DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 29100: Aplicação Prática no Open Banking Brasil

Sâmmara Éllen Renner Ferrão

Brasília, 12 de julho de 2022

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSAL FOR A PRIVACY REQUIREMENT TAXONOMY BASED ON THE LGPD AND ISO/IEC 29100: PRACTICAL APPLICATION AT THE OPEN BANKING BRASIL

PROPOSTA DE UMA TAXONOMIA DE REQUISITOS DE PRIVACIDADE BASEADA NA LGPD E ISO/IEC 29100: APLICAÇÃO PRÁTICA NO OPEN BANKING BRASIL

SÂMMARA ÉLLEN RENNER FERRÃO

ORIENTADORA: EDNA DIAS CANEDO

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.018
BRASÍLIA/DF, JULHO - 2022

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 29100: Aplicação Prática no Open Banking Brasil

Sâmmara Éllen Renner Ferrão

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Professora Dra. Edna Dias Canedo, Ph.D, FT/UnB _____
Orientadora

João Paulo Abreu Maranhão, Ph.D, Exército Brasileiro, Centro de Desenvolvimento de Sistemas _____
Examinador Externo

Professora Dra. Fabiana Freitas Mendes, FGA/UnB _____
Examinadora Interna

Prof. Dr. Georges Daniel Amvame-Nze, FT/UnB _____
Membro Suplente

FICHA CATALOGRÁFICA

FERRÃO, SÂMMARA ÉLLEN RENNER
Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 29100:Aplicação Prática no Open Banking Brasil [Distrito Federal] 2022.
xvi, 148 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Requisitos de Privacidade
2. Taxonomia
3. LGPD
4. ISO 29100
5. Open Banking

I. ENE/FT/UnB
II. Proposta de uma Taxonomia de Requisitos de Privacidade e sua aplicação ao Open Banking Brasil

REFERÊNCIA BIBLIOGRÁFICA

FERRÃO, S.E.R. (2022). *Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 29100:Aplicação Prática no Open Banking Brasil*. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.018, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 148 p.

CESSÃO DE DIREITOS

AUTOR: Sâmmara Éllen Renner Ferrão
TÍTULO: Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 29100:Aplicação Prática no Open Banking Brasil.
GRAU: Mestre em Engenharia Elétrica ANO: 2022

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado Profissional e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Os autores reservam outros direitos de publicação e nenhuma parte dessa Dissertação de Mestrado Profissional pode ser reproduzida sem autorização por escrito dos autores.

Sâmmara Éllen Renner Ferrão
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho aos meus pais que são meu alicerce e fonte de inspiração na busca de crescimento pessoal e intelectual. Mas principalmente dedico à minha mãe que como professora me mostrou o valor de contribuir para a educação e por ser uma força da natureza que me inspira na buscar pelo conhecimento.

AGRADECIMENTOS

Agradeço primeiramente à Deus pela dádiva da vida e pela oportunidade de construir conhecimento. Agradeço especialmente à minha família e meu companheiro de vida por todo apoio nos momentos mais difíceis e por não me deixar desistir, por entender os momentos de ausência e por continuarem a me dar amor e compreensão. Também agradeço à minha orientadora Edna Dias Canedo por não desistir de me apoiar neste desafio, por todas as inúmeras contribuições para esse trabalho e por me inspirar nessa longa jornada. Não poderia deixar de agradecer também à Universidade de Brasília pela oportunidade impar de contribuir mesmo que minimamente para esse curso e pelos professores pela dedicação mesmo durante essa fase tão incerta de nossas vidas devido a esta pandemia. Por fim, gostaria de agradecer a CAPES pelos convênios estabelecidos nos permitindo a execução de nossas pesquisas utilizando as diversas bases internacionais que contribuíram diretamente nos resultados deste trabalho.

RESUMO

Contexto: A preocupação com a privacidade de dados é algo que vem se destacando ao longo dos anos no mundo. No Brasil a Lei Geral de Proteção de Dados (LGPD) [42] foi publicada em agosto de 2018 e entrou em vigor dois anos após a sua publicação. Porém, algumas dificuldades ainda são enfrentadas pelas equipes de desenvolvimento na adequação dos mecanismos tecnológicos por parte das organizações que ainda estão em processo inicial de conformidade à LGPD [56]. **Objetivo:** Este trabalho propõe uma taxonomia de requisitos de privacidade baseada na LGPD e na ISO/IEC 29100 com o objetivo de apoiar as equipes de desenvolvimento de software no alcance da conformidade com os princípios da LGPD. **Método:** Foi realizada uma revisão sistemática de literatura (RSL) para identificar as taxonomias de privacidade de dados existentes na literatura com o objetivo de apoiar a elaboração da taxonomia proposta neste trabalho e a sua aplicação no projeto do Open Banking Brasil (OPB). Esse projeto é adequado pois compartilha os dados dos seus clientes a partir de seu consentimento, que está fundamentado na LGPD, tornando-se um projeto interessante para avaliação da aderência à legislação. A aplicação prática da taxonomia proposta foi realizada no processo de solicitação de consentimento e nos termos e condições de três bancos brasileiros a partir da aplicação da taxonomia proposta através de um formulário. **Resultado:** A RSL identificou 10 estudos primários, mas nenhum deles propuseram uma taxonomia de requisitos de privacidade no contexto da LGPD. A taxonomia proposta gerou 129 requisitos, divididos em 10 categorias e 5 contextos. A aplicação prática da taxonomia resultou em um percentual satisfatório de aderência aos requisitos de privacidade. **Conclusão:** Portanto, a aplicação da taxonomia em um contexto real demonstrou que a taxonomia pode apoiar as equipes de desenvolvimento de software na busca pela adequação à LGPD dos requisitos de privacidade especificados pelas equipes de desenvolvimento.

ABSTRACT

Context: The concerning about data privacy has been highlighted over the years on the world. In Brazil the General Data Protection Law (LGPD) [42] was published in August 2018 and entered into force two years after its publication. However, some primor difficulties are still faced into the institution by the praticioners in the process of complying to LGPD [56] yet. **Goal:** This work proposes a taxonomy of privacy requirements based on LGPD and ISO/IEC 29100 in order to support software development teams in achieving compliance with LGPD principles. **Method:** A Systematic Literature Review (SLR) was carried out to identify existing data privacy taxonomies in the literature in order to support the elaboration of the taxonomy proposed in this work and

its application in the Open Banking Brazil project (OPB). This project is suitable as it shares its customers' data based on their consent, which is based on LGPD, making it an interesting project to assess compliance with the legislation. The practical application of the proposed taxonomy was carried out in the consent request process and in the terms and conditions of three Brazilian banks from the application of the proposed taxonomy through a form. **Result:** The SLR identified 10 primary studies, but none of them proposed a taxonomy of privacy requirements in the context of LGPD. The proposed taxonomy generated 129 requirements, divided into 10 categories and 5 contexts. The practical application of the taxonomy resulted in a satisfactory percentage of adherence to privacy requirements. **Conclusion:** Therefore, the application of the taxonomy in a real context demonstrated that the taxonomy can support software development teams in the search for compliance with LGPD of the privacy requirements specified by the development teams.

SUMÁRIO

1 Introdução 1
1.1 Problema de Pesquisa 3
1.2 Justificativa 4
1.3 Objetivos 5
1.3.1 Objetivo Geral 5
1.3.2 Objetivo Específico 5
1.4 Metodologia de Pesquisa 5
1.5 Resultados Esperados e Contribuição 6
1.6 Publicações 7
1.7 Estrutura da Dissertação 7

2 Fundamentação Teórica 8
2.1 Engenharia de Requisitos 8
2.2 Privacidade de dados 9
2.3 General Data Protection Regulation - GDPR 10
2.4 Lei Geral de Proteção de Dados Pessoais - LGPD 12
2.5 ISO/IEC 29100 15
2.6 Open Banking 17
2.7 Trabalhos correlatos 20
2.8 Síntese do Capítulo 22

3 Revisão Sistemática de Literatura 24
3.1 Planejamento da Revisão 24
3.2 Condução 25
3.2.1 Estratégia de Pesquisa 25
3.2.2 Critérios de Seleção 25
3.2.3 Avaliação da Qualidade dos Estudos 26
3.2.4 Extração dos dados 27
3.3 Resultado da RSL 28
3.3.1 Resultado da triagem dos artigos e Avaliação de Qualidade 28
3.3.2 QP.1 Quais são as taxonomias de requisitos de privacidade existentes na literatura? 30
3.3.3 QP.2 Existe na literatura alguma taxonomia de requisitos de privacidade baseada na LGPD and ISO/IEC? 36
3.4 Síntese do Capítulo 36

4 Taxonomia 37

4.1 Desenvolvimento da Taxonomia Proposta 37
4.2 TP1 - Identificação de Requisitos de Privacidade 39
4.3 TP2 - Classificação dos requisitos de privacidade 43
4.4 TP3 - Refinamento dos requisitos de privacidade 49
4.5 Taxonomia de Requisitos de Privacidade LGPD+ISO/IEC 29100 50
4.6 Comparação da composição das taxonomias 62
4.7 Síntese do Capítulo 65

5 Aplicação da Taxonomia de Requisitos de Privacidade no Open Banking Brasil 66
5.1 Síntese do Capítulo 69

6 Resultados 70
6.1 Resultados da aplicação da Taxonomia em um contexto real ... 70
6.1.1 Finalidade 71
6.1.2 Adequação 75
6.1.3 Necessidade 76
6.1.4 Livre Acesso 77
6.1.5 Qualidade dos Dados 78
6.1.6 Transparência 78
6.1.7 Segurança 80
6.1.8 Prevenção 80
6.1.9 Não Discriminação 81
6.1.10 Responsabilização e Prestação de Contas 81
6.2 Discussão dos Resultados 82
6.3 Limitações do Estudo 83
6.3.1 Ameaças à Validade 84

7 Conclusão 86
7.1 Trabalhos Futuros 86

REFERÊNCIAS BIBLIOGRÁFICAS 87

Apêndices 95
I.1 Desenvolvimento da Taxonomia 96
I.2 Tabelas de Requisitos geradas na proposição da taxonomia ... 101
I.3 Processo de solicitação de Consentimento para o Compartilhamento de Dados do Open Banking 133

LISTA DE FIGURAS

1.1 Metodologia de Pesquisa. (Fonte: Autora) 6

2.1 Papéis da LGPD e o relacionamento com o processo de tratamento de dados. (Fonte: Autora) 14
2.2 Violações por Segmento. (Elaborado pela autora a partir de [11]) 15
2.3 Passos para o compartilhamento de dados. (Fonte: Elaborado pela autora inspirado na [35]). 19

3.1 Procedimentos de pesquisa da RSL. (Fonte: Autora) 28
3.2 Distribuição dos artigos selecionados ao longo dos anos. (Fonte: Autora) 30

4.1 Estruturação das técnicas utilizadas na concepção desta taxonomia. (Fonte: Autora) 37
4.2 TP1 - Processo de Identi cação de Requisitos de Privacidade. (Fonte: Autora) 40
4.3 Estrutura da taxonomia de requisitos de Privacidade. (Fonte: Autora) 48
4.4 Taxonomia de requisitos de Privacidade. (Fonte: Autora) 61

6.1 Evidências do resultado da aplicação do FAAT para o RQ008 ao Banco do Brasil .. 72
6.2 Evidências do resultado da aplicação do FAAT para o RQ001 ao Itaú 73
6.3 Evidências do resultado da aplicação do FAAT para o RQ002 ao Itaú 74
6.4 Evidências do resultado da aplicação do FAAT para o RQ009 ao Itaú 75

1 Processo de Solicitação de Consentimento do Open Banking no Banco do Brasil ... 133
2 Termos e Condições do Open Banking no Banco do Brasil 134
3 Processo de Solicitação de Consentimento do Open Banking no Bradesco 138
4 Termos e Condições do Open Banking no Bradesco 139
5 Processo de Solicitação de Consentimento do Open Banking no Itaú 143
6 Termos e Condições do Open Banking no Itaú 144

LISTA DE TABELAS

3.1 Lista de trabalhos selecionados e removidos após a aplicação da avaliação de qualidade..... 29
3.2 Relação de taxonomias identi cadas na RSL..... 35

4.1 Relação entre os princípios da LGPD e ISO/IEC 29100..... 45
4.2 Taxonomia de Requisitos de Privacidade..... 60
4.3 Verbos utilizados nas taxonomias para estruturação dos requisitos..... 62
4.4 Artigos das respectivas legislações utilizados na taxonomia..... 64
4.5 Comparativo entre as duas taxonomias..... 64

5.1 Composição do Formulário de Avaliação de Aderência à Taxonomia..... 68

6.1 Comparação dos resultados por instituição 71
6.2 Resultados da aplicação da taxonomia para a Categoria Finalidade. 71
6.3 Resultados da aplicação da taxonomia para a Categoria Adequação..... 76
6.4 Resultados da aplicação da taxonomia para a Categoria Necessidade..... 76
6.5 Resultados da aplicação da taxonomia para a Categoria Livre acesso..... 77
6.6 Resultados da aplicação da taxonomia para a Categoria Qualidade de Dados..... 78
6.7 Resultados da aplicação da taxonomia para a Categoria Transparência..... 79
6.8 Resultados da aplicação da taxonomia para a Categoria Segurança..... 80
6.9 Resultados da aplicação da taxonomia para a Categoria Prevenção..... 80
6.10 Resultados da aplicação da taxonomia para a Categoria Não Discriminação..... 81
6.11 Resultados da aplicação da taxonomia para a Categoria Responsabilização e Prestação de Contas..... 81

1 Lista de requisitos primários obtidos a partir LGPD..... 121
2 Requisitos primários obtidos a partir da ISO/IEC 29100. 132

1 INTRODUÇÃO

Com o aumento da quantidade de dados gerados e armazenados atualmente e com a conscientização dos usuários sobre a importância de seus dados desde o advento do marco civil da internet [41], a privacidade dos dados se tornou algo necessário e importante. Não obstante, a preocupação dos usuários é agravada com eventos de vazamento de dados [10, 49, 7, 50] que tornam ainda mais evidente a necessidade de garantir a proteção de seus dados pessoais, especialmente no cenário brasileiro em que apenas 20% das empresas estabeleceram processos de comunicação sobre possíveis vazamentos de dados pessoais [56] e apenas 23% realizam gerenciamento de incidentes para lidar de forma e caz com possíveis vazamentos de dados [56].

Para regulamentação da utilização dos dados pessoais, o governo brasileiro criou a lei nº 13.709, a Lei Geral de Proteção de Dados (LGPD) [42], publicada em 14 de agosto de 2018, com entrada em vigor para 24 meses após sua publicação, em agosto de 2020. A legislação tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa física [42]. A redação da LGPD foi inspirada na General Data Protection Regulation (GDPR) [104], a legislação europeia para regulamentar a proteção de dados pessoais no continente Europeu.

A GDPR prevê que, durante todo o processo de desenvolvimento envolvendo dados pessoais, sejam seguidos os princípios de nalidade, adequação, necessidade, qualidade de dados, segurança e transparência, atendidos por completo. Com abordagem semelhante, a LGPD de ne que o processo de tratamento de dados pessoais deve observar a boa-fé e seguir os princípios de - nalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

No âmbito da engenharia de software, abordagem interdisciplinar em que esforços técnicos e de gestão são utilizados para transformar um conjunto de necessidades em soluções [65], a engenharia de requisitos é uma área que demanda grande atenção para evoluir junto à normas regulatórias. Isso por ser a disciplina em que são gerados os requisitos, itens que descrevem o que o sistema deve fazer e suas restrições [118]. Os requisitos não funcionais, por sua vez, descrevem como o sistema deve se comportar [20]. Por serem mais complexos e difíceis de elicitar, acabam não recebendo a prioridade necessária ou até mesmo não sendo executados, muitas vezes por completo.

Considera-se que a negligência tanto para documentá-los como a possibilidade de não considerá-los parece ser um dos maiores problemas relacionados a esse tipo de requisito [20, 30, 44, 102]. Alguns autores destacaram que esses requisitos comumente são descritos de maneira incompleta, [25, 8, 51] tornando a análise, desenvolvimento e consequentemente o teste das funcionalidades mais difíceis [51, 8, 25, 22].

Como requisitos de privacidade são geralmente categorizados como requisitos não funcionais,

eles acabam compartilhando os mesmos desafios. Como, em sua natureza, os requisitos de privacidade podem ser utilizados para registros de requisitos fundamentados em bases legais, esse contexto dificulta a elicitação por ser uma atividade geralmente exercida por analistas de requisitos e sistemas que não possuem experiência na interpretação de normas legais [17, 46, 91, 13]. Além disso, os requisitos de privacidade por vezes acabam sendo confundidos como parte da segurança [61, 82, 126, 98], o que diminui sua real aplicabilidade. Outros autores mencionaram a necessidade de especificar os requisitos de privacidade logo no início do ciclo de desenvolvimento do software [7, 17, 70, 60, 106]. Ansari et al. [12] destacaram que a identificação e modelagem correta dos requisitos de privacidade durante a fase de desenvolvimento de software é essencial para entregar o software com grau significativo de proteção da privacidade dos dados dos usuários.

Ainda no contexto de requisitos de privacidade, Anthonysamy et al. [13] descreveram que existem 4 tipos de requisitos de privacidade os quais são: (1) conformidade, (2) controle de acesso, (3) verificação e (4) usabilidade. Logo, é possível identificar que um deles é o requisito de conformidade. Esse tipo de requisito é o utilizado para abordar os princípios estabelecidos pela LGPD.

Não obstante, Guzmán et al. [69] afirmaram que os requisitos não funcionais possuem um papel importante no sucesso dos sistemas de software. Nesse sentido, identifica-se a necessidade de uma abordagem prática em relação a elicitação de requisitos de privacidade no contexto das legislações e frameworks de segurança e privacidade. Para atender este desafio de uma abordagem prática para elicitar os requisitos de privacidade, neste trabalho foi proposta uma taxonomia no contexto de requisitos de privacidade no contexto da LGPD.

Alguns autores abordaram sobre taxonomias de requisitos de privacidade [112, 83, 92, 19], mas apenas o trabalho de Sangaroonsilp et al. [112] se assemelha com esta pesquisa por abordar uma taxonomia especificamente de requisitos de privacidade. Kanwal et al. [83] propuseram uma taxonomia para preservação da privacidade dos pacientes em sistemas de E-Helth. Meis et al. [96] propuseram uma taxonomia de requisitos de transparência baseada na GDPR e ISO/29100. Alqassem e Svetinovic [6] em 2014 criaram uma taxonomia de segurança voltada para a Internet das Coisas (IoT). Barker et al. [19] em 2009 propuseram uma taxonomia de requisitos de privacidade para SGBDs. Massey e Antòn-Earp [92] propuseram uma taxonomia de danos legais de privacidade utilizando as fontes jurídicas para criar a taxonomia. Finalmente, Sangaroonsilp et al. [112] desenvolveram uma taxonomia de requisitos de privacidade baseada na GDPR e ISO/IEC 29100, que foi utilizada como parâmetro para este trabalho. Assim, nesta pesquisa, para a elaboração da taxonomia, os passos seguidos por Sangaroonsilp et al. [112] serão utilizados como inspiração para criação da taxonomia de requisitos de privacidade baseada na LGPD para o contexto brasileiro.

1.1 PROBLEMA DE PESQUISA

A elicitação de requisitos não funcionais possui desa os por esses serem abstratos e muitas vezes registrados fora do momento oportuno ou de maneira incompleta [20, 30, 44, 102, 25, 8, 51, 22]. Para os requisitos de privacidade a elicitação pode se tornar especialmente desa adora por envolver contexto legais em que as atividades geralmente são exercidas por pro ssionais sem expertise legal e por ser muitas vezes considerado uma parte da segurança [17, 46, 91, 13, 61, 82, 126, 98]. Essa di culdade de elicitar requisitos de privacidade é atenuada com o advento da LGPD que prevê sanções, inclusive nanceiras para as instituições que não estejam desenvolvendo seus softwares em conformidade com a legislação vigente.

No âmbito da engenharia de software os desa os da especi cação de requisitos não funcionais são uma preocupação antiga. Behutiye et al. [20] mencionaram que a falta de documentação dos requisitos não funcionais acarreta em problemas nos estágios nais do ciclo de desenvolvimento de software e a rmaram que essa falha de não considerar os requisitos não funcionais no início do desenvolvimento pode resultar em qualidade baixa do software e no aumento de custos e tempo de manutenção.

Alguns autores destacaram que o melhor momento para elicitar e documentar os requisitos de privacidade é logo no início do processo de desenvolvimento de software [7, 17, 70, 60, 106]. Ansari et al. [12] destacaram que a elicitação correta de requisitos de privacidade na fase de desenvolvimento de software é essencial à proteção da privacidade dos stakeholders incluindo os usuários.

Ainda no contexto da elicitação de requisitos, Ramingwong [107] destacou que a seleção correta de métodos e técnicas de engenharia de requisitos pode ser uma escolha difícil e nas piores situações pode levar o sistema a falhas, o que explicita a necessidade de abordagens mais práticas a m de mitigar riscos relacionados a elicitação desses requisitos. No entanto, Danezis et al. [43] destacaram que características de privacidade e proteção de dados são geralmente negligenciadas quando se utilizam métodos convencionais de engenharia de software. A causa dessa negligência pode estar relacionada com o baixo conhecimento dos pro ssionais de tecnologia em relação às leis e regulações de proteção de dados [12, 56, 17, 46].

Metodologias como Privacy by Design [32] fornecem apenas princípios e diretrizes de alto nível, deixando uma grande lacuna na elicitação de requisitos e implementação de sistemas com foco em privacidade [112, 68]. Necessidades emergentes de traduzir preocupações complexas de privacidade estabelecidas em regulamentos e padrões em requisitos de software foram registradas por Sangaroonsilp et al. [112]. Taxonomias, por sua vez, podem facilitar a identi cação de requisitos implícitos evitando sua operacionalização de forma errada [15]. Além disso uma descrição de requisitos bem formada, que depende da taxonomia de requisitos apropriada, é considerada necessária para superar as complexidades do desenvolvimento de requisitos [38]. Dessa forma, uma taxonomia para apoiar as equipes de desenvolvimento de software na elicitação dos requisitos de privacidade pode auxiliá-los na superação dos desa os citados na literatura e na melhoria

do tempo necessário para produção desses requisitos.

1.2 JUSTIFICATIVA

Com entrada em vigor da LGPD, as organizações públicas e privadas estão enfrentando desa os para se adequarem à LGPD e criar novas soluções de software já aderentes à legislação. Existem diversos desa os para alcançar os objetivos da elicitação de requisitos [7, 17, 70, 60, 106, 111], mesmo nos contextos de requisitos funcionais e não funcionais dentro o processo de desenvolvimento de software.

A adequação à LGPD parece ainda estar em ritmo pequeno, Menegazzi [97] destacou no início de 2021 que muitas organizações ainda não iniciaram o seu processo de conformidade com a lei, não estão cientes da necessidade ou não entendem as mudanças que a legislação trará para seus negócios e que esse cenário pode estar associado com a di culdade de interpretação da lei, muitas vezes ambígua, e pela falta de conhecimento jurídico dos pro ssionais de TI.

Também sobre a conformidade com a LGPD, Ferrão et al. [56] conduziram uma pesquisa demonstrando que as organizações ainda estão em processo inicial para o processamento de dados de acordo com os princípios da LGPD. Apenas pouco mais de 1/4 (um quarto) das organizações brasileiras utilizam como base a boa fé e os princípios LGPD no processamento de dados pessoais de acesso público. Contudo, 38% dessas organizações ainda não iniciaram um plano de iniciativas ou metodologias e cazes para implementar os princípios LGPD.

Canedo et al. [46] identi caram que os pro ssionais de TI não possuem conhecimento necessário para implementar princípios de privacidade e diretrizes da LGPD. O conhecimento desses pro ssionais sobre a lei parece não ser su ciente para o desenvolvimento de atividades sobre as quais eles atuam em seus projetos. Os autores indicam que a causa pode se dar pela falta de divulgação e comunicação aberta das organizações sobre os processos e soluções de privacidade que são produzidos para uso interno. Os autores concluíram que existe uma necessidade global da industria de desenvolvimento de software por uma abordagem de privacidade de dados voltada para os pro ssionais de TI.

Alves e Neves [7] corroboraram com Canedo et al. [46] em relação a como os pro ssionais entendem que há uma necessidade de capacitação dos times e registraram também encontrar di culdades para interpretação da lei por parte dos pro ssionais de TI. Além disso, registraram a di culdade na mudança de paradigma de rotinas de trabalho para a adequação dos novos sistemas assim como os sistemas legados em relação à legislação vigente. Nesse sentido, considerando que taxonomias fornecem meios para classi car e descrever as relações entre os elementos relevantes de um estudo [76], e quando bem formadas são consideradas necessárias para o desenvolvimento de requisitos [38], a de nição de uma taxonomia de requisitos de privacidade baseada na LGPD pode contribuir para o alcance da conformidade com a legislação.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é propor uma taxonomia de requisitos de privacidade baseada na Lei Geral de Proteção de Dados (LGPD) [42] e na ISO/IEC 29100 [75] para apoiar as equipes de desenvolvimento de software no alcance da conformidade com os princípios da Lei Geral de Proteção de Dados (LGPD).

1.3.2 Objetivo Especí co

Para alcançar o objetivo geral deste trabalho, os seguintes objetivos foram de nidos:

OE.1 Identi car na literatura os trabalhos que investigam os desa os na elicitação de requisitos de privacidade em conformidade com a LGPD;

OE.2 Identi car na literatura os trabalhos que de nem taxonomias;

OE.3 Elaborar a comparação entre a LGPD, GDPR e ISO/IEC 29100 para produção da taxonomia baseada em Sangaroonsilp et al. [112];

OE.4 Propor uma taxonomia para elicitar requisitos de privacidade em conformidade com a LGPD;

OE.5 Avaliar a aplicabilidade da taxonomia proposta e realizar possíveis ajustes.

1.4 METODOLOGIA DE PESQUISA

Este trabalho foi conduzido utilizando multi-metodologias conforme apresentado na Figura 1.1. Primeiro foi estabelecido o problema de pesquisa e suas justi cativas. Em seguida foram delimitadas as questões de pesquisa para conduzir a revisão sistemática de literatura. Como continuidade foi executada uma revisão sistemática da literatura para identi car os trabalhos correlatos e contextualização da pesquisa. A revisão sistemática de literatura foi realizada de acordo com guia proposto por Kitchenham e Charters [86].

A partir dos resultados da revisão de literatura que permite ao pesquisador analisar o cenário estudado perante a literatura acadêmica, foi possível embasar a necessidade da elaboração/proposta de uma taxonomia de requisitos de privacidade baseada na LGPD[42] e ISO/IEC 29000[75]. Na concepção da taxonomia proposta considerou-se as metodologias utilizadas no trabalho realizado por Sangaroonsilp et al. [112], as quais foram: processo de análise de conteúdo, Goal-Based Requirements Analysis Method (GBRAM) [15, 14] e Teoria Fundamentada dos Dados [63], conforme apresentado na Figura 1.1. O GBRAM é baseado na Teoria Fundamentada dos Dados. Os

passos executados por Sangaroonsilp et al. [112] foram replicados nessa pesquisa. Por m, a aplicação da taxonomia foi executada a partir de um estudo de caso.

Figura 1.1: Metodologia de Pesquisa. (Fonte: Autora)

Os métodos descritos foram escolhidos para o alcance dos objetivos. A RSL é necessária para avaliar o estado da arte na academia considerando as pesquisas existentes sobre o tema analisado. Para a criação da taxonomia os métodos GBRAM e Grounded Theory foram selecionados por serem utilizados no trabalho de [112] que é utilizado como inspiração para esta taxonomia. E, por m, a escolha do estudo de caso se deu pelo fato de ele ser considerado uma importante estratégia metodológica para a academia, aprofundando a relação entre o que está sendo estudado pois revela o que não seria enxergado sem a execução deste protocolo [].

1.5 RESULTADOS ESPERADOS E CONTRIBUIÇÃO

Como resultado nal desta pesquisa, apresenta-se uma taxonomia com 129 requisitos de privacidade, 10 categorias e 5 contextos para apoiar as equipes de desenvolvimento de software na atividade de elicitação dos requisitos de privacidade em conformidade com a LGPD e com a ISO/IEC 29100. A taxonomia pode ser considerada como um guidelinepara os pro ssionais de TIC se basearem durante a elicitação e especi cação de requisitos na busca pela conformidade com a LGPD nos sistemas que utilizam a taxonomia proposta. Assim, as principais contribuições desse trabalho podem ser consideradas: i) a elaboração de uma taxonomia de requisitos de privacidade fundamentada em um framework de mercado e na legislação brasileira para utiliza-

ção como um guideline pelos pro ssionais de Tecnologia da Informação e Comunicação (TIC) durante a elicitação e especi cação de requisitos; e ii) a disponibilização de um formulário para avaliar a adequação à LGPD dos sistemas já desenvolvidos, permitindo a identi cação dos pontos de não conformidade para regularização. As duas principais contribuições visam o alcance conformidade com a LGPD.

1.6 PUBLICAÇÕES

Como resultado desta dissertação, os artigos *Diagnostic of Data Processing by Brazilian Organizations—A Low Compliance Issue* publicado no Journal Information, Volume 12, Issue 4, publicado em 14 Abril 2021 [56] e *Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil* foi elaborado, submetido e aceito na trilha regular do WER, Workshop em Engenharia de Requisitos, que ocorrerá em modo virtal entre 23 e 26 de agosto de 2022. Artigo submetido ao ACM Computing Surveys, não avaliado nem publicado até esta defesa.

1.7 ESTRUTURA DA DISSERTAÇÃO

Este trabalho está organizado em 7 capítulos incluindo este. O Capítulo 2 apresenta a fundamentação teórica necessária para a elaboração desse trabalho, bem como os trabalhos correlatos.

O Capítulo 3 apresenta a revisão de literatura executada para esta pesquisa assim como o protocolo utilizado durante o processo de revisão sistêmica.

No Capítulo 4 o método de elaboração da taxonomia dessa dissertação é apresentado assim como os parâmetros de execução utilizados durante o processo de desenvolvimento da pesquisa.

No Capítulo 5 é apresentada a técnica utilizada para aplicação desta taxonomia.

O Capítulo 6 apresenta os resultados da SLR e da aplicação da taxonomia, discussões e as limitações do estudo executado. Por m, o Capítulo 7 apresenta as conclusões desta dissertação e os trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Sob o aspecto da fundamentação teórica, serão apresentados a seguir os conceitos que fundamentaram a elaboração desta dissertação sobre a engenharia de requisitos como contexto inicial da área de pesquisa. Em seguida o conceito de requisitos de privacidade são abordados. Após isso, o tema de privacidade de dados será introduzido para em seguida abordar as legislações de proteção de dados e o framework de privacidade. E por fim, o projeto ao a aplicação prática será executada é brevemente explicado. O objetivo no entanto não é explorar todos os aspectos dos assuntos, uma vez que este trabalho não visa abordar o estado da arte dos conceitos apresentados e sim contextualizá-los com o propósito de proposição de uma taxonomia.

