Submission date: 20/06/2022
Resubmission date: 15/09/2022
Camera ready submission: 12/12/2022

Section: regular article

1st round notification: 05/09/2022
2nd round notification: 17/11/2022
Available online: 15/02/2023
Publication date: 15/02/2023

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

Moisés Neves Camêlo, Carina Alves

Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco – Brasil

mnc3@cin.ufpe.br, cfa@cin.ufpe.br

Abstract. *The General Data Protection Law (LGPD in Portuguese) aims to protect personal data, including in digital media, processed by a natural person or legal entity governed by public or private law. Currently, organizations need to implement several measures to ensure that their software systems are compliant with the law. However, the LGPD is complex for requirements analysts. In particular, it is difficult to interpret, extract and operationalize privacy requirements. This paper proposes a catalog of privacy patterns and a guide G-Priv to support the specification of privacy requirements in accordance with the LGPD. Finally, we conducted a survey with 18 professionals to evaluate the acceptance of G-Priv.*

Keywords*. Requirements Engineering; Privacy Requirements; General Data Protection Law (LGPD); Privacy Patterns.*

Resumo. *A Lei Geral de Proteção de Dados (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 de analistas de requisitos. Em particular, existem dificuldades para extrair e operacionalizar requisitos de privacidade. Este artigo propõe um catálogo de padrões de privacidade e um guia G-Priv, para auxiliar a especificação de requisitos de privacidade em conformidade com a LGPD. Finalmente, conduzimos um survey com 18 profissionais para avaliar o G-Priv.*

Palavras-Chave. *Engenharia de Requisitos; Requisitos de Privacidade; Lei Geral de Proteção de Dados (LGPD); Padrões de Privacidade.*

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 [Veja 2018]. Outro caso, que foi considerado um dos maiores vazamentos no país, revelou

Cite as: Camelo, M. & Alves, C. (2023). G-Priv: A Guide to Support LGPD Compliant Specification of Privacy Requirements (G-Priv: Um Guia para Apoiar a Especificação de Requisitos de Privacidade em Conformidade com a LGPD). iSys: Revista Brasileira de Sistemas de Informação (Brazilian Journal of Information Systems), 16(1), 2:1-2:32. DOI: 10.5753/isys.2023.2743

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 [Olhar Digital 2021]. Essas situações reforçam a fragilidade dos sistemas de software em relação a aspectos de privacidade, retratados nos 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].

Atualmente, os sistemas e serviços de software 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.

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 no dia 18 de setembro de 2020, 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].

A importância em proteger a privacidade dos dados pessoais vem crescendo 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 sistemas legados [Maldonado e Blum 2018].

A motivação desta 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 tais requisitos [Hadar el al. 2018; Canedo et al. 2020].

Como contribuição científica, este artigo propõe um guia chamado G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. O guia foi concebido a partir de *insights* obtidos a partir de entrevistas exploratórias com cinco analistas de requisitos. O guia G-Priv descreve um conjunto de artefatos incluindo padrões de privacidade. A proposta foi avaliada através de um *survey* com 18 profissionais. 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.

Este artigo está estruturado da seguinte forma: a seção 2 descreve a fundamentação teórica. A seção 3 descreve o método de pesquisa e apresenta os principais achados obtidos nas entrevistas exploratórias. A seção 4 apresenta uma proposta para especificar requisitos em conformidade com a LGPD. Finalmente, a seção 5 discute as conclusões, limitações e trabalhos futuros.

2. Fundamentação Teórica

2.1. Requisitos 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 de software.

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. Finalmente, 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.

2.2. Lei Geral de Proteção de Dados Pessoais (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 2018 e 2019]. Dentre os principais conceitos, destacamos os tipos de dados: **dado pessoal**, que é a informação relacionada a pessoa natural identificada ou identificável; **dado pessoal sensível**, que trata sobre origem racial, religião, saúde e opção sexual; **dado anonimizado**, que se refere ao dado relativo ao titular que não possa ser identificável; e **dado pseudonimizado**, que é o tratamento para perder associação ou link direto ou indireto do indivíduo, mas com possibilidade de recuperar a origem.

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 2018 e 2019], 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.

Diversas pesquisas têm sido realizadas para apoiar a aderência de sistemas de software e processos 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, assim como metodologias e técnicas usadas para especificá-los. 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 resultados semelhantes, Peixoto et al. (2020) identificaram que desenvolvedores têm pouco conhecimento sobre privacidade, pois a maioria deles não sabe como interpretar adequadamente os requisitos de privacidade, assim como muitos deles desconhecem a própria lei (LGPD). Araújo et al. (2021), propuseram o método LGPD4BP (LGPD for Business Process) para orientar empresas a avaliar e alcançar a conformidade dos processos de negócios com a LGPD. Carvalho et al. (2019) abordaram diversos desafios entre requisitos de transparência (Lei de Acesso a Informação - LAI) e privacidade (LGPD) em sistemas da informação. Por fim, Carvalho et al. (2021) discutem princípios éticos na aplicabilidade das leis de proteção e privacidade de dados.

2.3. Privacy By Design

O *Privacy by Design* é um conceito incialmente proposto por Ann Cavoukian. De acordo com Cavoukian (2010), o termo *privacy by design,* que também pode ser referido com a sigla "PbD", descreve a abordagem 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.

De acordo com Cavoukian (2010), o PbD deve permear por toda tecnologia, processos, culturas e governança das empresas e instituições. A autora propõe sete princípios que são descritos a seguir. **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. **Privacidade por padrão (*by default*)**: o princípio busca oferecer o nível máximo de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema ou negócio de TI. **Funcionalidade Total – soma positiva**, não soma zero: esse princípio busca acomodar todos os objetivos e interesses legítimos de uma maneira positiva. **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.

Visibilidade e Transparência: o 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. **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.

Seguindo o raciocínio de Ann Cavoukian ao concluir que somente as leis não garantem a privacidade, são necessárias metodologias de apoio para garantir que a privacidade seja considerada durante todo projeto de software. 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 46, §1º e 2º da Lei Geral de Proteção de Dados Pessoais, que expõem no texto da lei a adoção dos conceitos de *privacy by design e privacy by default* no corpo da sua redação [Brasil 2018].

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 necessária para qualquer tipo de organização que tem o objetivo de definir os requisitos de privacidade e prover um modelo para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). 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. Nossa pesquisa 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 Trabalhos Relacionados

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. 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) propuseram um catálogo para especificação de privacidade, onde o objetivo é ter *softgoals* de privacidade refinados, que limitem o uso e a divulgação de dados pessoais.

3. Método de Pesquisa

A seção apresenta a abordagem metodológica selecionada para a pesquisa. O objetivo da pesquisa é especificar requisitos de privacidades em conformidade com a LGPD, por parte dos analistas de requisitos, com o propósito de propor uma abordagem que auxilie de forma prática a operacionalização dessa atividade. Diante disso, e da motivação destacada na Seção 1, este artigo tem como objetivo investigar 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 analistas de requisitos na especificação de requisitos de privacidade em conformidade com a LGPD?

