de privacidade.

5.4 SÍNTESE DO CAPÍTULO

Nesse capítulo, foi descrito o G-Priv, que é um guia para apoiar a conformidade na especificação de requisitos de privacidade com a LGPD. O guia proposto pode ser utilizado em diferentes contextos organizacionais, com o objetivo de otimizar a

especificação dos requisitos legais de privacidade em conformidade com a legislação de privacidade de dados pessoais. O guia G-Priv sugere a utilização de *templates* que podem ajudar na operacionalização da interpretação da lei, como também os seus artefatos servirão como fonte de armazenamento e disseminação de conhecimento sobre privacidade de dados pessoais e os catálogos de privacidade. O guia foi dividido em quatro etapas, cada etapa foi descrita com seus objetivos, entradas e saídas, e o detalhamento de suas atividades. O capítulo seguinte descreve a avaliação do guia proposto nessa dissertação com analistas de requisitos de várias organizações.

6 AVALIAÇÃO DO G-Priv e CATÁLOGO DE PADRÕES

Esse capítulo tem o objetivo de apresentar os resultados da avaliação do G-Priv, o guia para apoiar a conformidade na especificação de requisitos de privacidade com a LGPD e o Catálogo de Padrões de Privacidade. A avaliação foi realizada a partir do ponto de vista de profissionais de organizações privadas e públicas que atuam nas áreas de engenharia de requisitos, análise de sistemas, privacidade de dados, segurança da informação, desenvolvimento de software. A seção 6.1 descreve como foi conduzido o questionário de pesquisa. A seção 6.2 apresenta uma análise crítica dos resultados obtidos no questionário, relacionando as características dos participantes à utilização do guia. A seção 6.3 descreve a síntese do capítulo.

6.1 *SURVEY* DE AVALIAÇÃO

Para elaborar o questionário, foi utilizado um formulário no Google Forms. Nesse formulário, foi disponibilizado um vídeo explicativo sobre o G-Priv e uma documentação detalhada sobre o guia, apresentando de forma sistemática as suas etapas, interações entre os atores e os *templates* disponibilizados no capítulo 6. O questionário de avaliação está disponível no Apêndice G.

A pesquisa foi realizada no período de 18 de outubro até 07 de novembro de 2021. Os participantes foram convidados por conveniência a partir de contatos profissionais, por meio de mensagens, telefone e e-mail, a participação foi voluntária e livre de qualquer remuneração ou benefício e os participantes poderiam se recusar a participar, retirar o consentimento ou interromper a sua participação a qualquer momento.

Para participar do *survey*, o pesquisador enviou 21 convites e obteve a resposta de 18 participantes. Isso significa que obtivemos uma boa amostragem e com qualidade, pois a grande maioria dos participantes possuem mais de 11 anos de experiência na indústria de software, todos possuem titulação acima da graduação e atuam em áreas diversificadas.

Para apoiar no entendimento sobre o guia G-Priv e no preenchimento do *survey*, o pesquisador produziu um vídeo de orientações básicas que foi disponibilizado no link: https://tinyurl.com/g-priv. Em conjunto com o vídeo, também foi disponibilizada a documentação completa sobre o guia, essa documentação faz referência ao Capítulo 6.

O objetivo do *survey* foi avaliar o Guia de Privacidade (G-Priv) em relação a sua utilidade e facilidade de uso para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD, sob a perspectiva dos engenheiros e analistas de requisitos.

As questões do *survey* foram projetadas pelo pesquisador e validas pelo orientador, o piloto teve o objetivo de descartar, melhorar ou inserir novas questões, organizar as questões por seção, *design*, como também analisar o tratamento das respostas.

6.2 RESULTADOS

O questionário de avaliação está dividido em três seções de perguntas. A primeira seção trata do consentimento de participação, informando que o *survey* foi elaborado com base no Termo de Consentimento Livre e Esclarecido pelo Conselho Nacional de Saúde, regido pela Resolução 196/96 (Apêndice G). A segunda seção traça o perfil e a experiência dos participantes. A terceira e última seção explora da avaliação do G-Priv, com o objetivo de avaliar a facilidade de uso e utilidade do guia, para apoiar a especificação de requisitos de privacidade em conformidade à LGPD.

Em nossa pesquisa, utilizamos o TAM (*Technology Acceptance Model*), modelo plenamente aplicável ao problema da pesquisa por ser específico para usuários de tecnologia e ter vantagem de possuir uma forte base teórica, além do amplo apoio empírico através de validações, aplicações e replicações.

O modelo TAM foi projetado para compreender a relação casual entre variáveis externas de aceitação dos usuários e o uso real do computador, buscando entender o comportamento desses usuários através do conhecimento da utilidade e da facilidade de utilização percebida por eles (DAVIS, 1989).

E segundo Davis (1989), as pessoas tentam, usar ou não uma tecnologia com o objetivo de melhorar seu desempenho no trabalho, com base nessa tendência o modelo TAM está fundamentado basicamente em dois constructos: a utilidade percebida e a facilidade de uso percebida. A utilidade percebida mensura em grau em que a pessoa acredita que o uso de um sistema particular pode melhorar o seu desempenho e a facilidade de uso percebida, é o grau em que uma pessoa acredita que o uso de um sistema de informação será livre de esforço.

Diante do exposto, os construtos foram desenvolvidos de modo a captar opiniões pessoais e tratar suposições a respeito de terceiros, sendo assim, esse modelo foi útil para identificar o porquê da aceitação das características do G-Priv (atividade, pessoas envolvidas, fluxo das etapas e os *templates*).

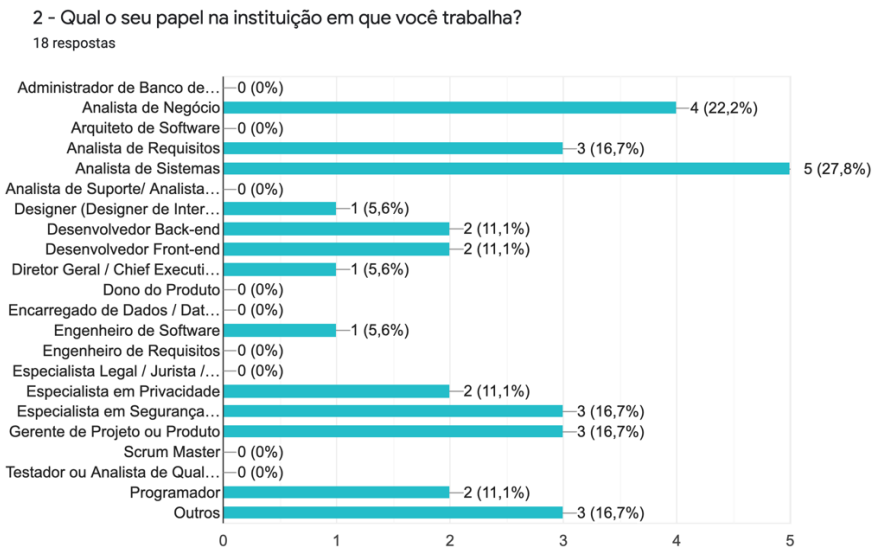
6.2.1 Perfil e Experiência

Essa seção tem como objetivo identificar o perfil do respondente, a experiência na área de privacidade de dados e na indústria de software. A seguir, são apresentadas as questões dessa seção e a análise das respostas obtidas.

Q2: Qual o seu papel na instituição em que você trabalha?

De acordo com a Figura 19, os participantes acumulam funções nas organizações onde trabalham, mas os dados apresentam que a grande maioria se intitula analista de sistemas. Sendo assim, temos 4 (quatro) analistas de negócio, 3 (três) analistas de requisitos, 5 (cinco) analistas de sistemas, 1 (um) *designer*, 4 (quatro) desenvolvedores *back-end* e *front-end,* 1 (um) diretor geral, 1 (um) engenheiro de software, 2 (dois) especialistas em privacidade, 3 (três) especialistas em segurança da informação, 3 (três) gerentes de projetos e 2 (dois) programadores. E por fim, os 3 (três) outros representam analista de processos, trainee e consultor de TI.

Figura 19 - Papel na instituição que trabalha.

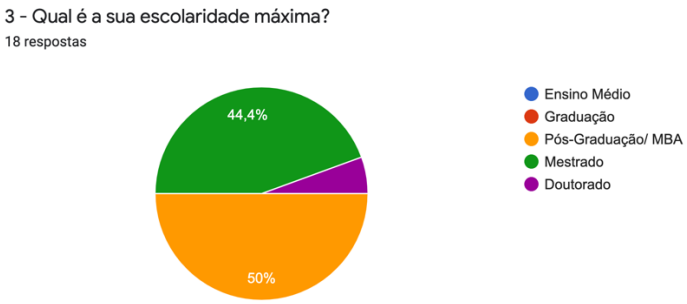


Fonte: O autor (2021).

Q3: Qual é a sua escolaridade máxima?

Segundo descrito na Figura 20, 50% (nove) dos participantes possuem Pós-Graduação/MBA, seguido de 44,4% (oito) dos participantes que são mestres e apenas 5,6%, ou seja, (um) participante possui doutorado.

Figura 20 - Escolaridade máxima.

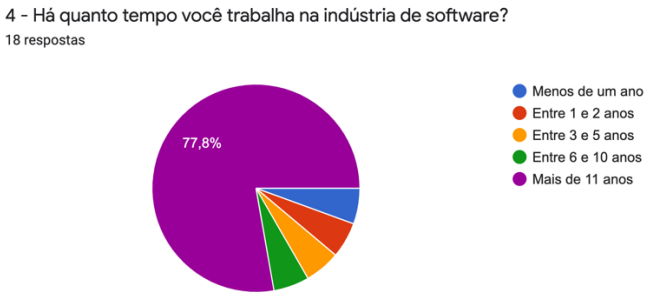


Fonte: O autor (2021).

Q4: Há quanto tempo você trabalha na indústria de software?

Podemos analisar na Figura 21 que a maioria possui mais de 11 anos de experiência, isso significa um total de 14 participantes. Esse resultado confirma que os participantes possuem longa experiência na indústria de software. Em seguida, tivemos 1 (um) participante com menos de um ano de experiência, 1 (um) participante com experiência entre 1 e 3 anos, 1 (um) participante com experiência entre 3 e 5 anos e 1 (um) participante com experiência entre 6 e 10 anos.

Figura 21 - Experiência na indústria de software.



Fonte: O autor (2021).

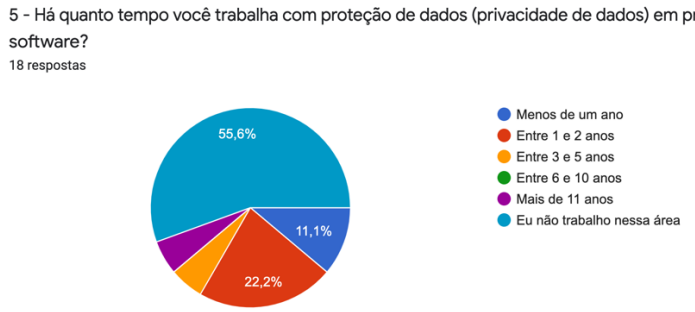
Q5: Há quanto tempo você trabalha com proteção de dados (privacidade de dados) em projetos de software?

De acordo com a Figura 22, a quantia de 55,6% (dez) dos participantes não trabalham nessa área, enquanto 22,2% (quatro) trabalham com proteção de dados em um período entre 1 e 2 anos, 11,1% (dois) trabalham há menos de um ano, 5,6%, ou seja, (um) participante possui experiência num período entre 3 e 5 anos. Apenas 1 (um)

participante tem mais de 11 anos de experiência com proteção de dados, isso representa na amostragem um ponto fora da curva.

Diante desses dados, podemos interpretar que ao longo dos anos o tema sobre proteção e privacidade de dados em projetos de software não foi tratado com a sua devida relevância nas organizações. Esses dados corroboram com os dados extraídos no protocolo de entrevista semiestruturado, que foi apresentado no Capítulo 4, naquela oportunidade os entrevistados relataram que, na rotina de trabalho, não há estratégia ou procedimento bem definido para os requisitos de privacidade. Então, como não há uma estratégia ou procedimento bem definido, os requisitos de privacidade são abordados de maneira *ad hoc* ou por intuição, assim justificando o alto número de participantes que não trabalham com proteção e privacidade de dados.

Figura 22 - Experiência com proteção de dados.

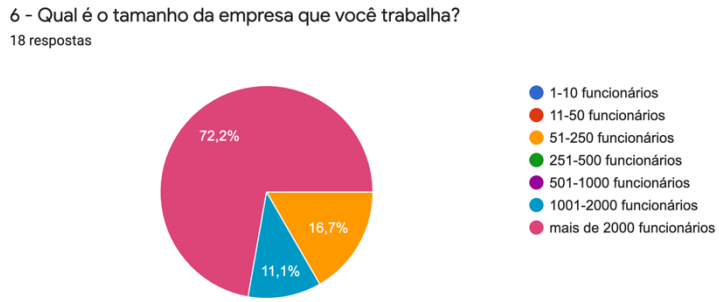


Fonte: O autor (2021).

Q6: Qual é o tamanho da empresa que você trabalha?

Pode-se observar na Figura 23 que 72,2% (treze) dos participantes trabalham em empresas com mais de 2.000 funcionários, com um quantitativo um pouco abaixo do índice anterior (entre 1.001 e 2.000 funcionários) 11,1% (dois) dos participantes estão nessa faixa quantitativa. E por fim, 16,7% (três) dos participantes atuam em empresas de pequeno e médio porte, com o quantitativo entre 51 e 250 funcionários.

Figura 23 - Tamanho da empresa.

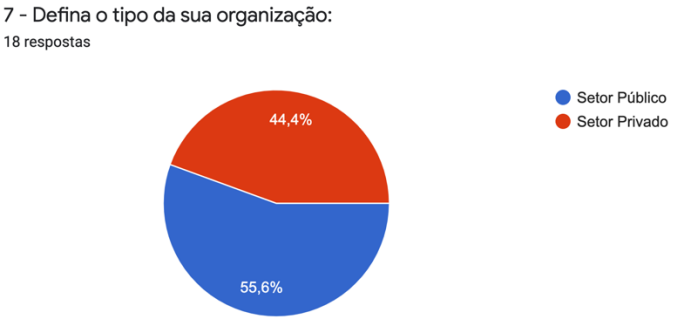


Fonte: O autor (2021).