2.1 ENGENHARIA DE REQUISITOS

A engenharia de requisitos (ER) é reconhecida como uma fase fundamental do processo de engenharia de software [67]. Ela pode ser entendida como o processo para definição, identificação e documentação de restrições para um sistema de software. Restrições essas que sejam adequadas para análise, comunicação e subsequente implementação do sistema. Além da identificação dos stakeholders envolvidos no sistema e de suas necessidades [67, 127, 100].

Ouhbi et al. [101] afirmaram que a ER está preocupada com os objetivos do mundo real para funcionalidades (ER funcional) e restrições (ER não funcional, por exemplo, restrições de qualidade e custos) nos sistemas. Nesse sentido, autores como Glinz [64], e Mabrok et al. [89] classificam os requisitos em dois tipos: 1) Requisito funcional e 2) Requisito não funcional (RNF). O primeiro descreve o que o sistema pode ou deve fazer [115] e o segundo determina as especificações técnicas do produto e aspectos não comportamentais do sistema [89].

Nesse sentido, os requisitos não funcionais (RNF) são geralmente restrições necessárias para serviços ou funções oferecidos pelo sistema [101]. Eles podem incluir diversas restrições como restrições de tempo para processamento, restrições no processo de desenvolvimento e restrições definidas por normas e legislações. Os RNF descrevem os requisitos que serão entregues com a imposição de restrições, capturando propriedades para operar o sistema [89].

Além disso, são utilizados também para registro de comportamentos em relação a alguns atributos observáveis, como confiabilidade, capacidade de reutilização, manutenção, entre outros [115]. Uma diferença dos requisitos não funcionais em relação aos funcionais é que os funcionais muitas vezes descrevem as características individuais ou serviços do sistema enquanto os requisitos não funcionais, em sua maioria, de nem características e/ou comportamentos que se aplicam ao sistema de forma geral e não a serviços específicos.

Entende-se então que os requisitos não funcionais descrevem como o sistema deve se com-

portar [20]. Como os RNF relatam as restrições que devem ser levadas em consideração para desenvolvimento do software, eles abrangem atributos relacionados com segurança, privacidade, desempenho, portabilidade, entre outros [79]. Por serem mais complexos e difíceis de elicitar, acabam não recebendo a prioridade necessária ou até mesmo não executados por completo em muitas situações.

A de nição de requisitos de privacidade, de acordo com Webster et al. [123], é o requisito capaz de registrar os objetivos de privacidade e as medidas associadas a esses objetivos para um determinado sistema. Por essa natureza subjetiva, os requisitos de privacidade são geralmente categorizados como requisitos não funcionais e com isso acabam compartilhando dos mesmos desa os em seu processo de elicitação destacados por [20, 30, 44, 102, 25, 8, 51, 22].

Como em sua natureza os requisitos de privacidade podem ser utilizados para registros de requisitos fundamentados em bases legais, esse contexto primariamente jurídico pode di cultar a elicitação por ser uma atividade geralmente exercida por analistas de requisitos, analistas de sistemas e engenheiros de software que não possuem experiência na interpretação de normas legais [17, 46, 91, 13].

Além disso, os requisitos de privacidade por vezes acabam sendo confundidos como parte da segurança ao invés de um objetivo especí co de garantia da privacidade [61, 82, 126, 98], o que diminui sua real aplicabilidade em contextos sistêmicos. Ansari et al. [12] destacaram que a identi cação e modelagem correta dos requisitos de privacidade durante a fase de desenvolvimento de software é essencial para entregar o software com grau signi cativo de proteção da privacidade dos dados dos usuários.

Hadar et al. [70] mencionaram que abordagens sistemáticas para especi car requisitos de privacidade são uma necessidade eminente considerando que engenheiros de software muitas vezes não possuem conhecimento e compreensão necessários sobre conceitos de privacidade para executar as atividades de elicitação desses requisitos.

2.2 PRIVACIDADE DE DADOS

A de nição de privacidade, no âmbito do direito, segundo com Rodotà [109] é de que a privacidade pode ser considerada como o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular. Ruaro et al. [110] declararam então que a privacidade passa fundamentalmente a se estruturar em torno da informação e especi camente dos dados pessoais.

No contexto da Engenharia de Software, Kalloniatis et al. [82] consideram que a privacidade dos usuários pode ser de nida como o direito de determinar quando os dados serão utilizados, como será sua utilização e tratamento e com que nalidade as informações sobre esses usuários são comunicadas a outros [105]. Da mesma forma, Canedo et al. [46] destacaram que a privacidade de dados compreende os dados do usuário, criados por ele mesmo ou terceiros e sua

utilização por meio de observações, análises, entre outros, por indivíduos.

O privacidade de dados, de forma geral, pode ter seu conceito considerado como subjetivo. Diferentes signi cados podem ser atribuídos para diversos tipos de pessoas, no entanto, a perspectiva de que a privacidade é um direito humano que dependente de contexto e do ambiente inserido, é comum a todas as interpretações [117].

As tratativas sobre privacidade vêm evoluindo ao longo do tempo. Por exemplo, Finkelstein, M. e Finkelstein, C. [57] consideram que a evolução tecnológica é um marco na história da privacidade, bem como o advento dos meios de comunicação, o desenvolvimento da internet e o surgimento das redes sociais. Isso pois atualmente os grandes players desses meios registram muitas informações dos usuários colocando sua privacidade em risco.

Ainda nesse sentido, Brito e Machado [28] a rmam que a privacidade de dados encontra uma barreira para sua existência no mundo tecnológico pela facilidade do uxo de informações, o que torna a preocupação com a privacidade de dados ainda mais relevante na âmbito da tecnologia da informação.

A preocupação com a privacidade também aumentou ao longo do tempo, principalmente pela rápida evolução no processamento de dados [113]. Leis como a GDPR [104] e a LGPD [42] buscam alcançar a privacidade dos dados pessoais dos usuários a partir do estabelecimento de critérios, regras e práticas para a obtenção, retenção e o processamento de dados.

Tendo contextualizado sobre a legislação brasileira e sobre a privacidade de dados, a seguir será apresentada a visão da ISO/IEC 29100 que se relaciona ao contexto de privacidade que está sendo abordado para este projeto.

2.3 GENERAL DATA PROTECTION REGULATION - GDPR

A General Data Protection Regulation (GDPR) [104] é a lei de proteção de dados pessoais da união europeia que surgiu em substituição e como evolução da Data Protection Directive 95/46/EC (DIR95) [47] e foi aprovada em maio de 2016. Segundo Tikkinen-Piri et al. [120] a GDPR visa melhorar o nível de proteção e harmonização do dados pessoais pela União Europeia, uma vez que a DIR95 não mais atende aos requisitos de privacidade demandados pelo ambiente digital. A GDPR, que entrou em vigor em maio de 2018, é aplicada a toda e qualquer instituição que trate dados de pessoas naturais da união Europeia independente de localização física. É composta por 99 artigos e seus princípios são:

I. Legalidade, justiça e transparência: os dados devem ser processados de forma legal, justa e transparente em relação ao titular dos dados;

II. Finalidade: os dados devem ser coletados para ns especí cos, explícitos, legítimos e não processados;

III. Minimização de dados os dados devem ser coletados em adequação com a nalidade, limitados ao que é necessário em relação aos ns para os quais são processados;

IV. Acurácia: os dados devem ser precisos e atualizados quando necessário, além disso dados inexatos devem ser descartados ou corrigidos o quanto antes;

V. Armazenamento limitado: os dados devem ser armazenados de forma a permitir a identi- cação de seus titulares por tempo não superior ao necessário de acordo com os ns para os quais os dados pessoais foram obtidos para o processamento;

VI. Integridade e con abilidade: os dados devem ser processados de forma a garantir sua se- gurança adequada usando medidas técnicas ou organizacionais apropriadas. Essas medidas devem incluir proteção contra o processamento não autorizado ou ilegal e também contra perda acidental, destruição ou dano;

VII. Responsabilidade A empresa pelo tratamento dos dados deve ser responsável e ser capaz de demonstrar conformidade com os princípios.

Para a GDPR os papéis estabelecidos no tratamento dos dados são [104]:

- Controlador: é a pessoal natural ou jurídica, de direito publico ou privado, que de forma individual ou coletiva determina a pessoa singular ou coletiva, determina os ns e os meios de tratamento dos dados pessoais;
- Processador:é a pessoal natural ou jurídica, de direito publico ou privado, que é responsá- vel pelo processamento dos dados pessoais em nome do responsável pelo tratamento;
- Autoridade de supervisão:é uma autoridade pública independente que é estabelecida por um Estado-Membro nos termos do artigo 51 da GDPR;
- Data Protection Of cer: pro ssional responsável por acompanhar a implementação da GDPR e sua implementação, deve conhecer a legislação.

A GDPR prevê multas e penalidades para violações de segurança que podem ser classi cadas de acordo com um catálogo de violações disponibilizado pelo regulador em [40]. Para violações menos graves a GDPR prevê multas de até 10 milhões de euros ou até 2% do faturamento global da organização. Para violações especialmente graves a multa pode ser até 20 milhões de euros ou até 4% do faturamento.

Tendo apresentado esta breve visão sobre a GDPR para que se possa estabelecer a relação originária da lei brasileira, a seguir será apresentada a LGPD.

2.4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

A Lei Geral de Proteção de Dados (LGPD) [42] é a lei brasileira para proteção de dados pessoais e foi inspirada na GDPR. Após o marco civil da internet [41] em 2014, o Brasil começou a enxergar a proteção de dados como necessária, uma vez que o tratamento de dados de forma indiscriminada pode acarretar em eventos de vazamentos de dados [10, 49, 7] evidenciando a necessidade de uma lei como a LGPD.

A publicação da LGPD aconteceu em agosto de 2018, com expectativa de entrada em vigor em agosto de 2020. Durante esse período, iniciativas do governo tentaram adiar a entrada em vigor da lei, como aconteceu em abril de 2020 com a publicação da medida provisória, 959/2020 [53] (ato do Poder Executivo que aplicabilidade de lei e requer aprovação subsequente do Poder Legislativo), que tinha o intuito de adiar a entrada em vigor da LGPD para 2021. No entanto, essa medida provisória teve o artigo de prorrogação vetado exatamente no mês previsto para entrada em vigor por lei, em agosto de 2020 [56], e sua vigência está ativa desde então.

Com essa legislação em vigor, o Brasil passou a compor um grupo de mais da metade de países do mundo que possuem leis para a proteção dos dados pessoais. Segundo dados de setembro de 2020 da organização intergovernamental ligada à ONU, United Nations Conference on Trade and Development (UNCTAD) [121], 66% dos países no mundo possuem alguma legislação relacionada a proteção e privacidade de dados enquanto 19% não possuem nenhuma iniciativa de legislação e 10% estão em processo de elaboração da legislação. A lei é constituída por 64 artigos e seus princípios, que estão de nidos no artigo 6 devem observar a boa-fé, são (PL - Princípios da Lei) [42].

PL.1 Finalidade: o tratamento de dados deve ser limitado uma nalidade determinada com propósito legítimo que deverá ser explicitado ao titular dos dados;

PL.2 Adequação: o tratamento de dados deve ser compatível com o objeto (nalidade) descrito ao titular do dado;

PL.3 Necessidade: os dados utilizados no tratamento devem ser limitados estritamente à nalidade determinada no momento de sua coleta;

PL.4 Livre acesso: permissão de consulta gratuita sobre a forma, a duração do tratamento e a integralidade de seus dados pessoais;

PL.5 Qualidade dos dados para o cumprimento da nalidade determinada no tratamento os dados devem estar exatos, claros, relevantes e atualizados;

PL.6 Transparência: deve-se garantir os titulares dos dados informações claras, precisas e de acesso facilitado sobre o tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

PL.7 Segurança promover a segurança dos dados pessoais a partir de medidas técnicas e administrativas que protejam de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PL.8 Prevenção estabelecimento e execução de medidas que previnam a ocorrência de danos em virtude do tratamento de dados pessoais;

PL.9 Não discriminação vedação à utilização dos dados para tratamentos com ns discriminatórios ilícitos ou abusivos;

PL.10 Responsabilização e prestação de contas o agente de tratamento deve demonstrar as medidas adotadas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais além de apresentar a e cácia dessas medidas.

Além disso, a LGPD em seu artigo 5 [42], de ne os papéis dos diversos atores presentes no processo de gestão do tratamento do dado inclusive no âmbito governamental de scalização. Os papeis são:

- titular : denominação da pessoa natural a qual se referem os dados pessoais objeto de tratamento;
- controlador: indica pessoa natural ou jurídica, de direito público ou privado, a qual é responsável pelas decisões referentes ao tratamento dos dados pessoais coletados;
- operador: é uma pessoa natural ou jurídica, também de direito público ou privado, que de fato realiza a operacionalização do tratamento de dados pessoais em nome do controlador;
- encarregado: é necessariamente uma pessoa natural que deve ser indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a autoridade nacional;
- agentes de tratamento: denominação para dirigir-se ao controlador e ao operador;
- autoridade nacional: é um órgão da administração pública responsável por zelar, implementar e scalizar o cumprimento da LGPD.

A relação entre esses papeis da LGPD e o relacionamento deles como o processo de tratamento de dados pessoais é exempli cado de forma visual na Figura 2.1.

A legislação estabelece também que o processamento de dados poderá ser executado pelas instituições de direto privado desde que seja solicitado ao titular do dado o consentimento. Esse consentimento deverá indicar uma nalidade especí ca. Para tanto, não são permitidas autorizações genéricas nem vícios de consentimento [42].

Aos titulares dos dados são resguardados os direitos de revogação do consentimento de tratamento de dados a qualquer momento de acordo com o artigo 8, § 5º da LGPD [42]. O acesso

Figura 2.1: Papéis da LGPD e o relacionamento com o processo de tratamento de dados. (Fonte: Autora)

facilitado ao tratamento dos dados de forma clara e objetiva por parte dos titulares também é autorizado por lei, atendendo o princípio de livre acesso, podendo consultar informações sobre a nalidade do consentimento, a forma e duração do tratamento, direitos do titular entre outros [42].

Os agentes de tratamento que não cumprirem os requisitos para o tratamento dos dados podem ser punidos com sansões administrativas que incluem tornar pública a infração após sua apuração e con rmação, suspensão do exercício de tratamento a que refere a infração, multas de até 2% do faturamento da empresa limitado a 50 milhões de reais por infração, entre outros [11].

A lei vem sendo aplicada e considerando os casos públicos analisados até outubro de 2021, existem quatro processos transitados em julgado (estado nal de um processo jurídico) que foram aplicadas multas e sanções baseados exclusivamente na LGPD [11]. Dos processos em andamento, identi ca-se que o setor com maior registros de violações é o setor bancário, conforme apresentado na Figura 2.2. Seguido pelos setores de vendas on-line e telefonia, os registros de processos estão dispersos sobre os vários âmbitos da sociedade.

Figura 2.2: Violações por Segmento. (Elaborado pela autora a partir de [11])

A perspectiva de que o setor bancário possui um percentual maior de violações registradas, demonstram a importância do desenvolvimento de iniciativas que proporcionem às instituições formas alcançarem a aderência à LGPD.

Sob a perspectiva de instrumentos para o alcance da conformidade com a LGPD, também há um *framework* para alcance da privacidade dos dados, que é apresentado a seguir.

2.5 ISO/IEC 29100

A ISO/IEC 29100 é um *framework* que visa estabelecer padrões para sistemas de tecnologia da informação e comunicação (TIC) para o alcance da privacidade de dados pessoais. Sua abordagem é voltada para os aspectos organizacionais, técnicos e processuais em uma estrutura abrangente de privacidade [75]. Sua importância é destacada pelo aumento do processamento de dados pessoais e pela necessidade de normas de segurança que estabeleçam uma base de entendimento comum para a proteção de dados pessoais [75].

Seu escopo inclui a de nição de uma terminologia comum para os termos de privacidade, de nição de atores e de seus papeis no processo de tratamento de dados, descrição dos requisitos de salvaguardas da privacidade e referências sobre os 11 princípios de privacidade, os quais são (PF - Princípio do *Framework*) [75]:

PF.1 Consentimento e escolha: Possibilitar ao titular de dados a escolha sobre o processamento de seus dados pessoais e fornecer informações claras sobre o processo se tratamento; Deve permitir que o titular decidir por não aceitar o tratamento de seus dados pessoais;

PF.2 Legitimidade e especi cação do propósito: Garantir a aderência a nalidade, noti cando ao usuário quando da utilização dos dados para uma nova nalidade. Garantir que a informação seja clara e objetiva;

PF.3 Limitação de coleta: Garantir que os dados pessoais coletados sejam apenas os estritamente necessários para o tratamento de dados necessário à nalidade que se propõe, além de ser necessário estar de acordo com as legislações existentes;

PF.4 Minimização de dados: Está intimamente ligado ao princípio de limitação de coleta de dados, indo além deste princípio por não estar relacionado apenas com a coleta mas também com o tratamento dos dados pessoais. Isso se dá pela minimização dos envolvidos no tratamento, usar sempre que possível soluções que primem pela não identi cação;

PF.5 Limitação de uso, retenção e divulgação: Limitar o uso, a retenção e a divulgação dos dados pessoais ao cumprimentos de seus ns e reter os dados pessoais apenas pelo tempo necessário para a nalidade pela qual esses dados foram obtidos, aplicando processos de anonimização ou destruindo-os com segurança;

PF.6 Precisão e qualidade: Garantir que os dados pessoais estejam precisos em relação a sua origem e obtenção e que estejam sempre atualizados garantindo a sua con abilidade. Assegurar que as alterações solicitadas pelo titular são legitimas e exatas. Propor processos para garantir a exatidão dos dados coletados e tratados.

PF.7 Abertura, transparência e noti cação: Tornar acessíveis as informações sobre o processo de tratamento de dados pessoais e seus controles, práticas utilizadas. Noti car o titular sobre as informações do controlador e do processamento principalmente na ocorrência de grandes mudanças no processo de tratamento dos dados;

PF.8 Participação individual e acesso: Possibilitar ao titular meios para acessar e revisar seus dados pessoais desde que o acesso seja autenticado com nível de segurança apropriado. Além disso, estabelecer procedimentos para que os titulares possam exercer seus direitos;

PF.9 Responsabilidade: Tornar registrados todos os procedimentos, controles, ferramentas e métodos utilizados no processamento de dados, fornecer treinamento adequado aos envolvidos no tratamento dos dados pessoais, considerar procedimentos de compensação quando situações reversíveis ocorram não permitindo ao titular voltar ao status de privacidade inicial;

PF.10 Segurança da informação: Proteger os dados nos níveis necessários de controles em procedimentos operacionais, funcionais e estratégicos com o intuito de garantir a integridade, con dencialidade e disponibilidade dos dados pessoais;

PF.11 Conformidade de privacidade: Avaliar e demonstrar que o processo de tratamento de dados está de acordo com os requisitos necessários para sua proteção. Possuir controles internos aderentes à proteção necessária e possuir mecanismos de avaliação externos para garantir a lisura do processo.

Esse framework define princípios de privacidade que podem ser utilizados, apresenta uma lista de dados que podem ser considerados para identificação de pessoas naturais, define os papeis no tratamento de dados e aborda os fatores que influenciam a gestão de riscos de privacidade. Também aborda fatores legais e regulatórios, fatores de negócios e outros e políticas e controles de privacidade [75].

Tendo a contextualização teórica destes tópicos, a seguir será apresentada brevemente a perspectiva do projeto escolhido para a aplicação prática desta dissertação.

2.6 OPEN BANKING

No Brasil, atualmente, grande parte das transações bancárias ocorrem através dos canais digitais. De acordo com a Febraban [45], para esses canais as transações de pessoas físicas no ano de 2020, durante a pandemia do COVID-19, chegaram a um percentual de 74%. A pesquisa também registrou que a cada 10 transações bancárias, 6 ocorrem por meios digitais. A transformação para o meio digital é uma realidade que no setor bancário pode ser concretizada com a chegada do conceito de Open Banking.

A área de tecnologia, de forma geral, já estava abordando o tema e começando a fazer suas implementações. No entanto, o Banco Central deu publicidade ao conceito de Open Banking em abril de 2019, através do comunicado nº 33.455/2019 [34] em que o regulador estabeleceu os requisitos fundamentais para a sua implementação. Seus princípios são a promoção da concorrência no sistema financeiro, o incentivo à inovação, o aumento da eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro e por fim a promoção da cidadania financeira [34]. Neste comunicado o Banco Central explica que a iniciativa tem por objetivo aumentar a eficiência no mercado de crédito e de pagamentos no Brasil, a partir da promoção de um ambiente de negócio mais inclusivo e competitivo, preservando a segurança do sistema financeiro e a proteção dos consumidores [34]. O Banco Central também registra que o contexto das inovações introduzidas no mercado financeiro em 2019 estava em destaque no cenário mundial. [34]. Acrescenta ainda que os reguladores de algumas jurisdições têm intervindo regulatoriamente na intenção de disciplinar o tema. Sobre a abordagem regulatória finaliza apresentando a correlação entre o Open Banking e a LGPD:

> Nesse contexto, o Banco Central do Brasil vem acompanhando as discussões internacionais e as iniciativas locais. Além disso, a discussão torna-se mais relevante com a edição da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados

pessoais no País. O Open Banking, na ótica do Banco Central do Brasil, é considerado o compartilhamento de dados, produtos e serviços pelas instituições nanceiras (IF) e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente [34].

Dando continuidade ao processo de regulação, em 5 de maio de 2020 o Banco Central e o Conselho Monetário Nacional publicam o primeiro instrumento normativo para estabelecimento da regulação do Open Banking no Brasil, a Resolução Conjunta nº 1/2020 [35]. Os participantes desse ecossistema estão de nidos pela Resolução nº 1, de 5 maio de 2020, em seu artigo sexto [35], que estabelece que instituições nanceiras enquadradas no Segmento S1 e S2, de acordo com a Resolução nº 4.553, de 30 de janeiro de 2017 [33], são participantes obrigatórios do Open Banking. Além disso outras instituições regulamentadas pelo Banco Central também podem participar de forma voluntária.

A resolução em seu artigo segundo traz de nições importantes sobre essa regulação, dentre elas, para o contexto desse trabalho têm-se:

- instituição transmissora de dados é a instituição participante do Open Banking que compartilha com a instituição receptora os dados compartilhados [35];
- instituição receptora de dados é a instituição participante do Open Banking que solicita o compartilhamento à instituição transmissora de dados para recepção dos dados compartilhados [35];
- instituição detentora de conta: é instituição participante do Open Banking que mantém conta de depósitos à vista ou de poupança ou conta de pagamento pré-paga de clientes no sistema nanceiro [35];
- consentimento é a manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou de serviços para nalidades determinadas [35].

A resolução estabelece também quatro fases para implantação desse ecossistema compostas pelo compartilhamento de:

F.1 dados públicos de canais de atendimento e produtos e serviços;

F.2 dados cadastrais de clientes e transações de produtos e serviços;

F.3 serviços de iniciação de pagamentos; e

F.4 dados de operações de câmbio, serviços de credenciamento em arranjos de pagamento, contas de depósito a prazo e outros produtos com natureza de investimento, seguros e previdência complementar aberta.

A fase 1 do Open Banking é de dados públicos, não envolvendo informações de usuários, e por isso ainda não há necessidade de consentimento. Para a fase 2, há consentimento do usuário para o compartilhamento de seus dados. Na resolução nº 1 [35] estão estabelecidos os requisitos mínimos para o compartilhamento de dados que deve acontecer, conforme as etapas apresentadas na Figura 2.3.

Figura 2.3: Passos para o compartilhamento de dados. (Fonte: Elaborado pela autora inspirado na [35]).

Essas etapas devem ser executadas considerando a segurança, agilidade, precisão e conveniência [35]. Além disso, precisam ocorrer exclusivamente em canais eletrônicos, de forma sucessiva e ininterrupta com duração competível ao objetivo e nível de complexidade.

Além disso, a prestação de informações aos clientes deve ser feita de forma clara, objetiva e adequada sobre as etapas do processo de compartilhamento, os procedimentos e o redirecionamento entre os ambientes ou sítios eletrônicos das instituições participantes [35].

Sobre o processo de solicitação de compartilhamento de dados, na etapa de consentimento, a resolução nº 1 determina itens mandatórios em sua composição conforme a seguir:

- solicitar por meio de linguagem clara, objetiva e adequada;
- apresentar a nalidade determinada para o objetivo do compartilhamento;
- conter prazo de validade compatível essa nalidade, porém limitado a doze meses;
- constar explicitamente a instituição transmissora de dados ou detentora de conta, de acordo com a solicitação de compartilhamento;
- detalhar os dados e/ou serviços para os quais o compartilhamento está sendo solicitado atendo-se estritamente às informações necessárias para o objeto do compartilhamento;
- constar a identi cação do cliente;
- ser obtido após a data de entrada em vigor da Resolução Conjunta e seus prazos por fases; e
- não ser obtido a partir de contrato de adesão, formulários com opção de aceite já preenchidos ou de forma presumida, sem a manifestação explícita feita pelo cliente.

Para que o cliente tenha domínio dos dados compartilhados, a revogação do compartilhamento poderá ser feita a qualquer momento a partir de sua solicitação, ao menos pelo mesmo canal de atendimento no qual o consentimento foi concedido [35].

Seguindo no processo de solicitação de compartilhamento de dados, a próxima etapa de nida pelo normativo é a autenticação. A norma estipula que a instituição transmissora dos dados deverá possuir mecanismos de autenticação de clientes e das instituições participantes. A autenticação do clientes deverá ser realizada a cada consentimento e a autenticação das instituições deverá ser feita a cada chamada das APIs.

Além disso, os procedimentos de autenticação deverão ser compatíveis com os já existentes nos canais eletrônicos da instituição inclusive em relação aos fatores, quantidades de etapas e duração também e compatíveis com a política de segurança cibernética da instituição.

Por m, relativo a con rmação do compartilhamento, a norma estabelece que a instituição transmissora de dados deve solicitar con rmação de compartilhamento ao cliente. A con rmação deverá ocorrer de forma simultânea aos procedimentos de autenticação e conter a identi cação da instituição receptora de dados, o período de validade do consentimento e os dados que serão objeto de compartilhamento.

A seguir serão apresentados os trabalhos correlatos ao objeto desta dissertação.

2.7 TRABALHOS CORRELATOS

A seguir são apresentados os trabalhos que possuem relação ao tema dessa pesquisa no contexto de taxonomias de requisitos, elicitação de requisitos e legislações como LGPD e GDPR.

Aberkane et al. [3] abordaram a utilização do processamento de linguagem natural (PNL) para oferecer um meio viável de automatizar a conformidade com a GDPR. Para tal, foi conduzida uma revisão sistemática da literatura (RSL) para explorar a literatura existente sobre a interseção de GDPR, PNL e Engenharia de Requisitos (ER). O Resultado da RSL identi cou 420 trabalhos que correlacionavam PNL x ER. Para a relação GDPR x PNL 9 trabalhos foram identi cados. Já no contexto da GDPR x ER, 20 trabalho e por m apenas 1 trabalho relacionando os três temas GDPR x PNL x ER. Os autores registraram que os resultados da RSL indicaram oportunidades para preencher a lacuna citada na convergência desses três temas. Também foram destacadas como resultados a identi cação de possibilidades para a introdução de técnicas de PNL na automatização de tarefas manuais de engenharia de requisitos em relação a GDPR assim como a utilização de técnicas de aprendizado de máquina baseadas em PNL para alcançar conformidade com GDPR na engenharia de requisitos. O trabalho dos autores se diferencia deste projeto por abordar uma possibilidade de automação no levantamento de requisitos e por não abordar taxonomias de requisitos.

Alves e Neves [7] estabeleceram uma análise empírica de questões sobre privacidade para elaboração de proposta de padrões de privacidade seguindo um guia de pesquisa qualitativa e Grounded Theory. Essa análise foi realizada a partir de entrevistas semi estruturadas (27 Questões) com pro ssionais com mais 10 de experiência e que acumulam cargos de gestão em uma organização pública. Foram feitas as análises nas transcrições das entrevistas que geraram como

resultado alguns pontos de perspectivas que podem auxiliar os pro ssionais de TI na elicitação de requisitos de privacidade e adicionalmente foram gerados padrões de privacidade aplicados pontualmente no Sistema piloto do contexto estudado. Este trabalho se difere do trabalho de Alves e Neves por propor uma taxonomia de requisitos de privacidade. Alves e Neves abordaram apenas a análise empírica das di culdades de elicitação dos requisitos de privacidade.

Kanwal et al. [83] desenvolveram o sistema de E-Health Cloud. As principais questões abordadas pelos autores relacionavam-se em como atender o trade-off entre privacidade e utilidade usando diferentes combinações de modelos de privacidade e técnicas de privacidade além de relacionar quais foram as técnicas de privacidade mais relevantes que poderiam ser adaptadas para obter privacidade na nuvem para o contexto e-Health. Um dos resultados da pesquisa foi uma taxonomia de Requisito de Preservação de Privacidade aplicado ao ambiente de nuvem do e-Health. Este trabalho difere da nossa pesquisa pois sua aplicação se limita à preservação da privacidade em ambientes de nuvem para sistemas de gestão de saúde.

Em 2015, Meis et al. [96] desenvolveram uma taxonomia de requisitos de transparência com base na ISO/IEC 29.000 [75] e no rascunho do Regulamento de Proteção de Dados da UE, uma vez que o GDPR[104] ainda não havia sido publicada. Essa taxonomia teve como objetivo fornecer aos engenheiros de software um método para identi car os requisitos de transparência. Eles analisaram a descrição dos princípios de privacidade na ISO e as formulações do projeto do regulamento. As palavras utilizadas para o processo de construção da taxonomia foram verbos como informar, noti car, documentar, apresentar, fornecer, explicar, comunicar e substantivos relacionados. Este trabalho encontrou trinta requisitos de transparência e sua validação foi executada comparando outras taxonomias encontradas em uma Revisão Sistemática da Literatura. O projeto de Meis et al. se difere deste por estar relacionado com requisitos de transparência e não de privacidade. Também se difere por ser baseado em um rascunho da GDPR, já este trabalho a LGPD, legislação brasileira vigente e aprovada em 2018.

Trabalhos anteriores à publicação da GDPR já abordavam a necessidade de taxonomias [6, 15, 19, 16, 108]. Alqassem e Svetinovic [6] no escopo da Internet das Coisas (IoT), apresentaram uma taxonomia de requisitos de segurança e privacidade para a IoT. Os autores a rmaram que a obtenção dos requisitos de privacidade e segurança em uma fase de concepção do projeto é crucial para criação de um vínculo com o público visando o desenvolvimento da uma satisfatória con ança pública, facilitando a adaptação desses sistemas de IoT. Para criar a taxonomia, os autores utilizaram a estrutura proposta por Firesmith [59], a qual fornece uma base para reorganizar os requisitos de segurança. Esta pesquisa se diferencia do trabalho proposto por Firesmith [59] porque o autor focou apenas em requisitos de segurança em ambientes de IoT.