Para responder a QP1, conduzimos entrevistas exploratórias com analistas de requisitos para entender como eles estão adequando suas atividades para garantir a conformidade dos sistemas de software em relação a LGPD. Em particular, 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. A análise de dados promoveu a interpretação dos dados e as suas codificações. Os dados foram categorizados e organizados por temas superiores. A síntese dos dados discute os achados da pesquisa. Foi gerado um diagnóstico dos aspectos mais relevantes sobre a atividade de especificar requisitos de privacidade em conformidade com Lei Geral de Proteção de Dados a partir do ponto de vista de analistas de requisitos.

Com os resultados e *insights* obtidos através das entrevistas com analistas de requisitos, iniciamos a concepção de um catálogo de padrões de requisitos de privacidade e propusemos um guia de privacidade chamado G-Priv para auxiliar analistas de requisitos durante a especificação dos requisitos de privacidade. A proposta do G-Priv visa responder a QP2.

Por fim, a última etapa do estudo envolveu a execução de um *survey* com o objetivo de avaliar o guia G-Priv. 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 e desenvolvimento de software. A Figura 1 descreve as etapas para o desenvolvimento desta pesquisa.

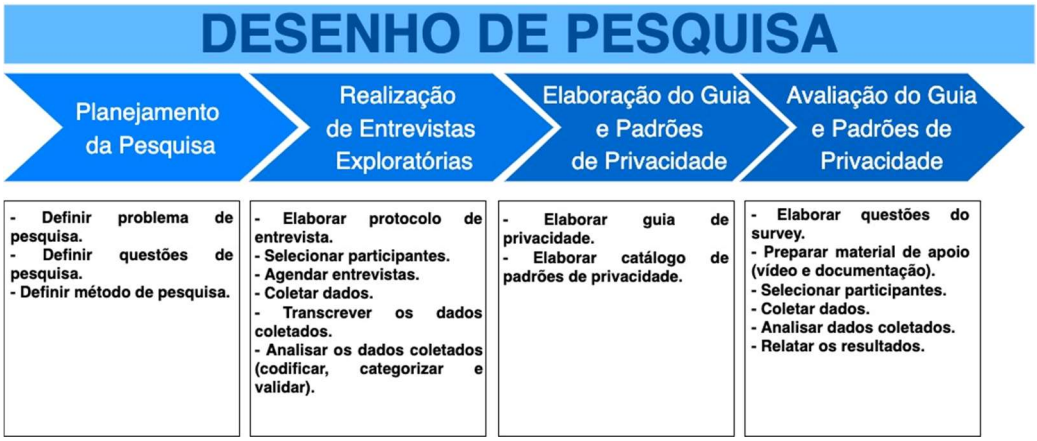


Figura 1. Etapas da pesquisa.

3.1. Realização de Entrevistas Exploratórias

Para entender o problema a partir de uma perspectiva prática, realizamos entrevistas exploratórias semiestruturadas com analistas de requisitos. Segundo Yin [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 com a elaboração de um protocolo de entrevista e a seleção de 5 (cinco) profissionais que atuam como analista de requisitos com o objetivo de investigar o ponto de vista 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 da Teoria Fundamentada de Dados – TFD [Flick, 2009; Merriam, 2009, Cruzes, 2014]. 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.

3.1.1 Coleta de Dados

Para realizar a coleta de dados, conduzimos entrevistas semiestruturadas com 5 analistas de requisitos de uma organização pública. 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 1 apresenta o perfil dos entrevistados.

As entrevistas ocorreram no período de outubro a dezembro de 2020 e utilizamos a ferramenta Cisco Webex de videoconferência. O protocolo de entrevista possui 27 questões e está disponível no Apêndice 1. Todas as entrevistas foram gravadas e

resultaram em cerca de seis horas e trinta minutos de gravação. 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.

Tabela 1. 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.

No momento de cada entrevista, foi feita a apresentação da motivação e do objetivo de pesquisa, política de confidencialidade, objetivos e resultados esperados. Na nossa pesquisa não houve submissão a um comitê de ética em pesquisa. No entanto, os pesquisadores se preocuparam com questões éticas explicitamente aplicado ao Termo de Consentimento Livre e Esclarecido (TCLE). Em cada entrevista, foram lidos o TCLE e a coleta de autorização realizada previamente no formulário elaborado no Google Forms. Além disso, solicitamos verbalmente a autorização para gravar a entrevista, e, se permitida, foi gravada. Estas informações estão disponíveis em [Camêlo, 2022].

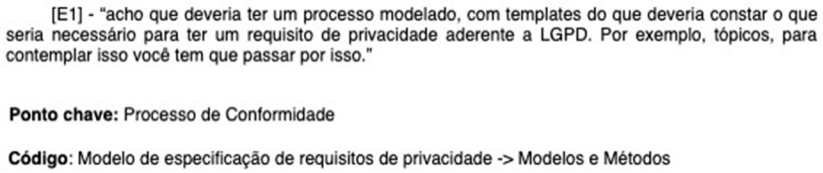
3.1.2 Análise de Dados

Durante a análise das entrevistas, 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. Segundo [Strauss e Corbin 1998], durante a codificação são identificados conceitos (ou códigos) e categorias. Um conceito 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 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. Este procedimento foi realizado nas cinco entrevistas, com o objetivo de identificar dados de potencial relevância, com semelhanças e diferenças para descrever o fenômeno em estudo e responder as 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 1998]. Na Figura 2, apresentamos o exemplo de um trecho de entrevista, com seu respectivo código. 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 onde elaboramos temas de ordem superior.


[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 a LGPD. Por exemplo, tópicos, para contemplar isso você tem que passar por isso."

Ponto chave: Processo de Conformidade

Código: Modelo de especificação de requisitos de privacidade -> Modelos e Métodos

Figura 2. Evidência da entrevista, ponto chave e código.

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, que são divididas em cinco passos: extrair dados; codificar dados, traduzir categorias; criar um modelo hierárquico de temas; avaliar a confiabilidade da síntese. Como apresentado na Figura 3, é possível identificar o processo de análise e refinamento dos dados, que iniciou com a leitura inicial das entrevistas transcritas, passando para a identificação de seguimentos específicos, seguindo para a codificação desses seguimentos, que identificados possibilitaram o agrupamento de códigos em categorias, para finalmente permitir o refinamento dos temas. 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. Cada etapa foi conduzida pelos autores de forma bastante cuidadosa e no final validamos as categorias obtidas com um dos profissionais que foram entrevistados.

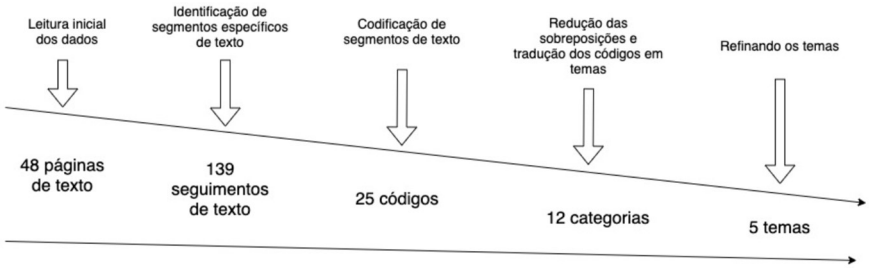


Figura 3. Processo de análise e refinamento de dados.