Q7: Defina o tipo da sua organização?

De acordo com a Figura 24, tivemos uma leve vantagem do setor público sobre o setor privado, 55,6% (dez) dos participantes são do setor público em diversos seguimentos, enquanto 44,4% (oito) dos participantes são do setor privado.

Figura 24 - Tipo da organização.



Fonte: O autor (2021).

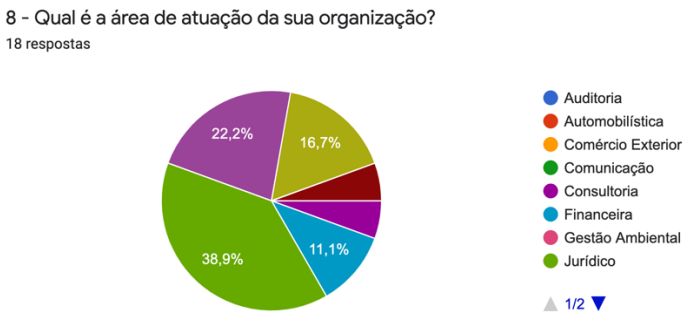
Q8: Qual é a área de atuação da sua organização?

Pode-se notar conforme apresentado na Figura 25, 38,9% (sete) dos participantes atuam com Tecnologia da Informação no setor jurídico, seguido de 22,2% (quatro) dos participantes que atuam na área de Tecnologia da Informação, 16,7% (três) dos participantes atuam com TI na área de saúde, 11,1% (dois) atuam com TI no mercado financeiro, 5,6%, ou seja, (um) dos participantes presta algum tipo de consultoria envolvendo privacidade de dados pessoais e o restante dos 5,6%, ou seja, (um) dos participantes atua em outras áreas.

Esses resultados demonstram uma ampla diversidade de áreas de atuação, essas características ajudam a enriquecer o propósito do guia proposto, que teve o objetivo de

propor um guia de privacidade genérico que se possa ser escalonado para qualquer segmento ou área de atuação. Diante disso, os dados revelam a preocupação do pesquisador em diversificar o perfil de atuação dos participantes, como também atingir o objetivo de provar o quanto o G-Priv pode ser genérico.

Figura 25 - Área de atuação da organização.



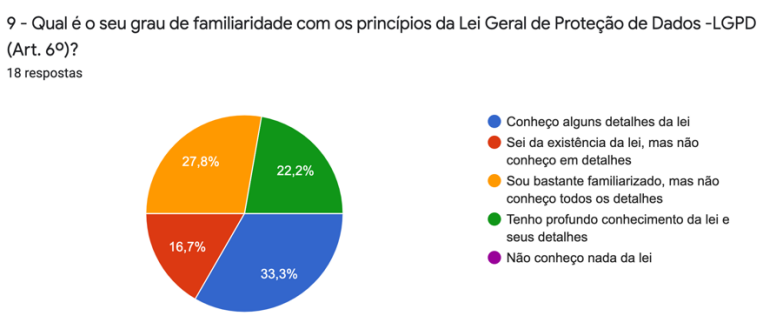
Fonte: O autor (2021).

Q9: Qual o seu grau de familiaridade com os princípios da Lei Geral de Proteção de Dados -LGPD (Art.6º)?

Conforme exposto na Figura 26, analisamos que 27,8% (cinco) dos participantes afirmam que são bastante familiarizados com a lei, mas desconhecem os seus detalhes, enquanto 33,3% (seis) dos participantes afirmam que conhecem alguns detalhes da lei, 22,2% (quatro) dos participantes afirmam que têm profundo conhecimento da LGPD e seus detalhes, por fim, a pesquisa aponta que 16,7% (três) dos participantes afirmam que sabem da existência da lei.

Esses resultados apontam que todos os participantes já tiveram algum tipo de contato com a lei, seja de forma mais básica, intermediária ou avançada. Sendo, assim, um ponto positivo para buscar a conformidade legal de privacidade.

Figura 26 - Grau de familiaridade com os princípios da LGPD.



Fonte: O autor (2021).

Q10: A sua organização realiza inciativas para garantir conformidade dos sistemas de software com a LGPD?

Pode-se notar conforme registrado na Figura 27, apresenta que 88,9% (dezesseis) dos participantes afirmam que suas organizações promovem inciativas para a conformidade de sistemas à LGPD. Em contrapartida, apenas 11,1% (dois) dos participantes entendem que suas organizações ainda não realizaram iniciativas para conformidade legal dos sistemas.

Figura 27 - Iniciativas para garantir a conformidade com LGPD.

Fonte: O autor (2021).

Q11: Caso sua resposta anterior tenha sido "sim", você poderia explicar brevemente quais são as iniciativas?

A Tabela 15 apresenta respostas dos participantes sobre iniciativas conduzidas pelas suas organizações a fim de garantir a sua conformidade com a LGPD. Os relatos destacados nas respostas são: capacitação, comitês para tratar o tema, inventário dos dados, auditorias e mudanças na rotina de trabalho.

As iniciativas mais citadas dizem respeito à capacitação para suprir a limitação do conhecimento sobre privacidade e proteção de dados, diante desses relatos, os participantes reforçam que é necessário investir em capacitação e conscientização sobre o tema. Essas informações corroboram com os dados extraídos no protocolo de entrevista semiestruturado, que foi apresentado no Capítulo 4, naquela oportunidade os entrevistados relataram a mesma preocupação e necessidade de investimento em capacitação.

Outros dois pontos que merecem destaque são: a necessidade de fazer um mapeamento/inventário dos dados pessoais, para melhor entendimento do contexto atual sobre os riscos e as ações que devem ser executadas, essa necessidade mostra como a

primeira etapa do G-Priv pode auxiliar nessa iniciativa, como também auxiliar no processo estruturado para adequação da LGPD.

Tabela 15 - Respostas referentes à iniciativa de conformidade com LGPD.

RESPOSTAS
"Workshop interno relacionado ao tema."
"Como trabalhamos com biometrias (digitais e faciais) a criptografia é o ponto crucial do nosso sistema, garantindo assim o sigilo total no tráfego das informações biométricas"
"A minha organização iniciou seu percurso rumo à implementação do Programa de Proteção de Dados Pessoais a partir de um projeto para cumprimento dos requisitos da Lei nº 13.709/2018 (LGPD), iniciando em janeiro de 2020, com a constituição de força tarefa composta por representantes da área de negócios, jurídica e de tecnologia da informação"
"Como resultado do trabalho dessa força tarefa, foram definidos conceitos, critérios e metodologias para possibilitar a realização do diagnóstico inicial da gestão de dados pessoais, a análise das lacunas de conformidade e a análise de risco dos processos."
"Auditorias e constantes atualizações nos padrões de desenvolvimento orientado a LGPD."
"Projeto de adequação à LGPD de forma a instituir um processo de gestão de privacidade."
"No momento, foi criado um comitê para gestão da LGPD dentro da instituição"
"As informações sobre LGPD são passadas aos funcionários através de treinamentos oferecidos pela ESMAPE - Escola Judicial de Pernambuco"
"Inventário dos dados dos sistemas atualmente em produção, avaliação de impacto, anonimização de dados, desenho das novas soluções já voltado à privacidade."
"Treinamentos obrigatórios para os funcionários a partir do ano passado (2020)."
"Cartilha na Intranet traz todas as informações sobre a LGPD. Termo Aditivo ao contrato de trabalho contendo cláusulas de proteção de dados."
"Mapeamento de operações de tratamento de dados, análise e avaliação de riscos de privacidade, treinamento e capacitação de funcionário com ênfase em LGPD e implementação de medidas de segurança com foco em conformidade com a LGPD"
"Foi montado um comitê com DPO e foram mapeados todos os processos que tratam de dados pessoais. Estão sendo feitas algumas auditorias nos softwares para garantir a conformidade."
"Criou um grupo de trabalho para tratar a questão."
"Existe uma unidade dedicada à segurança. Propõem utilizar algum tipo de criptografia em dados em bancos para equipes de desenvolvimento."
"Em projeto de implantação da LGPD foi executado trabalho de levantamento em todos os sistemas. E rotina implantada para qualquer nova mudança. Isto com o setor de LGPD."
"Mapeamento de lacunas em relação aos controles da NBR/ISO IEC 27701 para implantação da LGPD; Mapeamento dos riscos de privacidade de dados e direcionamento de ações de tratamento dos mesmos."

Fonte: O autor (2021).

Q12: Na sua opinião, quais são os principais desafios para garantir a conformidade dos sistemas de software com a LGPD?

A tabela 16 apresenta as respostas dos participantes referentes aos principais desafios para garantir a conformidade dos sistemas a LGPD. Os relatos dos participantes apresentaram como maiores desafios: a mudança cultural, a falta de compromisso das pessoas envolvidas no processo de conformidade, seguido do desafio de como adequar os sistemas e processos à LGPD.

O desafio de mudar a cultura e a falta de compromisso apareceu em 9 (nove) dos 18 (dezoito) relatos dos participantes. Esse dado corrobora com as informações coletadas durante a entrevista semiestruturada, que foi apresentada no Capítulo 4, um dos achados apresentados nesse capítulo descreve que um dos principais obstáculos para garantir a conformidade dos sistemas de software com a LGPD é a necessidade de mudança cultural e a mentalidade das pessoas envolvidas no processo de privacidade de dados pessoais.

Tabela 16 - Principais desafios para garantir a conformidade com LGPD.

RESPOSTAS
"O principal desafio é o entendimento da organização da importância em garantir essa conformidade e o investimento de tempo e dinheiro."
"O conhecimento dos solicitantes e desenvolvedores dos requisitos exigidos pela norma"
"As questões legais."
"O tráfego de informações entre as camadas de Aplicação, ainda mais quando se trafega dados pela WEB."
"Comprovar o cumprimento da lei. Muito se fala em adequar os sistemas e processos, mas pouco é mostrado sobre como comprovar a compliance com a lei na prática."
"Disponibilidade de recursos, principalmente humanos, para alocar em projetos derivados dessa iniciativa."
"Compromisso dos envolvidos"
"A implementação de uma cultura organizacional na qual todas as áreas da instituição assumam a sua parcela de responsabilidade para a garantia da proteção dos dados pessoais."
"(1) Atender ao princípio da minimização de dados pessoais. (2) Garantir que os softwares sejam suficientemente flexíveis para absorver os impactos das mudanças na gestão de consentimento (revogações de consentimento, novos consentimentos para novos tratamentos etc.). (3) Garantir integração suficiente do software com o inventário de dados para permitir o maior nível possível de automatização quanto ao exercício de direitos dos titulares de dados pessoais."
"PESSOAS são sempre o ponto falho. Estão sujeitas a falhas, erros, submissão, índole, etc."
"Acredito que um desafio é a mudança na cultura organizacional da empresa, pois envolve novos processos organizacionais."
"Mudança de cultura das pessoas (stakeholders e principalmente dos usuários)"
"A compreensão do time em relação a importância da proteção de dados, e a revisão de arquitetura de sistemas legados."
"Definir um guia de referência para aplicação das normas definidas pela LGPD."
"Estabelecer regras claras sobre o tratamento desses dados pessoais. Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras de sistemas de software."

"A falta de conhecimento dos clientes que pedem requisitos que são muitas vezes incompatíveis com os princípios da LGPD."
"Pessoas, costumes e uso abusivo de mídias sociais ou de mensageria."
"Implementar de fato os conceitos de privacy by design."

Fonte: O autor (2021).

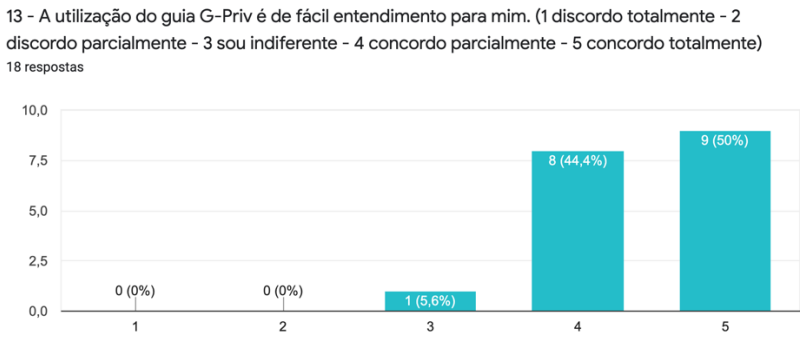
6.2.2 Avaliação do Guia – G-Priv

A terceira seção do questionário teve o objetivo de avaliar a facilidade de uso e utilidade do Guia G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. Nessa seção, os participantes avaliaram as etapas, os *templates* disponibilizados, os papéis dos atores envolvidos em cada etapa e sua operacionalização como um todo. A seguir são apresentadas as questões dessa seção, com as suas respostas obtidas e a respectiva análise.

Q13: A utilização do guia G-Priv é de fácil entendimento para mim?

A Figura 28 apresenta que 50% (nove) dos participantes concordam totalmente com o fácil entendimento da utilização do G-Priv, 44,4% (oito) dos participantes afirmam que concordam parcialmente e apenas 5,6%, ou seja, (um) dos participantes mostrou-se indiferente com a questão da facilidade do guia. Diante das respostas obtidas, podemos considerar que os participantes concordam de alguma maneira que o guia G-Priv é de fácil entendimento de acordo com a visão dos participantes.

Figura 28 - Facilidade em utilizar o G-Priv.



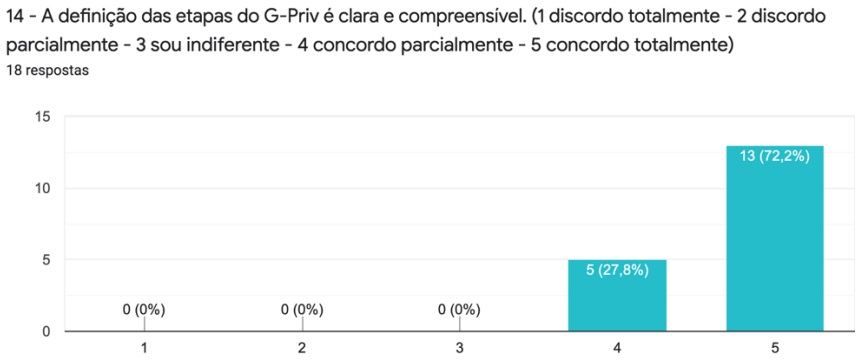
Fonte: O autor (2021).