Barker et al. [19] destacaram a importância da privacidade para a comunidade de banco de dados. Os autores forneceram uma de nição explícita de privacidade de dados adequada para Sistemas de Gerenciamento de Dados (SGBDs). Esta mininge propôs uma taxonomia capaz de abordar a privacidade de dados tecnologicamente. A principal contribuição destacada pelos autores foi uma de nição de privacidade. O trabalho de Barker et al difere-se da abordagem deste

projeto, uma vez que os autores utilizaram de nições da literatura além de seu foco de trabalho em SGBD de forma geral enquanto nesta dissertação é considerada a LGPD [42] como base para criação da taxonomia e de ne uma taxonomia prática listando os próprios requisitos.

Massey e Antón [92] realizaram uma comparação entre uma taxonomia de engenharia de requisitos de proteções de privacidade e vulnerabilidades com uma taxonomia de danos legais de privacidade. A abordagem metodológica para comparação consistiu em comparar cada vulnerabilidade da Taxonomia de Antón-Earp com cada categoria de danos legais de privacidade na Taxonomia Solove e determinar se a vulnerabilidade poderia ser razoavelmente interpretada como sendo um subconjunto, um superconjunto ou completamente não relacionado entre si. Como resultado seis das sete vulnerabilidades na taxonomia de Antón-Earp foram mapeadas para no máximo duas categorias de danos à privacidade. Sugerindo assim similaridade razoável entre essas duas taxonomias. O artigo em questão diferencia-se deste projeto por utilizar uma taxonomia jurídica como base para o processo comparativo, embora o Antón-Earp seja utilizado como base do artigo de Sangaroonsilp et al. [112].

Sangaroonsilp et al. [112] desenvolveram uma taxonomia de requisitos de privacidade baseada na GDPR e ISO/IEC 29100. Para o desenvolvimento desta taxonomia foram utilizadas as técnicas GBRAM e teoria fundamentada com um método de três passos para obtenção dos requisitos que resultou em uma lista de sete categorias com um total de 149 requisitos de privacidade. Todos os requisitos identi cados a partir da ISO/IEC 29100 estavam contemplados pelos encontrados na GDPR. Essa taxonomia foi utilizada como fundamentação para o desenvolvimento desta proposta de taxonomia baseada na LGPD e ISO/IEC 29100.

2.8 SÍNTESE DO CAPÍTULO

A engenharia de requisitos é disciplina na engenharia de software capaz de registrar as necessidades de um sistema. Os requisitos de privacidade, por sua vez, são a forma de documentar e colocar em execução nos sistemas a privacidade de dados necessária para a conformidade com essas legislações e alcance da proteção de dados. Nesse sentido, este capítulo apresentou a visão geral sobre esse tema e apresentou a GDPR e LGPD, legislações publicadas respectivamente pela união Europeia e Brasil com o intuito de preservar a privacidade dos dados pessoais dos cidadãos e assim aumentar a proteção desses dados. As duas legislações possuem princípios de privacidade que se assemelham e visam a preservação dos direitos fundamentais. A ISO/IEC 2900 é um frameworkque estabelece práticas para a privacidade de dados em sistemas de informação. Esses temas relacionam-se entre si quando requisitos de privacidade para a proteção de dados pessoais são necessários. O Open Banking é o sistema nanceiro aberto do Brasil que visa compartilhar os dados dos clientes entre instituições nanceiras a partir do consentimento fornecido pelo cliente. Esse processo é avaliado sob a perspectiva de engenharia de software, em relação a implementação dos requisitos de privacidade derivados da LGPD e por m, os trabalhos correlatos apresentados abordaram de diferentes formas a LGPD e taxonomias de requisitos porém nenhum

deles identi cou uma taxonomia de requisitos de privacidade voltada a legislação brasileira.

3 REVISÃO SISTEMÁTICA DE LITERATURA

Uma revisão sistemática de literatura (RSL) foi realizada para identi car as taxonomias de privacidade existentes na literatura com o objetivo de apoiar a elaboração da taxonomia proposta neste trabalho de dissertação.

As diretrizes de execução da RSL foram consideradas para identi cação das taxonomias existentes no âmbito da engenharia de software. A análise da literatura proposta objetiva identi car a unidade e a diversidade interpretativa existente para a temática na qual o problema em estudo está inserido. Além disso, esta revisão é necessária para compor as abstrações e sínteses requeridas em pesquisas dessa natureza colaborando para a coerência nas argumentações do pesquisador [54]. Assim, a revisão foi conduzida seguindo a abordagem proposta por Kitchenham at al [85], considerando as três principais fases da revisão:

F.1 Planejamento: a proposta desta fase é identi car a necessidade da revisão sistemática de literatura [86] e propor um protocolo para a sua condução. É necessário estabelecer os objetivos, de nir as questões de pesquisa e desenvolver um protocolo para conduzir a revisão;

F.2 Condução: Nesta fase é desenvolvida a estratégia de pesquisa para identi car os estudos e selecioná-los de acordo com o protocolo de nido na fase anterior [86]. Um conjunto de dados é criado para analisar e gerar os resultados para as questões de pesquisa;

F.3 Relatos: Após conduzir a fase de pré-visualizações, é preciso relatar as descobertas, comunicar as partes interessadas ou que podem estar interessadas [86] e responder as questões de pesquisa.

3.1 PLANEJAMENTO DA REVISÃO

A F.1 de planejamento da revisão foi executada em conjunto ao primeiro passo dessa dissertação, com a de nição dos objetivos de pesquisa apresentados na Seção 1.3 e questões de pesquisas nesta Seção em relação aos requisitos de privacidade e taxonomia proposta.

Com o objetivo de de nir uma taxonomia de requisitos de privacidade baseada na LGPD e ISO/IEC 29100, as seguintes questões de pesquisa foram de nidas:

QP.1 Quais as taxonomias de requisitos de privacidade existentes na literatura?

QP.2 Existe na literatura uma taxonomia de requisitos de privacidade baseada na LGPD e ISO/IEC?

3.2 CONDUÇÃO

A F2 da RSL consiste no desenvolvimento da estratégia de pesquisa (execução do protocolo proposto) para identi car os estudos, selecionar os trabalhos, extrair os dados dos estudos primários e gerar os resultados para a etapa 3, em que as questões de pesquisa serão respondidas.

3.2.1 Estratégia de Pesquisa

Tendo os objetivos e questões de pesquisa de nidas, os parâmetros da estratégia de pesquisa foram estabelecidos para que fossem executadas pesquisas automatizadas nas bases de dados digitais ACM Digital Library, Scopus e Web of Science, com intuito de coletar e analisar os trabalhos relacionados ao contexto de taxonomias e requisitos de privacidade. A escolha das bases digitais para essa RSL baseia-se em [86, 27], autores que listam estes repositórios como bases de relevância na execução exaustiva de pesquisas em engenharia de software. Além da pesquisa automatizada foram executadas pesquisas manuais em anais de congresso e em periódicos que possuem trilhas voltadas para a área. A string de busca utilizada foi: ("Taxonomy" AND ("Requirements Taxonomy" OR "Privacy Requirement Taxonomy" OR "Privacy Requirement Elicitation" OR "Requirements Gathering"))

Os estudos selecionados a partir da string de busca foram analisados utilizando a ferramenta Parsifal[1]. Foram seguidos os passos descritos por Kitchenham e Charters [86], conforme apresentado nas seções a seguir.

3.2.2 Critérios de Seleção

Os critérios de seleção dos estudos são utilizados para identi car os estudos primários capazes de fornecer evidências diretas sobre uma questão de pesquisa. Para reduzir a probabilidade de viés, os critérios de seleção foram decididos durante a de nição do protocolo, antes da execução das pesquisas. Essa seleção foi baseada na análise dos critérios de seleção de nidos desta revisão.

Em relação aos critérios de inclusão, foram consideradas as seguintes a rmações: IC.1) estar disponível para leitura em língua portuguesa ou inglesa em uma das bibliotecas digitais desta pesquisa; IC.2) estar em conformidade com a string de busca; e IC.3) propor, analisar, aplicar ou contemplar taxonomias no contexto de requisitos de privacidade.

Em relação aos critérios de exclusão foram de nidos: EC.1) o não atendimento dos critérios de inclusão de nidos acima implicam na exclusão dos trabalhos; EC.2) trabalhos que não apresentam informações su cientemente elaboradas (que não tenham a apresentação estrutura dos argumentos, impedindo o entendimento); e EC.3) trabalhos que impactam na extração os dados necessários para o seu entendimento (trabalhos que não possuam estruturação dos resultados impedindo a identi cação dos itens mapeados para a extração) e prejudicando a qualidade ou

[1] https://parsif.al/

relevância desta revisão.

3.2.3 Avaliação da Qualidade dos Estudos

As questões de avaliação de qualidade, consideradas críticas por Kitchenham e Charters [86], foram de nidas considerando a adequação ao objetivo e questões de pesquisa com intuito de minimizar viés e maximizar a validade do processo. As questões a serem avaliadas em cada um dos estudos pré-selecionados e estão listadas a seguir:

QA1) Os aspectos relacionados à elicitação de requisitos de privacidade são abordados no estudo?

QA2) A taxonomia proposta é relacionada à requisitos de privacidade?

QA3) Os autores apresentam o método de proposição da taxonomia?; e

QA4) O estudo apresenta os resultados da aplicabilidade dos métodos?

As duas primeiras questões forma construídas considerando que de acordo com o Guideline de [86], podem-se estabelecer questões relacionadas com itens especí cos relacionados à área de assunto da revisão. As duas últimas questões, estão relacionadas com qualidade do método de pesquisa executado nos trabalhos avaliados.

Para que métricas quantitativas das QA pudessem ser obtidas, foram atribuídas escalas numéricas às perguntas. As pontuações são:

- QA1: S (Sim) são apresentadas informações relacionadas à elicitação de requisitos de privacidade; P (Parcialmente), são identi cados aspectos de elicitação de requisitos implícitos, por dedução, por análise empírica deste autor; N (Não), nenhum aspecto de elicitação de requisitos de privacidade pode ser identi cado.
- QA2: S (Sim), a taxonomia é relativa à requisitos de privacidade; P (Parcialmente), a taxonomia proposta está parcialmente relacionada com requisitos de privacidade e a ns por análise empírica deste autor; N (Não), a taxonomia não está relacionada com requisitos de privacidade.
- QA3: S (Sim), o método de proposição da taxonomia está apresentado; P (Parcialmente), o método de proposição da taxonomia não está completamente apresentado; N (Não), o método de proposição da taxonomia não foi apresentado.
- QA4: S (Sim), os resultados da aplicabilidade dos métodos foram apresentados; P (Parcialmente), os resultados da aplicabilidade dos métodos foram parcialmente apresentados; N (Não) os resultados da aplicabilidade não foram apresentados.

Para o processo de avaliação de qualidade, temas que possuem semelhança com os conceitos de privacidade foram considerados para atribuição das notas em relação ao item QA2 referente

a requisitos de privacidade, os quais foram: contexto de segurança, contexto regulatório (leis governamentais), conceitos de transparência e intervenabilidade.

O processo de pontuação para as perguntas de avaliação de qualidade foram S = 1, P = 0.5, N = 0. Como parte do processo de avaliação de qualidade, foi de nida a métrica de taxa média conforme fórmula apresentada 3.1, para que fossem calculadas as notas de corte para adequação às avaliações de qualidade (QA). Assim, a nota de corte é o valor igual ou superior ao obtido na aplicação da fórmula em que é divido o somatório de pelo .

$$x = \frac{(\quad P \quad)}{} \tag{3.1}$$

Onde:
x = média entre os trabalhos
= notas atribuídas aos trabalhos na QA
= quantidade total de trabalhos avaliados

3.2.4 Extração dos dados

A extração dos dados foi iniciada com a obtenção dos arquivos no formato bibtex, a partir das pesquisas realizadas nas bases digitais. Nos arquivos as seguintes informações sobre os artigos foram extraídas:

- título,
- autor,
- ano,
- tipo de publicação e suas informações,
- palavras-chave,
- resumo
- e método de concepção da taxonomia.

Esses dados foram utilizados para a condução da fase F2 da RSL.

Para seguir com o processo de resposta das questões de pesquisa, que são de natureza qualitativa, e estão apresentadas na F3, foi necessária a extração de todos os artigos em formato PDF para leitura, análise e composição das respostas para as questões desta RSL.

3.3 RESULTADO DA RSL

A análise e resultado da execução desta RSL, para a fase F3, contendo os resultados obtidos na condução da pesquisa, análise da qualidade e os achados relativos às respostas para as questões de pesquisa estão apresentados a seguir.

3.3.1 Resultado da triagem dos artigos e Avaliação de Qualidade

O procedimento aqui descrito para condução desta RSL e a quantidade de trabalhos restantes após cada etapa são apresentados na Figura 3.1.

Figura 3.1: Procedimentos de pesquisa da RSL. (Fonte: Autora)

A aplicação da *string* de busca nas 3 bases digitais e busca manual que resultou em 111 artigos. Foram gerados arquivos .bib, conforme a execução da extração de dados contendo as informações dos trabalhos para importação na ferramenta de condução da RSL. Os arquivos estão disponibilizados no pacote de reprodução disponível em [55]. Primeiro, foram veri cados os trabalhos duplicados resultando em 15 exclusões. A base Scopus foi a que mais apresentou artigos duplicados em relação às outras bases (12 trabalhos duplicados). Em seguida os trabalhos candidatos foram classi cados conforme os critérios de seleção, inclusão e exclusão de nidos. A execução dos critérios de seleção resultou em 74 trabalhos rejeitados por não estarem em conformidade com os critérios estabelecidos. No total, essa primeira etapa da revisão resultou em 22 estudos selecionados.

Com a aplicação dos critérios de qualidade, os 22 trabalhos foram avaliados e pontuados de acordo com as métricas de nidas neste protocolo. Esses trabalhos e suas pontuações são apresentados na tabela 3.1. Apenas um trabalho obtive a pontuação máxima no processo, um trabalho pontuou 3.5, enquanto três trabalhos obtiveram pontuação 3.0, um trabalho se posicionou com metade da pontuação (2.0 pontos), quatro trabalhos obtiveram 1.5 pontos, três trabalhos obtiveram apenas 1 ponto, quatro obtiveram 0.5 pontos e por m dois trabalhos não pontuaram em nenhuma das perguntas do processo de avaliação de qualidade.

A partir do somatório da pontuação dos artigos analisados na avaliação da qualidade do estudo, foi efetuado o cálculo do valor médio de pontos obtidos pelos trabalhos com o objetivo de estabelecer uma nota de corte que indique o parâmetro aceitável para seguir para a próxima etapa.

Considerando a quantidade total de trabalhos (= 22) e o somatório das notas em pontos (= 32.5), a média obtida foi $x = 1.47$ (vide a fórmula 3.1). Como a pontuação atribuída às respostas das QAs não permite o valor decimal obtido para x, foram os trabalhos primários com 1.5 ou menos para eliminação por não atenderem os critérios estabelecidos na avaliação de qualidade demonstrando baixa aderência aos critérios esperados para este estudo. Os 11 estudos primeiros selecionados estão dispostos na seção selecionados da Tabela 3.1. Os outros trabalhos não foram selecionados devido ao score abaixo do estabelecido na condução dessa RSL.

A Tabela 3.1 é composta pelos seguintes campos: ID - Identi cador do estudo, utilizado para referenciá-lo a partir deste momento; Autor - nome dos autores e referência ao trabalho; Ano - ano de publicação; colunas QA1 a QA4 - Questões de avaliação de qualidade e as respectivas notas para os estudos nas linhas; Score - nota atribuída ao trabalho considerando a soma das 4 notas obtidas nas QAs.

	ID	Autor	Ano	QA1	QA2	QA3	QA4	Score
Selecionados	S1	Antón and Earp [15]	2004	S	S	S	S	4.0
	S22	Sangaroonsilp et al [112]	2021	S	S	P	S	3.5
	S2	Meis and Heisel [94]	2016	P	P	S	S	3.0
	S3	Hernández et al [71]	2010	P	P	S	S	3.0
	S4	Meis and Heisel [95]	2017	P	P	S	S	3.0
	S5	Siegfried et al. [116]	2020	N	N	S	S	2.0
	S6	Rjaibi and Rabai [108]	2015	P	P	P	N	1.5
	S7	Lehnert [88]	2011	S	P	N	N	1.5
	S8	Bolchini et al. [24]	2003	N	N	P	S	1.5
	S9	Alhirabi et al. [5]	2021	S	N	N	P	1.5
	S10	Tang et al. [119]	2021	S	N	N	S	1.5
Removidos	S11	Azad and Martens [18]	2021	N	N	S	N	1.0
	S12	Lauenroth et al. [87]	2017	N	N	N	S	1.0
	S13	Bhatia et al. [23]	2016	P	N	N	P	1.0
	S14	Gómez Sotelo et al. [65]	2018	N	N	P	N	1.0
	S15	Zafar et al. [125]	2020	N	N	P	N	0.5
	S16	Ahmed et al. [4]	2019	N	N	P	N	0.5
	S17	Belani [21]	2012	N	N	P	N	0.5
	S18	Abdelmaboud [2]	2021	N	N	P	N	0.5
	S19	Gordieiev and Kharchenko [66]	2020	N	N	N	P	0.5
	S20	Chen and Dong [38]	2013	N	N	N	N	0.0
	S21	MacRuairi et al. [90]	2008	N	N	N	N	0.0

Tabela 3.1: Lista de trabalhos selecionados e removidos após a aplicação da avaliação de qualidade.

Após a realização da fase de avaliação de qualidade, os 11 trabalhos restantes foram lidos pelo processo de leitura de texto completo para identi car e con rmar sua relação com o contexto dos requisitos de privacidade. Durante este processo, 4 artigos foram identi cados como não relacionados a este contexto da RSL (S5, S7, S9 e S10 da Tabela 3.1).

Isso ocorreu devido ao fato de que S5 [116] forneceu uma taxonomia de requisitos de sistema

no contexto da Indústria da Internet das Coisas. S7 [88] propôs uma taxonomia para análise de impacto de mudanças de software, uma taxonomia não relacionada diretamente aos requisitos, e sua abordagem não foi considerada signi cativa para esta RSL. Em S9 [5], embora os autores indiquem entre as principais contribuições a proposição de uma taxonomia, não há indicação de taxonomia no desenvolvimento ou conclusão do trabalho, tornando-o inadequado para esta RSL. E por último, S10 [119] não apresentou proposições de taxonomias, e foi considerado como não adequado para este protocolo RSL.

A distribuição dos artigos selecionados nessa RSL ao longo dos anos, conforme apresentado na Figura 3.2, demonstra que os anos com mais publicações relacionadas ao assunto são 2017 e 2020, considerando que o ano de 2021 é relativo apenas aos 10 primeiros meses do ano pelo período em que as consultas foram executadas, conforme datas de execução destas pesquisas para o protocolo de RSL. Os anos com mais publicações estão relacionados aos anos em que as legislações GDPR [104] e LGPD [42], respectivamente, entraram em vigor podendo demonstrar alguma relação positiva com a preocupação com as questões relacionadas à privacidade de dados pela literatura.

Figura 3.2: Distribuição dos artigos selecionados ao longo dos anos. (Fonte: Autora)

3.3.2 QP.1 Quais são as taxonomias de requisitos de privacidade existentes na literatura?

S1 - Antón e Earp [15] propuseram uma taxonomia de requisitos de privacidade baseada nas políticas de websites com o objetivo de mitigar a vulnerabilidade desses sites. Os autores utilizaram a mineração de metas (Goal Mining) e a extração de objetivos dos pré-requisitos de artefatos de texto (normas dos sites). Além disso, os autores analisaram um conjunto inicial de políticas de privacidade da Internet para desenvolver a taxonomia. A validação da taxonomia foi realizada a partir da extração das metas que envolviam políticas de privacidade de alguns sites relacionados à saúde. A partir dos resultados da validação, a taxonomia foi re nada, resultando em duas

classes de requisitos de privacidade: metas de proteção e vulnerabilidades. Nesse sentido, as metas de proteção foram utilizadas para tratar da proteção desejada dos direitos de privacidade do consumidor, enquanto as vulnerabilidades descrevem requisitos que potencialmente ameaçariam a privacidade do consumidor. Essa taxonomia possui uma aplicabilidade direcionada e exclusiva ao âmbito de *websites* e registra-se ter sido desenvolvida anteriormente a implantação da GDPR, pode ser considerada defasada.

S22 - Os autores Sangaroonsilp [112] propuseram uma taxonomia de requisitos de privacidade baseada na GPDR e ISO/IEC 29100 e também efetuaram uma análise para avaliar como duas grandes plataformas open source (Moodle e Google Chrome) endereçam o assunto de privacidade. Os autores começam estabelecendo a taxonomia e em seguida efetuam o processo para a mineração de erros nas plataformas em busca de avaliar a aderência dessa plataforma com os requisitos propostos na taxonomia gerada. O método de proposição da taxonomia foi baseado em um processo adaptado do GBRAM. A taxonomia proposta pelos autores foi dividida em 7 categorias e 71 requisitos de privacidade.

S2 - Meis e Heisel [94], abordaram a importância da privacidade como qualidade no âmbito do desenvolvimento de software. Os autores trataram especi camente de um objetivo de privacidade relativo à capacitação dos usuários nais e como estes podem ter controle sobre como os seus dados pessoais são processados pelos sistemas de informação. Esse objetivo de privacidade é denominado pelos autores como intervenabilidade. Os autores destacaram a falta de opções de intervenibilidade nos sistemas de informação, identi cada a partir de *surveys* conduzidas com usuários nais. Os autores executaram um processo de re namento do objetivo de intervenabilidade em uma taxonomia de requisitos de software e a relacionaram a uma taxonomia de requisitos de transparência, pois segundo os autores, a transparência pode ser considerada um pré-requisito para a intervenibilidade. O objetivo da taxonomia combinada de requisitos de intervenabilidade e transparência é o de orientar os engenheiros de requisitos na identi cação dos requisitos de intervenabilidade relevantes para o sistema. Na construção da taxonomia os autores utilizaram a ISO/IEC 29100 e o rascunho da GDPR (ressalta-se que a GDPR ainda não estava em vigor). Os autores executaram uma comparação desta taxonomia com a literatura, a partir de uma RSL com a técnica *snowballing* para validação de sua completude de requisitos em relação aos achados da RSL. A intervenabilidade pode ser assemelhada aos requisitos de privacidade, no entanto, este trabalho não apresentou aplicabilidade prática da taxonomia, não tendo sido realizada nenhuma validação em um contexto real além de ter sido concebido com o rascunho da GDPR.

S3 - O contexto do estudo primário dos autores Hernández et al. [71] contemplou a construção de software para e-commerces. Considerando esse cenário, os autores propuseram uma taxonomia de requisitos composta pelos fatores de segurança, usabilidade bem como características para sites de e-commerce B2C (Business-to-Business - comércio entre empresas) e C2C (Consumer-to-consumer - comércio entre usuários pessoas físicas) com o objetivo de apoiar o desenvolvimento desses sites de comércio eletrônico para que se tornem utilizáveis e seguros. A taxonomia proposta pelos autores é baseada em três fatores: segurança, usabilidade e e-commerce. No âmbito da segurança os autores se basearam no trabalho de Calderón [29] que propôs uma

taxonomia de requisitos de segurança dividida nos atributos de con dencialidade, integridade, disponibilidade e não repúdio em requisitos. Para o fator de usabilidade os autores se basearam em Cheikhi et al. [37], Jinling et al. [80], and Shaikh et al. [114] que também dividiram os atributos desse fator em requisitos. Para o fator de e-commerce, um survey foi conduzido para obtenção dos requisitos desejados pelos usuários a partir de grandes sites do ramo. Para validação da taxonomia, os autores desenvolveram um modelo composto por uma fórmula baseada em cálculo de média e uma técnica para avaliar a conformidade das funcionalidades de um site B2C (Business-to-Consumer - comércio de empresa para clientes pessoa física) ou C2C, no que diz respeito aos requisitos propostos na taxonomia de requisitos. A técnica utilizada para a validação consistiu em de nir uma meta, estabelecer construtores a serem avaliados, de nir questões para identi - car como medir os atributos, veri car o percentual de conformidade entre as funcionalidades de um sistema e seus requisitos, e por m obter a taxa do sistema pela média da conformidade dos construtores. Essa taxonomia não está diretamente relacionada a privacidade, e sim a segurança, o que é comum uma vez que muitos autores consideram a privacidade como parte da segurança [61, 82, 126, 98].

S4 - É uma continuação do trabalho de Meis and Heisel [94] (S2) sobre requisitos de intervenabilidade. As diferenças apresentadas em relação ao trabalho anterior foram que a GDPR estava em vigor no período dessa publicação, o que permitiu a criação da taxonomia a partir da lei aprovada. Além disso, os autores propuseram um método denominado ProPAn para análise de problemas baseados em privacidade. Neste método, os requisitos de intervenabilidade e transparência podem ser gerados automaticamente com base em artefatos fornecidos pelo método ProPAn e regras derivadas da GDPR. Ademais, o método fornece condições de validação dos requisitos que podem ser usadas para veri car automaticamente ajustes dos usuários nas especi cações de forma a garantir o atendimento às necessidades implícitas da GDPR. Todas essas etapas do método estão integradas na ferramenta ProPAn que é executada na geração e validação de forma automática. Apesar de ser denominada taxonomia de intervenabilidade e transparência, o estudo apresenta alguma relação subjetiva com os requisitos de privacidade.

S6 - Rjaibi e Rabai [108] propuseram uma taxonomia de segurança com uma visão holística. A proposta da taxonomia foi baseada nas taxonomias existentes na literatura e identi cadas pelos autores, também foram considerados os padrões de segurança, sendo eles: ISO 7498-2:1989 [72], CIA Triad, Donn Parker [103], Firesmith [58], Mead and Stehney [93], Christian e Mead [39], Jrjens [81] e Calderón [29]. O trabalho discorreu sobre cada uma das fontes para a taxonomia e apresentou uma comparação entre a colocação dos fatores de segurança em cada uma das taxonomias. Não ocorreu aplicação prática da taxonomia em um cenário real. A privacidade foi abordada como um fator de segurança nessa taxonomia que apresenta 8 (oito) sub-fatores.

S8 - Bolchini et al. [24] propuseram uma taxonomia para classi cação de requisitos de hipermídia. O modelo proposto adotou uma abordagem orientada a objetivos juntamente com técnicas baseadas em cenários, introduzindo a taxonomia de requisitos de hipermídia para facilitar o design conceitual da Web. A taxonomia proposta foi baseada no modelo AWARE que é uma especialização do framework. A taxonomia gerou 8 (oito) categorias principais e os autores

zeram a validação empírica do modelo com base na teoria dos atributos de qualidade percebida. Além disso, um estudo de caso foi desenvolvido para validação prática com parceiros industriais que demonstraram, em geral, considerar o AWARE [31] uma proposta de boa qualidade para os requisitos de modelagem de aplicativos da web. Apesar de ser uma taxonomia de requisitos, essa proposta não abordou o contexto de privacidade, focando apenas na abordagem de requisitos funcionais para aplicativos web.

Por m, as taxonomias analisadas nesta RSL com seus respectivos detalhes são apresentados na Tabela 3.2. A tabela é composta pelas colunas: ID - Identi cador do estudo primário; Fonte - fonte da qual os requisitos da taxonomia foram inspirados; Método - método utilizado para elaboração da taxonomia (mantidas em inglês para preservação do entendimento); Categorias - primeiro nível da categoria de requisitos obtida a partir das taxonomias (mantidas em inglês para preservação do entendimento); Relação com PR? - indica se a taxonomia possui relação com requisitos de privacidade (RP).

ID	Fonte	Método	Categorias	Relação com RP?
S1 [15]	traditional e-commerce web site privacy policies	GBRAM [14]	Privacy Vulnerability Information monitoring Information aggregation Information storage Information transfer Information collection Information personalisation Contact Protection Goal Taxonomy Notice/Awareness Choice/Consent Access/Participation Integrity/Security Enforcement/Redress	Parcialmente

ID	Fonte	Método	Categorias	Relação com RP?
S22 [112]	-ISO/IEC29100 [75] -GDPR [104]	GBRAM [14] e Grounded Theory [62]	Lawfulness, fairness and transparency Purpose limitation Data minimisation Accuracy Storage limitation Integrity and con den-tiality Accountability	Sim
S2 [94]	- ISO/IEC29100 [75] - GDPR Draft	proposto pelos autores, ne-nhuma técnica explicitada	Transparency Presentation Exceptional Informa-tion Processing Information Collection Information Storage Information Flow Information	Parcialmente
S3 [71]	- ISO/IEC27000 [74] - ISO/IEC9126 [73] - Survey nos e-commerces	Baseado on Calderón [29], nenhuma técnica explicitada	Security Con dentiality Integrity Availability Non-repudiation Usability Understandability Learnability Operability Attractiveness e-Commerce Product lookup User account Information/Help Spe-cial offers	Parcialmente

ID	Fonte	Método	Categorias	Relação com RP?
S4 [95]	- ISO/IEC29100 [75] - GDPR [104]	Proposto pelos autores: ProPan	Intervenability Data Subject Intervention Authority Intervention Processing Information Exceptional Information Intervention Information	Parcialmente
S6 [108]	- ISO 7498-2 [72] - CIA Triad [9] - Donn Parker [103] - Firesmith [58] - Mead and Stehney [93] - Christian and Mead [39] - Jrjens [81] - Calderón [29]	Compilação desses modelos	Security Conformance Secure Information Flow Freshness Fare Exchange Usability Attack/Harm Dectection Access Control Manageability Non-repudiation Integrity Privacy	Parcialmente
S8 [24]	- AWARE [31]	AWARE	Content Structure of Content Access Paths to Content Navigation Presentation User Operation System Operation Interaction	Parcialmente

Tabela 3.2: Relação de taxonomias identi cadas na RSL.

3.3.3 QP.2 Existe na literatura alguma taxonomia de requisitos de privacidade baseada na LGPD and ISO/IEC?

Essa revisão sistemática de literatura não identi cou taxonomia de requisitos de privacidade na literatura avaliada no contexto estabelecido para esta pesquisa. A taxonomia de Sangaroonsilp el al [112] aborda o contexto de requisitos de privacidade sob a perspectiva da GDPR. E foram identi cadas, no entanto, taxonomias que demonstram alguma relação com requisitos de privacidade as quais são os trabalhos desenvolvidos por Antón e Earp [15], Meis e Heisel [94], Hernández et al. [71], Meis e Heisel [95], Rjaibi e Rabai [108] e Bolchini et al. [24] Esses estudos abordaram o tema de forma indireta ou apenas por perspectivas.