3.1.3 Síntese de Dados

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. Ao final do procedimento de análise dos dados coletados (codificação, categorização e refinamento dos temas superiores), os autores do artigo validaram durante várias reuniões os códigos, categorias e os achados de pesquisa extraídos nos trechos das entrevistas exploratórias. A Tabela 2 apresenta as categorias obtidas na síntese dos dados, e para cada categoria, apresentamos a frequência de ocorrências nas falas dos entrevistados. As categorias obtidas como síntese final das entrevistas são: processo de conformidade, obstáculos na conformidade, *tradeoff* entre privacidade e transparência, rotina de trabalho, conceitos de privacidade.

A partir da análise das percepções dos entrevistados, destacamos a necessidade de facilitar a interpretação da LGPD, com o objetivo de garantir a conformidade dos sistemas de software. Segundo os entrevistados, essa necessidade é originada dos desafios e dificuldades envolvidos para interpretar os detalhes da legislação. Em síntese, os entrevistados ressaltaram a necessidade de uma abordagem ágil e sistemática que auxilie os analistas de requisitos durante a especificação de requisitos de privacidade. Eles também citaram que as suas equipes possuem pouco conhecimento sobre a legislação de privacidade atual e tem dificuldades de como interpretá-la nos sistemas em desenvolvimento. Além disso, os entrevistados ressaltaram os conflitos com outras leis vigentes (e.g. LAI - Lei de Acesso à Informação). Finalmente, eles reforçaram a necessidade de mudança cultural das pessoas envolvidas no processo de conformidade entre os sistemas de software e a legislação vigente. Eles reforçaram a necessidade de uma melhor comunicação interna para disseminar boas práticas em privacidade de dados pessoais.

Tabela 2. Categorias obtidas nas Entrevistas

Categoria	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%

3.2 Elaboração do Guia G-Priv 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 guia G-Priv foi inspirado nos resultados das entrevistas exploratórias conforme detalhado na Seção anterior, onde os entrevistados reforçaram 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 Design*, conforme apresentado na seção 2.3 do referencial teórico, que tem o objetivo metodológico de proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação. 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. A elaboração do catálogo seguiu os conceitos e modelos de padrões de privacidade propostos na literatura. O catálogo de controles sugeridos pela Norma Técnica ISO 27701 também serviu de inspiração, que contém controles de privacidade mapeados pelos artigos da LGPD e suas respectivas diretrizes de privacidade, conforme descrito na seção 2.4.

3.3 *Survey* para Avaliação do Guia G-Priv

O *survey* é um método abrangente de pesquisa para coletar informações com o objetivo de descrever, comparar ou explicar o conhecimento, atitudes e comportamentos. Nesse artigo, elaboramos um *survey* através de um questionário eletrônico do Google Forms. O questionário apresentou informações gerais, como explicação do objetivo do estudo, uma explicação do tempo estimado para preencher o questionário e informações sobre a pesquisa.

Ao formular as perguntas, elaboramos 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. Dessa forma, as respostas abertas podem ser difíceis de codificar e analisar. As perguntas foram colocadas em uma 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 relação ao recrutamento de participantes, buscamos profissionais no círculo de contatos dos autores que se enquadravam no objetivo do estudo, ou seja, trabalham nas áreas de Engenharia de requisitos, Privacidade de dados, Desenvolvimento de software, Segurança da Informação e Análise de Sistemas. Diante disso, segundo Kitchenham (2008), podemos concluir que nossa amostragem é do tipo não probabilístico, 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. Dessa forma, consideramos que a seleção de participantes seguiu o critério de conveniência. Uma consideração importante durante a construção do questionário é o possível impacto de nosso próprio viés. Então, tomamos o cuidado na forma de elaborar o *survey*, evitando que as perguntas fossem descritas de uma forma tendenciosa visando confirmar um resultado desejado. Para isso, escrevemos instruções claras e imparciais, como também tentamos desenvolver perguntas neutras que cobriam adequadamente o tópico. Para validar a adequação e entendimento das questões do *survey* realizamos um teste piloto com um analista de requisitos sênior. Este analista também participou da entrevista da etapa anterior e estava familiarizado com o tema da pesquisa. Os resultados do teste piloto tiveram o objetivo de descartar, melhorar ou inserir novas questões, organizar as questões por seção, design, como também analisar o tratamento das respostas.

O objetivo principal do *survey* foi avaliar a facilidade de uso e a utilidade dos artefatos propostos no guia de privacidade (G-Priv) e no catálogo de padrões de privacidade, assim como obter a visão crítica dos participantes em relação ao funcionamento sistemático das etapas do guia. O *survey* foi respondido por 18 profissionais especialistas nas áreas de privacidade de dados e/ou engenharia de requisitos. Em nossa pesquisa, utilizamos o TAM (*Technology Acceptance Model*) para guiar a elaboração do *survey*. O TAM é um modelo 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, buscando entender o comportamento desses usuários através do conhecimento da utilidade e da facilidade de utilização percebida por eles (Davis 1989). Os construtos foram desenvolvidos de modo a captar opiniões pessoais, sendo assim, esse modelo foi útil para identificar o porquê da aceitação das características do G-Priv (atividade, atores envolvidos, fluxo das etapas e *templates*).

4 Abordagem Proposta

A partir da análise das percepções dos entrevistados, 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 organizacional 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, Lenhard et al. 2017]. A seguir apresentamos o catálogo de padrões de privacidade e o guia G-Priv.

4.1 Catálogo de Padrões de Privacidade

O catálogo de padrões de privacidade serve para guiar a especificação de requisitos de privacidade em conformidade aos princípios da LGPD. Ele é usado como orientação para reutilização de conhecimento sobre os controles de privacidade.

Para a elaboração do catálogo, seguimos o seguinte processo: incialmente, 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* que é descrito na Etapa 3 da Seção 4.5. As Tabelas 3 e 4 apresentam dois padrões, descrevendo os elementos:

- **Conceito de Privacidade** – são aspectos de privacidade e seus respectivos objetivos;
- **Contexto** – exemplifica uma situação em que se enquadra o conceito de privacidade;
- **Diretrizes** – têm o objetivo de direcionar a melhor estratégia para especificar e operacionalizar os requisitos de privacidade;
- **Referências** – fundamentam o referencial teórico de cada elemento de privacidade conforme o regimento da lei e da norma.

A Tabela 3 faz referência ao catálogo de padrão de privacidade de **Acesso à Informação**, extraído da Norma Técnica 27701. Esse padrão 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 2.2 da LGPD. De acordo com esse padrão, a organização deve limitar o acesso à informação e aos recursos de processamento de dados.