Q14: A definição das etapas do G-Priv é clara e compreensível?

A Figura 29 apresenta que 72,2% (treze) dos participantes concordam totalmente que a definição das etapas do guia é bastante clara, enquanto apenas 27,8% (cinco) dos participantes afirmaram que concordam parcialmente com a clareza e compreensão. As

respostas mostram que os participantes concordam de alguma maneira, que a definição das etapas do G-Priv é clara e compreensível.

Figura 29 - Compreensão das etapas do G-Priv.



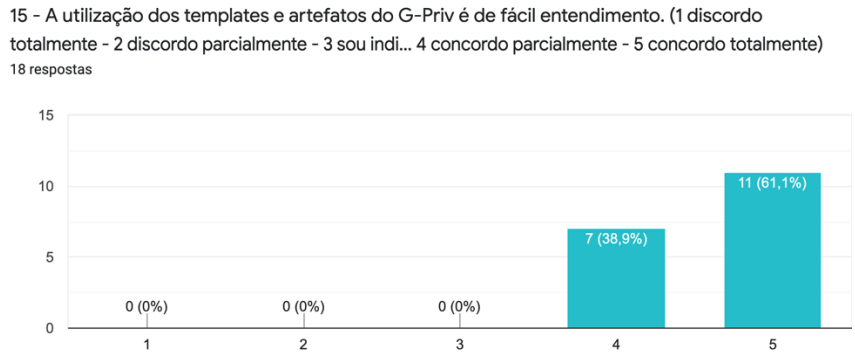
Fonte: O autor (2021).

Q15: A utilização dos templates e artefatos do G-Priv é de fácil entendimento?

A Figura 30 apresenta que 61,1% (onze) dos participantes concordam totalmente com a facilidade da utilização dos *templates* do guia e 38,9% (sete) dos participantes afirmaram que concordam parcialmente.

Diante das respostas podemos concluir que os participantes concordam que a utilização dos *templates* e os artefatos do G-Priv são de fácil entendimento.

Figura 30 - Utilização dos templates do G-Priv.



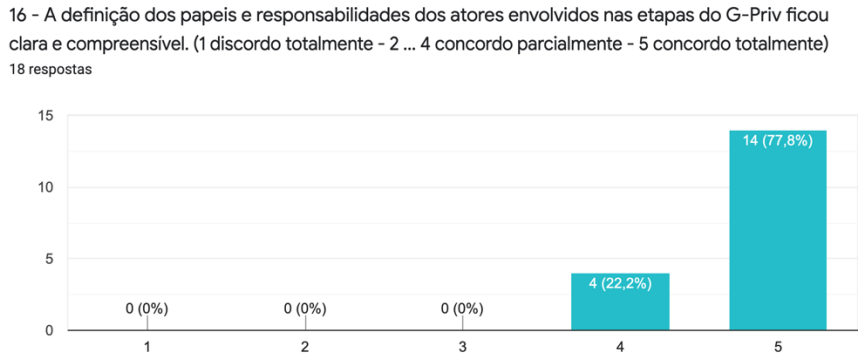
Fonte: O autor (2021).

Q16: A definição dos papéis e responsabilidades dos atores envolvidos nas etapas do G-Priv ficou clara e compreensível?

A Figura 31 apresenta que 77,8% (quatorze) dos participantes concordam totalmente com as definições e responsabilidades dos atores envolvidos nas etapas do guia, enquanto apenas 22,2% (quatro) dos participantes concordam parcialmente.

As respostas apontam que, de maneira geral, os participantes concordam que as definições dos papéis e responsabilidades dos atores envolvidos nas etapas do G-Priv ficou clara e compreensível.

Figura 31 - Definição dos papéis e responsabilidades dos atores no G-Priv.



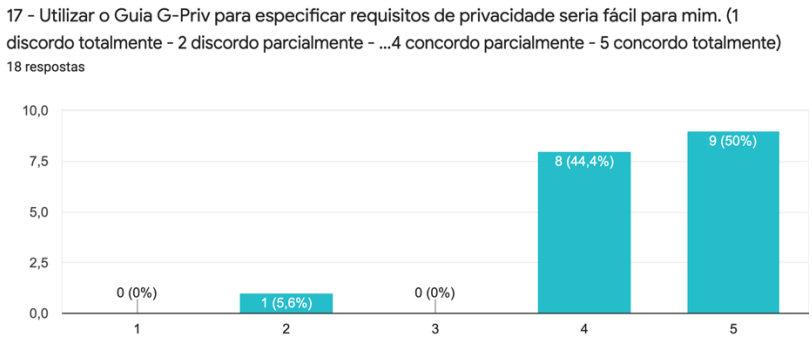
Fonte: O autor (2021).

Q17: Utilizar o guia G-Priv para especificar requisitos de privacidade seria fácil para mim?

A Figura 32 apresenta que 50% (nove) dos participantes concordam totalmente com a facilidade para especificar requisitos de privacidade utilizando o G-Priv, 44,4% (oito) dos participantes concordam parcialmente. Apenas 1 (um) participante discordou parcialmente com a facilidade proposta pelo guia.

Os resultados obtidos nas respostas dos participantes apontam que a maioria, ou seja, 94,4% dos participantes concordam que especificar requisitos de privacidade utilizando o G-Priv pode facilitar o seu trabalho.

Figura 32 - Facilidade para especificar requisitos de privacidade utilizando o G-Priv.



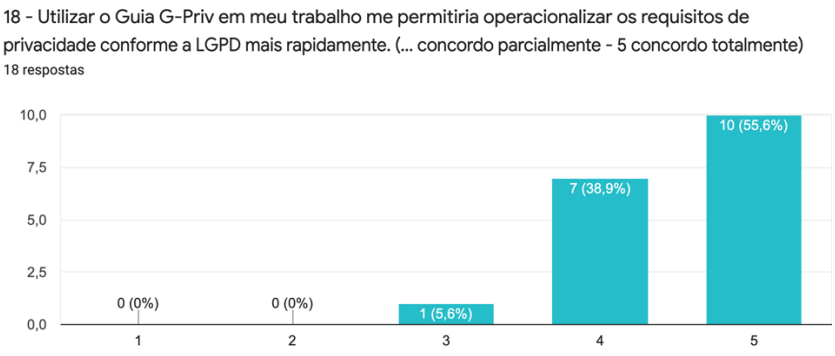
Fonte: O autor (2021).

Q18: Utilizar o guia G-Priv em meu trabalho me permitiria operacionalizar os requisitos de privacidade conforme a LGPD mais rapidamente?

A Figura 33 apresenta que 55,6% (dez) dos participantes concordam totalmente que a utilização do guia permitiria operacionalizar os requisitos de privacidade em conformidade com a LGPD com mais facilidade, 38,9% (sete) dos participantes concordam parcialmente e apenas 5,6%, ou seja, (um) participante mostrou-se indiferente com a utilização do guia.

Os dados obtidos nas respostas dos participantes apontam que a maioria dos participantes entendem que o G-Priv permitiria operacionalizar os requisitos de privacidade com mais agilidade conforme as regras da LGPD.

Figura 33 - Utilidade do G-Priv no ambiente de trabalho permite operacionalizar os requisitos de privacidade mais rapidamente.



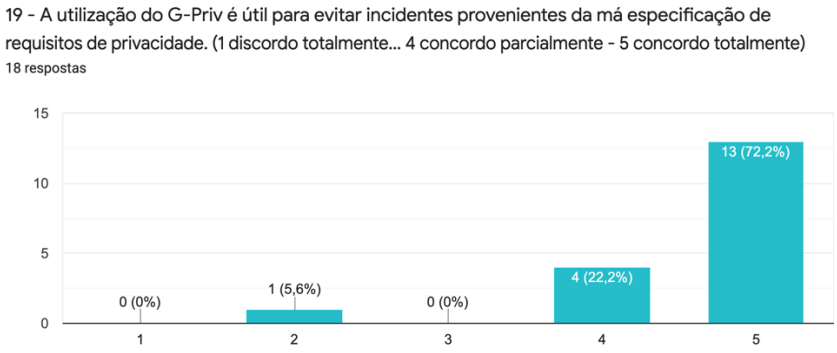
Fonte: O autor (2021).

Q19: A utilização do G-Priv é útil para evitar incidentes provenientes da má especificação de requisitos de privacidade?

A Figura 34 apresenta que 72,2% (treze) dos participantes concordam totalmente que a utilização do G-Priv será útil para evitar incidentes provenientes da má especificação dos requisitos de privacidade, 22,2% (quatro) dos participantes concordam parcialmente. Apenas 1 (um) participante discordou parcialmente com a sua utilidade.

Esses resultados apontam que a grande maioria (94,4%) concordam que o G-Priv pode ser útil para evitar incidentes, que a origem é a má especificação dos requisitos de privacidade.

Figura 34 - Utilidade do G-Priv para evitar incidentes com origem na especificação dos requisitos de privacidade.



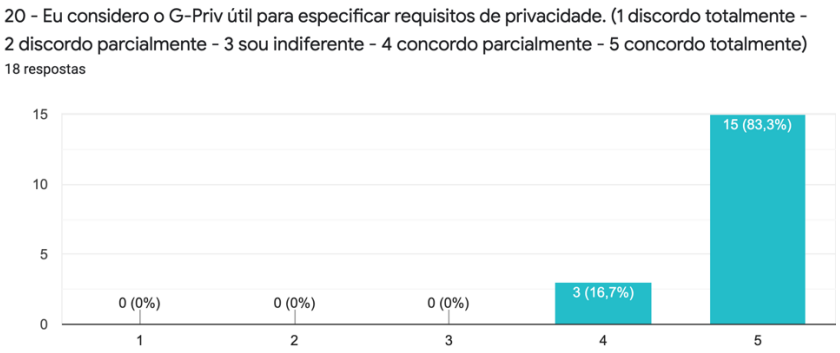
Fonte: O autor (2021).

Q20: Eu considero o G-Priv útil para especificar requisitos de privacidade?

A Figura 35 descreve que 83,3% (quinze) dos participantes concordam totalmente com a utilidade do G-Priv para especificar requisitos de privacidade, e apenas 16,7% (três) dos participantes concordaram parcialmente.

A análise obtida nos resultados aponta que, quase todos, os participantes concordam de alguma maneira que o G-Priv é útil para especificar requisitos de privacidade.

Figura 35 - Utilidade do G-Priv para especificar requisitos de privacidade.



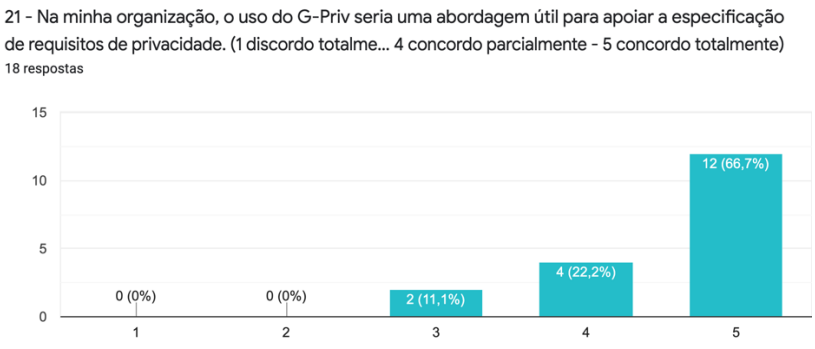
Fonte: O autor (2021).

Q21: Na minha organização, o uso do G-Priv seria uma abordagem útil para apoiar a especificação de requisitos de privacidade?

A Figura 36 apresenta que 66,7% (doze) dos participantes concordam totalmente que o uso do guia na sua organização seria útil para apoiar a especificação dos requisitos de privacidade, 22,2% (quatro) dos participantes concordam parcialmente. Apenas 11,1% (dois) dos participantes se mostraram indiferente com sua utilidade.

Desta forma, os dados obtidos nos resultados apontam que a maioria dos participantes concordam de alguma maneira que o G-Priv seria útil na sua organização para apoiar a especificação dos requisitos de privacidade.

Figura 36 - Utilidade do G-Priv nas organizações.



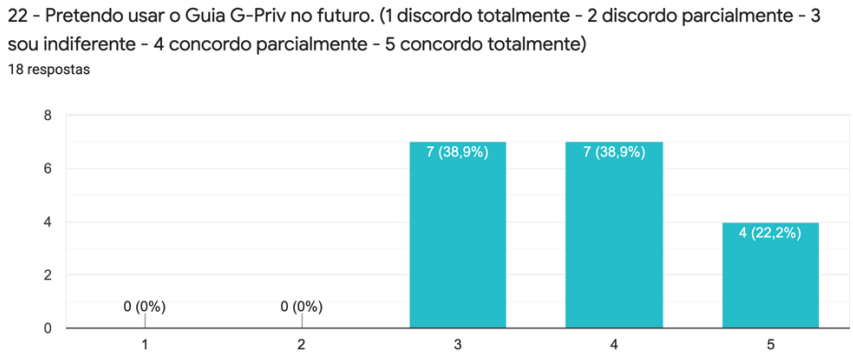
Fonte: O autor (2021).

Q22: Pretendo usar o guia G-Priv no futuro?

A Figura 37 apresenta que 22,2% (quatro) dos participantes concordam totalmente em utilizar o G-Priv no futuro, 38,9% (sete) dos participantes concordam parcialmente. Como também 38,9% (sete) dos participantes se mostraram indiferentes em utilizar no futuro.

Os resultados da análise dos dados levam ao entendimento da relevância do guia e mostram que mais da metade dos participantes (61,1%) pretendem utilizar o G-Priv no futuro.

Figura 37 - Utilidade do G-Priv nas organizações.