Os resultados das questões QP.1 e QP.2 demonstram a lacuna na literatura referente a requisitos de privacidade, principalmente no âmbito das legislações de proteção de dados pessoais.

3.4 SÍNTESE DO CAPÍTULO

Essa RSL foi conduzida seguindo o protocolo de Kitchenham e Charters [86] com a de nição das etapas de planejamento, Condução e Relatos. Durante o planejamento as questões de pesquisa foram estabelecidas, a estratégia de pesquisa, os critérios de seleção e a avaliação de qualidade foram determinados. A partir da condução desta RSL, foram encontrados 111 trabalhos relacionados ao critérios da string de busca. Após do protocolo de RSL 7 estudos analisados. O trabalho desenvolvido por Sangaroonsilp el al [112] aborda o contexto de requisitos de privacidade sob a perspectiva da GDPR. Os trabalhos desenvolvidos por Antón e Earp [15], Meis e Heisel [94], Hernández et al. [71], Meis e Heisel [95], Rjaibi e Rabai [108] e Bolchini et al. [24] foram os que apresentaram taxonomias com alguma relação com requisitos de privacidade. No total, foram considerados 7 trabalhos com proposições de taxonomias que podem se relacionar a requisitos de privacidade porém a lacuna referente a existência de uma taxonomia de requisitos de privacidade foi identi cada.

4 TAXONOMIA

4.1 DESENVOLVIMENTO DA TAXONOMIA PROPOSTA

A proposição da taxonomia de requisitos de privacidade é baseada em Goal Based Requirements Analysis Method (GBRAM) [14], método utilizado para identi car, elaborar, re nar e organizar objetivos para a especi cação de requisitos. Esse método foi utilizado por Antón e Earp [15] no desenvolvimento da taxonomia de requisitos para redução de vulnerabilidades em websites e na taxonomia de requisitos de privacidade proposta por Sangaroonsilp et al. [112] baseada na GDPR e ISO/IEC 29100, processos utilizados como referência para este trabalho. A estruturação das técnicas utilizadas na concepção desta taxonomia são apresentadas na Figura 4.1.

Figura 4.1: Estruturação das técnicas utilizadas na concepção desta taxonomia. (Fonte: Autora)

O processo de Goal Analysis foi a técnica adaptada do GBRAM para criação dos 3 passos principais de elaboração da taxonomia. Goal Analysis tem o objetivo de explorar documentos

com a intenção de identi car metas, organizá-las e classi cá-las, criando-se assim os dois primeiros passos. Goal Evaluation também foi utilizado sob o aspecto da análise e adaptação de como as metas mudam desde o momento em que são identi cadas pela primeira vez até o momento em que se tornam requisitos de fato, criando-se assim o último passo da taxonomia.

Além disso, para elaboração do processo de concepção do primeiro passo a técnica Grounded Theory [62] foi utilizada. Dela foi utilizado o processo de codi cação aberta, que consiste em decompor os dados em unidades de análise e criar questões abertas sobre o tema.

Nickerson et al. [99] de nem que uma taxonomia é um agrupamento de conceitos em dimensões, cada uma dessas dimensões é composta por duas ou mais características. Para o desenvolvimento desta taxonomia utilizou-se uma regulamentação framework amplamente conhecido e estabelecido em relação à privacidade de dados que daqui em diante, quando referenciados em conjuntos serão endereçados como base taxonômica: a legislação brasileira de proteção de dados pessoais, a LGPD [42] e a ISO/IEC 29100 [75].

Na LGPD são protegidos os direitos da pessoa natural em relação ao tratamento de dados e estabelecidos princípios para o tratamento além de punições quando identi cadas irregularidades por parte dos agentes de tratamento [42]. A ISO/IEC 29100 [75], por sua vez, é um framework amplamente conhecido por de nir modelos também destinados a proteção de dados durante o seu tratamento. Como observado por Nickerson et al. [99], a necessidade de dimensões é implícita à taxonomia e para a proposição deste trabalho as dimensões atribuídas no contexto desta taxonomia de requisitos são os princípios da LGPD: Finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Além disso, a dimensão complementar relativa a classi cação dos requisitos estabelecida neste processo apresenta os contextos: software, estudos e pesquisa, governança, gestão pública e infraestrutura.

O método para o desenvolvimento desta taxonomia é divido em 3 passos principais que foram criados inspirados em [112] e de nidos a partir das técnicas do GBRAM [14]:

TP1 Identi cação dos requisitos de privacidade: responsável por analisar a legislação framework em busca dos requisitos de privacidade para composição da taxonomia. É um passo executado a partir de uma análise crítica dos documentos para composição dos itens.

TP2 Classi cação dos requisitos de privacidade: Elaborada a classi cação dos requisitos em categorias baseada em uma lista de objetivos de privacidade.

TP3 Re namento dos requisitos de privacidade: remoção dos possíveis itens duplicados e ajuste de possíveis inconsistências considerando duas fontes de identi cação para os requisitos.

4.2 TP1 - IDENTIFICAÇÃO DE REQUISITOS DE PRIVACIDADE

Para execução desta etapa foram analisadas declarações na LGPD e ISO/IEC 29100 com intuito de identi car declarações relacionadas ao tratamento de dados e direitos pessoais. Para tal foram analisados os 28 artigos da LGPD nos quais as declarações foram encontradas. Na ISO/IEC 29100 foram analisadas 58 declarações dentro dos princípios de privacidade estabelecidos por essa norma. Foram ao todo identi cados 112 requisitos de privacidade a partir da LGPD e 57 requisitos de privacidade a partir da ISO/IEC 29100. As instruções sobre cada um dos passos e o processo executado são apresentados a seguir.

TP1.a Identi cação de ações: As declarações da base taxonômica foram avaliadas com intuito de identi car declarações que remetam a ações necessárias por parte dos agentes de tratamento de dados, com intuito de permitir ao titular dos dados o alcance de seus direitos. Também foram analisadas as declarações na perspectiva dos titulares dos dados para identi cação de seus direitos. Essa análise visou identi car ações que remetam a requisitos que demandem implementação pelos sistemas, seja para atendimento de obrigações dos agentes de tratamento como também para contemplação de diretos dos titulares de dados. A pergunta feita pelos autores para identi cação das declarações foi: "Que ação deve ser executada com base nessa declaração?".

TP1.b Determinação das partes envolvidas/afetadas: Após o levantamento das sentenças que identi cam ações, o próximo passo foi analisar as ações no sentido da identi cação de seu objeto. Com isso, foi executada a identi cação dos responsáveis pela execução das ações. A pergunta que representa esta necessidade é "Quem está envolvido/afetado por essa a rmação?".

TP1.c Ponderação do resultado esperado: Esta etapa tem o objetivo de analisar as declarações mapeadas na base taxonômica para avaliar a sua aderência ao resultado esperado para a taxonomia em relação à privacidade dos usuários. A perspectiva a ser analisada é em relação a pergunta "O que deve ser alcançado com base na ação dessa declaração?".

TP1.d Estruturação em um padrão de requisito: Após a execução dos passos anteriores, o requisito de privacidade derivado do processo é estruturado no formato de verbo de ação, seguido por objeto e complemento objetivo. Formando o requisito para composição da taxonomia. Apesar de não haver registro dos autores [112] sobre a motivação da escolha da classe de palavras "verbo"para iniciar a estruturação dos requisitos, entende-se que no contexto da taxonomia, verbos de ação podem contribuir diretamente para a clari cação dos requisitos por indicarem atos a serem executados ou passíveis de execução. De acordo com Kaspary [84], o verbo é a peça-chave na enunciação dos diversos conceitos jurídicos, o que sustenta a estruturação iniciando com essa classe verbal.

A seguir são apresentados os exemplos de aplicação dos passos descritos em TP1 para a base taxonômica.

LGPD

A análise das declarações destacadas da LGPD pode começar com a execução da seção TP1.a ou pela seção TP1.b. Nesta exemplificação, será iniciado pelo passo TP1.a com a identificação das ações nas sentenças destacadas da LGPD. Para o primeiro exemplo, analisou-se a declaração 1, conforme Figura 4.2:

Figura 4.2: TP1 - Processo de Identificação de Requisitos de Privacidade. (Fonte: Autora)

TP1.a: Nela é identificado que o controlador de dados tem por obrigação indicar um encarregado para o tratamento de dados pessoais. A ação necessária nesta declaração é a indicação por parte do controlador, o verbo de ação utilizado então será o INDICAR .

TP1.b: o papel envolvido na declaração 1 apresentada na Figura 4.2 é o controlador, que é o ator que possui uma obrigação.

TP1.c: verifica-se que o objetivo da declaração é a indicação do encarregado pelo tratamento de dados pessoais.

TP1.d: Com a estruturação, o requisito fica da seguinte forma: RLGPD069 - INDICAR o encarregado pelo tratamento de dados pessoais

Seguindo para um exemplo que possui uma complexidade um pouco mais elevada em relação ao anterior, analisa-se a declaração 2, em que:

> Art. 14. § 2º No tratamento de dados de que trata o § 1º deste artigo (§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.), os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei (Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados

a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.)

TP1.a: é identificado que o controlador de dados deve manter pública a forma como os dados são coletados (...). Logo, a ação esperada do ator para o qual a declaração foi estabelecida é a manutenção, o verbo utilizado é o MANTER.

TP1.b: Os envolvidos/afetados identificados foram: 1) controladores de dados para a necessidade de (...) manter a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos (...); 2) titulares de dados sobre o trecho (...) para o exercício dos direitos a que se refere o art. 18 desta Lei. (...) possibilitar a exerção de seus direitos.

TP1.c: Como o artigo 14, relaciona-se com o artigo 18, são identificados alguns objetivos para o controlador para manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular a que se refere o art. 18 desta Lei.

TP1.d: Os requisitos gerados nesse processo são:

RLGPD039 - MANTER disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças;

RLGPD084 - MANTER disponível em área pública os procedimentos necessários para confirmação da existência de tratamento pelo titular;

RLGPD085 - MANTER disponível em área pública os procedimentos necessários para acesso aos dados pelo titular;

RLGPD086 - MANTER disponível em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados;

RLGPD087 - MANTER disponível em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;

RLGPD088 - MANTER disponível em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e in-

dustrial;

RLGPD089 - MANTER disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular;

RLGPD090 - MANTER disponível em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

RLGPD091 - MANTER disponível em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

RLGPD092 - MANTER disponível em área pública os procedimentos necessários para revogação do consentimento.

Os requisitos obtidos a partir da LGPD estruturados conforme os passos acima são listados na Tabela 1 do Apêndice I.2.

ISO/IEC 29100

Agora exempli cando o processo de análise das declarações destacadas da ISO/IEC 29100, iniciado pelo passo TP1.a com a identi cação das ações nas sentenças destacadas do framework. Para o primeiro exemplo, analisou-se a declaração 3, conforme citação:

> Aderir ao princípio de legitimidade e especi cação de propósito signi ca: garantir que a(s) nalidade(s) esteja(m) em conformidade com a lei aplicável e se baseie em uma base legal permitida.

TP1.a: Nela é identi cado que é necessário garantir que a nalidade do tratamento de dados esteja de acordo com as bases legais existentes e aplicáveis. A ação necessária nesta declaração é a garantia por parte do controlador, o verbo de ação utilizado então será GARANTIR .

TP1.b: tem-se que o envolvido nesta declaração é controlador, o ator que aparece implicitamente na declaração.

TP1.c: veri ca-se que o objetivo da declaração é garantir que a(s) nalidade(s) esteja(m) em conformidade com a lei aplicável e se baseie em uma base legal permitida

TP1.d: Com a estruturação, o requisito ca da seguinte forma: GARANTIR que a(s) nalidade(s) esteja(m) em conformidade com a lei aplicável e fundamentado(s) em uma base legal permitida

Os requisitos gerados neste processo de identi cação e estruturação para as declarações obtidas a partir da ISO/IEC 29100 são listados na Tabela 2 do Apêndice I.2.

4.3 TP2 - CLASSIFICAÇÃO DOS REQUISITOS DE PRIVACIDADE

Nesta etapa, foram de nidas as categorias da Taxonomia e executada a classi cação dos 169 requisitos obtidos na fase anterior de acordo com seus objetivos e então foi gerado o agrupamento dos requisitos de privacidade em categorias com base em seus objetivos. Esse processo foi divido em duas partes conforme a seguir.

TP2.a De nição das conquistas de cada meta de privacidade. Este passo descreve o esperado para cada princípio da LGPD, que será a categoria das metas dessa Taxonomia. Essa de nição será utilizada para identi car e reunir os requisitos de privacidade que possuem o mesmo objetivo do disposto em uma categoria. A execução deste passo ocorrerá apenas uma vez.

TP2.b Consideração do resultado esperado para um requisito. Classi cação dos requisitos de privacidade de acordo com a meta a qual sua realização é mais adequada.

Para a execução da TP2.a foram considerados os princípios de nidos na LGPD e na ISO/IEC 29100. A LGPD possui em sua composição 10 princípios que regem o tratamento de dados pessoais. A ISO/IEC 29100, por sua vez, possui 9 princípios porém para a implementação e para o desenvolvimento de sistemas de Tecnologia da Informação e Comunicação. Os princípios da LGPD e ISO/IEC 29000 possuem grande semelhança entre si, conforme demonstrado na Tabela 4.1:

LGPD	ISO/IEC29100
LP.1 Finalidade: o tratamento de dados deve ser limitado uma nalidade determinada com propósito legítimo que deverá ser explicitado ao titular dos dados;	PF.1 Consentimento e escolha: Possibilitar ao titular de dados a escolha sobre o processamento de seus dados pessoais e fornecer informações claras sobre o processo se tratamento; Deve permitir que o titular decidir por não aceitar o tratamento de seus dados pessoais; PF.2 Legitimidade e especi cação do propósito: Garantir a aderência a nalidade, noti cando ao usuário quando da utilização dos dados para uma nova nalidade. Garantir que a informação seja clara e objetiva;
LP.2 Adequação: o tratamento de dados deve ser compatível com o objeto (nalidade) descrito ao detentor do dado;	PF.3 Limitação de coleta: Garantir que os dados pessoais coletados sejam os apenas os estritamente necessários para o tratamento de dados necessário à nalidade que se propõe, além de ser necessário estar de acordo com as legislações existentes;

LGPD	ISO/IEC29100
LP.3 Necessidade: os dados utilizados no tratamento devem ser limitados estritamente à nalidade determinada no momento de sua coleta;	PF.4 Minimização de dados: Está intimamente ligado ao princípio de limitação de coleta de dados, indo além deste princípio por não estar relacionado apenas com a coleta mas também com o tratamento dos dados pessoais. Isso se dá pela minimização dos envolvidos no tratamento, usar sempre que possível soluções que primem pela não identi cação; PF.5 Limitação de uso, retenção e divulgação: Limitar o uso, a retenção e a divulgação dos dados pessoais ao cumprimentos de seus ns e reter os dados pessoais apenas pelo tempo necessário para a nalidade pela qual esses dados foram obtidos, aplicando processos de anonimização ou destruindo-os com segurança;
LP.4 livre acesso: permissão de consulta gratuita sobre a forma, a duração do tratamento e a integralidade de seus dados pessoais;	PF.8 Participação individual e acesso: Possibilitar ao titular meios para acessar e revisar seus dados pessoais desde que o acesso seja autenticado com nível de segurança apropriado. Além disso, estabelecer procedimentos para que os titulares possam exercer seus direitos;
PF.5 qualidade dos dados para o cumprimento da nalidade determinada no tratamento os dados devem estar exatos, claros, relevantes e atualizados;	PF.6 Precisão e qualidade: Garantir que os dados pessoais estejam precisos em relação a sua origem e obtenção e que estejam sempre atualizados garantindo a sua con abilidade. Assegurar que as alterações solicitadas pelo titular são legitimas e exatas. Propor processos para garantir a exatidão dos dados coletados e tratados.

LGPD	ISO/IEC29100
LP.6 transparência: deve-se garantir os titulares dos dados informações claras, precisas e de acesso facilitado sobre o tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;	PF.7 Abertura, transparência e noticação: Tornar acessíveis as informações sobre o processo de tratamento de dados pessoais e seus controles, práticas utilizadas. Noticar o titular sobre as informações do controlador e do processamento principalmente na ocorrência de grandes mudanças no processo de tratamento dos dados;
LP.7 segurança promover a segurança dos dados pessoais a partir de medidas técnicas e administrativas que protejam de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;	PF.10 Segurança da informação: Proteger os dados nos níveis necessários de controles em procedimentos operacionais, funcionais e estratégicos com o intuito de garantir a integridade, condencialidade e disponibilidade dos dados pessoais;
LP.8 prevenção estabelecimento e execução de medidas que previnam a ocorrência de danos em virtude do tratamento de dados pessoais;	PF.11 Conformidade de privacidade: Avaliar e demonstrar que o processo de tratamento de dados está de acordo com os requisitos necessários para sua proteção. Possuir controles internos aderentes à proteção necessária e possuir mecanismos de avaliação externos para garantir a lisura do processo.
LP.9 não discriminação: vedação à utilização dos dados para tratamentos com ns discriminatórios ilícitos ou abusivos;	
LP.10 responsabilização e prestação de contas: o agente de tratamento deve demonstrar as medidas adotadas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, além de apresentar a e cácia dessas medidas.	PF.9 Responsabilidade: Tornar registrados todos os procedimentos, controles, ferramentas e métodos utilizados no processamento de dados, fornecer treinamento adequado aos envolvidos no tratamento dos dados pessoais, considerar procedimentos de compensação quando situações reversíveis ocorram não permitindo ao titular voltar ao status de privacidade inicial;

Tabela 4.1: Relação entre os princípios da LGPD e ISO/IEC 29100.

Como foi demonstrado na tabela acima, todos os princípios da ISO/IEC 29100 são cobertos pelos princípios da LGPD. E o princípio da não discriminação da LGPD não está incluído em nenhum dos princípios da ISO. Princípios como os princípios I e II da ISO são cobertos pelo princípio I da lei. Além desses, os princípios IV e V da ISO são cobertos pelo princípio III

da LGPD. Considerando os pontos expostos, essa taxonomia se utilizará dos princípios da LGPD para a criação de suas categorias. A de nição das categorias é apresentada conforme as de nições:

LP.1 Finalidade: Esse objetivo de privacidade agrupa requisitos em que se registram que o tratamento de dados deve ser limitado uma nalidade determinada. Sua utilização e processamento não devem extrapolar a nalidade da qual o titular autorizou. Além disso, o propósito do tratamento de dados deverá ser legítimo e estar explicitado ao titular dos dados;

LP.2 Adequação Esse objetivo de privacidade refere-se a compatibilidade do tratamento de dados em relação à sua nalidade, que foi descrita ao titular dos dados no momento do consentimento. O tratamento de dados deve ocorrer de acordo com a nalidade e para seu alcance;

LP.3 Necessidade: Esse objetivo de privacidade compreende os requisitos que são relacionados com a utilização dos dados no tratamento de acordo com a necessidade descrita previamente no momento de seu consentimento e sua coleta. Ou seja, o tratamento deve ser limitado estritamente à sua nalidade;

LP.4 Livre acesso Esse objetivo de privacidade trata da permissão, por parte do titular dos dados, para consulta gratuita sobre a forma utilizada no tratamento de dados, a sua duração e a integralidade de seus dados pessoais que os agentes de tratamento possuem;

LP.5 Qualidade dos dados Esse objetivo de privacidade endossa o cumprimento da nalidade especí ca, conforme autorização do titular dos dados no momento de sua obtenção, no tratamento dos dados de forma a estarem exatos, claros, relevantes a nalidade e atualizados. Assim possibilitando mecanismos que garantam essas condições;

LP.6 Transparência: Esse objetivo de privacidade deve garantir aos titulares dos dados informações claras, precisas e de acesso facilitado sobre o processo de tratamento dos dados. Permitindo ao titular o conhecimento sobre como o tratamento ocorre. A transparência deve ser exercida também sobre os respectivos agentes de tratamento envolvidos no processo, observados os segredos comercial e industrial;

LP.7 Segurança Esse objetivo de privacidade visa promover a segurança dos dados pessoais a partir de medidas técnicas e administrativas que os protejam de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Essas medidas devem envolver controles e mecanismos de segurança adequados para garantia do processo de tratamento seguro;

LP.8 Prevenção Esse objetivo de privacidade aborda o estabelecimento e execução de medidas para prevenção da ocorrência de danos, aos titulares de dados assim como aos agentes de tratamento, em virtude do processo de tratamento de dados pessoais;

LP.9 Não discriminação Esse objetivo de privacidade contempla a vedação à utilização dos dados pessoais, previamente obtidos, para tratamentos com ns discriminatórios ilícitos ou

abusivos. Os dados obtidos dos titulares não devem ser usados para os propósitos diferentes, principalmente para exercício do crime de discriminação;

LP.10 Responsabilização e prestação de contas: Esse objetivo de privacidade endereça que o agente de tratamento deve demonstrar as medidas adotadas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Além disso, precisam apresentar a e cácia dessas medidas no cumprimento de seus objetivos.

Durante o processo de criação das categorias de requisitos para a taxonomia foi veri cada a necessidade de criar uma classi cação adicional para os requisitos de software dada a abrangência da LGPD [42] que contempla vários âmbitos da engenharia de software como processos e governança sobre o aspecto de proteção dos direitos pessoais.

Isso pois foram identi cados contextos além dos sistêmicos para os quais os requisitos se aplicam. Com isso, a perspectiva de construção da estrutura da taxonomia foi alterada para contemplar os contextos que re etem essas novas divisões de assunto identi cadas. Esses contextos serão de nidos adicionalmente à categoria para que os analistas de sistemas consigam classi car as necessidades dentro de sua instituição para a completa adequação à LGPD. São eles:

C.1 Software: identi ca requisitos de privacidade que podem ser implementados em softwares. Ou seja, requisitos de sistema que podem ser validados por regras de negócio em requisitos de privacidade;

C.2 Estudos e pesquisa: são requisitos de privacidade processuais que determinam como órgãos de pesquisa devem seguir para o tratamento de dados;

C.3 Governança: identi ca os requisitos que não necessariamente podem ser atendidos por sistemas, mas que precisam ser implementados pela organização, com controles e mecanismos de governança para a garantia dos princípios da LGPD;

C.4 Gestão Pública: os requisitos que são obrigatórios para órgãos de natureza pública, que precisam ser implementados pela organização para garantir a aderência à legislação principalmente para o tratamento de dados sem a necessidade de consentimento, resguardados pelo direito da natureza dessas instituições; e

C.5 Infraestrutura : requisitos sobre o processo de transferência internacional de dados com terceiros além processos e controles de armazenamento de dados.

Os requisitos de privacidade podem estar relacionados a uma categoria e também a um contexto. Os contextos podem se repetir pelas categorias. A categoria ainda é o agrupador principal dessa taxonomia por re etir os princípios da LGPD. Na Figura 4.3 são apresentados os relacionamentos identi cados entre categorias e contextos para os requisitos de privacidade elicitados para esta taxonomia. As linhas os relacionamentos entre as categorias e os contextos. Por exemplo,

Figura 4.3: Estrutura da taxonomia de requisitos de Privacidade. (Fonte: Autora)

o contexto Software se relaciona com todas as categorias enquanto o contexto Gestão Pública se relaciona apenas com as categorias de Finalidade, Necessidade e qualidade de dados.

A seguir são apresentados os exemplos de aplicação dos passos descritos em TP2 para a base taxonômica.

LGPD - Exemplificando a execução da etapa TP2.b, para classificar o requisito INDICAR o encarregado pelo tratamento de dados pessoais em uma das categorias acima. Seguindo o estipulado na etapa, é necessário considerar o resultado esperado para se alcançar com esse requisito. O objetivo desse requisito é indicar o encarregado pelo tratamento de dados pessoais ao titular dos dados, podendo assim ser categorizado no objetivo P.6 Transparência. Por se tratar de algo que não necessariamente será registrado/controlado por sistemas de informação e sim por processos de governança, por isso ele se classifica no contexto C.3 Governança.

ISO/IEC29100 - Para a ISO/IEC 29100, tem-se que para classificar o exemplo o requisito GARANTIR que a(s) finalidade(s) esteja(m) em conformidade com a lei aplicável e se baseie em uma base legal permitida refere-se a garantia do direito do titular de que o processamento de seus dados pessoais seja executado dentro da finalidade estabelecida. Desta forma, identifica-se que o requisito está aderente as definições do objetivo F.1 Finalidade. Para este requisito o contexto é o de software, por ser um requisito que precisa ser garantido no tratamento dos dados, com isso sua classificação de contexto é C.1 Software.

Nesta etapa os requisitos ainda podem estar duplicados entre si, o que será analisado na próxima etapa. A Seção 4.5 apresenta a classificação dos requisitos de privacidade para cada objetivo de privacidade detalhadamente.

4.4 TP3 - REFINAMENTO DOS REQUISITOS DE PRIVACIDADE

Para o refinamento foram avaliados os 169 requisitos obtidos a partir da base taxonômica (LGPD e ISO/IEC 29100), que podem ter semelhanças ou podem ser redundantes entre si. Com a classificação dos requisitos em categorias ocorreu a identificação dos requisitos semelhantes, que foram adequados para uma versão única e os duplicados foram excluídos.

Como exemplificação, a declaração da LGPD ("...) Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.(...") gerou o requisito RLGPD013 - COLETAR o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Enquanto na ISO/IEC 29100 o trecho ("...) obter o consentimento opcional do principal de PII para coletar ou processar PII confidenciais, exceto quando a lei aplicável permitir o processamento de PII confidenciais sem o consentimento da pessoa física") deriva o requisito RQISO3 - OBTER o consentimento opcional do titular de dados para coletar ou processar os dados confidenciais, exceto quando a lei aplicável permitir o processamento de dados confidenciais sem o consentimento da pessoa física. Os dois requisitos estão classificados na categoria P.1

Finalidade e podem ser mesclados para um requisito único o qual é OBTER o consentimento opcional do titular de dados para coletar ou processar os dados con denciais a partir de manifestação declarada deste, exceto quando a lei aplicável permitir o processamento de dados con denciais sem o consentimento da pessoa física

Com o processo de re namento 27 requisitos foram uni cados entre si enquanto 17 requisitos foram identi cados como duplicados, 3 requisitos obtidos da ISO/IEC e 3 requisitos obtidos da LGPD foram excluídos após análise por estarem fora do escopo dos requisitos de privacidade, restando 129 requisitos de privacidade.

4.5 TAXONOMIA DE REQUISITOS DE PRIVACIDADE LGPD+ISO/IEC 29100

A taxonomia de requisitos de privacidade proposta é composta por 129 requisitos que estão divididos em 10 categorias e 5 contextos, conforme ilustrado na Figura 4.4. O detalhamento da taxonomia é apresentada na Tabela 4.2.