Tabela 3. 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 *(LOGIN)*
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 DE DADOS
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 devem incluir informação do titular sobre quais as mudanças foram feitas, e as razões porque as correções não foram realizadas (quando este for o caso).
Referências	NBR ISO/IEC 27701 7.3.6; Lei 13.709 – LGPD Art. 9º

A Tabela 4 apresenta o padrão de privacidade **Coleta de Dados Pessoais**, extraído da Norma Técnica 27701. Esse padrão 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 2.2 da LGPD. A organização deve limitar a coleta de dados pessoais a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados. Vale salientar que os analistas de requisitos podem reusar os padrões propostos e elaborar outros padrões que sejam adequados para o seu contexto organizacional e características do sistema de informação em desenvolvimento.

Tabela 4 – 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	DETERMINAR 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	OBTER E REGISTRAR 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

4.2 G-Priv: Guia para Apoiar a Especificação de Requisitos de Privacidade em Conformidade om a LGPD

Com o objetivo de apoiar a especificação dos requisitos de privacidade com a LGPD, propomos o guia G-Priv. O guia visa auxiliar analistas de requisitos, logo após a fase de

elicitação dos requisitos, quando há o entendimento do negócio, entendimento das necessidades dos *stakeholders*, entendimento do problema de privacidade e suas possíveis limitações. Nesse contexto, os analistas de requisitos necessitam 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*).

O guia G-Priv é composto por um fluxo de quatro etapas. 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 usando a notação BPMN (*Business Process Model and Notation*) na Figura 4. As etapas do guia estão descritas na Tabela 5. O guia disponibiliza vários 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. Os *templates* de artefatos estão disponíveis em https://figshare.com/s/e413e68c81c6cdcf9939.

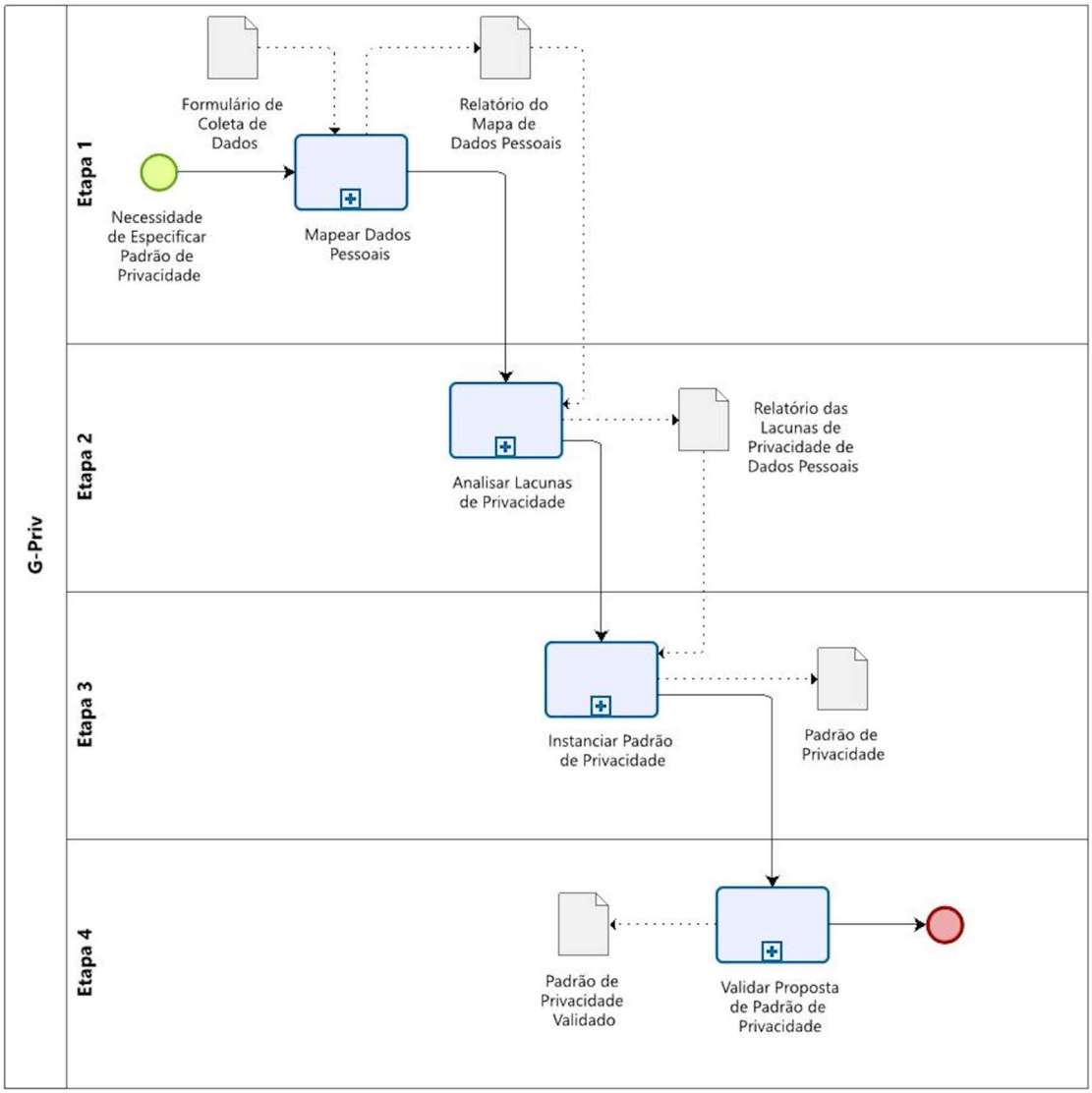


Figura 4 – Visão geral do Guia G-Priv.

Tabela 5 – 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.

A Tabela 6 apresenta os atores e suas respectivas responsabilidades, a fim de garantir uma definição clara das responsabilidades dos atores envolvidos no contexto de aplicação do guia. Nas seções a seguir, apresentamos cada etapa do guia G-Priv.

Tabela 6 – 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.

4.3 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, recomendamos 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 5 apresenta o detalhamento da Etapa 1. 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.

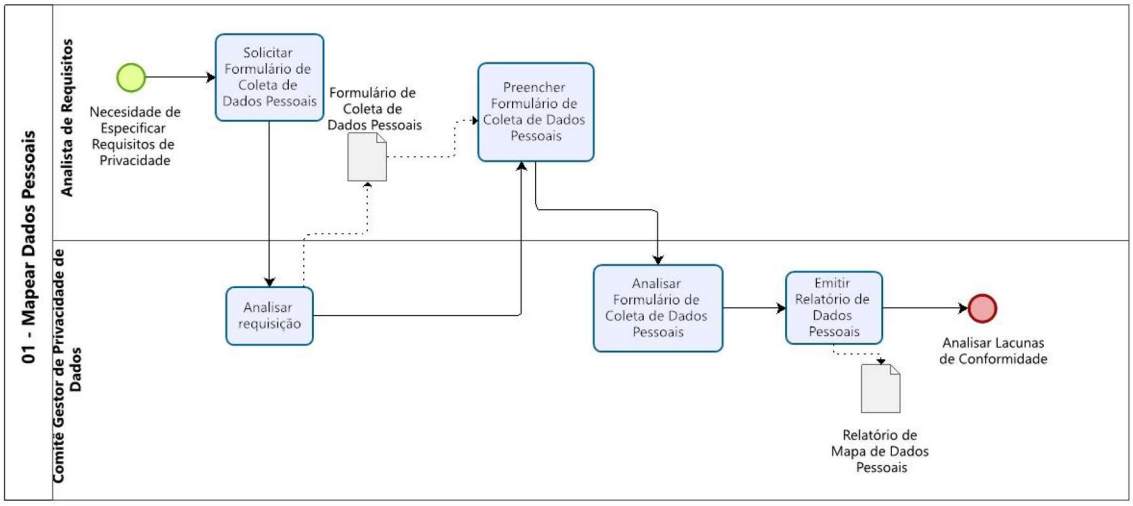


Figura 5. Etapa 1: Mapear Dados Pessoais.