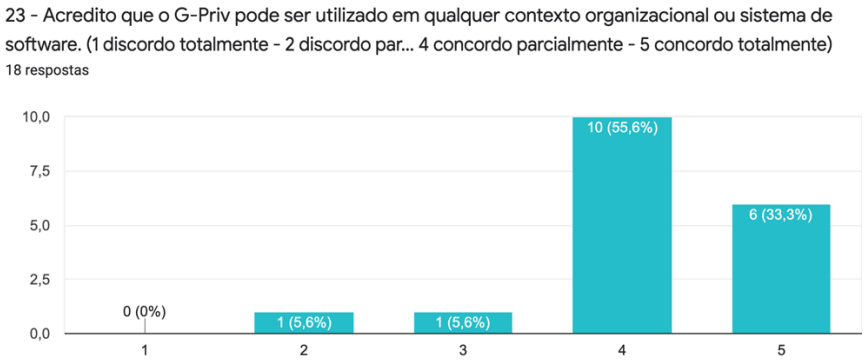
Fonte: O autor (2021).

Q23: Acredito que o G-Priv pode ser utilizado em qualquer contexto organizacional ou sistema de software?

A Figura 38 apresenta que 33,3% (seis) dos participantes acreditam totalmente que o G-Priv pode ser utilizado em qualquer contexto organizacional ou sistema de software, 56,6% (dez) dos participantes concordam parcialmente. Apenas 1 (um) participante mostrou-se indiferente com a utilização e outro 1 (um) participante discordou parcialmente.

Sendo assim, os dados revelam que 88,9% dos participantes acreditam que o G-Priv foi concebido de maneira genérica e pode ser utilizado em qualquer contexto organizacional ou sistema de software.

Figura 38 - Utilidade do G-Priv de maneira genérica.



Fonte: O autor (2021).

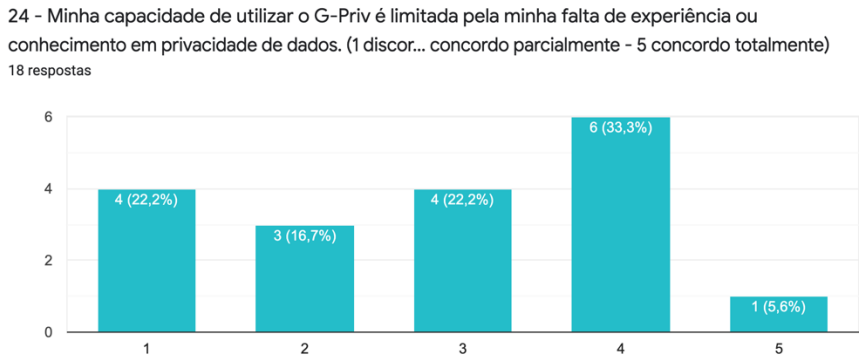
Q24: Minha capacidade de utilizar o G-Priv é limitada pela minha falta de experiência ou conhecimento em privacidade de dados?

A Figura 39 apresenta que 33,3% (seis) dos participantes concordam parcialmente que têm a capacidade limitada ao conhecimento sobre privacidade de dados para utilizar o G-Priv, apenas 1 (um) participante concorda totalmente que tem a capacidade limitada para utilizar o guia, 22,2% (quatro) participantes se mostraram indiferentes ao tema.

Por outro lado, tivemos 16,7% (três) dos participantes que discordam parcialmente e 22,2% (quatro) dos participantes discordaram totalmente. Sendo assim, podemos afirmar que há um equilíbrio entre 38,9% dos que têm plena capacidade de utilizar o G-Priv e 38,9% que se mostraram com capacidade limitada para utilizar o guia.

Diante dessas informações coletadas, podemos interpretar que aqueles participantes que se mostraram incapazes de utilizar o G-Priv ou se mostraram indiferentes, talvez necessitem de mais tempo na prática com projetos reais para adquirir mais confiança de como utilizar o guia, pois o G-Priv se trata de um novo artefato.

Figura 39 - Capacidade técnica de utilizar o G-Priv.

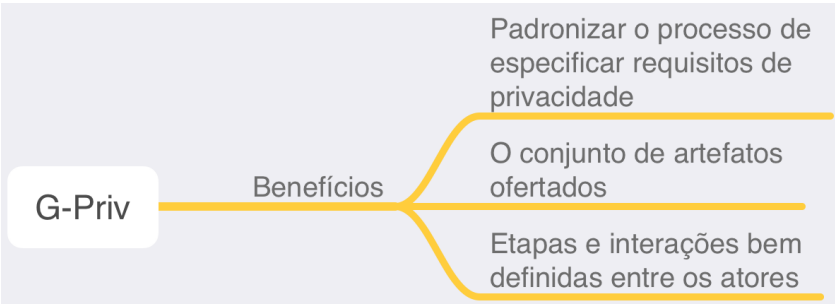


Fonte: O autor (2021).

Q25: Na sua opinião, quais são os principais benefícios do guia G-Priv?

A Tabela 17 apresenta as respostas dos participantes em relação aos principais benefícios do G-Priv. Os relatos dos participantes destacam que os maiores benefícios do G-Priv são: padronizar o processo de especificar requisitos de privacidade, o conjunto de artefatos ofertados, etapas e interações bem definidas entre os atores. Na Figura 40, pode-se notar a ilustração sintética dos benefícios.

Figura 40 - Mapa mental dos benefícios do G-Priv.



Fonte: O autor (2021).

Tabela 17 - Opinião dos principais benefícios do G-Priv.

RESPOSTAS
"Ao meu entendimento os principais benefícios são os abordados pelas etapas de Coleta de dados pessoais e Análise de lacunas de privacidade."
"Deixar claro a não especialistas o que deve ser observado na especificação de requisitos, reduzindo a curva de aprendizagem e como um artefato obrigatório tornando o processo mais rapidamente incorporado a cultura."
"A LGPD ainda está amadurecendo em nosso país e dispor de um guia que permita ORIENTAR-SE para iniciar a aplicação da LGPD no Desenvolvimento de Software é fantástico."
"Acredito que dentre os principais benefícios do Guia G-Priv, estão:

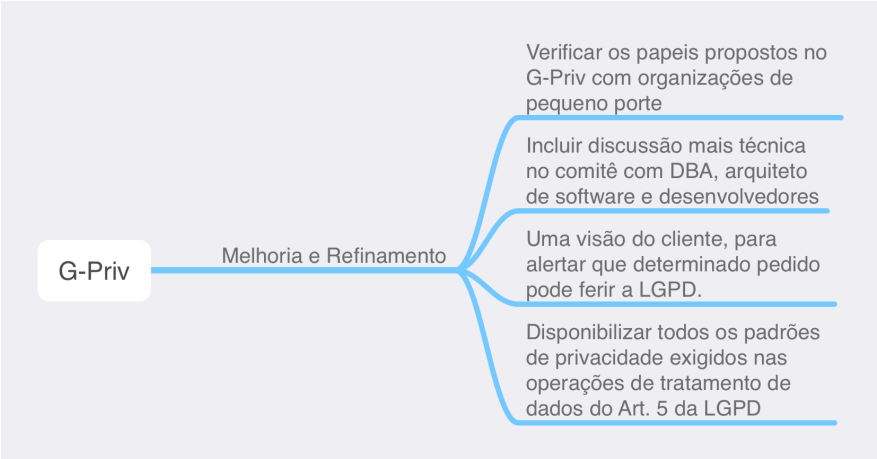
1) Fornecer um processo padronizado e de fácil entendimento e implementação para expressar os requisitos de segurança, privacidade e proteção de dados pessoais dos usuários no desenvolvimento de sistemas de software; 2) Fornecer um conjunto geral de artefatos suficientes para a especificação dos requisitos de privacidade e proteção de dados com o intuito de implementá-los de forma efetiva em sistemas de software; 3) Ajudar a identificar falhas na fase de elicitação de requisitos em relação à privacidade e proteção de dados pessoais no processo de desenvolvimento de sistemas de software em geral."
"Geração dos artefatos que poderão ser uteis no mapeamento de lacunas e produção de evidências que respaldam a organização com a LGPD."
"Cobrir um vácuo existente no mercado oferecendo uma abordagem metodológica para encaminhar demandas de proteção de dados pessoais focada no desenvolvimento de software, mais especificamente na fase de levantamento de requisitos."
"Padronizar a especificação dos requisitos de privacidade em conformidade com a LGPD"
"Acredito que uma padronização auxiliaria tanto a gestão de TI para implementar a lei, tanto es durante essa transição de cultura organizacional. Assim como agilizaria a aplicação da lei no dia a dia."
"Possui etapas bem definidas, cada uma com seu objetivo claro. Responsabilidade de cada ator é especificada com fácil entendimento."
"Estabelecer um roadmap claro para o analista de requisitos/analista de negócio (e até mesmo product owner) que precise atentar às questões envolvendo a proteção de dados."
"É um norte para auxiliar na identificação de possíveis requisitos podem ferir a LGPD."
"Garantir que os dados utilizados nos sistemas, quando relevantes à LGPD, tenham o tratamento adequado ao que preconiza a nova Lei."
"Mais do que um guia, o G-PRIV pode ser considerado um framework para especificação de requisitos de privacidade em projetos de desenvolvimento de software, uma vez que cobre aspectos prescritivos sobre padrões de privacidade para operações de tratamento de dados pessoais em sistemas de informação."
"o G-PRIV oferece um modelo claro e objetivo de um fluxo de trabalho para o levantamento de requisitos em privacidade de dados, além de trazer todos os templates."
"Modelo para não partir do zero"
"Garantir um padrão mínimo de segurança. Também é um ótimo ponto de partida"
"Facilidade para mapeamento inicial dos pontos relativos a legislação."
"A utilização de um método pré-estabelecido acelera o trabalho de levantamento de requisitos relativos à privacidade de dados de sistemas de sw."

Fonte: O autor (2021).

Q26: Você teria sugestões para melhoria e refinamento do guia G-Priv?

A Tabela 18 apresenta sugestões dos participantes em relação a possíveis melhorias e refinamentos do G-Priv. Nos relatos dos participantes, eles sugerem os seguintes pontos de melhoria: incluir no uso do guia discussões mais técnicas no comitê gestor de privacidade, como pessoas com funções de arquiteto de software, administrador de banco de dados e o responsável pelo time de desenvolvimento; disponibilizar todos os padrões de privacidade exigidos nas operações de tratamento de dados do Art. 5 da LGPD. Na Figura 41, pode-se notar a ilustração sintética das melhorias sugeridas nos relatos.

Figura 41 - Mapa mental das melhorias sugeridas no G-Priv.



Fonte: O autor (2021).

Tabela 18 - Sugestões para melhoria e refinamento do G-Priv.

RESPOSTAS
"Poderia se verificar a possibilidade de o analista/especialista de dados fazer uma validação do formulário de coleta de dados antes de ir para o comitê gestor. Analista de Requisitos -> especialista em dados -> Comitê gestor."
"Deixar explícito que está tratando de requisito não funcional (requisito legal)."
"Para se ORIENTAR o guia está bem objetivo, as dificuldades vão ser encontradas e devem ser refinadas no decorrer do projeto de Desenvolvimento, então, atualmente não teria sugestões."
"Na minha pouca experiência com G-Priv não consigo enxergar melhorias ou refinamentos para o mesmo."
"Para um trabalho futuro sugiro que seja verificada a compatibilidade dos papéis propostos no Guia G-Priv com organizações de menor porte, acompanhando inclusive as regulamentações ainda em construção pela ANPD para organizações com esta característica."
"Aplicar qualquer prática requer experiência e maturidade. Sugiro sempre, inicialmente, modelos simples que possam ser detalhados à medida que a maturidade da instituição cresce no tema, e também conforme necessidade. O objetivo é evitar burocracias desnecessárias."
"Por enquanto não. Adorei o trabalho, parabéns!"
"Seria necessário uma "convivência" maior com este processo para poder identificar pontos de melhoria. Ou seja, na medida em que você implementa o processo e começa a utilizá-lo é que surgiriam então as observações a cerca dos pontos fortes e dos pontos fracos do Guia G-Priv. Mas me pareceu bastante interessante e pode ajudar no processo de criar uma nova cultura a respeito do tratamento dos dados pessoais no que diz respeito ao desenvolvimento de sistemas."
"Frisas a adequação mesmo em abordagem ágil e não apenas (como parece, implicitamente) em abordagens mais tradicionais. Incluir discussão técnica (com arquiteto de software, DBA, time de desenvolvimento como um todo) antes da instanciação."
"Como é voltada para aplicação no levantamento de requisitos, acredito que abranja de forma eficiente, claro que com o uso contínuo é natural que surjam melhorias."
"Não teria nenhuma sugestão. Gostaria de parabenizar pelo excelente trabalho, pois acredito que esse Guia irá ser bastante útil e irá ajudar muito empresas e órgãos em geral durante o desenvolvimento de sistemas em relação à preocupação (cada mais constante) sobre a privacidade dos dados dos usuários. Parabéns!"
"Que houvesse uma versão com a visão do cliente, que pede um requisito, para que ele antes de fazer o pedido ser "alertado" que determinado requisito pode ferir a LGPD."
"Importante adicionar formulário de incidente/notificação para apoio no dia a dia."
"Minha sugestão seria a de incluir padrões de privacidade para todas as operações de tratamento de dados pessoais previstas no Art. 5, inciso X da Lei Geral de Proteção de Dados (ex: processamento, extração etc), dessa forma tonando o G-PRIV capaz de atender plenamente todos os aspectos de privacidade na elicitação de requisitos no processo de software."

Fonte: O autor (2021).

6.3 SÍNTESE DO CAPÍTULO

Nesse capítulo, foi apresentada a avaliação do guia G-Priv através de um questionário de avaliação.

A partir das respostas de 18 profissionais que participaram do questionário, foi possível obter resultados positivos e relevantes para avaliar a facilidade de uso e utilidade do G-Priv. Em geral, os participantes afirmaram que as etapas do G-Priv são de fácil entendimento e compreensível. Os participantes trabalham em diversas áreas e desempenham diferentes papéis nas suas organizações, mas em sua maioria são analistas de sistemas. Todos fazem parte do setor público e privado, 14 (quatorze) dos participantes possuem mais de 11 anos de experiência.

De acordo com a avaliação dos participantes, o G-Priv foi considerado de fácil entendimento, principalmente nas definições dos papéis e responsabilidades dos atores envolvidos nas quatro etapas do guia. Os participantes também citaram a agilidade na operacionalização de especificação dos requisitos de privacidade, assim colaborando para evitar incidentes provenientes da especificação dos requisitos de privacidade. Consideramos que o guia obteve uma boa aceitação, pois mais da metade dos participantes afirmaram a possibilidade de utilizar o guia no futuro.