Taxonomia de Requisitos de Privacidade
Finalidade
Software
RQ001 - COLETAR e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, especí ca e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento
RQ002 - LIMITAR o uso de dados à nalidade da coleta a menos que uma nalidade seja explicitamente exigida por lei aplicável
RQ003 - APAGAR os dados sempre que a nalidade do processamento de dados for alcançada e não houver requisitos legais para mantê-las
RQ004 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados ou para cumprimento de obrigação legal/regulatória pelo controlador
RQ005 - FINALIZAR o tratamento de dados pessoais no m do período de tratamento
RQ006 - MANTER disponível em área pública os procedimentos necessários para revogação do consentimento
RQ007 - INFORMAR que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador
RQ008 - COLETAR somente dos dados pessoais estritamente necessários para a nalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse
RQ009 - PERMITIR o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação

Taxonomia de Requisitos de Privacidade
RQ010 - PERMITIR o controlador de dados fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exijindo a proteção dos dados pessoais
RQ011 - PERMITIR o controlador de dados fazer o tratamento de dados pessoais para a proteção do crédito
RQ012 - DISPENSAR a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados
RQ013 - OBTER consentimento especí co para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais
RQ014 - PERMITIR ao controlador que seja feito o tratamento de dados para a nalidade de apoio e promoção a atividades
RQ015 - PERMITIR o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido
RQ016 - COLETAR consentimento especí co concedido por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças
RQ017 - COLETAR dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento
RQ018 - REALIZAR todos os esforços razoáveis para veri car que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador
Estudos e pesquisa
RQ019 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
Gestão Pública
RQ020 - TORNAR pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para execução de suas atribuições
RQ021 - INFORMAR ao titular de dados que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor

Taxonomia de Requisitos de Privacidade
RQ022 - NOTIFICAR o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a nalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua nalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público
RQ023 - FORNECER por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as nalidades públicas
RQ024 - GARANTIR que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a nalidades especí cas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais
RQ025 - PERMITIR por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse m especí co e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras nalidades
Adequação
Software
RQ026 - USAR ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identi cação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas
RQ027 - VEDAR o tratamento de dados mediante vicio de consentimento
RQ028 - PERMITIR ao titular a qualquer momento e mediante requisição, a revogação do consentimento
RQ029 - PERMITIR que o controlador efetue o tratamento de dados para proteção do exercício regular de seus direitos ou prestação de serviços que o bene ciem, respeitados os direitos e liberdades fundamentais do titular
Estudos e pesquisa
RQ030 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
Necessidade
Software

Taxonomia de Requisitos de Privacidade
RQ031 - PERMITIR o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma especí ca e destacada, para nalidades especí cas RQ032 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular apenas quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador RQ033 - PERMITIR o tratamento de dados pessoais mediante o consentimento expresso do titular de dados RQ034 - COMUNICAR o titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito RQ035 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral e também quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identi cação e autenticação de cadastro em sistemas eletrônicos
Estudos e pesquisa
RQ036 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis
Governança
RQ037 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por pro ssionais de saúde, serviços de saúde ou autoridade sanitária
Gestão Pública
RQ038 - PERMITIR a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres RQ039 - ASSEGURAR a adoção de um princípio de “necessidade de conhecimento”, ou seja, deve-se ter acesso apenas às informações que sejam necessárias para o desempenho de suas funções o ciais no âmbito do propósito legítimo do processamento de dados RQ040 - INFORMAR a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado RQ041 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública
Infraestrutura

Taxonomia de Requisitos de Privacidade
RQ042 - PERMITIR a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certi cados e códigos de conduta regularmente emitidos RQ043 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política RQ044 - PERMITIR a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento especí co e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras nalidades RQ045 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional RQ046 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro RQ047 - PERMITIR a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência RQ048 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional
Livre Acesso
Software
RQ049 - FORNECER aos titulares de dados a capacidade de acessar e revisar suas informações e obter cópia eletrônica integral de seus dados pessoais RQ050 - PERMITIR ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses
Qualidade de Dados
Software
RQ051 - GARANTIR que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a nalidade de uso; RQ052 - PERMITIR que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto especí co

Taxonomia de Requisitos de Privacidade
RQ053 - FORNECER qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos RQ054 - VERIFICAR, por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado
Governança
RQ055 - ESTABELECER procedimentos de coleta de dados para ajudar a garantir precisão e qualidade RQ056 - ESTABELECER mecanismos de controle para veri car periodicamente a precisão e a qualidade das informações coletadas e armazenadas
Gestão Pública
RQ057 - ARMAZENAR os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral
Transparência
Software
RQ058 - APRESENTAR as informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança RQ059 - INFORMAR ao titular dos dados, antes de qualquer novo processamento, de forma explícita, o teor das alterações de nalidade especí ca do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identi cação do controlador; e informações de contato do controlador, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração RQ060 - PERMITIR e providenciar ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a nalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular, a con rmação de existência ou o acesso aos dados pessoais e fornecer o acesso as informações e aos dados por meio eletrônico, seguro e idôneo para esse m ou sob forma impressa, a critério do titular RQ061 - PERMITIR ao titular revogar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, rati cados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação RQ062 - APRESENTAR a nalidade, a boa-fé e o interesse público que justi caram o tratamento de dados pessoais de acesso público

Taxonomia de Requisitos de Privacidade
RQ063 - PERMITIR que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento
RQ064 - ARMAZENAR os dados pessoais em formato que favoreça o exercício do direito de acesso por parte do titular de dados
RQ065 - INFORMAR aos titulares de dados, antes de obter consentimento, sobre seus direitos e possibilitar o entendimento das especi cidades exigidas para a nalidade especi cada no consentimento
RQ066 - USAR uma linguagem para esta especi cação que seja clara e apropriadamente adaptada a circunstâncias
RQ067 - FORNECER aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados
RQ068 - DIVULGAR as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações
RQ069 - PERMITIR que o titular de dados entenda os requisitos especi cados de retenção e eliminação de dados
Governança
RQ070 - INDICAR o encarregado pelo tratamento de dados pessoais
Segurança
Software
RQ071 - IMPEDIR a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades
RQ072 - BLOQUEAR os dados pessoais a que se refere a infração até a sua regularização
RQ073 - APAGAR os dados pessoais a que se refere a infração quando aplicável e legal
RQ074 - IMPLEMENTAR as preferências do titular de dados conforme expresso em seu consentimento
RQ075 - PERMITIR o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por pro ssionais de saúde ou por entidades sanitárias
Estudos e pesquisa
RQ076 - PERMITIR o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais
RQ077 - GARANTIR que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro
Governança

Taxonomia de Requisitos de Privacidade
RQ078 - PROTEGER as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, con dencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modi cação, divulgação ou perda ao longo do todo o seu ciclo de vida RQ079 - ASSEGURAR esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício RQ080 - IMPLEMENTAR controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas RQ081 - LIMITAR o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções RQ082 - RESOLVER riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos RQ083 - SUBMETER os controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo RQ084 - POSSUIR controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade RQ085 - DESENVOLVER e manter avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade
Infraestrutura
RQ086 - SELECIONAR processadores de dados que forneçam garantias su cientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles
Prevenção
Software
RQ087 - TORNAR o consentimento do titular nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca RQ088 - GARANTIR a adoção de 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 por parte dos agentes de tratamento

Taxonomia de Requisitos de Privacidade
RQ089 - TORNAR o consentimento do titular nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca
Estudos e pesquisa
RQ090 - PROTEGER a divulgação de dados pessoais em resultados de pesquisas de saúde
Governança
RQ091 - GARANTIR a adoção de 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 por parte dos agentes de tratamento
Não Discriminação
Software
RQ092 - PROTEGER para que os dados pessoais do titular não sejam utilizados em seu prejuízo RQ093 - VEDAR às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de bene ciários
Responsabilização e Prestação de Contas
Software
RQ094 - MANTER disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças RQ095 - NOTIFICAR todas as partes interessadas de privacidade relevantes sobre violações de privacidade RQ096 - PERMITIR que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e e cazes, como reti cação, expurgo ou restituição se ocorrer uma violação de privacidade RQ097 - FINALIZAR o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional RQ098 - NOTIFICAR o titular de dados da impossibilidade de adoção de medida imediata por não ser agente de tratamento dos dados e indicar, sempre que possível, o agente RQ099 - NOTIFICAR o titular de dados quando da impossibilidade de adoção imediata em relação a sua requisição indicando as razões de fato ou de direito que impedem a adoção imediata da providência RQ100 - FORNECER ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial RQ101 - APRESENTAR quando aplicável explicações su cientes para a necessidade de processar dados sensíveis

Taxonomia de Requisitos de Privacidade
RQ102 - MANTER disponível em área pública os procedimentos necessários para con r-mação da existência de tratamento pelo titular e as formas para o seu acesso
RQ103 - MANTER disponível em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados
RQ104 - MANTER disponível em área pública os procedimentos necessários para anonimi-zação, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em descon-formidade com a LGPD
RQ105 - MANTER disponível em área pública os procedimentos necessários para portabi-lidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial
RQ106 - MANTER disponível em área pública os procedimentos necessários para elimina-ção dos dados pessoais tratados com o consentimento do titular
RQ107 - MANTER disponível em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
RQ108 - MANTER disponível em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
RQ109 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados
RQ110 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados
RQ111 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desneces-sários, excessivos ou tratados em desconformidade
RQ112 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial
RQ113 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consenti-mento do titular, observadas as exceções previstas
RQ114 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
RQ115 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qual-quer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
Governança

Taxonomia de Requisitos de Privacidade
RQ116 - ADOTAR medidas para garantir a transparência do tratamento de dados por parte do controlador
RQ117 - APRESENTAR a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial
RQ118 - ATENDER a realização de auditoria, por parte da autoridade nacional, para ve-ri cação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial
RQ119 - GARANTIR a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador
RQ120 - COMUNICAR à autoridade nacional da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador
RQ121 - IMPLEMENTAR os requisitos de segurança, os padrões de boas práticas e de governança e as princípios gerais de tratamento de dados previstos e às demais normas regulamentares nos sistemas utilizados para o tratamento de dados pessoais
RQ122 - PUBLICIZAR a infração após devidamente apurada e con rmada a sua ocorrência
RQ123 - DOCUMENTAR e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade
RQ124 - ATRIBUIR a um indivíduo especí co dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade
RQ125 - FORNECER treinamento adequado para o pessoal do controlador de dados que terá acesso a informações
RQ126 - ESTABELECER procedimentos internos e cientes de tratamento de reclamações e reparação para uso pelos titulares de dados
RQ127 - PONDERAR os procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido
RQ128 - VERIFICAR e demonstrar que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados con áveis
Infraestrutura
RQ129 - GARANTIR que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados)

Tabela 4.2: Taxonomia de Requisitos de Privacidade.

Figura 4.4: Taxonomia de requisitos de Privacidade. (Fonte: Autora)

A taxonomia foi disponibilizada no pacote de reprodução [55].

4.6 COMPARAÇÃO DA COMPOSIÇÃO DAS TAXONOMIAS

O processo de obtenção dos requisitos de privacidade para composição da taxonomia baseada na LGPD e ISO/IEC 29100 foi apresentado nas seções anteriores. Nessa seção são apresentadas as principais diferenças encontradas entre os processo adotado nesta proposta de taxonomia e na proposta de Sangaroonsilp et al. [112].

Os verbos utilizados pelos autores da taxonomia GPDR+ISO/IEC 29100 [112], respeitando a tradução para a língua portuguesa são 17, enquanto para a taxonomia proposta neste trabalho, LGPD+ISO/IEC 29100, foram utilizados 44, conforme apresentado na Tabela 4.3. Os verbos comuns às duas taxonomias foram destacados em negrito, totalizando assim 12 interseções.

GPDR+ISO/IEC 29100 [112]	LGPD+ISO/IEC 29100 [Nossa proposta]
Apagar, Apresentar, Armazenar, Arquivar, Coletar, Fornecer, Implementar, Informar, Manter, Mostrar, Noti car, Obter, Permitir, Proteger, Solicitar, Transmitir e Usar	Adotar, Apagar, Apresentar, Armazenar, Assegurar, Atender, Atribuir, Bloquear, Coletar, Comunicar, Considerar, Desenvolver, Dispensar, Divulgar, Documentar, Estabelecer, Explicar, Finalizar, Fornecer, Garantir, Impedir, Implementar, Incluir, Indicar, Informar, Limitar, Manter, Minimizar, Noti car, Obter, Permitir, Ponderar, Possuir, Proteger, Publicizar, Realizar, Resolver, Reter, Selecionar, Submeter, Tornar, Usar, Vedar, Veri car

Tabela 4.3: Verbos utilizados nas taxonomias para estruturação dos requisitos.

Comparando a quantidade de artigos nos quais os autores Sangaroonsilp et al. [112] identi - caram declarações para composição da base taxonômica, tem-se que 18 artigos da GDPR foram analisados para criação da taxonomia, enquanto neste trabalho foram analisados 27 artigos da LGPD. Dos 65 artigos da LGPD, apenas 27 artigos possuíam declarações que se relacionavam com o processo de tratamento de dados pessoais e se encaixavam nas características destacadas nas etapas do procedimento para análise e concepção dos requisitos de privacidade. A sumarização dos artigos utilizados para pesquisa das palavras-chave na GDPR e na LGPD é apresentada na Tabela 4.4.

Artigos GDPR [104]	Artigos LGPD [42]
6º - Legalidade do tratamento;	7º – Condições para o tratamento de dados pessoais;
7º - Condições de consentimento;	8º – Condições para a obtenção do consentimento;

Artigos GDPR [104]	Artigos LGPD [42]
12º - Informação, comunicação e modalidades transparentes para o exercício dos direitos do titular dos dados;	9º – Acesso pelo Titular sobre o processamento de dados;
13º - Informação a prestar sempre que sejam recolhidos dados pessoais do titular dos dados;	10º – Tratamento de dados apenas para nalidades legítimas;
14º - Informação a prestar quando os dados pessoais não tenham sido obtidos junto do titular dos dados;	11º – Condições para o tratamento de dados pessoais sensíveis;
15º - Direito de acesso do titular dos dados;	12º – Critérios para anonimização;
16º - Direito à reti cação;	13º – Condições para o tratamento de dados pessoais para estudos em saúde pública;
17º – Direito ao apagamento ("direito ao esquecimento");	14º – Condições para o tratamento de dados pessoais de crianças e adolescentes;
18º - Direito à restrição do tratamento;	15º – Condições para o término do tratamento dos dados;
19º - Obrigação de noti cação relativa à reti cação ou apagamento de dados pessoais ou restrição de tratamento;	16º – Condições para conservação dos dados;
20º - Direito à portabilidade dos dados;	17º – Direitos do Titular de dados;
21º - Direito de oposição;	18º – Tipos de direitos do titular de dados;
22º - Tomada de decisão individual automatizada, incluindo a de nição de per s;	19º – Condições para con rmação de existência ou o acesso ao dados pessoais pelo titular;
25º - Proteção de dados desde a conceção e por defeito;	20º – Direito de solicitação de revisão de decisões tomadas a partir de tratamentos automatizados;
29º - Processamento sob a autoridade do controlador ou processador;	21º – Garantia de não prejuízo ao titular pelos seus dados;
30º - Registros de atividades de processamento;	23º – Condições para o tratamento de dados pessoais pelo poder público;
32.º - Segurança do processamento;	25º – Manutenção de dados em formatos interoperáveis entre os órgãos do poder público;
33º - Noti cação de violação de dados pessoais à autoridade de controle;	26º – Condições para o compartilhamento de dados entre os órgãos do poder público;
34º - Comunicação de violação de dados pessoais ao titular dos dados.	27º – Condições para compartilhamento de dados entre poderes público e privado;
	33º – Condições para transferência internacional de dados;
	37º – Controles das operações de tratamento de dados pessoais pelos agentes de tratamento;

Artigos GDPR [104]	Artigos LGPD [42]
	41º – indicação do encarregado de dados por parte do controlador; 46º – Medidas de segurança e sigilo de dados; 48º – Procedimentos para incidentes de segurança; 49º - Premissas dos sistemas de segurança; 52º - Sanções administrativas.

Tabela 4.4: Artigos das respectivas legislações utilizados na taxonomia.

Analisando a execução do procedimento na ISO/IEC 29100, foram analisadas 63 declarações para a taxonomia GDPR+ISO/IEC 29100 resultando em 33 requisitos enquanto a para a taxonomia LGPD+ISO/IEC 29100 analisou 58 declarações resultando em 57 requisitos. No processo de re namento, a GDPR+ISO/IEC 29100 uni cou 78 requisitos considerados similares ou duplicados enquanto a LGPD+ISO/IEC 29100 executou o processo de uni cação ocorreu para 44 requisitos que estavam duplicados e/ou foram uni cados, conforme Tabela 4.5.

		LGPD + ISO/IEC 29100 [Nossa Proposta]	GPDR + ISO/IEC 29100 [112]
Quantidade	TP1		
	artigos analisados	27	18
	declarações ISO/IEC analisadas	58	63
	requisitos obtidos para a Lei	112	116
	requisitos obtidos para a ISO/IEC	57	33
	total de requisitos obtidos	169	149
	TP2		
	categorias	10	7
	TP3		
	verbos utilizados	44	17
	requisitos excluídos	6	-
	requisitos duplicados/uni cados	44	78
	nal de requisitos	129	71

Tabela 4.5: Comparativo entre as duas taxonomias.

Apesar de Sangaroonsilp et al. [112] a rmarem que analisaram as declarações sobre a perspectiva geral de tratamento de dados e por a GDPR estabelecer parâmetros para o tratamento de dados por entidades públicas, não foram identi cados requisitos que re itam as entidades públicas naquela taxonomia. Enquanto isso, em nossa proposta foram registrados 11 requisitos diretamente relacionados ao tratamento de dados por pessoas jurídicas de natureza pública.

Além disso, 5 requisitos sobre o tratamento de dados para ns de estudos e pesquisas foram identi cados. 26 requisitos relativos a governança das instituições foram mapeados. 9 requisitos de privacidade relativos a soluções de infraestrutura foram levantados na nossa proposta de taxonomia LGPD+ISO/IEC 29100, enquanto não foram identi cados registros de requisitos com esses intuitos na taxonomia baseada na GDPR+ISO/IEC 29100.

A quantidade de requisitos gerados pelas taxonomias também se difere, enquanto a taxonomia GDPR+ISO/IEC 29100 gerou 71 requisitos a nossa proposta de taxonomia identi cou 129 requisitos de privacidade.

4.7 SÍNTESE DO CAPÍTULO

Neste capítulo foram apresentados os passos para proposição da taxonomia de requisitos de privacidade baseada na LGPD e ISO/IEC 29000. O desenvolvimento da taxonomia foi baseado em 3 passos principais com sua execução aqui descritos. A execução do TP1 resultou em 112 requisitos de privacidade extraídos da LGPD e 57 extraídos da ISO/IEC 29000. O TP2 gerou 10 categorias para a taxonomia e 5 contextos de aplicação dos requisitos. A execução do TP3, re nou os requisitos resultando em 129 requisitos de privacidade. E por m foi apresentada a comparação da taxonomia proposta com a taxonomia baseada na GDPR.

5 APLICAÇÃO DA TAXONOMIA DE REQUISITOS DE PRIVACIDADE NO OPEN BANKING BRASIL

O Open Banking Brasil é um projeto do Banco Central do Brasil (BCB) que visa aprimorar a competitividade no sistema nanceiro. Uma de suas principais funções é o compartilhamento de dados de usuários entre instituições nanceiras (IF) a partir de seu consentimento. Esse processo é regulamentado Resolução Conjunta n° 1 do Conselho Monetário Nacional e do Banco Central, de 4 de maio de 2020 [36] e nessa resolução existe a premissa de que todo o processo deve seguir fundamentado na Lei Geral de Proteção de Dados Brasileira (LGPD) [42].

Por estar relacionando com o compartilhamento de dados e ser fundamento na LGPD, o projeto torna-se um projeto promissor para avaliação da adequação a taxonomia de requisitos de privacidade elaborada neste trabalho. Com isso, foi conduzido um estudo de caso para avaliar a partir de um formulário a aderência dos processos de compartilhamento de dados das instituições nanceiras (IF) em relação a LGPD.

A execução deste estudo de caso foi conduzida considerando quatro passos previstos por Verner et al [122]: (i) pré-planejamento, (ii) administração, (iii) planejamento, (iv) desenho do plano de estudo de caso, (v) coleta de dados, (vi) análise de dados e (vii) relatórios.

A fase de (i) pré-planejamento pode ser contemplada pela de nição dos objetivos dessa dissertação e Revisão Sistemática de Literatura aqui executada, que indica a necessidade de um estudo de caso para validar a taxonomia proposta.

A fase de (ii) administração foi considerada no levantamento das informações, tendo os processos analisados como parte da rotina de um usuário das instituições. As informações analisadas foram registradas no anexo I.3 com o intuito de evidenciar as informações utilizadas como dados de entrada para a execução deste estudo de caso.

o (iii) planejamento do estudo de caso considerou a criação dos artefatos execução do estudo de caso e o cronograma de execução das atividades manuais para realização dos passos do estudo.

O (iv) desenho do estudo de caso foi efetuado a partir da de nição do formulário foi denominado Formulário de Avaliação de Aderência à Taxonomia (FAAT). A construção do formulário teve o intuito de confeccionar o instrumento de (v) coleta de dados, execução do estudo e registro de evidências e análise (vi) prévia dos resultados. Nele foram listados os requisitos de privacidade com opções para indicar a aplicação do requisito em relação a instituição nanceira avaliada, a partir dos dados coletados.

O formulário é composto por duas abas, uma para aplicação do formulário e outra com grá cos para análise estatística da aplicação do formulário. Maiores detalhes são apresentados na Tabela 5.1.

Aba	Coluna	Objetivo
Taxonomia	Categoria	Indicação da categoria do requisito de privacidade;
	Contexto	Indicação do contexto do requisito de privacidade;
	Requisito	O requisito de privacidade em si;
	Aplicação	Indicação da aplicação do requisito na solução avaliada as opções: Sim - é identi cada a aplicação do requisito de forma completa; Não - não é identi cada a aplicação do requisito; Parcialmente - é identi cada a aplicação do requisito de forma parcial; Não Avaliável - não é possível avaliar a aplicação do requisito; Não Aplicável - requisito não é aplicável ao cenário deste trabalho.
Qtd RQ Situação Aplicação* *Quantidade de Requisitos por Situação de Aplicação	Aplicação	Apresentação dos 5 tipos de resposta para a coluna aplicação;
	%	Percentual de requisitos para determinada aplicação;
	Qtd	Quantidade de requisitos para determinada aplicação.
Qtd RQ Situação Aplicação Filtrado** **Quantidade de Requisitos por Situação de Aplicação retirando não avaliável e não se aplica	Aplicação	Apresentação dos 3 tipos de resposta para a coluna aplicação;
	%	Percentual de requisitos para determinada aplicação;

Qtd	Quantidade de requisitos para determinada aplicação.

Tabela 5.1: Composição do Formulário de Avaliação de Aderência à Taxonomia.

Em seguida foi conduzida a aplicação do Formulário de Avaliação de Aderência à Taxonomia (FAAT) nos três maiores bancos do país, identi cados pelo prêmio Exame.Melhores & Maiores 2021 [52] em atendimento ao passo (v) do protocolo de estudo de caso. Evidências do processo de solicitação de compartilhamento de dados foram obtidas e o documento de termos e condições (T&C) para Open Banking foi transcrito e analisado durante a aplicação do FAAT, além disso as políticas de privacidade dessas instituições, que estavam indicadas em seus respectivos T&C também foram insumo para essa análise. Essas informações constam no anexo I.3 em 06/03/2022.

Dessa forma, a coleta dos dados foi efetuada a partir da aplicação do FAAT que foi preenchido de forma manual pela autora. O preenchimento dos formulários foi conduzido entre março e maio de 2022. Cada item do formulário demandou uma análise do processo de consentimento da IF analisada.

Por exemplo, para analisar a aderência ao RQ001 - COLETAR e armazenar o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de forma livre, especí ca e com conhecimento, exceto quando a lei aplicável permitir o processamento de dados sem o consentimento foi necessário avaliar o processo de consentimento sob as seguintes perspectivas:

- manifestação de vontade do titular - a solicitação do consentimento partiu do titular? há obrigação do consentimento para fornecimento de algum serviço?
- de forma livre - existe alguma obrigação vinculada à solicitação? o usuário tem a liberdade de selecionar as permissões que desejar dentro do objetivo da nalidade? o tempo de processamento dos dados pode ser editado de forma exível pelo usuário?
- especí ca - está clara a nalidade para a qual o consentimento está sendo criado?
- conhecimento - o usuário tem instrumentos para entender o motivo do consentimento e suas consequências?

Quando pelo menos uma dessas perspectivas não era favorável a aplicação era considerada parcial para o requisito analisado.

Ainda sobre a análise do RQ001, foi necessário analisar telas do processo de consentimento e além disso os termos de uso descritos para o consentimento. A análise necessária foi textual, a procura de declarações que atendessem ao esperado pelos requisitos.

Para alguns outros requisitos, também foi necessário analisar as telas, os termos de uso e as páginas públicas das instituições sobre privacidade (as páginas geralmente constavam referenciadas nos termos de uso).

Todos estes passos de análise de telas, uxos de interações, termos de uso e páginas de privacidade foram efetuados a partir de uma análise manual efetuada pela autora, o que demandou bastante tempo para a execução e limitou a quantidade de instituições analisadas, considerando limitações de tempo para esta dissertação.

5.1 SÍNTESE DO CAPÍTULO

A aplicação deste taxonomia se deu a partir do estudo de caso com o objetivo de avaliar a aderência do processo de consentimento de grandes bancos no país permitindo a análise da aderência a taxonomia de requisitos de privacidade proposta.

6 RESULTADOS

A aplicação da taxonomia de requisitos de privacidade proposta nessa pesquisa identi cou uma aderência positiva das Instituições Financeiras (IF) em relação a LGPD que é demonstrada a seguir.

6.1 RESULTADOS DA APLICAÇÃO DA TAXONOMIA EM UM CONTEXTO REAL

A Aplicação do Formulário de Avaliação de Aderência à Taxonomia (FAAT) para o Banco do Brasil identi cou que um percentual 24.81% de requisitos foram interpretados como implementados no projeto de Open Banking desta instituição, enquanto 2.33% dos requisitos foram interpretados como não identi cados nas soluções deste banco, 13.18% foram interpretados como aplicados parcialmente, 19.38% não se relacionavam ao contexto de IFs e 40.31% dos requisitos não puderam ser avaliados com as informações disponíveis.

Analisando os resultados, descartando os requisitos não avaliáveis ou não aplicáveis às IFs, tem-se que 61.54% dos requisitos foram identi cados como aplicados pelo Banco, enquanto 32.69% foram considerados parcialmente aplicados e 5.77% foram considerados não aplicados.

Para o Itaú, a aplicação do FAAT resultou em 16.28% de requisitos considerados como implementados no projeto Open Banking, 2.33% dos requisitos foram considerados como não aplicados, 21.71% foram considerados aplicados de forma parcial pela IF, 40.31% foram considerados não avaliáveis com as informações disponíveis e por m 19.38% dos requisitos foram considerados não relacionados ao contexto das instituições nanceiras - não se aplica.

Com os resultados na perspectiva dos requisitos identi cados como aplicados - Sim - , não aplicados - Não - ou aplicados parcialmente - Parcialmente -, a instituição alcançou o registro de 53.85% dos requisitos identi cados como atendidos parcialmente, enquanto 40.38% foram considerados aplicados e 5.77% foram considerados não aplicados.

Por m, para o Bradesco, o FAAT resultou em 28.68% dos requisitos considerados como aplicados - Sim -, 10.85% dos requisitos considerados como parcialmente aplicáveis ao contexto de Open Banking, 0.78% dos requisitos foram considerados não aplicados pela IF - Não -, 40.31% foram considerados não avaliáveis com as informações disponíveis e por m 19.38% dos requisitos foram considerados não relacionados ao contexto das instituições nanceiras - não se aplica.

Sob a perspectiva dos requisitos de privacidade descartando os requisitos identi cados como não aplicáveis e não avaliáveis, registra-se que 71.15% dos requisitos de privacidade foram considerados aplicados - Sim - no contexto da IF em questão, 26.92% foram considerados parcialmente aplicados e apenas 1.92% foram considerados não aplicados. A visão geral do resultado da aderência das instituições à taxonomia a partir da aplicação do FAAT é apresentada na Tabela 6.1.

Banco	Aplicação dos requisitos de privacidade					
	Sim		Parcialmente		Não	
	Percentual	Número	Percentual	Número	Percentual	Número
Banco do Brasil	61.54%	32	32.69%	17	5.77%	3
Itaú	40.38%	21	53.85%	28	5.77%	3
Bradesco	71.15%	37	26.92%	14	1.92%	1

Tabela 6.1: Comparação dos resultados por instituição

Nas seções seguintes são descritos os resultados da aplicabilidade dos requisitos de acordo com as categorias as quais eles se enquadram.

6.1.1 Finalidade

Essa categoria possui 25 requisitos distribuídos nos 3 contextos de Software, Estudos e pesquisa e Governança. 16 dos requisitos foram identi cados como não avaliáveis ou não aplicáveis para todas as IFs. A Tabela 6.2 sintetiza os resultados que são apresentados a seguir.

Banco	Aplicação	Qtd Requisitos	%
	Não	1	0,26%
	Não avaliável	9	2,33%
Banco do Brasil	Não se aplica	7	1,81%
	Parcialmente	4	1,03%
	Sim	4	1,03%
		25	6,46%
Bradesco	Não	1	0,26%
	Não avaliável	9	2,33%
	Não se aplica	7	1,81%
	Parcialmente	1	0,26%
	Sim	7	1,81%
		25	6,46%
Itaú	Não	2	0,52%
	Não avaliável	9	2,33%
	Não se aplica	7	1,81%
	Parcialmente	7	1,81%
		25	6,46%
	Total Geral	75	19,38%

Tabela 6.2: Resultados da aplicação da taxonomia para a Categoria Finalidade.

Para oBanco do Brasil, 4 requisitos (RQ002, RQ09, RQ014 e RQ015) foram identi cados como completamente aplicados para essa nalidade por esta instituição. 5 requisitos foram identi cados como não ou parcialmente aplicados. Detalhes sobre as observações dos requisitos identi cados com essas duas últimas classi cações são apresentados a seguir.

Para os requisitos do contexto de Software com aplicação parcial tem-se os requisitos RQ001, RQ004, RQ006 e RQ008. O RQ001 foi considerado como aplicado parcialmente tendo em vista que a instituição não permite a edição do escopo de dados compartilhados e por permitir apenas

dois tipos de prazo de compartilhamento, não se atentando a forma livre e específica prevista para este requisito.

O RQ004 teve a aplicação considerada como parcial por não haver a determinação do período de tratamento por parte da IF, apenas do período de compartilhamento.

Já o RQ006 teve a aplicação identificada como parcial pois não foi identificada página pública sobre os procedimentos para revogação de consentimento. No entanto, no Termos e Condições (T&C), há seção específica sobre o processo de revogação mas ainda assim não há determinação dos procedimentos.

Para finalizar, a análise da aplicabilidade dos requisitos atendidos parcialmente, para o RQ008 a finalidade é definida como (RQ008.a) oferecer soluções mais aderentes ao seu perfil de forma segura e sigilosa, porém a instituição não permite a alteração do escopo de dados compartilhados (RQ008.b), conforme apresentado na Figura 6.1.

(a) Evidência RQ008.a - Finalidade

(b) Evidência RQ008.b - Escopo não selecionável

Figura 6.1: Evidências do resultado da aplicação do FAAT para o RQ008 ao Banco do Brasil

E por fim, no contexto de Gestão Pública, não foi identificada a implementação do RQ021 por não ter sido possível identificar a menção à possibilidade de requerer informações por organismos de defesa do consumidor no T&C e na página de privacidade da IF.

Para o Itaú, o RQ001 foi identificado como atendido de forma parcial, pois permite apenas quatro tipos de prazo de compartilhamento, não se atentando à forma livre e específica do

requisito, conforme apresentado na Figura 6.2.

(a) Evidência RQ001.a - Período limitado

Figura 6.2: Evidências do resultado da aplicação do FAAT para o RQ001 ao Itaú

Já o requisito RQ002 foi identi cado como parcialmente aplicado pois é apresentado um texto que parecer ser a nalidade do tratamento de dados no uxo de compartilhamento de dados de forma subjetiva (RQ002.a) o que pode prejudicar a identi cação por parte do cliente, também é apresentado um detalhamento subjetivo sobre algumas nalidades (RQ002.b) porém no processo não há possibilidade de escolha entre esses itens e no item 7 da T&C a rmar que os dados serão utilizados para as nalidades indicadas no consentimento (RQ002.c), conforme apresentado na Figura 6.3.

(a) Evidência RQ002.a - Fluxo de Compartilhamento

(b) Evidência RQ002.b - Detalhamento das Finalidades

(c) Evidência RQ002.c - Termos e Condições

Figura 6.3: Evidências do resultado da aplicação do FAAT para o RQ002 ao Itaú

Outrossim, o requisito RQ004 foi considerado como atendido de maneira parcial visto que não há estipulação do período de tratamento, apenas do período de compartilhamento apesar de na página [78] haver a informação que o prazo pelo qual o Itaú Unibanco mantém os Dados Pessoais coletados depende do propósito e da natureza do tratamento dos dados

O requisito RQ006 também foi considerado atendido de maneira parcial, pois a partir do endereço [78] disponível no T&C foi encontrado no endereço [77] discorre-se sobre o canal para revogação, porém não há detalhes dos procedimentos necessários. O requisito RQ008, RQ014 e RQ015 tiveram o status atribuído como atendido parcialmente, em razão da nalidade estar apresentada de forma subjetiva e abrangente em sua apresentação ao usuário.

Ademais o requisito RQ009, foi considerado atendido parcialmente, pois a nalidade está apresentada de forma subjetiva no momento do compartilhamento e não há menção explícita da nalidade prevista neste requisito no T&C, há apenas o item 4 (RQ009.a) a declaração preservativa o direito de tratar seus dados, em consonância com os limites da LGPD, conforme apresentado na Figura 6.4.

(a) Evidência RQ009.a - Termos e Condições

Figura 6.4: Evidências do resultado da aplicação do FAAT para o RQ009 ao Itaú

Para o Itaú, por m, o RQ021 foi considerado como não implementado pois não foi identi- cada menção à possibilidade de requerer informações por parte dos organismos de defesa do consumidor no T&C e na página de privacidade da IF: [77].