4.4 Etapa 2: Analisar Lacunas de Privacidade

Após realizar o mapeamento dos dados pessoais, a segunda etapa do guia tem o objetivo de auxiliar na identificação e análise de 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. As questões do formulário de lacunas de privacidade foram inspiradas nas questões da proposta LGPD4BP [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 6 apresenta o detalhamento da Etapa 2. 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.

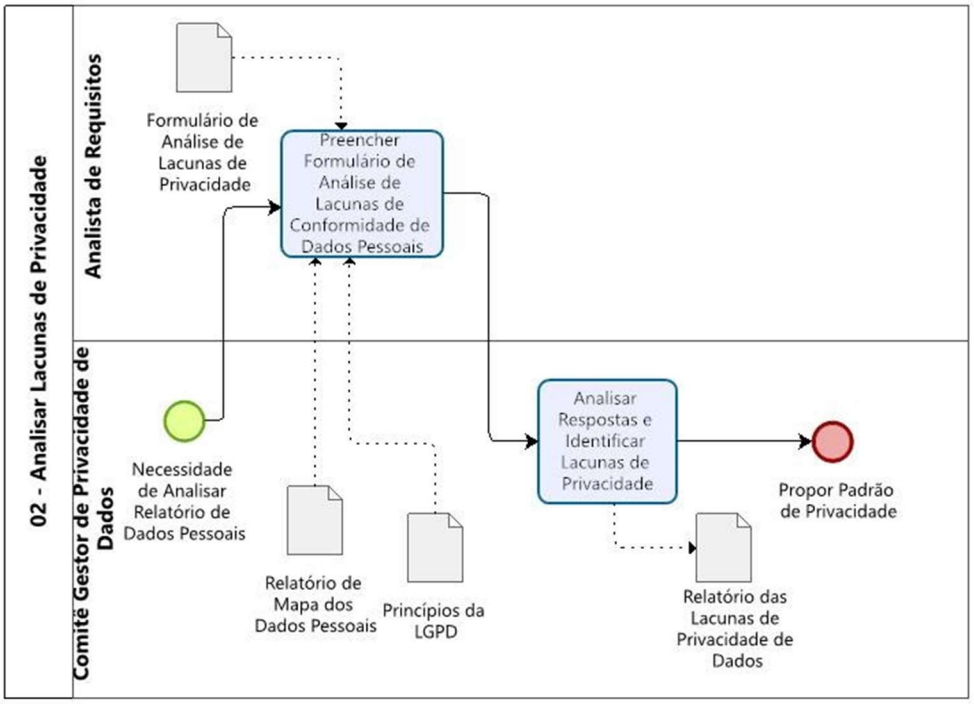


Figura 6. Etapa 2: Analisar Lacunas de Privacidade.

4.5 Etapa 3: Instanciar Padrão de Privacidade

A terceira etapa contempla a instanciação do padrão de privacidade e utiliza os 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 requisitos de privacidade, 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. 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. A Figura 7 apresenta o detalhamento da Etapa 3.

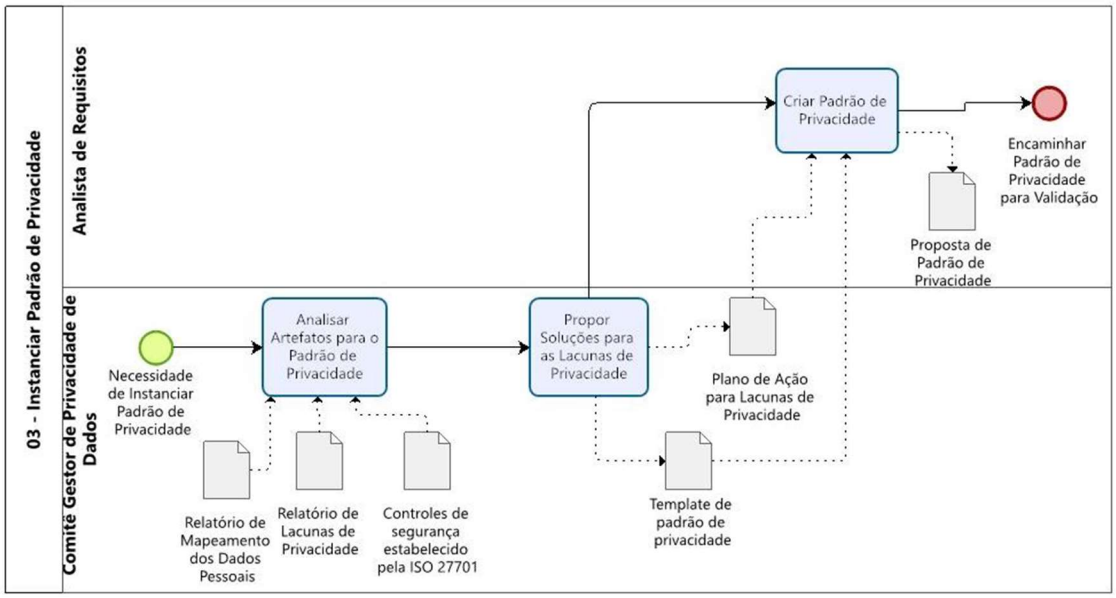


Figura 7 – Etapa 3: Instanciar Padrão de Privacidade.

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. Os padrões de privacidade precisam ser instanciados para atender as necessidades específicas de cada projeto de desenvolvimento e contexto organizacional que o sistema será inserido.

4.6 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, 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 envolvidos nessa 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 participação de especialistas jurídicos é fundamental para esclarecer dúvidas e apoiar a equipe de TI na operacionalização de requisitos de privacidade.

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 implementará a solução conforme especificado no padrão de privacidade. A Figura 8 apresenta o detalhamento da Etapa 4. 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.