Nas perguntas abertas, abordamos os temas sobre os benefícios e as sugestões de melhorias do G-Priv. Dentre as respostas referentes aos benefícios, há destaque para o processo de padronizar a especificação dos requisitos de privacidade em conjunto com os artefatos ofertados, assim facilitando a operacionalização de especificar os requisitos de privacidade, etapas e interações bem definidas entre os atores.

A partir da análise das respostas, foi possível identificar uma série de ações ou iniciativas, com algumas delas já em execução, como a preocupação em especificar requisitos de privacidade e a busca de um mecanismo para atuar como facilitador para especificar os requisitos de privacidade em conformidade com a LGPD. E dentre as sugestões de melhoria, o que ganhou destaque foi a sugestão de disponibilizar todos os padrões de privacidade exigidos nas operações de tratamento de dados discutidos no Art. 5º da LGPD.

7 CONCLUSÕES, LIMITAÇÕES E TRABALHOS FUTUROS

Esse trabalho teve como objetivo inicial apresentar os resultados de entrevistas exploratórias, a fim de investigar a perspectiva de analistas de requisitos sobre privacidade e proteção de dados. Trabalhos semelhantes que também buscavam entender a visão de desenvolvedores incluem os estudos (PEIXOTO ET AL., 2020; CANEDO ET AL., 2020).

Com o objetivo de operacionalizar a interpretação da LGPD, propomos um catálogo de padrões de privacidade e um guia de privacidade chamado de G-Priv, que têm o objetivo de auxiliar os analistas de requisitos durante a especificação dos requisitos de privacidade, esse guia de privacidade foi inspirado no GuiMe das autoras Ayala-Rivera (2018) e nos conceitos do *Privacy by Design* (CAVOUKIAN, 2020).

Os resultados obtidos no estudo exploratório, através de entrevistas semiestruturadas, revelaram que os analistas da organização estudada consideram que é necessário investir em capacitação e comunicação interna, para disseminar aspectos de privacidade em conformidade com a LGPD. Esse mesmo resultado também foi identificado após obter as respostas dos participantes em um *survey* de avaliação do guia de privacidade proposto pelo pesquisador, assim reforçando a necessidade de se investir em capacitação e conscientização.

Outra percepção que teve destaque nos resultados das entrevistas semiestruturadas e no *survey* foi em relação à rotina de trabalho. Os entrevistados e os participantes do *survey* relataram que possuem equipes com pessoal bastante limitado para atender novas demandas. Eles reforçaram que já existe um sentimento sobre a relevância da privacidade presente nas equipes, pois alguns sistemas já exigiam que tais requisitos fossem satisfeitos antes da lei entrar em vigor.

Os entrevistados compartilharam a dificuldade de interpretar e operacionalizar a LGPD no contexto dos sistemas e serviços prestados. Como forma para tratar tais desafios, os entrevistados mencionaram a necessidade de uma abordagem ágil e simples para especificar requisitos de privacidade. A partir dos *insights* das entrevistas, elaboramos uma abordagem baseada em padrões de privacidade. Como demonstração da proposta, definimos um padrão de privacidade específico para o contexto do Sistema Nísia. E para validar esse sentimento de dificuldade ao interpretar e operacionalizar a lei, os participantes do *survey* também relataram que falta uma estratégia ou procedimento bem definido para auxiliar a interpretação e operacionalização da LGPD.

Outro ponto que teve interseção entre a entrevista e o *survey* foi um dos principais obstáculos para garantir a conformidade dos sistemas de software com a LGPD, que é a mudança cultural e a mentalidade das pessoas envolvidas no processo de privacidade de dados pessoais.

7.1 CONTRIBUIÇÕES PARA A ACADEMIA E INDÚSTRIA

Dentre as contribuições dessa pesquisa tivemos a descoberta de achados a partir de entrevistas com analistas de requisitos, tais como: **conceitos de privacidade**, que diz respeito à limitação de conhecimento sobre os princípios de privacidade e proteção de dados; **processo de conformidade**, que trata do modo sistemático como a organização deve operacionalizar a adequação dos seus processos internos à LGPD; **obstáculos na conformidade**, que trata a forma como as organizações encara os obstáculos para alinhar os seus sistemas, bases de dados, e a própria mentalidade das pessoas envolvidas em relação aos aspectos de privacidade; ***tradeoff* entre privacidade e transparência**, que se refere a como a organização sofre influência das leis internas e externas vigentes e os impactos das novas legislações nos seus serviços prestados; **rotina de trabalho**, que refere-se ao modo como as equipes de TI da organização realizam seu trabalho, envolvendo suas competências e atividades do dia a dia. Esse conjunto de resultados estão relatados no Capítulo 4, onde são destacadas cada uma dessas características para entender as percepções dos analistas de requisitos em relação à privacidade e proteção de dados.

Considerando as percepções dos entrevistados, identificamos a relevância do impacto nas organizações na especificação dos requisitos de privacidade e a lacuna existente na literatura quanto ao tema, a pesquisa consiste em uma relevante contribuição para a academia e para a indústria, especialmente para organizações carentes de um processo formal que contemple o desenvolvimento de software sob o prisma de privacidade de dados pessoais. Para isso, elaboramos um catálogo de padrões de privacidade aplicável para qualquer organização, que queira desenvolver sistemas em conformidade com a LGPD.

Como principal contribuição da dissertação, propomos uma guia de privacidade, chamado de G-Priv, que tem o objetivo de especificar requisitos de privacidade de maneira ágil e que fornece diretrizes simples em formato de *templates* ou *checklists*. Esse guia está detalhado no Capítulo 5, onde são destacados cada etapa do guia, os artefatos

ofertados e os atores envolvidos. O G-Priv segue o raciocínio de Ann Cavoukian ao concluir, que só as leis não garantem a privacidade, necessita-se de uma metodologia de apoio como o conceito de *Privacy by Design* e *Privacy by Default* apresentado na Seção 2.3.3 do capítulo de referencial teórico.

Em seguida, executamos uma avaliação do guia de privacidade (G-Priv) com analistas de requisitos de várias organizações, com a finalidade de obter um *feedback* da proposta de pesquisa, em relação a sua utilidade e facilidade de uso para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD, conforme apresentado anteriormente no Capítulo 6.

Em síntese, a pesquisa envolveu a realização de estudos empíricos para investigar como os analistas de requisitos e as organizações estão evoluindo seus processos de engenharia de requisitos, para garantir que os sistemas de software estejam em conformidade com a LGPD.

7.2 LIMITAÇÕES E AMEAÇAS À VALIDADE

Segundo Runeson e Höst (2009), a validade de um estudo denota a confiabilidade dos resultados, em que a medida dos resultados são verdadeiros e não são influenciadas pelo ponto de vista subjetivo dos pesquisadores. E existem diferentes maneiras de classificar os aspectos de validade e ameaças à validade na literatura:

- **Validade de construção**: esse aspecto de validade reflete a capacidade de operacionalizar a mensuração da pesquisa estudada, garantindo a qualidade dos procedimentos aplicados. Para exemplificar, as questões discutidas durante uma entrevista (numa coleta de dados), nem sempre são interpretadas da mesma forma pelo pesquisador e o entrevistado, pois assim há uma ameaça à validade do constructo (RUNESON e HÖST, 2009; YIN, 2003);
- **Validade interna**: esse aspecto de validade consiste no quanto os resultados correspondem à realidade, o quanto são fidedignos e até que ponto são originados do contexto da pesquisa. Para tratar essa ameaça, utilizamos múltiplos métodos de coleta de dados e triangulação dos dados (dados da entrevista semiestruturada, documentos do Nísia e dados do *survey*), além de validação pela própria orientadora e conversas informais com analistas de requisitos e de privacidade de diversas organizações;

- **Validade externa**: esse aspecto de validade se preocupa em saber até que ponto é possível generalizar as descobertas em outros domínios e em que medida as descobertas são de interesse para outras pessoas que estão fora do caso investigado. Durante a análise de validade externa, o pesquisador tenta analisar como os resultados são relevantes para outros casos, pois o propósito do guia nessa pesquisa é generalizar para todos os tipos de organizações e de forma prática a sua operacionalização, sendo assim, o objetivo é atingir a conformidade legal dos sistemas, quanto à especificação dos requisitos de privacidade;
- **Confiabilidade**: esse aspecto consiste em certificar que os procedimentos e aplicações de técnicas descritos na pesquisa, como coleta, análise e síntese de dados, foram conduzidas de forma semelhante por outros pesquisadores, assim os estudos deverão ter resultados similares. Esse tipo de ameaça a validade, por exemplo, se dá quando não está claro como foi feita a condução da codificação dos dados coletados. Para aumentar a confiabilidade, foi elaborado um protocolo de entrevista único que foi utilizado em todas entrevistas. A análise dos dados seguiu de forma cuidadosa todas as recomendações para o uso da síntese temática.

Uma limitação da pesquisa foi a realização de entrevistas semiestruturadas com analistas de requisitos, os dados coletados são referentes às opiniões pessoais desses participantes. Como forma de atacar essa limitação, buscamos selecionar analistas de diferentes equipes, com mais de 10 anos de experiência na área e que, atualmente, assumiram cargos gerenciais na organização. Como o estudo foi realizado com apenas cinco analistas de uma única organização, não podemos afirmar que os resultados das entrevistas exploratórias possam ser amplamente generalizados. Apesar dessas limitações, nossos resultados apresentam evidências qualitativas e *insights* ricos para avançar no entendimento sobre requisitos de privacidade.

Outra limitação do estudo consiste na Validade do constructo, que trata no viés decorrente de interpretações pessoais do pesquisador induzidas por conceitos e preconceitos, como por exemplo, a crença de que sempre é necessário capacitar pessoas antes de operacionalizar a atividade de especificar os requisitos de privacidade, pois a capacitação e conscientização podem auxiliar as pessoas a enxergar novos horizontes, como também na mudança cultural das pessoas. Essa interpretação do pesquisador partiu

das características dos participantes nas entrevistas exploratórias e no *survey*, que a maioria não dominava os conceitos e os termos sobre proteção e privacidade de dados.

Embora tenhamos procurado analisar e reportar as evidências com imparcialidade e objetividade, é possível que a pesquisa tenha sido influenciada por julgamentos de valor da pesquisa. Essas interpretações pessoais representam um risco à validade interna descrita anteriormente.

Por fim, uma consideração importante durante a construção do questionário do *survey* é o impacto de nosso próprio viés. Então tomamos o cuidado na forma de elaborar o *survey* de forma objetiva e imparcial, assim evitando que nossas perguntas fossem dirigidas de uma forma que é para confirmar o resultado desejado. Mesmo assim, outra limitação que pode afetar a validade da pesquisa trata-se da interpretação e entendimento dos participantes aos termos das questões do *survey*. É possível, que eles tenham tido dificuldade de interpretar algumas questões do survey. Além disso, consideramos uma eventual dificuldade de comprometimento com o tempo para estudar os artefatos do guia e a obrigação de participar podem influenciar nas respostas sem compromisso adequado com a pesquisa.

7.3 TRABALHOS FUTUROS

Como trabalho futuro, pretendemos automatizar o catálogo de padrões de privacidade e o guia para apoiar a conformidade coma LGPD (G-Priv), desenvolvendo em uma aplicação web na linguagem de programação Python. Assim, tornando o guia mais prático e ágil na sua operacionalização.

Além disso, pretendemos executar o G-Priv em projetos reais. Após participação no *survey*, alguns servidores de órgãos públicos e profissionais da indústria solicitaram a sua utilização para especificar requisitos de privacidade no desenvolvimento de software em conformidade com a LGPD. A partir dessas futuras propostas na prática, será possível realizar novos estudos para analisar e identificar os resultados, com o objetivo de evoluir ou melhorar pontos de dificuldade do guia.

REFERÊNCIAS

ALVES, C., NEVES, M.: **Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso**. 24º Workshop em Engenharia de Requisitos. 2021.

ANTHONYSAMY, P., RASHID A., CHITCHYAN, R.: **Privacy Requirements: Present & Future.** IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track, 2017.

AYALA-RIVERA, V., e PASQUALE, L.: **"The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements**. IEEE 26th International Requirements Engineering Conference. 2018.

ARAÚJO, E., VILELA, J., SILVA, C., ALVES, C.: **"Are My Business Process Model Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes"** SBSI 2021: XVII Brazilian Symposium on Information Systems. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27.701: Tecnologia da Informação – Técnicas de Segurança – Extensão da ABNT ISO 27.001 e ABN ISO BR ISO 27.002 para gestão de privacidade da informação – Requisitos e Diretrizes**. Rio de Janeiro, 2019.

BRASIL. Decreto N° 13.709, De 14 DE Agosto De 2018. **Lei Geral de Proteção de Dados Pessoais**, Brasília, DF, ago 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 13 abr. 2021.

BOAR, B. H. **Application Prototyping**. 1ed. New York: John Wiley & Sons, pp210, 1984.

CANEDO, E. D., CALAZANS, A. T. S., MASSON, E. T. S., COSTA, P. H. T., LIMA, F.: **Perceptions of ITC Practitioners Regarding Software Privacy**. Entropy, (2020).

FLICK, U. **Introdução à pesquisa qualitativa**; tradução Joice Elias Costa – 3ª ed. - Porto Alegre, pp. 37, 2009.

CAVOUKIAN, A. 2010. **Privacy by Design: The 7 Foudational Principles – Implementation and Mapping of Fair Information Practices**. Acessado dia 11 de abril de 2020, disponível em https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

CYSNEIROS, L. M., YU, E.: **Non-Functional Requirements Elicitation**. The Springer International Series in Engineering and Computer Science, pp 115-138, 2004.

CHENG, B., ATLEE, J. **Research Directions in Requirements Engineering**. Future of Software Engineering – fose´07. 2007

DAVIS, F. D.: **Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information technology**. MIS Quartely, Vol. 13, 1989.

DIRECTIVA 95/46/CE, Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995. **Relativa à Proteção das Pessoas Singulares no que Diz Respeito ao Tratamento de Dados Pessoais e à Livre Circulação Desses Dados**, 1995.

EU, Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, **General Data Protection Regulation**, 2016.