Para o Bradesco, 7 requisitos foram considerados como aplicados - Sim - os quais são RQ001, RQ002, RQ006, RQ008, RQ009, RQ014 e RQ015. O requisito RQ004 foi considerado atendido de maneira parcial, posto que não há estipulação do período de tratamento, apenas do período de compartilhamento. O RQ021 foi considerado como não implementado, uma vez que não foi identi cada menção à possibilidade de requerer informações por organismos de defesa do consumidor no T&C e na página de privacidade da IF [26].

6.1.2 Adequação

Essa categoria é composta por 5 requisitos divididos entre os contextos Software e Estudos e pesquisa. Desses, dois requisitos, um de cada contexto foram considerados como não aplicáveis. A visão geral desses requisitos é apresentada na tabela 6.3.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não se aplica	2	0,52%
	Sim	3	0,78%
		5	1,29%
Bradesco	Não se aplica	2	0,52%
	Sim	3	0,78%
		5	1,29%
Itaú	Não se aplica	2	0,52%
	Sim	3	0,78%
		5	1,29%
	Total Geral	15	3,88%

Tabela 6.3: Resultados da aplicação da taxonomia para a Categoria Adequação.

Para o Banco do Brasil e para o Itaú 3 foram considerados aplicados por todas as IFs (Bancos do Brasil, Itaú e Bradesco), os quais são RQ027, RQ028 e RQ029. Nenhum requisito foi identi cado como não aplicado ou parcialmente aplicado.

6.1.3 Necessidade

A categoria é composta 18 requisitos, divididos em 5 contextos. Desses requisitos, 9 foram considerados não aplicáveis ou não avaliáveis, conforme tabela 6.4.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não avaliável	1	0,26%
	Não se aplica	8	2,07%
	Parcialmente	6	1,55%
	Sim	3	0,78%
		18	4,65%
Bradesco	Não avaliável	1	0,26%
	Não se aplica	8	2,07%
	Parcialmente	6	1,55%
	Sim	3	0,78%
		18	4,65%
Itaú	Não	1	0,26%
	Não avaliável	1	0,26%
	Não se aplica	8	2,07%
	Parcialmente	5	1,29%
	Sim	3	0,78%
		18	4,65%
	Total Geral	54	13,95%

Tabela 6.4: Resultados da aplicação da taxonomia para a Categoria Necessidade.

Para o Banco do Brasil e Bradesco, nenhum requisito foi considerado não aplicado. Os requisitos RQ031, RQ033 e RQ034, os três do contexto de Software, foram considerados aplicados - Sim - pela IF e 6 requisitos foram considerados como aplicados parcialmente, que serão

detalhados a seguir.

Os 6 requisitos RQ042, RQ044, RQ045, RQ046, RQ047 e RQ048 desta categoria, todos do contexto de infraestrutura, foram considerados como atendidos parcialmente, pois, para o primeiro banco a página [48], referenciada no T&C, consta que o processo de transferência é feito conforme a LGPD porém não há evidências para comprovar a aplicação. Para o segundo, o disposto na página [26] constante no T&C não faz menção sobre o processo de transferência o que pode indicar que a instituição não o faz ou não contemplou a situação em sua política de privacidade.

Para o Itaú, 5 foram considerados como atendidos parcialmente, sendo eles RQ042, RQ045, RQ046, RQ047 e RQ048, pois a partir do endereço [78] disponível no T&C, foi encontrado o endereço [77] que discorre sobre a transferência internacional de dados estar de acordo com a LGPD porém é possível comprovar com evidências a partir das informações utilizadas nesse trabalho.

O requisito RQ044 foi considerado como não implementado pois apesar de a partir do endereço [78] disponível no T&C, ser encontrado no endereço [77] que discorre sobre a transferência internacional de dados estar de acordo com a LGPD, no T&C a leitura dos termos no endereço [78] parece ser algo opcional.

6.1.4 Livre Acesso

Essa categoria é composta por 2 requisitos, os dois do contexto Software que estão distribuídos conforme a tabela 6.5.

Banco	Aplicação	Qtd	%
Banco do Brasil	Parcialmente	2	0,52%
		2	0,52%
Bradesco	Parcialmente	2	0,52%
		2	0,52%
Itaú	Parcialmente	2	0,52%
		2	0,52%
	Total Geral	6	1,55%

Tabela 6.5: Resultados da aplicação da taxonomia para a Categoria Livre acesso.

Para o Banco do Brasil, Itaú e Bradesco os RQ049 e RQ050 foram considerados como atendidos parcialmente pois apesar de não estar diretamente disponível no processo de consentimento o T&C das IFs menciona na página [48] do primeiro banco que contém uma seção "seus dados, seus direitos", para a segunda IF o T&C menciona de forma abstrata a página [78] que contém uma seção "Seus direitos" que explica sobre os direitos e como exercê-los. E para o terceiro pois apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página [26] contém uma seção "seus direitos" referente ao acesso aos dados.

6.1.5 Qualidade dos Dados

Para a categoria Qualidade de Dados, divida em 3 contextos, os quais são Software, Governança e Gestão Pública, 5 requisitos foram considerados não avaliáveis, 2 do contexto de Software, 2 de Governança e 1 de Gestão Pública. A visão sintetizada dos requisitos é apresentada na Tabela 6.6.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não avaliável	5	1,29%
	Parcialmente	1	0,26%
	Sim	1	0,26%
		7	1,81%
Bradesco	Não avaliável	5	1,29%
	Parcialmente	1	0,26%
	Sim	1	0,26%
		7	1,81%
Itaú	Não avaliável	5	1,29%
	Parcialmente	1	0,26%
	Sim	1	0,26%
		7	1,81%
	Total Geral	21	5,43%

Tabela 6.6: Resultados da aplicação da taxonomia para a Categoria Qualidade de Dados.

O requisito RQ051 foi considerado como aplicado - Sim - por todas as IFs: Banco do Brasil, Itaú e Bradesco.

O RQ052, do contexto de software, foi considerado como atendido parcialmente, também todas as IFs: Banco do Brasil, Itaú e Bradesco, pois apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página [48] do primeiro banco que contém uma seção "seus dados, seus direitos", para o segundo o T&C menciona de forma abstrata a página [78] que contém uma seção "Seus direitos"que explica sobre os direitos e como exercê-los. E para o terceiro porque apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página [26] que contém uma seção "seus direitos"referente ao acesso aos dados.

6.1.6 Transparência

Na categoria transparência composta por 13 requisitos, divididos entre os contextos de software e governança. 4 requisitos, da categoria de software foram considerados não avaliáveis ou não aplicáveis. A Tabela 6.7 apresenta a visão dos requisitos conforme a seguir.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não avaliável	1	0,26%
	Não se aplica	3	0,78%
	Parcialmente	1	0,26%
	Sim	8	2,07%
		13	3,36%
Bradesco	Não avaliável	1	0,26%
	Não se aplica	3	0,78%
	Parcialmente	2	0,52%
	Sim	7	1,81%
		13	3,36%
Itaú	Não avaliável	1	0,26%
	Não se aplica	3	0,78%
	Parcialmente	5	1,29%
	Sim	4	1,03%
		13	3,36%
	Total Geral	39	10,08%

Tabela 6.7: Resultados da aplicação da taxonomia para a Categoria Transparência.

Nenhum requisito desta categoria foi considerado como não aplicado pelas todas as 3 Bancos (do Brasil, Itaú e Bradesco).

Para o Banco do Brasil, 8 requisitos foram considerados como aplicados - Sim - sendo eles RQ060, RQ061, RQ063, RQ065, RQ066, RQ067, RQ68 e RQ070. E o RQ069 foi considerado como atendido parcialmente pois apesar de o T&C mencionar a página [48] que faz referência ao processo de exclusão, não há muitas instruções que permitam o entendimento por parte do usuário.

Para o Itaú, 4 requisitos foram considerados implementados - Sim - os quais são RQ061, RQ065, RQ066 e RQ067. Enquanto 5 requisitos foram considerados como aplicados parcialmente sendo que os requisitos RQ060, RQ063, RQ068 e RQ069 receberam esse status pois apesar de não estar diretamente disponível no processo de consentimento e de não haver menção no T&C sobre o como exercer os direitos, o T&C menciona de forma abstrata a página [78] que contém uma seção "Seus direitos"que explica sobre os direitos e como exercê-los.

Já requisito RQ070, também considerado atendido de maneira parcial, em seu T&C menciona de forma abstrata a página [78] e nela há a seção 10. ENCARREGADO DE PROTEÇÃO DE DADOS, porém não há indicação do nome do encarregado, apenas um e-mail institucional para acioná-lo.

Para o Bradesco, os requisitos RQ060 e RQ069 foram considerados atendidos de maneira parcial. O primeiro pelo fato de que é informado na página [26] sobre a possibilidade das solicitações porém o prazo de 15 dias não é fornecido nessa página e há uma justi cativa prévia para um possível atraso. Já o segundo requisito, pois apesar de o T&C mencionar a página [26] que faz referência a exclusão, não há muitas instruções que permitam o entendimento por parte do usuário.

6.1.7 Segurança

Nessa categoria composta por 16 requisitos distribuídos entre os contextos Software, Estudos e pesquisa, Governança e infraestrutura. Desses, 15 requisitos foram considerados não aplicáveis ou não avaliáveis. A visão geral dos requisitos é apresentada na Tabela 6.8

Banco	Aplicação	Qtd	%
Banco do Brasil	Não avaliável	12	3,10%
	Não se aplica	3	0,78%
	Parcialmente	1	0,26%
		16	4,13%
Bradesco	Não avaliável	12	3,10%
	Não se aplica	3	0,78%
	Parcialmente	1	0,26%
		16	4,13%
Itaú	Não avaliável	12	3,10%
	Não se aplica	3	0,78%
	Parcialmente	1	0,26%
		16	4,13%
	Total Geral	48	12,40%

Tabela 6.8: Resultados da aplicação da taxonomia para a Categoria Segurança.

O RQ084 foi considerado como atendimento parcialmente por todas as três (Banco do Brasil, Itaú E Bradesco), pois alguns controles estão registrados pelos bancos em seus respectivos sites de privacidade, porém não é possível avaliar apenas com as informações públicas disponíveis se a aplicabilidade do requisito é completa.

6.1.8 Prevenção

A categoria Prevenção é composta por 5 requisitos divididos entre os contextos Software, Estudos e pesquisa e Governança. Os 5 requisitos foram considerados como não avaliáveis ou não aplicáveis, conforme Tabela 6.9.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não avaliável	4	1,03%
	Não se aplica	1	0,26%
		5	1,29%
Bradesco	Não avaliável	4	1,03%
	Não se aplica	1	0,26%
		5	1,29%
Itaú	Não avaliável	4	1,03%
	Não se aplica	1	0,26%
		5	1,29%
	Total Geral	15	3,88%

Tabela 6.9: Resultados da aplicação da taxonomia para a Categoria Prevenção.

6.1.9 Não Discriminação

Essa é a menor categoria com apenas 2 requisitos no contexto de Software, os dois foram considerados como não aplicáveis ou não avaliáveis. Nenhum requisito foi considerado como aplicado, não aplicado ou parcialmente aplicado pelas IFs, conforme Tabela 6.10.

Banco	Aplicação	Qtd	%
Banco do Brasil	Parcialmente	2	0,52%
		2	0,52%
Bradesco	Parcialmente	2	0,52%
		2	0,52%
Itaú	Parcialmente	2	0,52%
		2	0,52%
	Total Geral	6	1,55%

Tabela 6.10: Resultados da aplicação da taxonomia para a Categoria Não Discriminação.

6.1.10 Responsabilização e Prestação de Contas

Essa categoria é composta por 36 requisitos distribuídos entre os contextos Software, Governança e Infraestrutura. 19 requisitos foram considerados como não avaliáveis enquanto nenhum requisito foi considerado não aplicável. A visão geral dos requisitos é apresentada na Tabela 6.11.

Banco	Aplicação	Qtd	%
Banco do Brasil	Não	2	0,52%
	Não avaliável	19	4,91%
	Parcialmente	2	0,52%
	Sim	13	3,36%
		36	9,30%
Bradesco	Não avaliável	19	4,91%
	Parcialmente	1	0,26%
	Sim	16	4,13%
		36	9,30%
Itaú	Não	1	0,26%
	Não avaliável	19	4,91%
	Parcialmente	6	1,55%
	Sim	10	2,58%
		36	9,30%
	Total Parcial	108	27,91%

Tabela 6.11: Resultados da aplicação da taxonomia para a Categoria Responsabilização e Prestação de Contas.

Para oBanco do Brasil, 13 requisitos dos contextos de Software e Governança foram considerados como aplicados pela IF - Sim -, os quais são RQ102, RQ103, RQ105, RQ106, RQ107, RQ108, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116 e RQ123. 2 requisitos foram considerados como não aplicados e 2 foram considerado aplicados de forma parcial, os quais são detalhados a seguir.

Os requisitos RQ094 e RQ104 foram considerados não implementados - Não - pois durante a análise não foi identi cada seção sobre os tipos de dados pessoais coletados na página [48] a qual o T&C se refere.

O requisito RQ111 foi considerado atendido parcialmente pois não foi identi cada seção relativa a anonimização, apenas sobre a correção. Enquanto para o RQ129 o status parcial foi atribuído pois a garantia de sua aplicação não é avaliável, entretanto, a IF declara que segue os procedimentos, conforme disposto na página [48].

Para dtaú, 10 requisitos do contexto de Software e Governança foram considerados aplicados - Sim -, os quais são RQ102, RQ103, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116 e RQ123.

Os requisitos RQ104, RQ105, RQ106, RQ107, RQ108 foram considerados como atendidos parcialmente pois há menção da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade porém não há explicação dos procedimentos, conforme observa-se [78]. Enquanto o RQ129, também atendido de maneira parcial, difere em sua avaliação, pois a garantia não é avaliável porém a IF declara que segue os procedimentos na página [78]. Ainda para dtaú, o requisito RQ094 foi considerado como não implementado em razão de não ter sido identi cada seção sobre os tipos de dados pessoais coletados nas páginas [78] disponível no T&C e no endereço [77].

Por m, o Bradescoteve 16 requisitos considerados como aplicados - Sim -, os quais são RQ094, RQ102, RQ103, RQ104, RQ105, RQ106, RQ107, RQ108, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116 e RQ123. O requisito RQ129 foi considerado atendido de maneira parcial, pois, a garantia não é avaliável porém a IF declara que segue os procedimentos na página: [26].

6.2 DISCUSSÃO DOS RESULTADOS

A partir da condução da revisão sistemática de literatura, 21 estudos primários foram selecionados para análise e extração dos dados e 7 trabalhos foram identi cados com alguma relação ao tema. Destaca-se a di culdade na identi cação das abordagens para construção das taxonomias, isso pois os artigos fornecem poucas informações sobre o método que os autores usaram para desenvolver suas taxonomias, algo já registrado na literatura por Nickerson et al. [99]. Os trabalhos desenvolvidos por Sangaroonsilp et al [112], Antón e Earp [15], Meis e Heisel [94], Hernández et al. [71], Meis e Heisel [95], Rjaibi e Rabai [108] e Bolchini et al. [24] foram os que apresentaram taxonomias com alguma relação com requisitos de privacidade. No total, foram considerados 7 trabalhos com proposições de taxonomias que poderiam se relacionar aos requisitos de privacidade demonstrando. Demonstrando assim a necessidade da elaboração de uma taxonomia de Requisitos de Privacidade principalmente para o cenário Brasileiro, o qual não destacou nenhum achado na SLR.

Partindo disso, a taxonomia de requisitos de privacidade baseada na LGPD e ISO/IEC 29000

foi proposta nesse trabalho. A taxonomia de requisitos de privacidade foi baseada no processo utilizado por Sangaroonsilp et al. [112] que segue a Goal-Based Requirements Analysis Method (GBRAM) [14]. Esse método também foi utilizado por Antón e Earp [15] no desenvolvimento da taxonomia de requisitos para redução de vulnerabilidades em websites. A taxonomia proposta por esta dissertação gerou 10 categorias e 5 contextos de aplicação dos requisitos e 129 requisitos de privacidade. A criação dos contextos foi uma contribuição deste trabalho considerando a abrangência da LGPD em diversas áreas da engenharia de software, isso pois foram identi cados contextos além dos sistêmicos para os quais os requisitos se aplicam, possibilitando a criação de diversas perspectivas de análises e aplicação sobre essa taxonomia.

A aplicabilidade da taxonomia foi avaliada a partir de um formulário de avaliação de aplicação da taxonomia - FAAT, utilizado no processo de Open Banking dos três maiores bancos do país segundo [52] em uma pesquisa de 2021. A aplicação do FAAT resultou em 71.15% de aderência à taxonomia para o Bradesco, enquanto o Banco do Brasil de 61.54%, e por m o Itaú teve 40.38%. A baixa aderência do Itaú pode se dar pela forma não explícita escolhida para apresentação da nalidade no processo de consentimento, já que alguns requisitos se baseiam na existência da nalidade no processo de consentimento.

A aplicabilidade parcial do Itaú foi maior apresentando 53.85% dos requisitos de privacidade, seguida do Banco do Brasil com 32.69% dos requisitos de privacidade com aplicabilidade parcial e por m o Bradesco com 26.92%. Esses resultados podem indicar que as instituições nanceiras estão de forma geral mais próximas do que distantes da aderência a LGPD no processo de Open Banking

Trabalhos anteriores executados sob a perspectiva dos funcionários indicaram que as instituições ainda estavam iniciando a aplicação da LGPD [56]. Os resultados obtidos nesse trabalho indicam maior aderência aos requisitos de privacidade obtidos na LGPD para o projeto de Open Banking o que pode ter acontecido por este projeto ter sido de nido após a publicação da LGPD e durante sua entrada em vigor (2020), além de ser um projeto regulado pelo Banco Central, instituição com poder de supervisão [36].

Os resultados iniciais deste estudo demonstram que a taxonomia pode ser utilizada para a avaliação da aderência à LGPD.

6.3 LIMITAÇÕES DO ESTUDO

Em relação à execução deste trabalho, no que se refere a revisão de literatura, pode-se considerar como limitação a quantidade de trabalhos identi cados pela string de busca e principalmente a falta de aderência dos trabalhos primários em relação ao escopo de pesquisa de requisitos de privacidade. Como forma de minimização destas limitações, as pesquisas foram executadas de forma individualizada, em cada base digital, para garantir o atendimento das particularidades dos seus processos de busca.

Outra ameaça identi cada em relação a pesquisa está relacionada à análise qualitativa dos achados, tanto para a RSL quanto para a aplicação da taxonomia, o que pode eventualmente gerar equívocos de interpretação e/ou inconsistências, para minimização dessa limitação, as atividades foram revisadas e disponibilizadas pela autora.

O trabalho foi conduzido com informações coletadas sob a perspectiva de usuário do processo de Open Bankingdas instituições, limitando a sua aplicação principalmente para os requisitos que se relacionavam com informações de processos de infraestrutura e responsabilização das instituições. Para tal mitigação do problema, todas as instituições tiveram este tipo de requisito de nidos como não avaliável e os resultados considerados para ns de conclusão foram os dos requisitos que não tiveram esse status atribuído.

6.3.1 Ameaças à Validade

Para avaliação das ameaças à validade deste estudo, a abordagem proposta por Wohlin [124] foi considerada. Nela, entende-se que conclusões sobre a teoria de nida nas hipóteses são tiradas a partir das observações geradas. Ao tirar conclusões, tem-se quatro etapas, em cada uma das quais há um tipo de ameaça à validade dos resultados que são apresentadas a seguir.

Validade de construção. A qualidade dos procedimentos estabelecidos para a validação do trabalho é fundamental para o seu resultado. Neste sentido, a de nição do formulário primou pelo estabelecimento de questões objetivas construídas a partir da taxonomia proposta (causa). Entende-se que os resultados identi cados com essa pesquisa re etem o efeito esperado de que a taxonomia é passível de utilização pelos pro ssionais de engenharia de requisitos. Ameaças podem estar relacionadas com a população reduzida de pesquisa para aplicação da taxonomia, no entanto, a população de pesquisa foi selecionada a partir do impactado no mercado nanceiro em relação ao tamanho das instituições e em como elas re etem a uma parcela considerável deste marcado no cenário brasileiro. Como forma de minimização também se considerou a preocupação com a reprodução do estudo para que futuras replicações possam gerar con rmar os resultados aqui observados e permitir novas análises sob diferentes perspectivas.

Validade interna. Por outro lado, a seleção dos objetos de estudo podem ter interferido na validade interna deste trabalho uma vez que considerou apenas o porte da instituição. Esse critério teve o intuito de delimitar uma amostragem do mercado nanceiro, sem a proposição de nenhuma pre-deleção em relação às instituições selecionadas.

Validade externa. Embora essa pesquisa não possa ser considerada como passível de cobertura do cenário industrial nanceiro brasileiro em relação a LGPD, a população escolhida cobre uma parte considerável por incluir os 3 maiores bancos do país. A intenção não é delimitar um linear de coberta da LGPD e sim trazer evidências de que a taxonomia proposta pode auxiliar os times de desenvolvimento na adequação a legislação.

Validade da conclusão. Para esse construto, a con abilidade da implementação do tratamento foi uma preocupação na realização da pesquisa. Como a aplicação de foi executada a partir de

uma análise subjetiva executada por uma pessoa e não por uma máquina ou um código, sempre há o risco de viés do executor. Como forma de minimização desta ameaça o formulário foi confeccionado com respostas padronizadas e justi cativas para respostas com possível impacto negativo para a pesquisa foram adicionadas como forma de registro das análises atribuídas durante o tratamento. Também foi considerada a minimização da heterogeneidade aleatória da população de estudo com a seleção de instituições nanceiras com grande porte no país, o que permitiu que a pesquisa fosse analisada sob um perspectiva homogenia, trazendo uma boa caracterização do grupo analisado.

7 CONCLUSÃO

Nesse trabalho, foi conduzida uma revisão sistemática de literatura, que identi cou 110 trabalhos preliminares e após aplicar os critérios de inclusão e exclusão, resultou na seleção de 10 estudos primários para extração dos dados. Como resultado da revisão, é possível perceber uma ausência de taxonomias relativas aos requisitos de privacidade, principalmente no âmbito da legislação brasileira, demonstrando uma lacuna na literatura sob o aspecto de taxonomias de requisito de privacidade. Nesse sentido, este trabalho propõe uma taxonomia que resultou em 129 requisitos de privacidade divididos em 10 categorias e 5 contextos de aplicação para esses requisitos.

A aplicação da taxonomia no projeto de Open Banking de três instituições nanceiras (IFs) demonstrou percentuais entre 40% e 71% de aderência à taxonomia, indicando evolução por parte das instituições na implantação dos requisitos de privacidade em relação a pesquisas anteriores. Os resultados demonstraram que a taxonomia pode ser aplicada em contextos reais permitindo a avaliação da aderência a legislação Brasileira.

7.1 TRABALHOS FUTUROS

Para os trabalhos futuros, espera-se poder aplicar a taxonomia de requisitos de privacidade proposta nesse trabalho em um estudo de caso supervisionado com a aplicação um sistema em construção com o apoio da instituição envolvida no estudo para que que seja possível avaliar a completude do requisitos de privacidade dessa taxonomia.

REFERÊNCIAS BIBLIOGRÁFICAS

1

2 ABDELMABOUD, A. The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. Sensors 21, 17 (2021).

3 ABERKANE, A. J., POELS, G., AND BROUCKE, S. V. Exploring automated gdpr-compliance in requirements engineering: A systematic mapping study. IEEE Access 9 (2021), 66542–66559.

4 AHMED, A. I. A., GANI, A., HAMID, S. H. A., ABDELMABOUD, A., SYED, H. J., HABEEB MOHAMED, R. A. A., AND ALI, I. Service management for iot: Requirements, taxonomy, recent advances and open research challenges. IEEE Access 7 (2019), 155472–155488.

5 ALHIRABI, N., RANA, O., AND PERERA, C. Security and Privacy Requirements for the Internet of Things. ACM Transactions on Internet of Things 1, 2 (2021), 1–37.

6 ALQASSEM, I., AND SVETINOVIC, D. A taxonomy of security and privacy requirements for the internet of things (iot). In 2014 IEEE International Conference on Industrial Engineering and Engineering Management, IEEM 2014, Selangor Darul Ehsan, Malaysia, December 9-12, 2014 (2014), IEEE, pp. 1244–1248.

7 ALVES, C., AND NEVES, M. Especi cação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso. Anais do WER21 - Workshop em Engenharia de Requisitos (Brasília, DF, 2021), B. Cruz, Maria Lencastre Pinheiro de Menezes (UPE, A. Hadad, Graciela Dora Susana (UNO, and B. Marques, Johnny Cardoso (ITA, Eds., Editora PUC-Rio.

8 AMELLER, D., AYALA, C., CABOT, J., AND FRANCH, X. How do software architects consider non-functional requirements: An exploratory study. 2012 20th IEEE International Requirements Engineering Conference, RE 2012 - Proceedings (2012).

9 ANDRESS, J. What is information security? The Basics of Information Security (2014), 1–22.

10 ANPD. Anpd está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas, 2021. <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas>, último acesso em 16 de agosto de 2021.

11 ANPPD. Portal das violações - lgpd, 2021. <https://anppd.org/violacoes>, último acesso em 13 de outubro de 2021.

12 ANSARI, M. T. J., BAZ, A., ALHAKAMI, H., ALHAKAMI, W., KUMAR, R., AND KHAN, R. A. P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements. Arabian Journal for Science and Engineering (2021).

13 ANTHONYSAMY, P., RASHID, A., AND CHITCHYAN, R. Privacy requirements: Present & future. In 39th IEEE/ACM International Conference on Software Engineering: Software Engineering in Society Track, ICSE-SEIS 2017, Bueons Aires, Argentina, May 20-28, 2017 (2017), IEEE Computer Society, pp. 13–22.

14 ANTON, A. I. Goal-based requirements analysis. In Proceedings of the IEEE International Conference on Requirements Engineering (1996).

15 ANTÓN, A. I., AND EARP, J. B. A requirements taxonomy for reducing Web site privacy vulnerabilities. Requirements Engineering 9 (2004), 169–185.

16 ANTÓN, A. I., EARP, J. B., AND REESE, A. Analyzing Website privacy requirements using a privacy goal taxonomy. Proceedings of the IEEE International Conference on Requirements Engineering 2002-January (2002), 23–31.

17 AYALA-RIVERA, V., AND PASQUALE, L. The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements. 2018 IEEE 26th International Requirements Engineering Conference (RE) (2018), pp. 136–146.

18 AZAD, S., AND MARTENS, C. Little Computer People: A Survey and Taxonomy of Simulated Models of Social Interaction. Proceedings of the ACM on Human-Computer Interaction, CHI PLAY (2021).

19 BARKER, K., ASKARI, M., BANERJEE, M., GHAZINOUR, K., MACKAS, B., MAJEDI, M., PUN, S., AND WILLIAMS, A. A data privacy taxonomy. Lecture Notes in Computer Science (including subseries Lecture Notes in Arti cial Intelligence and Lecture Notes in Bioinformatics) 5588 LNCS (2009), 42–54.

20 BEHUTIYE, W., KARHAPÄÄ, P., COSTAL, D., OIVO, M., AND FRANCH, X. Non-functional requirements documentation in agile software development: Challenges and solution proposals. Lecture Notes in Computer Science (including subseries Lecture Notes in Arti cial Intelligence and Lecture Notes in Bioinformatics) 10611 LNCS, December (2017), 515–522.

21 BELANI, H. Towards a usability requirements taxonomy for mobile AAC services. 2012 1st International Workshop on Usability and Accessibility Focused Requirements Engineering, UsARE 2012 - Proceedings (2012), 36–39.

22 BERNTSSON SVENSSON, R., GORSCHEK, T., AND REGNELL, B. Quality requirements in practice: An interview study in requirements engineering for embedded systems. In Lecture Notes in Computer Science (including subseries Lecture Notes in Arti cial Intelligence and Lecture Notes in Bioinformatics) (2009), vol. 5512 LNCS.

23 BHATIA, J., BREAUX, T. D., AND SCHAUB, F. Mining privacy goals from privacy policies using hybridized task recomposition. ACM Transactions on Software Engineering and Methodology 25 (2016).

24 BOLCHINI, D., PAOLINI, P., AND RANDAZZO, G. Adding hypermedia requirements to goal-driven analysis. In Proceedings. 11th IEEE International Requirements Engineering Conference, (2003) (2003), pp. 127–137.

25 BORG, A., YONG, A., CARLSHAMRE, P., AND SANDAHL, K. The Bad Conscience of Requirements Engineering : An Investigation in Real-World Treatment of Non-Functional Requirements. In Proceedings of the 3rd Conference on Software Engineering Research and Practice in Sweden (SERPS'03) (2003).

26 BRADESCO. Bradesco | diretiva de privacidade, 2022. Disponível em: <https://www.bradescosegurança.com.br/html/seguranca_corporativa/pf/seguranca-informacao/privacidade.shtm>. Último acesso em 26 de março de 2022.

27 BRERETON, P., KITCHENHAM, B. A., BUDGEN, D., TURNER, M., AND KHALIL, M. Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 80 (2007), 571–583.

28 BRITO, F., AND MACHADO, J. Preservação de Privacidade de Dados: Fundamentos, Técnicas e Aplicações. Sociedade Brasileira de Computação - SBC, Porto Alegre, 07 2017, ch. 3, p. 40.

29 Calderón C., M. A taxonomy of software security requirements. Revista Avances en Sistemas e Informática 4 (2007).

30 Cao, L., and Ramesh, B. Agile requirements engineering practices: An empirical study. IEEE Software 25, 1 (2008).

31 Castro, J., Kolp, M., and Mylopoulos, J. Towards requirements-driven information systems engineering: the tropos project. Information Systems 27, 6 (2002), 365–389.

32 Cavoukian, A. Operationalizing privacy by design. Communications of the ACM 55, 9 (2012), 7.

33 Central, B. Resolução nº 4.553, de 30 de janeiro de 2017, 1 2017.

34 Central, B. Comunicado n 33.455, de 24 de abril de 2019, 2019.

35 Central, B., and Nacional, C. M. Resolução conjunta n. 1, de 4 de maio de 2020. 1–24.

36 Central, B., and Nacional, C. M. Resolução conjunta n. 1, de 4 de maio de 2020, 5 2020.

37 Cheikhi, L., Abran, A., and Suryn, W. Harmonization of usability measurements in iso9126 software engineering standards. 2006 IEEE International Symposium on Industrial Electronics (2006), vol. 4, pp. 3246–3251.

38 Chen, B., and Dong, Q. A taxonomy system for information system requirements. In Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012 (London, 2013), Z. Zhong, Ed., Springer London, pp. 633–643.

39 Christian, T., and Mead, N. Security requirements reusability and the square methodology. Tech. Rep. CMU/SEI-2010-TN-027, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2010.

40 Commission, E. Guidelines on the application and setting of administrative fines, 2021. <https://ec.europa.eu/newsroom/article29/items/611237>, último acesso em 13 de outubro de 2021.