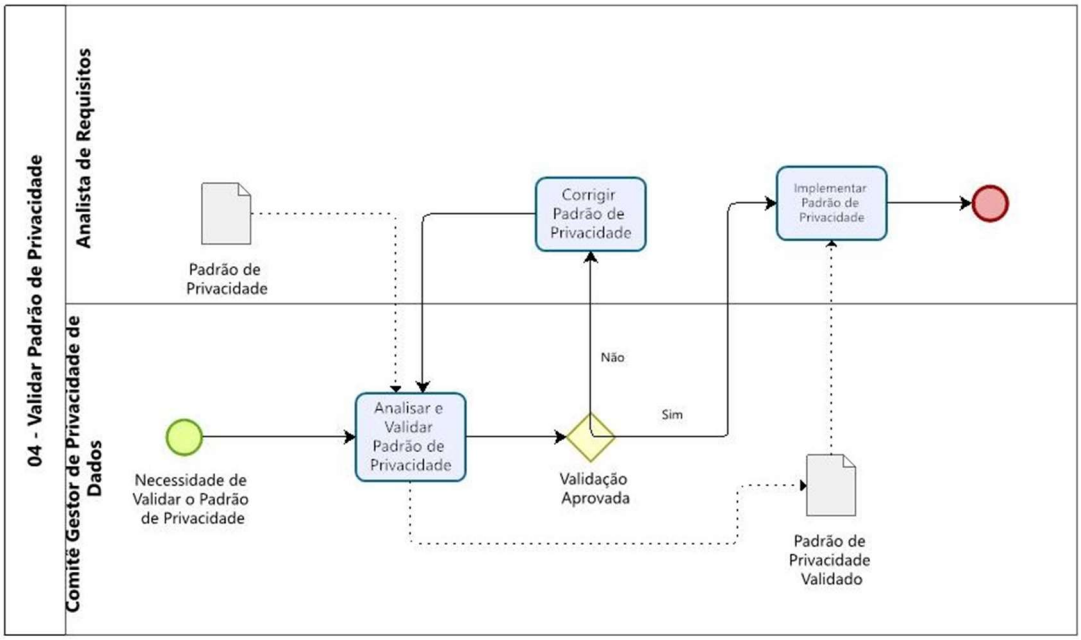


Figura 8 – Etapa 3: Validar Padrão de Privacidade.

5 *Survey* de Avaliação do G-Priv e Catálogo de Padrões de Privacidade

Para avaliar o guia G-Priv, conduzimos um *survey* com 18 profissionais. O objetivo do *survey* foi avaliar o G-Priv em relação a sua utilidade e facilidade de uso para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. A seleção dos participantes foi feita por conveniência a partir do círculo de contatos dos autores. O critério de seleção dos participantes do *survey* foi que eles estejam envolvidos em atividades relacionadas com a especificação de requisitos de privacidade em suas organizações. A pesquisa foi realizada no período de 18 de outubro até 07 de novembro de 2021. Para apoiar no entendimento sobre o guia G-Priv e no preenchimento do *survey*, produzimos um vídeo com orientações básicas sobre o uso do guia. Em conjunto com o vídeo, também foi disponibilizada a documentação completa do guia, essa descrição foi apresentada na seção anterior.

Os participantes trabalham em diversas organizações do setor público (55,6%) e privado (44,4%) de diferentes segmentos, conforme descrito na Figura 9. Eles desempenham diferentes papéis relacionados ao desenvolvimento de software, sendo em sua maioria analistas de requisitos/negócios (8 participantes), 7 engenheiros de software, 3 especialistas em segurança da informação. 14 (quatorze) dos participantes possuem mais de 11 anos de experiência na área de TI.

Figura 9 – Área de atuação dos participantes do *survey*

Observamos que 88,9% (dezesseis) dos participantes afirmam que suas organizações promovem iniciativas 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. Este resultado demonstra a relevância da área de privacidade no contexto do desenvolvimento de software.

De acordo com os resultados, todos participantes concordaram que o G-Priv é útil para apoiar a especificação de requisitos de privacidade. A maioria dos profissionais (16 participantes) acredita que o G-Priv foi concebido de maneira genérica e pode ser utilizado em qualquer contexto organizacional ou sistema de software, conforme ilustrado na Figura 10. O G-Priv foi considerado de fácil entendimento por 17 participantes, conforme descrito na Figura 11. Os participantes também concordaram com a agilidade na operacionalização de especificação dos requisitos de privacidade, como ilustra a Figura 12.

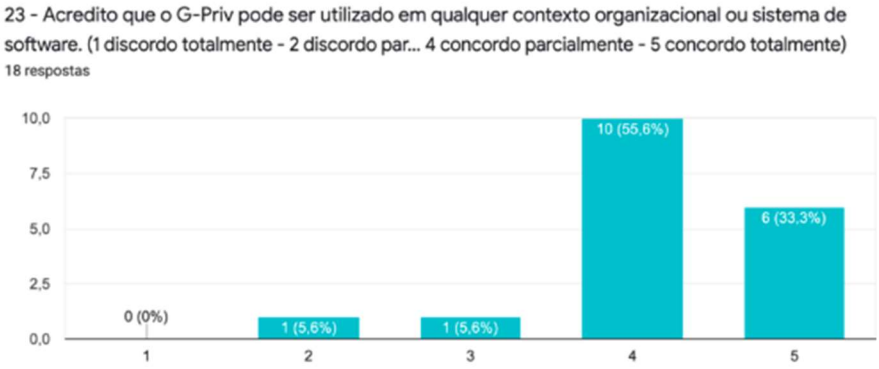


Figura 10 – Utilidade do G-Priv em diferentes contextos.

Figura 11 – Percepção dos participantes sobre a facilidade de entendimento do G-Priv.

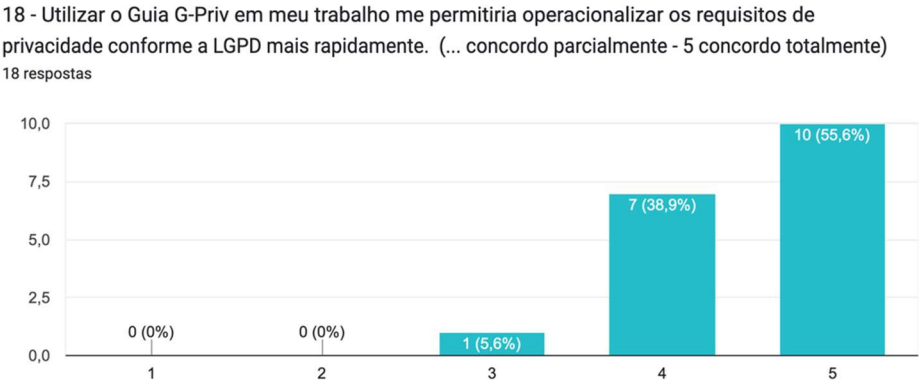


Figura 12 – Percepção dos participantes sobre a agilidade de operacionalizar requisitos de privacidade com a adoção do G-Priv.

Nas perguntas abertas, abordamos os temas de benefícios e as sugestões de melhorias do G-Priv. Em relação aos benefícios, os participantes citaram: padronização da especificação dos requisitos de privacidade, conjunto dos artefatos ofertados pelo guia, etapas e interações bem definidas entre os atores. Dentre as principais sugestões de melhorias, eles propuseram: disponibilizar todos os padrões de privacidade exigidos para tratamento de dados discutidos no Art. 5º da LGPD, adequar os papéis propostos pelo guia no contexto de organizações de pequeno porte, incluir a visão do cliente para alertar que uma determinada solicitação pode ferir a LGPD. Em síntese, consideramos que o guia obteve uma boa aceitação pelos profissionais que participaram do *survey*.