FERNÁNDEZ, D. M., WAGNER, S., KALINOWSJI, M., FELDERE, M., MAFRA, P., VETRÒ. A., CONTE, T., CRISTIANSSON, T., GREER, D., LASSENIUS, C., MÄNNISTÖ, T., NAYEBI, M., OIVO, M., PENZENSTADLER, B., PFAHL, D., PRIKLADNICKI, R., RUHE, G., SCHEKELMANN, A., SEN, S., SPINOLA, R., TUZCU, A., de la VARA, J. L., WIERINGA, R. **Naming the Pain in Requirements Engineering Contemporary Problems, Causes, and Effects in Practice.** Empirical Software Engineering, 2016.

FONTES, E.: **Políticas e Normas para a Segurança da Informação**. Brasport. Rio de Janeiro, 2012.

FRANCH, X., PALOMARES, C., QUER, C., RENAULT, S., LAZZER, F.: **A Metamodel for Software Requirements Patterns**, International Working Conference on Requirements Engineering: Foundation for Software Quality. REFSQ 2010. 2010.

GAVA, W. L. P**rocesso para Especificação de Requisitos de Software com Foco de Aplicação em Trabalho Cooperativo**. tese (doutorado em engenharia). Escola Politécnica da Universidade de São Paulo. São Paulo, poli-usp, 2009.

Gharib, M., Mylopoulos J., Giorgini P. **A core ontology for privacy requirements engineering.** Research Challenges in Information Science. RCIS 2020. Lecture Notes in Business Information Processing, vol 385. Springer, 2020.

GENERAL DATA PROTECTION REGULATION (GDPR): The paradigm Shift in Privacy, august 2018. Acessado dia 08 de agosto de 2019. Disponível em https://issuu.com/bhavyabedha/docs/ey-gdpr-aug-2018

KALLONIATIS, C.: **Incorporating privacy in the design of cloud-based systems: a conceptual meta-model**. Information & Computer Security. Vol. 25, No. 5, 2017.

KARLSSON, L., DAHLSTEDT, A., NATT och DAG, J., REGNELL, B., PERSSON, A. **Challenges inMarket-Driven Requirements Engineering – an Industrial Interview Study**. Eighth International Workshop on Requirements Engineering: Foundation for Software Quality, 2002.

KITCHENHAM B.A., PFLEEGER S. L. Personal Opinion Surveys. In: Shull F., Singer J., Sjøberg D.I.K. (eds) **Guide to Advanced Empirical Software Engineering**. Springer, London. 2008. https://doi.org/10.1007/978-1-84800-044-5_3

KONTONYA G. SOMMERVILLE I. **Requirements Engineering: Processes and Techniques**, Ed. Wiley, pp. 25 – 41, 1998.

KOPCZNSKA, S., NAWROCKI, J., OCHODEK, M.: **An Empirical Study on Catalog of Non-Functional Requirement Templates: Usefulness and Maintenance Issues**. Information and Software Technology, Volume 103, pp. 75-91, 2018.

LEITE, J.C.S.P., HADAD, G.D.S., DOOM, J. H., KAPLAN, G. N.: **A Scenario Construction Process**. Requirement Engineering, Springer Verlag, London, pp. 38-61, 2000.

LENHARD, J., FRITSCH, L. e HEROLD, S.: **A Literature Study on Privacy Patterns Research**, 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA, 2017.

MAGUIRE, M.: **Methods to Support Human-Centered Design**. international Journal of Human-Computer Studies, 2001.

Maior Vazamento de Dados. (2021). https://tinyurl.com/maiorvazamentodedados, último acesso em 08/02/2021.

MARCONI, M. A.; LAKATOS, Eva M. **Metodologia Científica**. 7. ed. São Paulo: Atlas, 2019.

MATULEVICIUS R., TOM J., KALA K., SING E. **A Method for Managing GDPR Compliance in Business Processes**. In: Herbaut N., La Rosa M. (eds) Advanced Information Systems Engineering. CAiSE 2020. Lecture Notes in Business Information Processing, vol 386. Springer, Cham. HTTPS://DOI.ORG/10.1007/978-3-030-58135-0_9. 2020.

MERRIAN, S. B. **Qualitative Research: a guide to design and implementation**. 2009.

Ministério Público Acusa Vivo por Vender Indevidamente Dados de Usuários. (2019). https://securityinformationnews.com/2019/09/07/ministerio-publico-acusa-vivo-por-vender-indevidamente-dados-de-73-milhoes-de-usuarios/, último acesso em 08/02/2021.

MURPHY, E. DINGWALL, R. T**he ethics of ethnography**. london: sage. pp. 339-351, 2001.

NUSEIBEH, B. EASTERBROOK, S. R**equirements Engineering: A Roadmap**. ICSE '00: Proceedings of the Conference on The Future of Software Engineering, pp. 35–46 HTTPS://DOI.ORG/10.1145/336512.336523, 2000.

Padrões de Privacidade. 2021. https://privacypatterns.eu/ último acesso em 31/03/2021.

PEIXOTO, M., SILVA, C. MAIA, H. ARAÚJO, J.: **Towards a Catalog of Privacy Related Concepts**. Joint Proceedings of REFSQ 2020, Workshops, Doctoral Symposium, Live Studies Track. 2020.

PEIXOTO M. et al.: **On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview**. International Working Conference on Requirements Engineering: Foundation for Software Quality. REFSQ 2020. (2020).

PRESSMAN R. S. **Engenharia de Software: Uma abordagem profissional**, AMGH Editora Ltda, 7ª edição, pp. 126 – 137, 2011.

Resolução 196/96 – consentimento. 1996. HTTPS://TINYURL.COM/RESOLUCAO196-96 , disponível em 28/04/2021.

Report Chaos. 2014. HTTPS://WWW.PROJECTSMART.CO.UK/WHITE-PAPERS/CHAOS-REPORT.PDF , Disponível em 10/05/2021.

RUNESON, P. HÖST, M. G**uidelines for conducting and reporting case study research in software engineering**. empir software engineering. 2009.

SALINI, P. e KANMANI, S.: **A Knowledge-Oriented Approach to Security Requirements Engineering for E-Voting System**, International Journal of Computer Applications, 2012.

SANTANDER, V. F. A. **Integrando modelagem organizacional com modelagem funcional**. tese (doutorado em ciência da computação). Universidade Federal de Pernambuco. Recife: UFPE, 2002.

SEAMAN, C. B. **Qualitative Methods in Empirical Studies of Software Engineering**. IEEE Transactions on Software Engineering, 1999.

SOMMERVILLE, I. **Engenharia de Software**, Editora Pearson, 9ª edição, pp. 57 – 79, 2011.

STRAUSS, A. L. e CORBIN, J. **Pesquisa Qualitativa: Técnicas e procedimentos para o desenvolvimento de teoria fundamentada**. Tradução Luciane de Oliveira da Rocha. Título original: Basics of Qualitative Research. 2. ed. Porto Alegre: Artmed, 2008.

Terreno Fértil para Vazamento de Dados. 2021. HTTPS://TINYURL.COM/VAZAMENTODADOS, último acesso em 28/04/2021

TOM, J., SING, E., MATULEVICIUS, R.: **Conceptual Representation of the GDPR: Model and Application Directions**, 17th International Conference, BRI 2018, 2018.

XUAN, X., WANG Y., LI, S.: **Privacy Requirements Patterns for mobile Operating Systems**, IEEE 4th International Workshop on Requirements Patterns (RePa), 2014.

YIN, R. K.: **Estudo de Caso: Planejamento e Métodos**. 2ª Edição, pp. 32 e 42, 2003.

APÊNDICE A – TCLE

Esse acordo foi redigido com base no Termo de Consentimento Livre e Esclarecido pelo Conselho Nacional de Saúde, Resolução 196/96.

Título da Pesquisa

Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Um Estudo de Caso em uma Organização do Poder Judiciário.

Pesquisadores Responsáveis:

- Carina Frota Alves
  Professora Doutora do Centro de Informática da Universidade Federal de Pernambuco.
- Moisés Neves Camelo
  Mestrando em Ciência da Computação pela Universidade Federal de Pernambuco.

Caro participante **[Nome do entrevistado]**, obrigado por dedicar um pouco do seu tempo para responder à nossa pesquisa. O objetivo é investigar a importância de requisitos de privacidade durante o desenvolvimento de produtos e serviços com uso intensivo de software, sob a perspectiva dos engenheiros e analistas de requisitos.

Os dados pessoais de cada participante não serão apresentados, apenas serão publicadas sínteses dos dados coletados, que resultará numa produção de um modelo genérico, com uma visão geral do fluxo do processo de especificação de requisitos.

Esse formulário tem como objetivo conscientizar os entrevistados sobre a utilização dos dados de forma segura e privada, apenas para fins acadêmicos do mestrado em Ciência da Computação do aluno Moisés Neves Camelo no Centro de Informática da UFPE.

Você está sendo convidado a participar da pesquisa de “Como auxiliar engenheiros de requisitos, na especificação de requisitos de privacidade e proteção de dados, em conformidade com as legislações de privacidade (LGPD)?”, de responsabilidade do aluno de mestrado Moisés Neves Camelo, da UFPE, tendo como orientadora a professora Carina Alves.

O objetivo é investigar a importância de requisitos de privacidade durante o desenvolvimento de produtos e serviços com uso intensivo de software, sob a

perspectiva dos engenheiros de software analistas de requisitos. Assim, gostaria de consultá-lo(a) sobre seu interesse e disponibilidade de cooperar com a pesquisa.

Você receberá todos os esclarecimentos necessários antes, durante e após a finalização da pesquisa, e lhe asseguro que o seu nome não será divulgado, sendo mantido o mais rigoroso sigilo mediante a omissão de informações que permitam identificá-lo(a). Os dados provenientes de sua participação na pesquisa, tais como gravação da entrevista e documentos fornecidos, ficarão sob a guarda do pesquisador responsável pela pesquisa.

A coleta de dados será realizada por meio de entrevistas. É para esse procedimento que você está sendo convidado a participar. Sua participação na pesquisa não implica em nenhum risco.

Espera-se que essa pesquisa possa contribuir para o melhor entendimento por parte dos analistas de requisitos, as iniciativas de especificação de requisitos de privacidade e proteção de dados em conformidade com a LGPD.

Sua participação é voluntária e livre de qualquer remuneração ou benefício. Você é livre para recusar-se a participar, retirar seu consentimento ou interromper sua participação a qualquer momento. A recusa em participar não irá acarretar qualquer penalidade ou perda de benefícios. Se você tiver qualquer dúvida em relação à pesquisa, você pode me contactar através do telefone (83) 99122-3465 ou e-mail: mn3@cin.ufpe.br. Nesse caso, você concorda em participar da entrevista? Permite que ela seja gravada?

APÊNDICE B – ROTEIRO DE ENTREVISTA

[Questões de pesquisa]

QP1. "Quais são as percepções dos engenheiros de requisitos em relação à privacidade e proteção de dados?"
QP2. "Como auxiliar analistas de requisitos na especificação de requisitos de privacidade e proteção de dados, em conformidade com a LGPD?"

[Apresentação da pesquisa]

Caro participante, nome do entrevistado, bom dia/ boa tarde!

Obrigado por dedicar um pouco do seu tempo para responder à nossa pesquisa.

O objetivo é investigar a importância de requisitos de privacidade durante o desenvolvimento de produtos e serviços com uso intensivo de software em conformidade com a legislação vigente da LGPD, sob a perspectiva dos engenheiros e analistas de requisitos.

Os dados pessoais de cada participante não serão apresentados, apenas serão publicadas sínteses dos dados coletados, que resultará numa produção de um artefato genérico, com uma visão geral do processo de especificação de requisitos.

Informações sobre processamento de dados (Por quanto tempo seus dados pessoais serão processados):
Sem período de tempo predefinido.

Informação pessoal:

No final da pesquisa, coletamos endereços de e-mail de forma voluntária. O objetivo é informar aos participantes sobre os próximos passos da pesquisa. Os endereços de email não serão associados às respostas fornecidas. Nenhum outro dado pessoal / sensível será coletado.

Quais categorias especiais de dados pessoais serão coletadas e usadas:

Nenhum.

Base jurídica do processamento:

Acordo de consentimento.

https://docs.google.com/forms/d/e/1FAIpQLSeqDRsASHTjK_Sn4pBrkxL4SWDChHiR_nRB5gpcu8ZgaGKoag/viewform

Entrevistados:

- Analista de requisitos
- Engenheiro de requisitos
- Gerente de projetos
- Diretor de sistemas
- Gestor de processos e serviços de TI
- Gestor de segurança da informação

ETAPAS	PERGUNTAS
Apresentação	1. Realizar apresentação, explicar sobre a confiabilidade e pedir permissão para gravar.
Introdução	2. Explicar o objetivo da entrevista. 3. "O objetivo é investigar a importância de requisitos de privacidade, durante o desenvolvimento de produtos e serviços, com uso intensivo de software, sob a perspectiva dos engenheiros e analistas de requisitos."
Dados Demográficos	4. Nome da empresa ou instituição. 5. Qual o segmento ou principal setor que sua organização opera? 6. Qual a sua função atual na organização? 7. Quantos anos de experiência você possui na área indicada?
Conhecimentos sobre privacidade	8. Na sua opinião, como a sua equipe entende o conceito de privacidade e proteção de dados pessoais, ao desenvolver um produto ou serviço? 9. Como você ou sua equipe considera os aspectos de privacidade de clientes e usuários são importantes ao desenvolver um produto ou serviço (valor do negócio)? 10. Quais políticas e medidas de segurança estão em vigor para proteger os dados pessoais nos aspectos de privacidade ao desenvolver um produto no seu ambiente de trabalho? 11. Sua organização especifica de forma explícita requisitos de privacidade e proteção de dados? De que forma? 12. Após a especificação dos requisitos, como são realizadas a verificação e validação dos requisitos de privacidade para garantir a conformidade legal? 13. Para garantir a conformidade legal dos requisitos de privacidade especificados, existe apoio jurídico? 14. Sua organização faz algum tipo de distinção por usuário? Como por exemplo, determinados usuários são mais críticos que outros, então, nesse caso, há uma preocupação maior com a privacidade.