41 da República, P. Lei nº 12.965, Marco Civil da Internet, 4 2014.

42 da República, P. Lei nº 13.709, Lei Geral de Proteção de Dados (lgpd), 8 2018. <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, último acesso 10 de abril de 2022.

43 Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Métayer, D. L., Tirtea, R., and Schiffner, S. Privacy and data protection by design - from policy to engineering. CoRR abs/1501.03726 (2015).

44 De Lucia, A., and Qusef, A. Requirements engineering in agile software development. Journal of Emerging Technologies in Web Intelligence 2, 3 (2010).

45 Deloitte, and FEBRABAN. Pesquisa FEBRABAN de Tecnologia Bancária 2020. Tech. rep., FEBRABAN, São Paulo, 2020.

46 Dias Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P. H., and Lima, F. Perceptions of ict practitioners regarding software privacy. Entropy 22, 4 (2020).

47 Directive, E. U. 95/46/EC protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC 23 (1995).

48 DO BRASIL, B. Políticas de uso e privacidade - você - banco do brasil, 2022. Disponível em: <https://www.bb.com.br/pbb/pagina-inicial/minha-privacidade/politicas-de-uso-e-privacidade#/>, último acesso em 20 de março de 2022.

49 EBC. Procon de sp noti ca empresas de telefonia sobre vazamentos de dados., 2021. <https://agenciabrasil.ebc.com.br/justica/noticia/2021-02/procon-de-sp-noti ca-empresas-de-telefonia-sobre-vazamentos-de-dados>, último acesso em 16 de agosto de 2021.

50 EBC. Sites e aplicativo do ministério da saúde sofrem ataque cibernético, 2021. <https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico>, último acesso 15 de janeiro de 2022.

51 ECKHARDT, J., VOGELSANG, A., AND FERNÁNDEZ, D. M. Are non-functional requirements really non-functional? an investigation of non-functional requirements in practice. Proceedings - International Conference on Software Engineering (2016), vol. 14-22-May-2016.

52 EXAME. Maiores bancos - maiores e melhores, 2021. Disponível em: <https://mm.exame.com/maiores-bancos/>, acessado em 06 de março de 2022.

53 EXECUTIVO, P. Medida provisória 959/2020, 2020. Acessado em 13 de outubro de 2021.

54 FERENHOF, H., AND FERNANDES, R. Desmisti cando a revisão de literatura como base para redação cientí ca: método SFF DEMYSTIFYING THE LITERATURE REVIEW AS BASIS FOR SCIENTIFIC WRITING: SSF METHOD. Revista ACB 21, 13 (2016), 550–563.

55 FERRAO, S., AND CANEDO, E. Pacote de Reprodução da taxonomia para requisitos de privacidade, Mar. 2022. <https://doi.org/10.5281/zenodo.6975709>, último acesso 08 de agosto de 2022.

56 FERRAO, S. E. R., CARVALHO, A. P., CANEDO, E. D., MOTA, A. P. B., COSTA, P. H. T., AND CERQUEIRA, A. J. Diagnostic of data processing by brazilian organizations—a low compliance issue. Information 12, 4 (2021).

57 FINKELSTEIN, M., AND FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais privacy and general personal data protection law. Revista de Direito Brasileira 28, 3 (2020), 284–301.

58 FRESMITH, D. Specifying reusable security requirements. Journal of Object Technology 3, 1 (2004), 61–75.

59 FRESMITH, D. G. Analyzing and Specifying Reusable Security Requirements. Proceedings of the 11th International IEEE Conference on Requirements Engineering, RHAS (**2003**), 507–514.

60 GHARIB, M., MYLOPOULOS, J., AND GIORGINI, P. Copri - A core ontology for privacy requirements engineering. Research Challenges in Information Science - 14th International Conference, RCIS 2020, Limassol, Cyprus, September 23-25, 2020, Proceedings (2020), F. Dalpiaz, J. Zdravkovic, and P. Loucopoulos, Eds., vol. 385 of Lecture Notes in Business Information Processing, Springer, pp. 472–489.

61 GHARIB, M., SALNITRI, M., PAJA, E., GIORGINI, P., MOURATIDIS, H., PAVLIDIS, M., RUIZ, J. F., FERNANDEZ, S., AND SIRIA, A. D. Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform. Proceedings - 2016 IEEE 24th International Requirements Engineering Conference, RE 2016 (2016), 256–265.

62 GLASER, B. Discovery of Grounded Theory: Strategies for Qualitative Research. Taylor & Francis, 2017.

63 GLASER, B. G., AND STRAUSS, A. L. Discovery of grounded theory: Strategies for qualitative research. Aldine Transaction, 2017.

64 GLINZ, M. Rethinking the Notion of Non-Functional Requirements. In Proceedings of the Third World Congress for Software Quality (3WCSQ'05) (2005), pp. 55–64.

65 GÓMEZ SOTELO, K. I., BARON, C., ESTEBAN, P., ESTRADA, C. Y., AND LAREDO VELÁZQUEZ, L. D. J. How to find non-functional requirements in system development. IFAC-PapersOnLine 51, 11 (2018), 1573–1578.

66 GORDIEIEV, O., AND KHARCHENKO, V. Profile-oriented assessment of software requirements quality: Models, metrics, case study. International Journal of Computing 19, 4 (Dec. 2020), 656–665.

67 GÜRSES, S., SEGURAN, M., AND ZANNONE, N. Requirements engineering within a large-scale security-oriented research project: Lessons learned. Requirements Engineering 18, 1 (2013), 43–66.

68 GÜRSES, S. F., TRONCOSO, C., AND DÍAZ, C. Engineering privacy by design. In Fourth Conference on Computers, Privacy and Data Protection (2011), pp. 25–27.

69 GUZMÁN, L., ORIOL, M., RODRÍGUEZ, P., FRANCH, X., JEDLITSCHKA, A., AND OIVO, M. How can quality awareness support rapid software development? - A research preview. In Requirements Engineering: Foundation for Software Quality - 23rd International Working Conference, REFSQ 2017, Essen, Germany, February 27 - March 2, 2017, Proceedings (2017), P. Grünbacher and A. Perini, Eds., vol. 10153 of Lecture Notes in Computer Science, Springer, pp. 167–173.

70 HADAR, I., HASSON, T., AYALON, O., TOCH, E., BIRNHACK, M., SHERMAN, S., AND BALISSA, A. Privacy by designers: software developers' privacy mindset. Empirical Software Engineering 23, 1 (2018), 259–289.

71 HERNÁNDEZ, U. I., MARTIN, M. V., RODRÍGUEZ, F. J. Á., GONZÁLE, R. M., AND TORIBIO, F. A. G. A requirements taxonomy and rating model for secure and usable b2c/c2c e-commerce websites. 2010 5th International Conference on Digital Information Management, ICDIM 2010 (2010), 367–372.

72 ISO. Iso 7498-2:1989 - information processing systems - open systems interconnection - basic reference model , part 2: Security architecture, 1989.

73 ISO/IEC. Iso/iec-9126:2001 - software engineering – product quality, 2001-2004.

74 ISO/IEC. Iso/iec-27000:2005 - information technology - security techniques - information security management systems - overview and vocabulary, 2009.

75 ISO/IEC. Iso/iec 29100:2011 information technology - security techniques - privacy framework, 2011.

76 ISO/IEC/IEEE. Iso/iec/ieee international standard - systems and software engineering – taxonomy of systems of systems, 2019.

77 ITAÚ. Privacidade | itaú, 2022. Disponível em: <https://www.itau.com.br/privacidade/>, último acesso em 21 de março de 2022.

78 ITAÚ. Termos e condições | itaú, 2022. Disponível em: <https://www.itau.com.br/seguranca/termos-de-uso/> , último acesso em 21 de março de 2022.

79 JARAMILLO , A. F. Non-functional requirements elicitation from business process models. In 2011 FIFTH INTERNATIONAL CONFERENCE ON RESEARCH CHALLENGES IN INFORMATION SCIENCE (2011), pp. 1–7.

80 JINLING, C., TONG, S., CHUNCAN, L., AND TAO, S. Modeling e-commerce website quality with quality function deployment. In 2009 IEEE International Conference on e-Business Engineering (2009), pp. 417–422.

81 JÜRJENS, J. Secure Systems Development with UML. Springer-Verlag, Berlin, Heidelberg, 2010.

82 KALLONIATIS, C., KAVAKLI, E., AND GRITZALIS, S. Addressing privacy requirements in system design: the pris method. Requir. Eng. 13, 3 (2008), 241–255.

83 KANWAL, T., ANJUM, A., AND KHAN, A. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Clust. Comput. 24, 1 (2021), 293–317.

84 KASPARY, A. O Verbo na Linguagem Jurídica: Acepções e Regimes. Livraria do Advogado Editora, 2021.

85 KITCHENHAM, B. A., BUDGEN, D., AND BRERETON, P. Evidence-Based Software Engineering and Systematic Reviews. Chapman & Hall/CRC, 2015.

86 KITCHENHAM, B. A., AND CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Tech. Rep. EBSE 2007-001, Keele University and Durham University Joint Report, 07 2007.

87 LAUENROTH, K., KAMSTIES, E., AND HEHLERT, O. Do Words Make a Difference? An Empirical Study on the Impact of Taxonomies on the Classi cation of Requirements. In Proceedings - 2017 IEEE 25th International Requirements Engineering Conference, RE 2017 (Sep 2017), Institute of Electrical and Electronics Engineers Inc., pp. 273–282.

88 LEHNERT, S. A taxonomy for software change impact analysis. In Proceedings of the 12th International Workshop on Principles of Software Evolution and the 7th annual ERCIM Workshop on Software Evolution, EVOL/IWPSE 2011, Szeged, Hungary, September 5-6, 2011 (2011), A. Cleve and R. Robbes, Eds., ACM, pp. 41–50.

89 MABROK, M. A., EFATMANESHNIK, M., AND RYAN, M. J. Integrating nonfunctional requirements into axiomatic design methodology. IEEE Systems Journal 11, 4 (2017), 2204–2214.

90 MACRUAIRI, R., KEANE, M. T., AND COLEMAN, G. A wireless sensor network application requirements taxonomy. In 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008) (2008), pp. 209–216.

91 MAIA PEIXOTO, M. A Privacy Requirements Speci cation Method for Agile Software Development Based on Exploratory Studies. PhD thesis, Universidade Federal de Pernambuco, 2021.

92 MASSEY, A. K., AND ANTÓN, A. I. A requirements-based comparison of privacy taxonomies. In First International Workshop on Requirements Engineering and Law, RELAW 2008, Barcelona, Spain, September 9, 2008 (2008), IEEE Computer Society, pp. 1–5.

93 MEAD, N. R., AND STEHNEY, T. Security quality requirements engineering (square) methodology. In Proceedings of the 2005 Workshop on Software Engineering for Secure Systems—Building Trustworthy Applications (New York, NY, USA, 2005), SESS '05, Association for Computing Machinery, p. 1–7.

94 MEIS, R., AND HEISEL, M. Understanding the privacy goal intervenability. In Trust, Privacy and Security in Digital Business (Cham, 2016), S. Katsikas, C. Lambrinoudakis, and S. Furnell, Eds., Springer International Publishing, pp. 79–94.

95 MEIS, R., AND HEISEL, M. Computer-aided identi cation and validation of intervenability requirements. Information 8, 1 (mar 2017).

96 Meis, R., Wirtz, R., and Heisel, M. A taxonomy of requirements for the privacy goal transparency. In Trust, Privacy and Security in Digital Business - 12th International Conference, TrustBus 2015, Valencia, Spain, September 1-2, 2015, Proceedings (2015), S. Fischer-Hübner, C. Lambrinoudakis, and J. López, Eds., vol. 9264 of Lecture Notes in Computer Science, Springer, pp. 195–209.

97 Menegazzi, D. Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução. PhD thesis, Universidade Federal de Pernambuco, 2021.

98 Mouratidis, H., and Giorgini, P. Secure tropos: a security-oriented extension of the tropos methodology. Int. J. Softw. Eng. Knowl. Eng. 17, 2 (2007), 285–309.

99 Nickerson, R. C., Varshney, U., and Muntermann, J. A method for taxonomy development and its application in information systems. European Journal of Information Systems 22, 2 (2013).

100 Nuseibeh, B., and Easterbrook, S. Requirements engineering: A roadmap. In Proceedings of the Conference on The Future of Software Engineering (New York, NY, USA, 2000), ICSE '00, Association for Computing Machinery, p. 35–46.

101 Ouhbi, S., Idri, A., Fernández-Alemán, J. L., and Toval, A. Requirements engineering education: a systematic mapping study. Requirements Engineering 20, 2 (2015), 119–138.

102 Paech, B., and Kerlow, D. Non-Functional Requirements Engineering - Quality is essential. In Proceedings of the 10th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'04) (2004).

103 Parker, D. B. Fighting computer crime: A new framework for protecting information. In Computer Security Handbook (1998), 512.

104 Parliament, E., and European Union, C. o. General Data Protection Regulation (GDPR), 2016. <https://gdpr-info.eu>, último acesso 10 de abril de 2022.

105 Peixoto, M., Silva, C., Maia, H., and Araújo, J. Towards a catalog of privacy related concepts. CEUR Workshop Proceedings 2584 (2020).

106 Peixoto, M. M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., and Gorschek, T. On understanding how developers perceive and interpret privacy requirements research preview. In Requirements Engineering: Foundation for Software Quality - 26th International Working Conference, REFSQ 2020, Pisa, Italy, March 24-27, 2020, Proceedings [REFSQ 2020 was postponed] (2020), N. H. Madhavji, L. Pasquale, A. Ferrari, and S. Gnesi, Eds., vol. 12045 of Lecture Notes in Computer Science, Springer, pp. 116–123.

107 Ramingwong, L. A review of requirements engineering processes, problems and models. International Journal of Engineering Science and Technology 6, 4 (2012).

108 Rjaibi, N., and Rabai, L. B. A. Developing a novel holistic taxonomy of security requirements. In Procedia Computer Science (2015), vol. 62, Elsevier B.V., pp. 213–220.

109 Rodotà, S. A vida na sociedade da vigilância: a privacidade hoje. Renovar, 2008.

110 Ruaro, R. L., Rodriguez, D. P., and Finger, B. O direito à proteção de dados pessoais e a privacidade. Revista da Faculdade de Direito UFPR 53 (2011).

111 Sajjad, U., and Hanif, M. Q. Issues and challenges of requirement elicitation in large web projects. Master's thesis, , School of Computing, 2010. Umar Sajjad Charhoi, Kotli, Azad Kashmir, Pakistan Muhammad Qaisar Hanif Bhimber, Azad Kashmir, Pakistan.

112 Sangaroonsilp, P., Dam, H. K., Choetkiertikul, M., Ragkhitwetsagul, C., and Ghose, A. A taxonomy for mining and classifying privacy requirements in issue reports. CoRR abs/2101.01298 (2021).

113 Schreiber, A. Right to Privacy and Personal Data Protection in Brazilian Law. Springer International Publishing, Cham, 2020.

114 Shaikh, M. A., Al-Badi, A. H., Al-Elaiwi, A. H., Al-Ameri, A., and Whittaker, J. A. E-commerce need analysis via quality function deployment. In IEMC'01 Proceedings. Change Management and the New Industrial Revolution. IEMC-2001 (Cat. No.01CH37286) (2001).

115 Shehadeh, K., Arman, N., and Khamayseh, F. Semi-Automated Classi cation of Arabic User Requirements into Functional and Non-Functional Requirements using NLP 2021. In International Conference on Information Technology, ICIT 2021 - Proceedings (2021), 527–532.

116 Siegfried, N., Rosenthal, T., and Benlian, A. Blockchain and the Industrial Internet of Things: A requirement taxonomy and systematic t analysis. Journal of Enterprise Information Management (2020).

117 Skinner, G., Han, S., and Chang, E. An information privacy taxonomy for collaborative environments. Information Management and Computer Security 14 (2006), 382–394.

118 Sommerville, I. Engenharia de Software, 9 ed. Pearson Prentice Hall, 2011.

119 Tang, Y., Brockman, M. L., and Patil, S. Promoting Privacy Considerations in Real-World Projects in Capstone Courses with Ideation Cards. ACM Transactions on Computing Education, 21 (2021), 1–28.

120 Tikkinen-Piri, C., Rohunen, A., and Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law and Security Review, 34 1 (2 2018), 134–153.

121 UNCTAD. Data protection and privacy legislation worldwide, 2020. Acessado em 13 de outubro de 2021.

122 Verner, J., Sampson, J., Tosic, V., Bakar, N. A., and Kitchenham, B. Guidelines for industrially-based multiple case studies in software engineering. In 2009 Third International Conference on Research Challenges in Information Science (2009), pp. 313–324.

123 Webster, I., Ivanova, V., and Cysneiros, L. M. Reusable knowledge for achieving privacy: A canadian health information technologies perspective. In WER 2005 - 8th Workshop on Requirements Engineering, Workshop em Engenharia de Requisitos (2005), 112–122.

124 Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wessln, A. Experimentation in Software Engineering. Springer Publishing Company, Incorporated, 2012.

125 Zafar, F., Khan, A., Anjum, A., Maple, C., and Shah, M. A. Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis. Electronics 9, 11 (nov 2020), 1–22.

126 Zannone, N. A requirements engineering methodology for trust, security, and privacy. PhD thesis, University of Trento, 2007.

127 Zave, P. Classi cation of research efforts in requirements engineering. ACM Comput. Surv. 29, 4 (Dec. 1997), 315–321.

APÊNDICES

I.1 DESENVOLVIMENTO DA TAXONOMIA

I - DescriçãoEste documento tem o objetivo de descrever os passos para obtenção da taxonomia de requisitos de privacidade a partir da LGPD e ISO/IEC 29100. As técnicas utilizadas para alcance da taxonomia são a teoria fundamentada e abordagens de análise de conteúdo (GBRAM) demonstradas a seguir. Para identi cação das declarações nas normas serão utilizadas alguns perguntas que visam componentes importantes para a taxonomia. Essas declarações serão transformadas em requisitos de privacidade agrupados em categorias para compor esta taxonomia. Sua utilidade será para desenvolvedores de software e analistas de sistemas que precisam trabalhar com sistemas que envolvam regras regulatórias mas que não possuem domínio sobre esses regulamentos. Na taxonomia os requisitos deixarão os termos jurídicos mais simples para o time de TI.

Entradas

- Lei Geral de Proteção de Dados - nº 13709. Artigos: 7-21, 23, 25-27, 33, 37, 41, 46, 48, 49, 52. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

- ISO/IEC 29100:2011. Primeira edição: 15/12/2011.

Processo

Este processo é composto por 4 etapas para identi cação de requisitos de privacidade.

Saídas

Requisitos de privacidade obtidos a partir da LGPD e ISO/IEC 29100.

Etapas

I - Identi cação dos Requisitos de Privacidade

Objetivo: Esta etapa tem o objetivo de extrair requisitos de declarações escritas no LGPD e no framework de privacidade. Serão usadas determinadas perguntas para identi cação dos componentes relevantes das declarações contidas nessas normas para a construção de um requisito de privacidade.

Passos:

a. identi cação de ações

Para cada a rmação nas regulações, são procuradas as ações perguntando "Qual ação deve ser fornecida com base nesta a rmação?". Alguns exemplos dos verbos de ação utilizados para mapeamento dos requisitos para a taxonomia: Permitir, arquivar, coletar, apagar, implementar, informar, manter, noti car, obter, apresentar, proteger, fornecer, solicitar, mostrar, armazenar, transmitir e usar.

b. Determinação das partes envolvidas/afetadas

Com a identi cação da ação, é necessário em seguida identi car o objeto dessa ação perguntando "Quem está envolvido/afetado por essa a rmação?". Por ser o objeto, ou seja, o envolvido ou afetado eles podem ser opcionais.

c. Ponderação do resultado esperado

Este passo especi ca o resultado esperado que pode ser alcançado para atender à privacidade e aos direitos do usuário, perguntando "O que deve ser alcançado com base na ação dessa declaração?".

d. Estruturação em um padrão de requisito

O requisito de privacidade derivado é codi cado no formato de verbo de ação, seguido pelo objeto e objetivo.

Os passos a-c podem ser executados em quaisquer ordem.

EXEMPLO

Declaração identi cada na LGPD:

(...) Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. (...)

Seguindo este manual, teremos a seguinte estrutura analisada passo a passo:

a. ação identi cada:

- INDICAR

Nela é identi cado que o controlador de dados tem por obrigação indicar um encarregado para o tratamento de dados pessoais. A ação necessária nesta declaração é a indicação por parte do controlador, o verbo de ação utilizado então será o INDICAR.

b. determinação das partes envolvidas:

- controlador

A parte envolvida na ação previamente identi cada, a parte que precisa tomar alguma ação em relação a declaração é o controlador.

c. ponderação do resultado esperado:

- encarregado pelo tratamento de dados pessoais.

Aqui é identi cado o objetivo do trecho, que refere-se a indicação do encarregado pelo tratamento de dados pessoais.

II - Classi cação dos Requisitos de Privacidade

Objetivo: Classi car os requisitos de privacidade obtidos na etapa anterior em uma das categorias de metas de privacidade com base em sua relevância. As metas são de nidas considerando os sete princípios do LGPD.

Passos:

a. De nação das conquistas de cada meta de privacidade

Este passo descreve o esperado para cada princípio da LGPD, que será a categoria das metas dessa Taxonomia. Essa de nição será utilizada para identi car e reunir os requisitos de privacidade que possuem o mesmo objetivo do disposto em uma categoria. A execução deste passo ocorrerá apenas uma vez.

b. Consideração do resultado esperado para um requisito

Classi cação dos requisitos de privacidade de acordo com a meta a qual sua realização é mais adequada.

Para cada requisito é necessário indicar a categoria a qual o requisito se enquadra. As categorias são apresentadas a seguir.

Categorias de Privacidade

P.1 Finalidade: Esse objetivo de privacidade agrupa requisitos em que se registram que o tratamento de dados deve ser limitado uma nalidade determinada. Sua utilização e processamento não devem extrapolar a nalidade da qual o titular autorizou. Além disso, o propósito do tratamento de dados deverá ser legítimo e estar explicitado ao titular dos dados;

P.2 Adequação Esse objetivo de privacidade refere-se a compatibilidade do tratamento de dados em relação à sua nalidade, que foi descrita ao titular dos dados no momento do consentimento. O tratamento de dados deve ocorrer de acordo com a nalidade e para seu alcance;

P.3 Necessidade Esse objetivo de privacidade compreende os requisitos que são relacionados com a utilização dos dados no tratamento de acordo com a necessidade descrita previamente no momento de seu consentimento e sua coleta. Ou seja, o tratamento deve ser limitado estritamente à sua nalidade;

P.4 Livre acesso Esse objetivo de privacidade trata da permissão, por parte do titular dos dados, para consulta gratuita sobre a forma utilizada no tratamento de dados, a sua duração e a integralidade de seus dados pessoais que os agentes de tratamento possuem;

P.5 Qualidade dos dados Esse objetivo de privacidade endossa o cumprimento da nalidade especí ca, conforme autorização do titular dos dados no momento de sua obtenção, no tratamento dos dados de forma a estarem exatos, claros, relevantes a nalidade e atualizados. Assim possibilitando mecanismos que garantam essas condições;

P.6 Transparência: Esse objetivo de privacidade deve garantir aos titulares dos dados informações claras, precisas e de acesso facilitado sobre o processo de tratamento dos dados. Permitindo ao titular o conhecimento sobre como o tratamento ocorre. A transparência deve ser exercida também sobre os respectivos agentes de tratamento envolvidos no processo, observados os segredos comercial e industrial;

P.7 Segurança: Esse objetivo de privacidade visa promover a segurança dos dados pessoais a partir de medidas técnicas e administrativas que os protejam de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Essas medidas devem envolver controles e mecanismos de segurança adequados para garantia do processo de tratamento seguro;

P.8 Prevenção: Esse objetivo de privacidade aborda o estabelecimento e execução de medidas para prevenção da ocorrência de danos, aos titulares de dados assim como aos agentes de tratamento, em virtude do processo de tratamento de dados pessoais;

P.9 Não discriminação: Esse objetivo de privacidade contempla a vedação à utilização dos dados pessoais, previamente obtidos, para tratamentos com ns discriminatórios ilícitos ou abusivos. Os dados obtidos dos titulares não devem ser usados para os propósitos diferentes, principalmente para exercício do crime de discriminação;

P.10 Responsabilização e prestação de contas: Esse objetivo de privacidade endereça que agente de tratamento deve demonstrar as medidas adotadas que são capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Além disso, precisam apresentar a e cácia dessas medidas no cumprimento de seus objetivos.

Como a LGPD abrange diversas áreas da engenharia de software, foram identi cados contextos além dos sistêmicos para os quais os requisitos se aplicam sendo esses denominados contextos. Esses contextos são de nidos adicionalmente à categoria para que os analistas de sistemas consigam identi car as necessidades dentro de sua instituição. Seguem os contextos:

C.1 Software: Identi ca requisitos de privacidade que podem ser implementados em softwares. Ou seja, requisitos de sistema que podem ser validados pelas regras de negócio;

C.2 Estudos e pesquisa: São requisitos que determinam como órgãos de pesquisa devem seguir para o tratamento de dados que pode ser operacionalizado por um sistema deste órgão de forma mais especí ca;

C.3 Governança: Identi ca os requisitos que não necessariamente podem ser atendidos por sistemas, mas que precisam ser implementados pela organização, neles podem haver controles e mecanismos de governança para a garantia dos princípios da LGPD;

C.4 Gestão Pública: Marca os requisitos que são obrigatórios para órgãos de natureza pública, mas que precisam ser implementados pela organização para garantir a aderência à legislação no que se refere ao compartilhamento de dados principalmente sem a necessidade de consentimento resguardados pelo direito de sua natureza;

C.5 Infraestrutura : Requisitos sobre o processo de compartilhamento de informações internacionalmente, transferência de dados com terceiros além processos e controles de armazenamento de dados.

Exemplificando a execução da etapa TP2.b, para classificar o requisito INDICAR o encarregado pelo tratamento de dados pessoais em uma das categorias acima. Seguindo o estipulado na etapa, é necessário considerar o resultado esperado para se alcançar com esse requisito. O objetivo desse requisito é indicar o encarregado pelo tratamento de dados pessoais ao titular dos dados, podendo assim ser categorizado no objetivo P.6 Transparência. Por se tratar de algo que não necessariamente será registrado/controlado por sistemas de informação e sim por processos de governança, por isso ele se classifica no contexto de C.8 Governança.

III - Refinamento dos requisitos de privacidade

Para o refinamento foram avaliados os 169 requisitos obtidos a partir da base taxonômica (LGPD e ISO/IEC 29100), que podem ter semelhanças ou podem ser redundantes entre si. Com a classificação dos requisitos em categorias ocorreu a identificação dos requisitos semelhantes, que foram adequados para uma versão única e os duplicados foram excluídos.

Como exemplificação, a declaração da LGPD ("...) Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.(...") gerou o requisito RLGPD013 - COLETAR o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Enquanto na ISO/IEC 29100 o trecho ("...) obter o consentimento opcional do principal de PII para coletar ou processar PII condenciais, exceto quando a lei aplicável permitir o processamento de PII condenciais sem o consentimento da pessoa física.") deriva o requisito RQISO3 - OBTER o consentimento opcional do titular de dados para coletar ou processar os dados condenciais, exceto quando a lei aplicável permitir o processamento de dados condenciais sem o consentimento da pessoa física. Os dois requisitos estão classificados na categoria P.1 Finalidade e podem ser mesclados para um requisito único o qual é OBTER o consentimento opcional do titular de dados para coletar ou processar os dados condenciais a partir de manifestação declarada deste, exceto quando a lei aplicável permitir o processamento de dados condenciais sem o consentimento da pessoa física.

Com o processo de refinamento 27 requisitos foram unificados entre si enquanto 17 requisitos foram identificados como duplicados, 3 requisitos obtidos da ISO/IEC e 3 requisitos obtidos da LGPD foram excluídos após análise por estarem fora do escopo dos requisitos de privacidade, restando 129 requisitos de privacidade.

I.2 TABELAS DE REQUISITOS GERADAS NA PROPOSIÇÃO DA TAXONOMIA

Art	Trecho	Requisito
7º	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por pro ssionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente	RLGPD001 - PERMITIR o tratamento de dados pessoais mediante o consentimento expresso do titular de dados; RLGPD002 - PERMITIR o controlador fazer o tratamento de dados para cumprimento de obrigação legal/regulatória; RLGPD003 - PERMITIR a administração pública o tratamento de dados assim como seu compartilhamento quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; RLGPD004 - PERMITIR o tratamento de dados para estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; RLGPD005 - PERMITIR o tratamento de dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular faça parte, a seu pedido; RLGPD006 - PERMITIR o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme legislação; RLGPD007 - PERMITIR o tratamento de dados para a proteção da vida, da incolumidade física do titular ou de terceiro, para a tutela da saúde exclusivamente em procedimento realizado por pro ssionais de saúde ou por entidades sanitárias;

Art	Trecho	Requisito
		RLGPD008 - PERMITIR o controlador de dados fazer o tratamento de dados quando necessário para atender aos seus interesses legítimos, com exceção das situações em que prevalecerem direitos e liberdades fundamentais do titular exijindo a proteção dos dados pessoais; RLGPD009 - PERMITIR o controlador de dados fazer o tratamento de dados pessoais para a proteção do crédito.
7º	§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justi caram sua disponibilização.	RLGPD010 - APRESENTAR a finalidade, a boa-fé e o interesse público que justi caram o tratamento de dados pessoais de acesso público;
7º	§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.	RLGPD011 - DISPENSAR a exigência de consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios de tratamento de dados.
7º	§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.	RLGPD012 - OBTER consentimento específico para a comunicação ou compartilhamento dos dados pessoais com outros controladores ressalvadas as hipóteses de dispensa do consentimento legais.
8º	Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.	RLGPD013 - COLETAR o consentimento por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
8º	§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.	RLGPD014 - ARMAZENAR o registro da obtenção do consentimento e da forma de sua obtenção, sendo dever do controlador
8º	§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.	RLGPD015 - VEDAR o tratamento de dados mediante vicio de consentimento.

Art	Trecho	Requisito
8º	§ 4º O consentimento deverá referir-se a nalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.	RLGPD016 - APRESENTAR o consentimento para a nalidades determinadas. RLGPD017 - IMPEDIR que consentimentos com autorizações genéricas para o tratamento de dados pessoais sejam gerados
8º	§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, rati cados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.	RLGPD018 - PERMITIR ao titular regovar a qualquer momento um consentimento mediante manifestação expressa por procedimento gratuito e facilitado, rati cados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.
8º	§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma especí ca do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.	RLGPD019 - INFORMAR ao titular dos dados de forma explícita o teor das alterações de nalidade especí ca do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identi cação do controlador; e informações de contato do controlador, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.
9º	Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:	RLGPD020 - FORNECER ao titular de maneira facilitada às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso
9º	§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.	RLGPD021 - TORNAR o consentimento do titular nulo, nas hipóteses em que é requerido, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Art	Trecho	Requisito
9º	§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da nalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de nalidade, podendo o titular revogar o consentimento, caso discorde das alterações	RLGPD022 - PERMITIR o titular revogar o consentimento, nas hipóteses em que é requerido, se houver mudanças da nalidade para o tratamento de dados pessoais não compatíveis com o consentimento original
9º	§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.	RLGPD023 - COMUNICAR o titular quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito.