6. Conclusões, Ameaças à Validade e Trabalhos Futuros

Nessa pesquisa, realizamos entrevistas exploratórias com analistas de requisitos para entender o ponto de vista desses profissionais em relação às práticas e desafios enfrentados na especificação de requisitos de privacidade em conformidade a LGPD. Os resultados das entrevistas exploratórias revelaram que os analistas de requisitos consideram que é necessário investir em capacitação e comunicação interna para

disseminar aspectos de privacidade. Eles também citaram que as suas equipes possuem pouco conhecimento sobre a LGPD e tem dificuldades de como interpretá-la nos sistemas em desenvolvimento. Em síntese, os entrevistados ressaltaram a necessidade de uma abordagem ágil e sistemática que auxilie os analistas de requisitos durante a especificação de requisitos de privacidade. Os *insights* obtidos durante as entrevistas foram bastante úteis para elaborarmos a nossa proposta.

Como principal contribuição desse artigo, elaboramos um catálogo de padrões de privacidade e guia G-Priv, que têm o objetivo de auxiliar os analistas de requisitos durante a especificação dos requisitos de privacidade em conformidade com a LGPD. Nosso guia de privacidade foi inspirado no GuideMe [Ayala-Rivera et al, 2018] e nos conceitos do *Privacy by Design* [Cavoukian 2020]. Vale salientar que a abordagem GuideMe tem como referencial a GDPR da União Europeia, enquanto nossa proposta é baseada na legislação brasileira da LGPD. Nossa proposta visa contribuir com a disseminação de conhecimento sobre a importância de garantir a privacidade de dados pessoais em sistemas de software.

Conforme discutido na Seção 2.1, as pesquisas realizadas por Peixoto et al. (2020), Gharib et al. (2020) e Cysneiros e Yu (2004) envolveram a definição de modelos para representar e sintetizar conceitos de privacidade. De forma diferente, nossa proposta de guia representa uma contribuição com enfoque mais prático para apoiar analistas de requisitos. Em particular, nossa proposta apresenta um conjunto de *templates* para apoiar a implantação do guia. Ela está embasada na construção de uma perspectiva de conformidade dos requisitos de um sistema de software com a LGPD, que se consolida com a elaboração de um Padrão de Privacidade. A partir do padrão de privacidade, os analistas de requisitos poderão assegurar a conformidade legal dos sistemas de software, que contenham o tratamento de dados pessoais de acordo com os princípios da LGPD. Assim, concluímos que o G-Priv tem o objetivo de auxiliar os analistas de requisitos na operacionalização da interpretação de lei de privacidade de dados pessoais de maneira prática e ágil, durante a fase de especificação de requisitos do processo de software.

Para avaliar a utilidade e facilidade de uso do guia, conduzimos um *survey* com 18 profissionais. Os resultados do survey confirmaram que o guia teve uma boa aceitação pelos participantes. Uma percepção que teve destaque nos resultados das entrevistas 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 referentes à conformidade dos sistemas com a LGPD. 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. Outro ponto que teve destaque nas falas dos entrevistados e participantes do *survey* foi referente aos desafios para conduzir uma mudança cultural e na mentalidade das pessoas envolvidas no processo de privacidade de dados pessoais.

Consideramos que esta pesquisa consiste em uma relevante contribuição para a academia e indústria, especialmente para organizações carentes de um processo sistemático que contemple a especificação de requisitos sob o prisma de privacidade de dados pessoais. Para isso, elaboramos um catálogo de padrões de privacidade e guia aplicável e instanciável para qualquer organização, que necessite desenvolver sistemas em conformidade com a LGPD. Em síntese, nossa 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.

Em relação às ameaças à validade da pesquisa, a validade de constructo foi um fator crítico durante o estudo pois vimos que participantes poderiam interpretar o guia de forma diferente do nosso propósito. Uma consideração importante durante a construção do survey é o impacto de um possível viés de como as perguntas foram elaboradas. Tomamos bastante cuidado na forma de elaborar o *survey* de maneira objetiva e imparcial, evitando que as perguntas fossem dirigidas de forma a confirmar um resultado desejado. Mesmo assim, outra limitação que pode afetar a validade da pesquisa trata-se da interpretação e entendimento dos participantes sobre os termos usados nas perguntas do *survey*. É possível que eles tenham tido dificuldade de interpretar algumas perguntas do *survey*. Além disso, consideramos uma eventual dificuldade de comprometimento com o tempo para assistir o vídeo explicativo e estudar os artefatos do guia a fim de responder o *survey*. Esta ameaça foi mitigada através de validações dos instrumentos de pesquisa com um analista de requisitos sênior para garantir a clareza das perguntas tanto da entrevista como do survey. Também é importante salientar que os dados coletados durante as entrevistas são referentes às opiniões pessoais dos entrevistados, não sendo necessariamente a realidade das suas organizações. Como forma de tratar esta ameaça, buscamos selecionar analistas de diferentes equipes, com mais de 10 anos de experiência na área e que desempenham cargos gerenciais, tendo assim uma visão mais ampla sobre os processos corporativos. Em relação à validade externa, como as entrevistas foram realizadas com apenas 5 analistas e o survey foi respondido por 18 participantes, não podemos afirmar que os resultados possam ser amplamente generalizados. Consideramos que é necessário realizar estudos de caso envolvendo a implantação do guia em diferentes contextos organizacionais para avaliar a sua adequação e ampla adoção. Para facilitar a utilização do guia, elaboramos diversos *templates* e exemplos de padrões de privacidade. Apesar dessas limitações, acreditamos que os nossos resultados apresentam evidências qualitativas e *insights* ricos para avançar no entendimento sobre requisitos de privacidade.

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 ferramenta Web. Acreditamos que uma ferramenta pode deixar o guia mais prático e ágil na sua operacionalização. Além disso, atualmente o guia está sendo aplicado em organizações. Após participação no survey, alguns servidores de órgãos públicos e profissionais da indústria solicitaram a utilização do guia para especificar requisitos de privacidade no desenvolvimento dos sistemas de software das suas organizações. A partir dessas experiências práticas, será possível realizar novos estudos para analisar a adequação do guia em diferentes contextos a fim de evoluir nossa pesquisa na área.

Referências

Anthonysamy, P., Rashid A., Chitchyan, R. (2017) Privacy Requirements: Present & Future. IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track.

Ayala-Rivera, V., e Pasquale, L. (2018) “The Grace Period Has Ended”: An Approach to Operationalize GDPR Requirements. IEEE 26th International Requirements Engineering Conference.

Araújo, E., Vilela, J., Silva, C., Alves, C. (2021) 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.

Associação Brasileira de Normas Técnicas (2019). 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.

Brasil (2018). 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 . Acessado: 13/04/2021 (em Português Brasileiro).