	15. Esses dados (requisitos) coletados, podem ser acessados a qualquer momento pelos *stakeholders*, como também atualizados ou corrigidos? 16. Sua organização compartilha requisitos ou regras de negócio? Se sim, com quem e qual a finalidade? 17. Sua organização possui algum mecanismo para mensurar o risco ou impacto de um requisito não estar em conformidade com aspectos legais de privacidade?
Experiências práticas	18. Pela sua experiência, quais são os requisitos não funcionais de segurança mais exigidos pelos usuários? E qual a relevância no desenvolvimento do produto? 19. A sua equipe documenta de forma explícita requisitos de privacidade ao desenvolver um produto ou serviço? Como esses requisitos são descritos? 20. A sua equipe usa alguma ferramenta, método ou modelo que contemplem os aspectos de privacidade de dados durante o desenvolvimento de um produto ou serviço? 21. Há histórico de incidentes de vazamento ou exposição de dados, por não se dar a devida atenção aos requisitos de privacidade e proteção de dados por parte da sua organização? Você pode responder apenas com sim ou não, sem citar detalhes, caso prefira.
Percepção e Valores sobre privacidade	22. Como a LGPD está impactando o desenvolvimento de novos sistemas ou a conformidade de sistemas já em operação? 23. Na sua opinião, quais são os principais desafios e as dificuldades para garantir a conformidade entre a LGPD e os sistemas da sua organização? 24. Na sua opinião, quais ferramentas, métodos ou modelos podem apoiar a especificação de requisitos de privacidade durante o desenvolvimento de um produto ou serviço? 25. Elabore uma visão prática de como sua equipe se resguarda ou enfrenta o problema de vazamento ou exposição de dados?
Encerramento e Agradecimento	26. Você tem alguma coisa a mais para acrescentar sobre o tema de requisitos de privacidade e proteção de dados? 27. Alguma pergunta que você gostaria de acrescentar que não foi colocada aqui?

APÊNDICE C – FORMULÁRIO DE MAPEAMENTO DE DADOS PESSOAIS

Mapeamento de Dados Pessoais	
Informações Gerais	
Organização	
Gestor dos dados	
Atividade de Processamento de Dados	
Descrição da atividade	
Dados – Coleta, Tratamento e Análise	
País onde os dados são armazenados ou tratados	
Titulares dos Dados	
Tipo de dado	( ) Dados pessoais ( ) Dados sensíveis ( ) Dados de crianças
Dados Pessoais Coletados	Nome, CPF, E-mail, Número do processo, Foto do rosto segurando o documento de identidade
Termo de consentimento do titular:	( )Sim ( )Não ( )Não se aplica
Propósito	
Segurança Aplicada	
Quem tem Acesso	
Quais são os perfis de acesso?	
Responsáveis	
Origem dos Dados	
Qual Software é Utilizado?	
Local de Armazenamento	
Compartilhado com terceiros?	
Quantidade estimada de dados armazenados pela atividade	
Há Políticas, Procedimentos e Práticas para coleta, Tratamento, Transferência, Retenção e Eliminação de Dados?	
Nível de interesse em caso de intrusão ou vazamento de dados	( ) Alto: Vazamento de informações sobre o andamento do processo de mulheres vítimas de violência sob medida protetiva. ( ) Médio: ( ) Baixo:
Processo de Anonimização ou Pseudoanonimização dos Dados	

Existem Políticas, procedimentos e práticas de anonimização de dados pessoais?	
Há indicação de utilização de procedimentos de anonimização durante os testes de desenvolvimento?	( ) Sim ( ) Não ( ) Não se aplica

APÊNDICE D – FORMULÁRIO DE LACUNAS DE CONFORMIDADE NOS DADOS PESSOAIS

Lacunas de Conformidade nos Dados Pessoais	
Informações Gerais	
Organização	
Gestor dos dados	
Atividade de Processamento de Dados	
Descrição da atividade	
Princípios	**Perguntas**
Finalidade **Transparência**	1- No cadastro dos usuários no sistema, a finalidade da coleta dos dados pessoais é apresentada? Como também é apresentado o tipo de dado que é coletado? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Transparência**	2- Caso não consiga enquadrar a coleta de dados em uma das 9 bases legais e apenas restou a hipótese do consentimento, antes de o usuário inserir seus dados para o cadastro, é apresentado a ele um termo de consentimento? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Adequação**	3- Os dados pessoais coletados são compatíveis com a finalidade informada para o usuário? Por exemplo, os dados são coletados para o cadastro no sistema e acompanhamento do processo judicial? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Adequação** **Necessidade**	4- Caso o sistema faça a coleta de algum dado inadequado, é informado ao usuário o motivo? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Transparência** **Necessidade**	5- O sistema coleta apenas os dados pessoais necessários para cumprir seu propósito? ( )Sim ( )Não ( )Não se aplica

Finalidade **Transparência** **Necessidade**	6- Existe prazo estimado para retenção dos dados? ( )Sim ( )Não ( )Não se aplica
Finalidade **Transparência** **Necessidade** **Segurança**	7- Existe procedimento para eliminação dos dados? ( )Sim ( )Não ( )Não se aplica
Finalidade **Necessidade**	8- Caso os dados coletados sejam necessários para cumprir o propósito, são informadas a finalidade e a hipótese legal para o tratamento de dados pelo sistema? ( )Sim ( )Não ( )Não se aplica
Finalidade **Necessidade** **Livre acesso** **Transparência**	9- Após realizar o cadastro, o usuário consegue acessar o sistema para saber quais dados pessoais estão sendo tratados? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Livre acesso** **Transparência**	10- Existe um painel no sistema para o usuário saber a finalidade de cada dado coletado, e a confirmação do consentimento do uso? ( ) Sim. ( ) Não. ( ) Não se aplica.
Livre acesso **Qualidade dos dados** **Transperência**	11- O usuário consegue realizar a correção de dados incompletos ou desatualizados no sistema? ( ) Sim. ( ) Não. ( ) Não se aplica.
Livre acesso **Qualidade dos dados** **Transperência**	12- Existe procedimento automatizado ou semiautomatizado de desativação de usuários? ( ) Sim. ( ) Não. ( ) Não se aplica.
Finalidade **Qualidade dos dados** **Transparência**	13- Após cumprir a finalidade, os dados são anonimizados ou excluídos do sistema? ( ) Sim. ( ) Não. ( ) Não se aplica.

Transparência	14- As informações coletadas pelo sistema ficam claras, precisas e verdadeiras para o usuário? ( ) Sim. ( ) Não. ( ) Não se aplica.
Transparência	15- Caso sejam compartilhados os dados pessoais com setores, órgãos externos público ou privado, o titular é informado sobre esse compartilhamento? ( ) Sim. ( ) Não. ( ) Não se aplica.
Segurança **Prevenção**	16- Existe algum método ou técnica segura para a transferência dos dados pessoais para outros setores, órgãos externos público ou privado? ( ) Sim. ( ) Não. ( ) Não se aplica.
Segurança **Prevenção**	17- O sistema utiliza meios tecnológicos que garantam a proteção de dados pessoais de acessos não autorizados por terceiros? ( ) Sim. ( ) Não. ( ) Não se aplica.
Segurança **Prevenção**	18- Existe algum dado pessoal que utilize criptografia para aumentar a segurança da informação? ( ) Sim. ( ) Não. ( ) Não se aplica.
Segurança **Prevenção**	19- A organização possui política ou procedimento para o desenvolvimento de sistemas? ( ) Sim. ( ) Não. ( ) Não se aplica.
Segurança **Prevenção**	20- A organização possui regras de firewall, que evite acesso externo aos dados pessoais armazenados no bando de dados? ( ) Sim. ( ) Não. ( ) Não se aplica.
Não discriminação	21- A instituição é contra discriminar ou promover abusos contra seus titulares, com o uso de dados pessoais sensíveis? ( ) Sim.

	( ) Não. ( ) Não se aplica.
Não discriminação	22- Caso a organização faça algum tratamento diferente com dados pessoais sensíveis, existe alguma lei que permite essa ação? Por exemplo, dados de mulheres vítimas de violência, ou crianças e adolescentes? ( ) Sim. ( ) Não. ( ) Não se aplica.
Responsabilização e Prestação de contas	23- Existe um responsável pelo sistema, que possui acesso aos dados pessoais, durante o processo de testes, homologação e implantação dos respectivos sistemas? ( ) Sim. ( ) Não. ( ) Não se aplica.

APÊNDICE E – CATÁLOGO DE CONTROLE DE PRIVACIDADE

Lacunas de Privacidade				
Informações Gerais				
Organização				
Sistema de Software				
Funcionalidade				
Problema				
Controles de Privacidade				
Princípios da LGPD: [1] Finalidade; [2] Adequação; [3] Necessidade; [4] Livre Acesso; [5] Qualidade de Dados; [6] Transparência; [7] Segurança; [8] Prevenção; [9] Não Discriminação; [10] Responsabilização e Prestação de Contas				
ID	**Controles de Privacidade**	**Artigos**	**Princípios**	**Diretrizes**
6.6.2.2	Provisionamento para acesso de usuário	Art. 46º e 49º	1, 3, 6, 7, 10	Convém que a organização mantenha um registro preciso e atualizado dos perfis dos usuários criados para os usuários que tenham sido autorizados a acessar o sistema de informação e os DP neles contidos. A implementação dos ID individuais de acesso do usuário permite que sistemas configurados identifiquem adequadamente quem acessou DP e quais acréscimos, exclusões ou mudanças foram feitas.
6.6.4.2	Procedimentos seguros de entrada no sistema (log-on)	Art. 46º e 49º	1, 3, 6, 7, 10	Onde requerido pelo cliente, convém que a organização forneça a capacidade para os procedimentos seguros

				de entrada para quaisquer contas de usuários sob o controle do cliente.
7.4.8	Descarte	Capítulo VII	1, 3, 6, 7	A escolha das técnicas de descarte do DP depende de um número de fatores, uma vez que uma técnica de descarte difere nas suas propriedades e resultado (granularidade da mídia física resultante, ou a capacidade para recuperar uma informação excluída de uma mídia eletrônica)
7.5.1	Identificando as bases para a transferência de DP entre jurisdições	Art. 7º	1, 5, 6, 7, 10	Uma transferência de DP pode estar sujeita a uma legislação e/ou regulamentação dependendo da jurisdição ou da organização internacional para a qual os dados estão para serem transferidos (e de onde eles se originam). Convém que a organização documente o *compliance* com estes requisitos como base para transferência.
7.5.2	Países e Organizações para os quais os DP podem ser transferidos	Capítulo V	1, 5, 6, 7, 10	Convém que as identidades dos países e das organizações internacionais, para os quais os DP possam possivelmente ser transferidos em uma

				operação normal, estejam disponíveis para os clientes. Convém que as identidades dos países que surjam do uso de subcontratados do tratamento de DP sejam incluídas.
7.5.3	Registro de transferência de DP	Capítulo V	1, 5, 6, 7, 10	Registros podem incluir transferências de terceiros de DP que tenham sido modificados como um resultado das obrigações no gerenciamento dos controladores, ou na transferência para terceiros para implementar solicitações legítimas dos titulares de DP, incluído solicitações para exclusão do DP (após o consentimento do cancelamento)
7.5.4	Registro de divulgação de DP para terceiros	Art. 37º	1, 5, 6, 7, 10	O DP pode ser divulgado durante o curso das operações normais. Convém que essas divulgações sejam registradas. Convém que quaisquer divulgações adcionais para terceiros, como aquelas que surgem de investigações legais ou de auditorias externas, sejam registradas. Convém que os registros incluam as fontes da divulgação e a

				fonte da autoridade que fez a divulgação.

APÊNDICE F – EXEMPLO DE PADRÃO DE PRIVACIDADE PARA O SISTEMA NISIA

Padrão de Privacidade de Acesso ao Sistema.

Conceito de Privacidade	Objetivo
Acesso	Limitar o acesso à informação e aos recursos de processamento da informação.
ID e Nome do Padrão	[PP01] Acesso ao Sistema
Problema	Convém que a organização forneça a capacidade para os procedimentos seguros de entrada para quaisquer contas de usuários sob o controle do cliente. E também forneça política de controle de acesso ao sistema e aplicações sejam controladas por um procedimento seguro.
Conformidade Legal (Referências)	Lei 13.709 – LGPD Art. 7º, inciso VI e VII; Art. 6º, inciso I, III, V e VII; Art. 46º e 49º. NBR ISO 27701, seção 6.6.4.2; NBR ISO 27002, seção 9.4.2
Descrição legal	Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, qualidade dos dados e segurança, responsabilidade e prestação de contas.
Ativos	Dados pessoais do titular e outras informações permitas durante o acesso ao sistema ou aplicação.
Vulnerabilidades	Evitar senhas transmitidas em texto claro durante o procedimento de entrada no sistema (log-on) pela rede, elas podem ser capturadas por um programa de *sniffer* de rede, instalado nela.
Solução ou Diretrizes	Convém que uma técnica de autenticação adequada seja escolhida para validar a identidade alegada de um usuário. Durante a autenticação, é requerida a verificação de identidade e uma forte autenticação, convém que métodos alternativos de autenticação para as senhas, como meios criptográficos, *smart cards*, *tokens* ou biometria, sejam usados. As senhas representam uma forma comum de prover identificação e autenticação com base no segredo de que somente o usuário é quem conhece, isso também pode ser obtido com protocolos criptográficos, então convém que a complexidade de autenticação do usuário seja apropriada para a classificação da informação a ser acessada.
Consequências	O procedimento para entrada no sistema deve ser configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada (log-on) revele o mínimo de informações desnecessárias a um usuário não autorizado.

Padrão de Privacidade de Coleta de Dados Pessoais.