Art	Trecho	Requisito
10º	Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para nalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o bene ciem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a nalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.	RLGPD024 - NOTIFICAR que o controlador somente poderá fundamentar o tratamento de dados pessoais para nalidades legítimas; RLGPD025 - PERMITIR ao controlador que seja feito o tratamento de dados para a nalidade de apoio e promoção a atividades; RLGPD026 - PERMITIR que o controlador efetue o tratamento de dados para proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o bene ciem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais; RLGPD027 - COLETAR somente dos dados pessoais estritamente necessários para a nalidade pretendida para o controlador fazer o tratamento de dados em seu legítimo interesse; RLGPD028 - ADOTAR medidas para garantir a transparência do tratamento de dados por parte do controlador; RLGPD029 - APRESENTAR a ANPD, quando por ela solicitado, relatório de impacto à proteção de dados pessoais para o tratamento fundamentado em seu legítimo interesse, observados os segredos comercial e industrial;

Art	Trecho	Requisito
11º	Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma especí ca e destacada, para nalidades especí cas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por pro ssionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência g) garantia da prevenção à fraude e à segurança do titular, nos processos de identi cação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	RLGPD030 - PERMITIR o tratamento de dados pessoais sensíveis somente quando o titular ou seu responsável legal consentir, de forma especí ca e destacada, para nalidades especí cas; RLGPD031 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador; RLGPD079 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos por parte da administração pública; RLGPD080 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; RLGPD081 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último conforme legislação vigente. RLGPD082 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiro e tutela da saúde, exclusivamente, em procedimento realizado por pro ssionais de saúde, serviços de saúde ou autoridade sanitária;

Art	Trecho	Requisito
11º	Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:	RLGPD083 - PERMITIR o tratamento de dados pessoais sensíveis sem fornecimento de consentimento do titular, quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identi cação e autenticação de cadastro em sistemas eletrônicos, resguardados os seus direitos e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
11º	§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação especí ca.	RLGPD032 - IMPLEMENTAR disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação especí ca.
11º	§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.	RLGPD033 - TORNAR pública a dispensa de consentimento por parte dos órgãos e entidades públicas quando necessário o tratamento de dados pessoais sensíveis para para execução de suas atribuições.
11º	§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de bene ciários.	RLGPD034 - VEDAR às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de bene ciários.
12º	§ 2º Poderão ser igualmente considerados, como dados pessoais, para os ns desta Lei, aqueles utilizados para formação do perl comportamental de determinada pessoa natural, se identi cada.	RLGPD035 - CONSIDERAR como dados pessoais, aqueles utilizados para formação do perl comportamental de determinada pessoa natural, se identi cada.
13º	§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.	RLGPD036 - PROTEGER a divulgação de dados pessoais em resultados de pesquisas de saúde.

Art	Trecho	Requisito
13º	§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.	RL-GPD037 - GARANTIR que o órgão de pesquisa seja o responsável pela segurança da informação dos dados pessoais, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
14º	§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.	RL-GPD038 - COLETAR consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal para tratamento de dados pessoais de crianças

Art	Trecho	Requisito
14º	§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.	RLGPD039 - MANTER disponível em área pública a informação sobre os tipos de dados pessoais coletados dos titulares de dados que são crianças. RLGPD084 - MANTER disponível em área pública os procedimentos necessários para con rmação da existência de tratamento pelo titular; RLGPD085 - MANTER disponível em área pública os procedimentos necessários para acesso aos dados pelo titular; RLGPD086 - MANTER disponível em área pública os procedimentos necessários para correção de dados incompletos, inexatos ou desatualizados; RLGPD087 - MANTER disponível em área pública os procedimentos necessários para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; RLGPD088 - MANTER disponível em área pública os procedimentos necessários para portabilidade dos dados a outro fornecedor de serviço/produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; RLGPD089 - MANTER disponível em área pública os procedimentos necessários para eliminação dos dados pessoais tratados com o consentimento do titular;

Art	Trecho	Requisito
	Continuação	RLGPD090 - MANTER disponível em área pública os procedimentos necessários para obtenção de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; RLGPD091 - MANTER disponível em área pública a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; RLGPD092 - MANTER disponível em área pública os procedimentos necessários para revogação do consentimento.
14º	§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.	RLGPD040 - COLETAR dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.
14º	§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.	RLGPD041 - IMPEDIR a obrigatoriedade de fornecimento de informações pessoais, além das estritamente necessárias à atividade, para a participação dos titulares de dados crianças e adolescentes em jogos, aplicações de internet ou outras atividades
14º	§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.	RLGPD042 - REALIZAR todos os esforços razoáveis para verificar que o consentimento de dados pessoais de crianças e adolescentes foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis, sendo dever do controlador

Art	Trecho	Requisito
14º	§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.	RLGPD043 - APRESENTAR as informações sobre o tratamento de dados pessoais de crianças e adolescentes de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.
15º	Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - veri cação de que a nalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da nalidade especí ca almejada; II - m do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.	RLGPD044 - FINALIZAR o tratamento de dados pessoais quando a nalidade for alcançada ou quando os dados deixarem de ser necessários ou pertinentes ao alcance da nalidade especí ca almejada; RLGPD093 - FINALIZAR o tratamento de dados pessoais no m do período de tratamento; RLGPD094 - FINALIZAR o tratamento de dados pessoais quando da comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; RLGPD095 - FINALIZAR o tratamento de dados pessoais quando houver violação da lei por determinação da autoridade nacional.

Art	Trecho	Requisito
16º	Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes nalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.	RLGPD045 - APAGAR os dados pessoais após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação em exceções especí cas. RLGPD097 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; RLGPD098 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para transferência a terceiro, desde que respeitados os requisitos de tratamento de dados RLGPD099 - PERMITIR a conservação dos dados pessoais após o término de seu tratamento para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Art	Trecho	Requisito
18º	Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - con rmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.	RLGPD046 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a con rmação da existência de tratamento; RLGPD100 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição o acesso aos dados; RLGPD101 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a correção de dados incompletos, inexatos ou desatualizados; RLGPD102 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; RLGPD103 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; RLGPD104 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a eliminação dos dados pessoais tratados com o consentimento do titular, observadas as exceções previstas; RLGPD105 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

Art	Trecho	Requisito
18º	Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)	RLGPD106 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; RLGPD107 - OBTER do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição a revogação do consentimento.
18º	§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.	RLGPD047 - PERMITIR ao titular opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento dos seus direitos.
18º	§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.	RLGPD048 - NOTIFICAR o titular de dados em caso de impossibilidade de adoção imediata comunicando caso não seja o agente de tratamento dos dados e indicar, sempre que possível, o agente; RLGPD049 - NOTIFICAR o titular de dados em caso de impossibilidade de adoção imediata indicando as razões de fato ou de direito que impedem a adoção imediata da providência.
18º	§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.	RLGPD050 - PERMITIR que o requerimento de informações sobre seus dados seja atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
18º	§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.	RLGPD051 - INFORMAR que a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador
18º	§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.	RLGPD052 - INFORMAR que o direito de requisição de informações também poderá ser exercido perante os organismos de defesa do consumidor.

Art	Trecho	Requisito
19º	Art. 19. A con rmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simpli cado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a na lidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.	RLGPD053 - PERMITIR e providenciar imediatamente ao titular, mediante requisição em formato simpli cado, a con rmação de existência ou o acesso aos dados pessoais; RLGPD108 - PERMITIR e providenciar ao titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a na lidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular, a con rmação de existência ou o acesso aos dados pessoais;
19º	§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.	RLGPD054 - ARMAZENAR os dados pessoais em formato que favoreça o exercício do direito de acesso por parte do titular de dados.
19º	§ 2º As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse m; ou II - sob forma impressa.	RLGPD055 - FORNECER as informações e os dados por meio eletrônico, seguro e idôneo para esse m ou sob forma impressa, a critério do titular.
19º	§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.	RLGPD056 - PERMITIR ao titular solicitar cópia eletrônica integral de seus dados pessoais, quando o tratamento tiver origem no consentimento ou em contrato, observados os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

Art	Trecho	Requisito
20º	Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência	RLGPD057 - PERMITIR ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
20º	§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.	RLGPD058 - FORNECER ao titular de dados, a partir de solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para decisões automatizadas, observados os segredos comercial e industrial.
20º	§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.	RLGPD059 - ATENDER a realização de auditoria, por parte da autoridade nacional, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, em caso de não oferecimento das e informações dos critérios e procedimentos utilizados para decisões automatizadas, baseado na observância de segredo comercial e industrial.
21º	Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.	RLGPD060 - PROTEGER para que os dados pessoais referentes ao exercício regular de direitos pelo titular não sejam utilizados em seu prejuízo.

Art	Trecho	Requisito
23º	Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua nalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a nalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;	RLGPD061 - NOTIFICAR o titular de dados, em veículos de fácil acesso preferencialmente em seus sítios eletrônicos, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público no exercício de suas competências são realizados fornecendo informações claras e atualizadas sobre a previsão legal, a nalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, para o atendimento de sua nalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.
23º	§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as nalidades de que trata o caput deste artigo.	RLGPD062 - FORNECER por parte dos órgãos notariais e de registro, acesso aos dados por meio eletrônico para a administração pública, tendo em vista as nalidades públicas.
25º	Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.	RLGPD063 - ARMAZENAR os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
26º	Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a nalidades especí cas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.	RLGPD064 - GARANTIR que o uso compartilhado de dados pessoais pelo Poder Público seja para atender a nalidades especí cas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

Art	Trecho	Requisito
26º	§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse m especí co e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ; III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019) V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras nalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência	RLGPD065 - PERMITIR por parte do poder público a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso apenas em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse m especí co e determinado, nos casos em que os dados forem acessíveis publicamente, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres ou na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras nalidades.
27º	Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei.	RLGPD066 - INFORMAR a autoridade nacional, por parte do agente de tratamento, quando da comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado.

Art	Trecho	Requisito
33º	Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais especí cas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certi cados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento especí co e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras nalidades; ou	RLGPD067 - PERMITIR a transferência internacional de dados pessoais somente nos casos em países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto no Brasil e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados brasileiros a partir de contratos, normas corporativas globais, selos, certi cados e códigos de conduta regularmente emitidos. RLGPD076 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade da política; RLGPD077 - PERMITIR a transferência internacional de dados pessoais somente quando o titular tiver fornecido o seu consentimento especí co e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras nalidades RLGPD109 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; RLGPD110 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Art	Trecho	Requisito
33º	Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: (...) IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os ns do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.	RLGPD111 - PERMITIR a transferência internacional de dados pessoais somente quando a autoridade nacional autorizar a transferência; RLGPD112 - PERMITIR a transferência internacional de dados pessoais somente quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
37º	Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.	RLGPD068 - GARANTIR a manutenção de registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, por parte do controlador e o operador.
41º	§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.	RLGPD069 - INDICAR o encarregado pelo tratamento de dados pessoais
46º	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.	RLGPD070 - GARANTIR a adoção de 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 por parte dos agentes de tratamento.

Art	Trecho	Requisito
48º	Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme de nido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.	RLGPD071 - COMUNICAR à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, por parte do controlador.
49º	Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.	RLGPD072 - IMPLEMENTAR nos sistemas utilizados para o tratamento de dados pessoais para serem estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.
52º	Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, cam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (...) IV - publicização da infração após devidamente apurada e con rmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração;	RLGPD073 - PUBLICIZAR a infração após devidamente apurada e con rmada a sua ocorrência; RLGPD074 - BLOQUEAR os dados pessoais a que se refere a infração até a sua regularização; RLGPD075 - APAGAR os dados pessoais a que se refere a infração;

Tabela 1: Lista de requisitos primários obtidos a partir LGPD.

Princípio	Trecho	Requisito
Consentimento e escolha		
	Aderir ao princípio do consentimento signi ca: apresentar ao titular de PII a escolha de permitir ou não o processamento de suas PII, exceto quando o titular de PII não puder recusar livremente o consentimento ou quando a lei aplicável permitir especi camente o processamento de PII sem o consentimento da pessoa física	RQISO1 - APRESENTAR ao titular de dados a escolha de permitir ou não o processamento de seus dados, exceto quando o titular de dados não puder recusar livremente o consentimento ou quando a lei aplicável permitir especi camente o processamento de dados sem o consentimento da pessoa física
	Aderir ao princípio do consentimento signi ca: A escolha do diretor de PII deve ser dada de forma livre, especí ca e com conhecimento de causa;	RQISO2 - PERMITIR que a escolha de consentimento seja dada de forma livre, especí ca e com conhecimento de causa;
	obter o consentimento opcional do principal de PII para coletar ou processar PII con denciais, exceto quando a lei aplicável permitir o processamento de PII con denciais sem o consentimento da pessoa física;	RQISO3 - OBTER o consentimento opcional do titular de dados para coletar ou processar os dados con denciais, exceto quando a lei aplicável permitir o processamento de dados con denciais sem o consentimento da pessoa física;
	informar os diretores de PII, antes de obter consentimento, sobre seus direitos sob a participação individual e princípio de acesso	RQISO4 - INFORMAR aos titulares de dados, antes de obter consentimento, sobre seus direitos sob a participação individual e princípio de acesso;
	fornecer aos titulares de PII, antes de obter o consentimento, as informações indicadas pela abertura, princípio de transparência e noti cação	RQISO5 - FORNECER aos titulares de dados, antes de obter o consentimento, as informações indicadas pela abertura, princípio de transparência e noti cação
	explicar aos diretores de PII as implicações de conceder ou recusar consentimento	RQISO6 - EXPLICAR aos titulares dos dados as implicações de conceder ou recusar consentimento

Princípio	Trecho	Requisito
Para um controlador PII, aderir ao princípio de escolha signi ca:	fornecer aos titulares de PII mecanismos claros, proeminentes, facilmente compreensíveis, acessíveis e acessíveis para exercer a escolha e dar consentimento em relação ao processamento de suas PII no momento da coleta, primeiro uso ou assim que possível	RQISO7 - FORNECER aos titulares de dados mecanismos claros, proeminentes, facilmente compreensíveis, acessíveis e acessíveis para exercer a escolha e dar consentimento em relação ao processamento de suas informaçnoes no momento da coleta, primeiro uso ou assim que possível
	implementar as preferências do principal PII conforme expresso em seu consentimento.	RQISO8 - IMPLEMENTAR as preferências do titular de dados conforme expresso em seu consentimento.
Legitimidade e especi cação do propósito		
Aderir ao princípio de legitimidade e especi cação de propósito signi ca:	garantir que a(s) nalidade(s) esteja(m) em conformidade com a lei aplicável e se baseie em uma base legal permitida;	RQISO9 - GARANTIR que a(s) nalidade(s) esteja(m) em conformidade com a lei aplicável e se baseie em uma base legal permitida;
	comunicar o(s) objetivo(s) ao principal PII antes do momento em que as informações são coletadas ou usadas pela primeira vez para um novo propósito;	RQISO10 - COMUNICAR o(s) objetivo(s) ao titular de dados antes do momento em que as informações são coletadas ou usadas pela primeira vez para um novo propósito;
	usar uma linguagem para esta especi cação que seja clara e apropriadamente adaptada a circunstâncias	RQISO11 - USAR uma linguagem para esta especi cação que seja clara e apropriadamente adaptada a circunstâncias
	se aplicável, dando explicações su cientes para a necessidade de processar PII sensíveis.	RQISO12 - APRESENTAR quando aplicável explicações su cientes para a necessidade de processar dados sensíveis.
Limitação de coleta		

Princípio	Trecho	Requisito
Aderir ao princípio da limitação de coleta signi- ca:	limitar a coleta de PII ao que está dentro dos limites da lei aplicável e estritamente necessário para a(s) nalidade(s) especi cada(s).	RQISO13 - LIMITAR a coleta de dados ao que está dentro dos limites da lei aplicável e estritamente necessário para a(s) nalidade(s) especi cada(s).
Minimização de dados		
Aderir ao princípio de minimização de dados signi ca projetar e implementar procedimentos de processamento de dados e sistemas de TIC de forma a:	minimizar as PII que são processadas e o número de partes interessadas em privacidade e pessoas a quem as PII é divulgada ou que a ela tenham acesso	RQISO14 - MINIMIZAR as informações que são processadas e o número de partes interessadas em privacidade e pessoas a quem as informações são divulgadas ou que a ela tenham acesso
	assegurar a adoção de um princípio de “necessidade de conhecimento”, ou seja, deve-se ter acesso apenas às PII que sejam necessárias para o desempenho de suas funções o ciais no âmbito do propósito legítimo do processamento de PII;	RQISO15 - ASSEGURAR a adoção de um princípio de “necessidade de conhecimento”, ou seja, deve-se ter acesso apenas às informções que sejam necessárias para o desempenho de suas funções o ciais no âmbito do propósito legítimo do processamento de dados;
	usar ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identi cação de PII principais, reduzam a observabilidade de seu comportamento e limitem a vinculação das PII coletadas	RQISO16 - USAR ou oferecer como opções padrão, sempre que possível, interações e transações que não envolvam a identi cação de titulares de dados, reduzam a observabilidade de seu comportamento e limitem a vinculação das informações coletadas
	excluir e descartar PII sempre que a nalidade do processamento de PII tiver expirado, não houver requisitos legais para manter as PII ou sempre que for prático fazê-lo.	RQISO17 - APAGAR e descartar dados sempre que a nalidade do processamento de PII tiver expirado, não houver requisitos legais para manter as informações ou sempre que for prático fazê-lo.

Princípio	Trecho	Requisito
Limitação de uso, retenção e divulgação		
Aderir ao princípio de limitação de uso, retenção e divulgação significa:	limitar o uso, retenção e divulgação (incluindo transferência) de PII ao que for necessário para cumprir propósitos especí cos, explícitos e legítimos;	RQISO18 - LIMITAR o uso, retenção e divulgação (incluindo transferência) de dados ao que for necessário para cumprir propósitos especí cos, explícitos e legítimos;
	limitar o uso de PII aos propósitos especi cados pelo controlador de PII antes da coleta a menos que um propósito diferente seja explicitamente exigido pela lei aplicável;	RQISO19 - LIMITAR o uso de dados aos propósitos especi cados pelo controlador de dados antes da coleta a menos que um propósito diferente seja explicitamente exigido pela lei aplicável;
	reter PII apenas pelo tempo necessário	
para cumprir os propósitos declarados e, posteriormente, destruí-los ou anonimá-los com segurança	RQISO20 - RETER os dados apenas pelo tempo necessário para cumprir os propósitos declarados e, posteriormente, destruí-los ou anonimá-los com segurança	
	bloquear (ou seja, arquivar, proteger e isentar as PII de processamento adicional) qualquer PII quando e enquanto os propósitos declarados expirarem, mas quando a retenção for exigida pelas leis aplicáveis	RQISO21 - BLOQUEAR (ou seja, arquivar, proteger e isentar os dados de processamento adicional) qualquer dados quando e enquanto os propósitos declarados expirarem, mas quando a retenção for exigida pelas leis aplicáveis
Precisão e qualidade		
Aderir ao princípio de precisão e qualidade significa:	garantir que as PII processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a nalidade de uso;	RQISO22 - GARANTIR que as informações processadas sejam precisas, completas e atualizadas (a menos que haja uma base legítima para manter dados desatualizados), adequados e relevantes para a nalidade de uso;

Princípio	Trecho	Requisito
	garantir a con abilidade das PII coletadas de uma fonte diferente do principal de PII antes de serem processado	RQISO23 - GARANTIR a con abilidade das informações coletadas de uma fonte diferente do titular de dados antes de serem processados
	veri car, por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas IIP antes de fazer qualquer alteração nas IIP (para garantir que as alterações sejam devidamente autorizadas), quando apropriado;	RQISO24 - VERIFICAR, por meios apropriados, a validade e exatidão das reivindicações feitas pelo responsável pelas informações antes de fazer qualquer alteração nas informações (para garantir que as alterações sejam devidamente autorizadas), quando apropriado
	estabelecer procedimentos de coleta de PII para ajudar a garantir precisão e qualidade;	RQISO25 - ESTABELECER procedimentos de coleta de dados para ajudar a garantir precisão e qualidade;
	estabelecer mecanismos de controle para veri car periodicamente a precisão e a qualidade das informações coletadas e armazenadas PII	RQISO26 - ESTABELECER mecanismos de controle para veri car periodicamente a precisão e a qualidade das informações coletadas e armazenadas.
Abertura, transparência e aviso		
Aderir ao princípio de abertura, transparência e noti cação signi ca:	fornecer aos diretores de PII informações claras e facilmente acessíveis sobre as políticas do controlador de PII, procedimentos e práticas com relação ao processamento de PII;	RQISO27 - FORNECER aos titulares de dados informações claras e facilmente acessíveis sobre as políticas do controlador, procedimentos e práticas com relação ao processamento de dados;
	incluir nos avisos o fato de que as PII estão sendo processadas, a nalidade para a qual isso é feito, os tipos de partes interessadas em privacidade a quem as PII podem ser divulgadas e a identidade do controlador de PII, incluindo informações sobre como entrar em contato com o controlador de PII;	RQISO28 - INCLUIR nos avisos o fato de que as informações estão sendo processadas, a nalidade para a qual isso é feito, os tipos de partes interessadas em privacidade a quem as informações podem ser divulgadas e a identidade do controlador, incluindo informações sobre como entrar em contato com o controlador;

Princípio	Trecho	Requisito
	divulgar as opções e os meios oferecidos pelo controlador de PII aos titulares de PII com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações	RQISO29 - DIVULGAR as opções e os meios oferecidos pelo controlador aos titulares de dados com o objetivo de limitar o processamento e acessar, corrigir e remover suas informações
	noti car os diretores de PII quando ocorrerem grandes mudanças nos procedimentos de tratamento de PII	RQISO30 - NOTIFICAR os titulares de dados quando ocorrerem grandes mudanças nos procedimentos de tratamento de dados
Além disso, a nalidade do processamento de PII deve ser su cientemente detalhada para permitir que o PII principal para entender:	as PII especi cadas exigidas para a nalidade especi cada	RQISO31 - PERMITIR que os titulares de dados entendam as especicidades exigidas para a nalidade especi cada
	a nalidade especi cada para a coleta de PII	RQISO32 - PERMITIR que os titulares de dados entendam a nalidade especi cada para a coleta dos dados
	os tipos de pessoas físicas autorizadas que acessarão as IPI e a quem as IPI podem ser transferido;	RQISO33 - PERMITIR que o titular de dados entenda os tipos de pessoas físicas autorizadas que acessarão as informações e a quem essas podem ser transferidas
	os requisitos especi cados de retenção e eliminação de dados PII.	RQISO34 - PERMITIR que o titular de dados entenda os requisitos especi cados de retenção e eliminação de dados.
Participação e acesso individual		

Princípio	Trecho	Requisito
Aderir ao princípio de participação e acesso individual signi ca:	dar aos titulares de PII a capacidade de acessar e revisar suas PII, desde que sua identidade seja autenticada primeiro com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;	RQISO35 - FORNECER aos titulares de dados a capacidade de acessar e revisar suas informações, desde que sua identidade seja autenticada primeiro com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;
	permitir que os diretores de PII contestem a precisão e integridade das PII e as alterem corrigido ou removido conforme apropriado e possível no contexto especí co;	RQISO36 - PERMITIR que os titulares de dados contestem a precisão e integridade das informações e as alterem corrigindo ou removendo conforme apropriado e possível no contexto especí co;
	fornecer qualquer alteração, correção ou remoção para processadores de PII e terceiros a quem os dados foram divulgados, onde são conhecidos	RQISO37 - FORNECER qualquer alteração, correção ou remoção para os processadores de dados e terceiros a quem os dados foram divulgados, onde são conhecidos
	estabelecer procedimentos para permitir que os titulares de PII exerçam esses direitos de forma simples, rápida e e ciente, que não acarrete atrasos ou custos indevidos	RQISO38 - ESTABELECER procedimentos para permitir que os titulares de dados exerçam esses direitos de forma simples, rápida e e ciente, que não acarrete atrasos ou custos indevidos
Responsabilidade O processamento de PII implica um dever de cuidado e a adoção de medidas concretas e práticas para sua proteção. Aderir ao princípio da responsabilidade signi ca:	documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade	RQISO39 - DOCUMENTAR e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade

Princípio	Trecho	Requisito
	atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade;	RQISO40 - ATRIBUIR a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros na organização conforme apropriado) a tarefa de implementar as políticas, procedimentos e práticas relacionadas à privacidade;
	ao transferir PII para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados);	RQISO41 - GARANTIR que ao transferir os dados para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção de privacidade por meio de meios contratuais ou outros, como políticas internas obrigatórias (a lei aplicável pode conter requisitos adicionais em relação às transferências internacionais de dados);
	fornecer treinamento adequado para o pessoal do controlador de PII que terá acesso a PII	RQISO42 - FORNECER treinamento adequado para o pessoal do controlador de dados que terá acesso a informações.
	estabelecimento de procedimentos internos e cientes de tratamento de reclamações e reparação para uso pelos diretores de PII	RQISO43 - ESTABELECER procedimentos internos e cientes de tratamento de reclamações e reparação para uso pelos titulares de dados
	- informar os diretores de PII sobre violações de privacidade que podem causar danos substanciais a eles (a menos que proibido, por exemplo, ao trabalhar com a aplicação da lei), bem como as medidas tomadas para resolução	RQISO44 - INFORMAR aos titulares de dados sobre violações de privacidade que podem causar danos substanciais a eles (a menos que proibido, por exemplo, ao trabalhar com a aplicação da lei), bem como as medidas tomadas para resolução

Princípio	Trecho	Requisito
	noti car todas as partes interessadas de privacidade relevantes sobre violações de privacidade conforme exigido em algumas jurisdições (por exemplo, as autoridades de proteção de dados) e dependendo do nível de risco;	RQISO45 - NOTIFICAR todas as partes interessadas de privacidade relevantes sobre violações de privacidade conforme exigido em algumas jurisdições (por exemplo, as autoridades de proteção de dados) e dependendo do nível de risco;
	permitir que um principal de PII lesado tenha acesso a sanções e/ou recursos apropriados e e cazes, como reti cação, expurgo ou restituição se ocorrer uma violação de privacidade	RQISO46 - PERMITIR que o titular de dados lesado tenha acesso a sanções e/ou recursos apropriados e e cazes, como reti cação, expurgo ou restituição se ocorrer uma violação de privacidade
	ponderar os procedimentos de indemnização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido	RQISO47 - PONDERAR os procedimentos de indenização para as situações em que seja difícil ou impossível repor a privacidade da pessoa singular como se nada tivesse acontecido
Segurança da informação		
Aderir ao princípio de segurança da informação signi ca:	proteger as PII sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, con dencialidade e disponibilidade das PII e protegê-las contra riscos como acesso não autorizado, destruição, uso, modi cação, divulgação ou perda ao longo do todo o seu ciclo de vida	RQISO48 - PROTEGER as informações sob sua autoridade com controles apropriados em nível operacional, funcional e estratégico para garantir a integridade, con dencialidade e disponibilidade das informações e protegê-las contra riscos como acesso não autorizado, destruição, uso, modi cação, divulgação ou perda ao longo do todo o seu ciclo de vida
	escolher processadores de PII que forneçam garantias su cientes em relação aos controles organizacionais, físicos e técnicos para o processamento de PII e garantir o cumprimento desses controles;	RQISO49 - SELECIONAR processadores de dados que forneçam garantias su cientes em relação aos controles organizacionais, físicos e técnicos para o processamento de dados e garantir o cumprimento desses controles;

Princípio	Trecho	Requisito
	basear esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício;	RQISO50 - ASSEGURAR esses controles em requisitos legais aplicáveis, padrões de segurança, resultados de avaliações sistemáticas de risco de segurança conforme descrito na ISO 31000 e os resultados de uma análise de custo/benefício;
	implementação de controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das PII, o número de PII principais que podem ser afetados e o contexto em que são realizadas	RQISO51 - IMPLEMENTAR controles na proporção da probabilidade e gravidade das consequências potenciais, a sensibilidade das informações, o número de titulares que podem ser afetados e o contexto em que são realizadas
	Limitar o acesso a PII aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso	
desses indivíduos apenas às IPI aos quais eles precisam acessar para desempenhar suas funções	RQISO52 - Limitar o acesso a informações aos indivíduos que precisam desse acesso para desempenhar suas funções e limitar o acesso desses indivíduos apenas às informações as quais eles precisam acessar para desempenhar suas funções	
	resolver riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos	RQISO53 - RESOLVER riscos e vulnerabilidades que são descobertos por meio de avaliações de risco de privacidade e auditoria e processos
	submeter os controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo	RQISO54 - SUBMETER os controles a revisão e reavaliação periódicas em um gerenciamento contínuo de riscos de segurança processo
Conformidade de privacidade		

Princípio	Trecho	Requisito
Aderir ao princípio de conformidade com a privacidade signi ca	veri car e demonstrar que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados con áveis	RQISO55 - VERIFICAR e demonstrar que o processamento atende aos requisitos de proteção de dados e proteção de privacidade, realizando auditorias periodicamente usando auditores internos ou auditores terceirizados con áveis
	ter controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade;	RQISO56 - POSSUIR controles internos apropriados e mecanismos de supervisão independentes que assegurem a conformidade com a lei de privacidade relevante e com suas políticas e procedimentos de segurança, proteção de dados e privacidade;
	desenvolver e manter avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de PII estão em conformidade com os requisitos de proteção de dados e privacidade.	RQISO57 - DESENVOLVER e manter avaliações de risco de privacidade para avaliar se as iniciativas de entrega de programas e serviços envolvendo o processamento de dados estão em conformidade com os requisitos de proteção de dados e privacidade.

Tabela 2: Requisitos primários obtidos a partir da ISO/IEC 29100.

I.3 PROCESSO DE SOLICITAÇÃO DE CONSENTIMENTO PARA O COMPARTILHAMENTO DE DADOS DO OPEN BANKING

Banco do Brasil

A seguir serão apresentadas as imagens do processo de solicitação de consentimento do Banco do Brasil conforme Figura 1. As informações foram obtidas a partir do aplicativo mobile do Banco do Brasil, após a autenticação do usuário. As imagens foram obtidas em 06/03/2022.

(a) Página 01 (b) Página 02 (c) Página 03

(d) Página 04 (e) Página 05

Figura 1: Processo de Solicitação de Consentimento do Open Banking no Banco do Brasil