Brasil (2019). Emenda Nº 13.853, De 8 De Junho De 2019. Emenda da Lei Nº13.709 de 14 de agosto de 2018, Brasília, DF, jun 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm . Acessado: 09/09/2022 (em Português Brasileiro).

Camêlo, N. M., (2022). G-Priv: um guia para especificação de requisitos de privacidade em conformidade com a LGPD. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2022.

Canedo, E. D., Calazans, A. T. S., Masson, E. T. S., Costa, P. H. T., Lima, F. (2020) Perceptions of ITC Practitioners Regarding Software Privacy. Entropy.

Carvalho, L. P., Oliveira, J., Cappelli, C., Majer, V. (2019) Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. Workshop de Transparência em Sistemas (WTRANS).

Carvalho, L. P., Oliveira, J., Santoro, F. M., Cappelli, C. (2021) Social Network Analysis, Ethics and LGPD, considerations in research. iSys: Revista Brasileira de Sistemas de Informação (Brazilian Journal of Information Systems), 14(2), 28-52. DOI: 10.5753/isys.2021.1235

Cavoukian, A. (2010). Privacy by Design: The 7 Foudational Principles –Implementation and Mapping of Fair Information Practices. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbdimplement-7found-principles.pdf. Acessado: 11/04/2020 (em Português Brasileiro).

Cruzes, D. e Dyba, T. (2011) Recommended Steps for Thematic Synthesis in Software Engineering. International Symposium on Empirical Software Engineering and Measurement.

Cysneiros, L. M., Yu, E. (2004) Non-Functional Requirements Elicitation. The Springer International Series in Engineering and Computer Science, pp 115-138.

Davis, F. D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information technology. MIS Quartely, Vol. 13.

EU (2016) Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. General Data Protection Regulation. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acessado: 18/04/2022 (em Português Brasileiro).

Flick, U. (2009) Introdução à pesquisa qualitativa; tradução Joice Elias Costa – 3ª ed. – Porto Alegre, pp. 37, 2009.

Franch, X., Palomares, C., Quer, C., Renaut, S., Lazzer, F. (2010) A Metamodel for Software Requirements Patterns, International Working Conference on Requirements Engineering: Foundation for Software Quality. REFSQ 2010.

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

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018) Privacy by designers: software developers' privacy mindset. Empirical Software Engineering.

Kalloniatis, C.; Kavakli, E.; Gritzalis, S. (2008) Addressing privacy requirements in system design: the PriS method. Requirements Engineering. v.13, pp. 241-255.

Kalloniatis, C. (2017) Incorporating privacy in the design of cloud-based systems: a conceptual meta-model. Information & Computer Security. vol. 25, No. 5.

Lenhard, J., Fritsch, L. e Herold, S. (2017) A Literature Study on Privacy Patterns Research, 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA.

Maldonado, V. N., Blum, R. O. (2018) GDRP: Regulamento Geral de Proteção de Dados da União Europeia, Thompson Reuters Brasil Conteúdo e Tecnologia Ltda.

Maldonado, V. N., Blum, R. O. (2019) LGPD: Lei Geral de Proteção de Dados Comentada, Thompson Reuters Brasil Conteúdo e Tecnologia Ltda.

Martin, Y. S., Kung, A. (2018) Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering, IEEE European Symposium on Security and Privacy Workshops.

Merrian, S. B. (2009) Qualitative Research: a guide to design and implementation. 2009.

Olhar Digital (2021). Maior Vazamento de Dados no País. Disponível em: https://tinyurl.com/maiorvazamentodedados. Acessado: 13/04/2022 (em Português Brasileiro).

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

Strauss, A. e Corbin J. (1998) Basics of Qualitative Research: Grounded Theory Procedures and Techniques. London, 2 edição, Sage Publications.

Veja (2018). MP Investiga Operadora Telefônica por Uso Indevido de Dados Pessoais. Disponível em: https://veja.abril.com.br/economia/mp-investiga-se-vivo-faz-uso-indevido-de-dados-de-73-mi-de-usuarios/. Acessado: 13/04/2022 (em Português Brasileiro).

Webster, I.; Ivanova, V.; Cysneiros, L.M. (2005) Reusable Knowledge for Achieving Privacy: A Canadian Health Information Technologies Perspective. In Proceedings of the Anais do WER05—Workshop em Engenharia de Requisitos, Porto, Portugal, 13–14 June, 2005; pp. 112–122.

Yin, R. K. (2003) Estudo de Caso: Planejamento e Métodos. 2ª Edição, pp. 32 e 42.

Apêndice 1 - Roteiro de Entrevista

ETAPAS	PERGUNTAS
Apresentação	1. Realizar apresentação, explicar sobre a confiabilidade e pedir permissão para gravar.
Introdução	1. Explicar o objetivo da entrevista. 2. "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	1. Nome da empresa ou instituição. 2. Qual o segmento ou principal setor que sua organização opera? 3. Qual a sua função atual na organização? 4. Quantos anos de experiência você possui na área indicada?
Conhecimentos sobre privacidade	1. Na sua opinião, como a sua equipe entende o conceito de privacidade e proteção de dados pessoais, ao desenvolver um produto ou serviço? 2. 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)? 3. 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? 4. Sua organização específica de forma explícita requisitos de privacidade e proteção de dados? De que forma? 5. Após a especificação dos requisitos, como é realizada a verificação e validação dos requisitos de privacidade para garantir a conformidade legal? 6. Para garantir a conformidade legal dos requisitos de privacidade especificados, existe apoio jurídico? 7. Sua organização faz algum tipo de distinção por usuário? Como por exemplo, determinados usuários são mais críticos que outros, então neste caso há uma preocupação maior com a privacidade. 8. Esses dados (requisitos) coletados, podem ser acessados a qualquer momento pelos stakeholders, como também atualizados ou corrigidos? 9. Sua organização compartilha requisitos ou regras de negócio? Se sim, com quem e qual a finalidade? 10. 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	1. Pela sua experiência, quais são os requisitos não funcionais de segurança mais exigidos pelos usuários? E qual a relevância no desenvolvimento do produto? 2. A sua equipe documenta de forma explícita requisitos de privacidade ao desenvolver um produto ou serviço? Como esses requisitos são descritos? 3. 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? 4. Há histórico de incidentes de vazamento ou exposição de dados, por não 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	1. Como a LGPD está impactando o desenvolvimento de novos sistemas ou a conformidade de sistemas já em operação? 2. Na sua opinião, quais são os principais desafios e as dificuldades para garantir a conformidade entre a LGPD e os sistemas da sua organização? 3. Na sua opinião, quais ferramentas, métodos ou modelos podem apoiar a especificação de requisitos de privacidade durante o desenvolvimento de um produto ou serviço? 4. Elabore uma visão prática de como sua equipe se resguarda ou enfrenta o problema de vazamento ou exposição de dados?
Encerramento e Agradecimento	1. Você tem alguma coisa a mais para acrescentar sobre o tema de requisitos de privacidade e proteção de dados? 2. Alguma pergunta que você gostaria de acrescentar que não foi colocada aqui?