Conceito de Privacidade	Objetivo
Coleta de Dados Pessoais	A organização deve limitar a coleta de dados pessoais a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.
ID e Nome do Padrão	[PP02] Coleta de Dados Pessoais
Problema	Assegurar que os processos e sistemas sejam projetados de tal forma que a coleta e o tratamento de dados pessoais estejam limitados ao que é necessário para o propósito identificado.
Conformidade Legal (Referências)	Lei 13.709 – LGPD Art. 6º, inciso III NBR ISO 27701, seção 7.2.1, 7.2.4, 7.4.1, B.8.2.3
Descrição legal	Antes de iniciar a coleta dos dados pessoais do(a) titular, o agente (i.e. comitê gestor dos dados) deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita. Sempre respeitando os limites legais, contratuais da finalidade, propósitos especificados e informados ao titular dos dados, limitando o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, livre acesso, qualidade dos dados, transparência e segurança, responsabilidade e prestação de contas.
Ativos	Dados pessoais e dados pessoais sensíveis do titular, durante o processo de coleta de dados.
Vulnerabilidades	Evitar que dados pessoais sejam utilizados para propósito de marketing e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de dado pessoal apropriado. A organização não pode fornecer este consentimento como uma condição para o recebimento do serviço.
Solução ou Diretrizes	Convém que a organização limite a coleta de dados pessoais para o uso adequado e o um mínimo que seja relevante e necessário na relação para os propósitos identificados. Isto inclui limitar a quantidade de dados pessoais que a organização coleta indiretamente (por exemplo, por meio de logs da web, logs de sistemas etc.). A organização deve obter e registrar o consentimento dos titulares de dados pessoais de acordo com os processos documentados. Convém que a organização assegure que os titulares de dados pessoais entendam o propósito para os quais os seus dados pessoais serão tratados. É responsabilidade da organização comunicar isto e documentar claramente para os titulares de dados pessoais. Sem uma clara declaração do propósito para tratamento, não é possível que o consentimento e as escolhas sejam dados adequadamente.
Consequências	A violação de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como uso indevido dos dados, fraude, danos materiais e comprometimento da reputação dos indivíduos.

Padrão de Privacidade de Armazenamento e Retenção de Dados Pessoais.

Conceito de Privacidade	Objetivo
Armazenamento	A organização deve determinar os elementos que são necessários para armazenar os dados pessoais tratados.
ID e Nome do Padrão	[PP03] Armazenamento e Retenção de Dados Pessoais
Problema	Convém que a organização não retenha dados pessoais por um tempo maior do que é necessário para os propósitos para os quais o dado pessoal é tratado. A organização deve documentar qualquer uso de mídia removível e/ou dispositivos para armazenamento de dados pessoais.
Conformidade Legal (Referências)	Lei 13.709 – LGPD Art. 16º NBR ISO 27701, seção 6.5.3 e 7.4.7
Descrição legal	Antes de iniciar a coleta dos dados de CPF e e-mail do(a) titular, o agente (i.e. comitê gestor dos dados) deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita. Sempre respeitando os limites legais, contratuais da finalidade, propósitos especificados e informados ao titular dos dados, e dispensando o consentimento por se tratar de execução de políticas públicas devidamente previstas em lei.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, livre acesso, qualidade dos dados, transparência, segurança, responsabilidade e prestação de contas.
Ativos	Dados pessoais e dados pessoais sensíveis do titular, durante a retenção e armazenamento dos dados pessoais.
Vulnerabilidades	Incidente de vazamentos de informações e uso inadequado dos dados pessoais.
Solução ou Diretrizes	A organização deve desenvolver e manter esquemas de retenção para as informações que ela guarda, considerando o requisito para retenção do dado pessoal por um tempo não maior do que é necessário. Esses esquemas devem considerar requisitos legais, regulamentares e de negócio, onde ocorrem conflitos com estes requisitos, uma decisão de negócio precisa ser tomada e documentada no que for apropriado. Convém que, quando possível, a organização use mídias físicas removíveis e/ou dispositivos que permitam a criptografia, quando do armazenamento de dados pessoais. Caso não sejam criptografadas, usar apenas quando for inevitável, e em situações em que a mídia e/ou os dispositivos não criptografados forem usados, convém que a organização implemente procedimentos e controles compensatórios (por exemplo, embalagens invioláveis) para tratar os riscos ao dado pessoal.
Consequências	O vazamento de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como uso indevido dos dados, fraude, danos materiais, multas e comprometimento da reputação dos indivíduos.

Padrão de Privacidade de Compartilhamento e Transferência de Dados Pessoais.

Conceito de Privacidade	Objetivo
Compartilhamento	A organização deve determinar os elementos que são necessários para o compartilhamento dos dados pessoais tratados.
ID e Nome do Padrão	[PP04] Compartilhamento e Transferência de Dados Pessoais
Problema	Em casos que os dados pessoais do(a) usuário(a) (i.e. titular do dado) poderão ser compartilhados, transferidos para outras jurisdições ou terceiros e/ou divulgados com outros órgãos externos.
Conformidade Legal (Referências)	Lei 13.709 – LGPD Art. 33º, inciso I, II, III, IV, V, VI, VII, VIII, IX; Art. 34º, inciso I, II, III, IV, V, VI; Capítulo V NBR ISO 27701, seção 7.5.3 e 8.5
Descrição legal	Convém que a organização informe ao usuário(a) (i.e. titular do dado) em tempo hábil sobre as bases para a transferência de dados pessoais entre jurisdições e de qualquer mudança pretendida nessa questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o consentimento ou contrato Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, qualidade dos dados e segurança, transparência, segurança, responsabilização e prestação de contas.
Ativos	Dados pessoais e dados pessoais sensíveis do titular, durante o compartilhamento, transferência e divulgação dos dados pessoais.
Vulnerabilidades	Compartilhar ou distribuir dados pessoais com terceiros fora da organização sem o consentimento do titular dos dados pessoais.
Solução ou Diretrizes	A transferência de dados pessoais entre jurisdições pode estar sujeita à legislação e/ou regulamentação, a depender da jurisdição ou organização para o qual o dado pessoal será transferido (e de onde se original). Convém que a organização documente a conformidade com esses requisitos com base para transferência. Convém que a organização informe ao titular do dado sobre qualquer transferência de dado pessoal incluindo transferência para: fornecedores; outras partes; outros países. Convém que a transmissão e o compartilhamento de dados pessoais precisam ser controlados, tipicamente para assegurar que somente pessoas autorizadas tenham acesso a sistemas de transmissão e sigam os processos apropriados para assegurar que dados pessoais sejam transmitidos sem comprometimento para os destinatários corretos.
Consequências	A violação de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como uso indevido dos dados, fraude, danos materiais, multa e comprometimento da reputação dos indivíduos.

Padrão de Privacidade de Descarte de Dados Pessoais

Conceito de Privacidade	Objetivo
Descarte	Convém que uma organização que trate dado pessoal assegure que, com base na jurisdição relevante, ela descarte o dado pessoal após um período especificado e que o sistema que opera aquela dado pessoal seja projetado de modo a facilitar esse requisito de exclusão.
ID e Nome do Padrão	[PP05] Descarte de Dados Pessoais
Problema	Convém que a organização tenha políticas, procedimentos e/ou mecanismos documentados para o descarte de dados pessoais e mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.
Conformidade Legal (Referências)	Lei 13.709 – LGPD CAPÍTULO VII NBR ISO 27701, seção 7.4.8
Descrição legal	Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, qualidade dos dados, segurança, responsabilidade e prestação de contas.
Ativos	Dados pessoais e dados pessoais sensíveis do titular, durante o descarte dos dados pessoais.
Vulnerabilidades	Vazamentos de informações de informações sensíveis para pessoas não autorizadas.
Solução ou Diretrizes	A escolha de técnicas de descarte dos dados pessoais depende de um número de fatores, uma vez que uma técnica de descarte difere nas suas propriedades e o resultado (por exemplo, na granularidade da mídia física resultante, ou a capacidade para recuperar uma informação excluída de uma mídia eletrônica). Fatores a considerar ao escolher uma técnica de descarte apropriada incluem, porém não estão limitados à natureza e a abrangência do dado pessoal a ser descartado, se existe ou não um metadado associado ao dado pessoal, e as características físicas da mídia na qual o dado pessoal é armazenado. Então convém que mídias contendo informações confidenciais sejam guardadas e destruídas de forma segura e protegida, como, por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização.
Consequências	A vazamentos de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como uso indevido dos dados, fraude, danos materiais, multa e comprometimento da reputação dos indivíduos.

APÊNDICE G – QUESTIONÁRIO DE AVALIAÇÃO DO G-Priv

G-Priv: Guia para Apoiar a Especificação de Requisitos de Privacidade em Conformidade com aLGPD

Caro(a) participante, obrigado por dedicar um pouco do seu tempo para responder a nossa pesquisa. O objetivo do survey é avaliar o Guia de Privacidade (G-Priv) em relação a sua utilidade e facilidade de uso para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD, sob a perspectiva dos engenheiros e analistas de requisitos.
Email:

SEÇÃO 1 - CONSENTIMENTO DE PARTICIPAÇÃO

O survey foi elaborado com base no Termo de Consentimento Livre e Esclarecido pelo Conselho Nacional de Saúde, Resolução 196/96.

A coleta de dados será realizada por meio de formulário eletrônico. É para esse procedimento que você está sendo convidado a participar.

Sua participação é voluntária e livre de qualquer remuneração ou benefício. Você é livre para recusar-se a participar, retirar seu consentimento ou interromper sua participação a qualquer momento.

Se você tiver qualquer dúvida em relação à pesquisa, pode me contactar através do telefone (83) 99122-3465 ou email: mn3@cin.ufpe.br.

1 - Neste caso, você concorda em participar do questionário?
( ) Sim
( ) Não

SEÇÃO 2 - PERFIL E EXPERIÊNCIA

Esta seção tem como objetivo identificar o perfil profissional do respondente e a experiência na área de privacidade de dados.

2 - Qual o seu papel na instituição em que você trabalha?
[ ] Administrador de Banco de Dados
[ ] Analista de Negócio
[ ] Arquiteto de Software
[ ] Analista de Requisitos
[ ] Analista de Sistemas
[ ] Analista de Suporte/ Analista de Infraestrutura
[ ] Designer (Designer de Interação) ou Especialista em Interação humano-Computador
[ ] Desenvolvedor *Back-end*
[ ] Desenvolvedor *Front-end*
[ ] Diretor Geral / *Chief Executive officer* (CEO), ou Proprietário
[ ] Dono do Produto
[ ] Encarregado de Dados / *Data protection Officer* (DPO)
[ ] Engenheiro de Software
[ ] Engenheiro de Requisitos
[ ] Especialista Legal / Jurista / Advogado(a)
[ ] Especialista em Privacidade

[ ] Especialista em Segurança da Informação
[ ] Gerente de Projeto ou Produto
[ ] Scrum Master
[ ] Testador ou Analista de Qualidade
[ ] Programador
[ ] Outros

3 - Qual é a sua escolaridade máxima?
[ ] Ensino Médio
[ ] Graduação
[ ] Pós-Graduação/ MBA
[ ] Mestrado
[ ] Doutorado

4 - Há quanto tempo você trabalha na indústria de software?
[ ] Menos de um ano
[ ] Entre 1 e 2 anos
[ ] Entre 3 e 5 anos
[ ] Entre 6 e 10 anos
[ ] Mais de 11 anos

5 - Há quanto tempo você trabalha com proteção de dados (privacidade de dados) em projetos de software?
[ ] Menos de um ano
[ ] Entre 1 e 2 anos
[ ] Entre 3 e 5 anos
[ ] Entre 6 e 10 anos
[ ] Mais de 11 anos
[ ] Eu não trabalho nessa área

6 - Qual é o tamanho da empresa que você trabalha?
[ ] 1-10 funcionários
[ ] 11-50 funcionários
[ ] 51-250 funcionários
[ ] 251-500 funcionários
[ ] 501-1000 funcionários
[ ] 1001-2000 funcionários
[ ] mais de 2000 funcionários

7 - Defina o tipo da sua organização:
( ) Setor Público
( ) Setor Privado

8 - Qual é a área de atuação da sua organização?
[ ] Auditoria
[ ] Automobilística
[ ] Comércio Exterior
[ ] Comunicação
[ ] Consultoria
[ ] Financeira
[ ] Gestão Ambiental

[ ] Jurídico
[ ] Logística
[ ] Marketing
[ ] Tecnologia e TI
[ ] Sustentabilidade
[ ] Saúde
[ ] Recursos Humanos
[ ] Universidade
[ ] Outros

9 - Qual é o seu grau de familiaridade com os princípios da Lei Geral de Proteção de Dados -LGPD (Art. 6º)?
( ) Conheço alguns detalhes da lei.
( ) Sei da existência da lei, mas não conheço em detalhes.
( ) Sou bastante familiarizado, mas não conheço todos os detalhes.
( ) Tenho profundo conhecimento da lei e seus detalhes.
( ) Não conheço nada da lei.

10 - A sua organização realiza iniciativas para garantir conformidade dos sistemas de software com a LGPD?
) Sim
( ) Não

11 - Caso sua resposta anterior tenha sido "sim", você poderia explicar brevemente quais são as iniciativas?

12 - Na sua opinião, quais são os principais desafios para garantir a conformidade dos sistemas de software com a LGPD?

SEÇÃO 3 - AVALIAÇÃO DO GUIA G-PRIV

O objetivo dessa seção é avaliar a facilidade de uso e utilidade do Guia G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD.

13 - A utilização do guia G-Priv é de fácil entendimento para mim. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

14 - A definição das etapas do G-Priv é clara e compreensível. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

15 - A utilização dos *templates* e artefatos do G-Priv é de fácil entendimento. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

16 - A definição dos papéis e responsabilidades dos atores envolvidos nas etapas do G-Priv ficou clara e compreensível. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)

( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

17 - Utilizar o Guia G-Priv para especificar requisitos de privacidade seria fácil para mim. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

18 - Utilizar o Guia G-Priv em meu trabalho me permitiria operacionalizar os requisitos de privacidade conforme a LGPD mais rapidamente. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

19 - A utilização do G-Priv é útil para evitar incidentes provenientes da má especificação de requisitos de privacidade. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

20 - Eu considero o G-Priv útil para especificar requisitos de privacidade. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

21 - Na minha organização, o uso do G-Priv seria uma abordagem útil para apoiar a especificação de requisitos de privacidade. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

22 - Pretendo usar o Guia G-Priv no futuro. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

23 - Acredito que o G-Priv pode ser utilizado em qualquer contexto organizacional ou sistema de software. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

24 - Minha capacidade de utilizar o G-Priv é limitada pela minha falta de experiência ou conhecimento em privacidade de dados. (1 discordo totalmente - 2 discordo parcialmente - 3 sou indiferente - 4 concordo parcialmente - 5 concordo totalmente)
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

25 - Na sua opinião, quais são os principais benefícios do Guia G-Priv?

26 - Você teria sugestões para melhoria e refinamento do Guia G-Priv?