RHODRIGO DEDA GOMES

CONFORMIDADE LEGAL EM PROTEÇÃO DE DADOS NO DESENVOLVIMENTO DE SOFTWARE EM STARTUPS: UMA ABORDAGEM ORIENTADA À TOMADA DE DECISÃO

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

Curitiba
2024

RHODRIGO DEDA GOMES

CONFORMIDADE LEGAL EM PROTEÇÃO DE DADOS NO DESENVOLVIMENTO DE SOFTWARE EM STARTUPS: UMA ABORDAGEM ORIENTADA À TOMADA DE DECISÃO

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

Área de concentração: Ciência da Computação

Orientadora: Profª. Drª. Sheila Reinehr
Coorientadora: Profª. Drª. Andreia Malucelli

Curitiba
2024

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor, com anuência de seu orientador.

Curitiba, dia do mês do ano de xxxx.

Assinatura do Autor

Assinatura do Orientador

FICHA CATALOGRÁFICA

Sobrenome do Autor, Nome do Autor
Título da Dissertação/Tese
/ Iniciais seguidas dos sobrenome. -- Curitiba, ANO.
Número de páginas p.

Tese (Doutorado) – Pontifícia Universidade Católica do Paraná.
Curitiba. Programa de Pós-Graduação em Informática.

1. Palavra-chave01 2. Palavra-chave02 3.
Palavra-chave03. Pontifícia Universidade Católica do Paraná.
Programa de Pós-Graduação em Informática.
II. t ou d.

DEDICATÓRIAS

Dedico esse trabalho a meu afilhado Davi Deda Markiewicz e à sua geração.
Que possamos ser gratos a eles.

AGRADECIMENTOS

É um equívoco tentar nominar todas as pessoas que contribuem para nossa caminhada, mas não ousar agradecer tende a ser um erro maior. A gratidão é daquelas virtudes que nos torna seres humanos melhores. À minha mãe, Marcia Scremim Krueger, e em seu nome cumprimento minha ancestralidade feminina, de um lado, Otília Zimmermann, Alice de Arruda Gomes, Terezinha Scremin Deda, Deolinda Gomes, Cristina Scremim Deda, Delci Gomes e, de outro, Tatiana Aben-Athar, Adriane de Aragon, Irene Visnadi. Ao meu pai, Dejair Gomes, em seu nome cumprimentos minha ancestralidade paterna, meus avós Durvalino Gomes e Luiz Deda, e a meu padrinho Diamir Gomes. Um agradecimento especial a Gabriel Krueger, por provar todos os dias que paternidade é também uma escolha e à Luis Vallim. Meus agradecimentos à Fernanda Marochi Silva, por me apoiar em meio ao frenético ritmo que a vida nos apresenta. Às minhas irmãs Karyn e Yasmin, por entenderem a vida atribulada do irmão e por apoiar as minhas decisões. À Roseana Aben-Athar Kipman, Cassiana Aben-Athar Gomes, Carolina Kaszprzak, e à Ederson Alves, Carlos Luciano Freiria e Newton Froés Jr.

Sinto-me muito feliz de poder agradecer ao Grupo de Pesquisa de Engenharia de Software do PPGIA-PUCPR, em especial aos colegas Adriano Pizzini, Manoel Valerio Silveira Neto, Regina Albuquerque, Regiane Orlovski, Ricardo Bortolo Vieira, Ricardo Theis, Tania Dors, Thober Detofeno, Vinicius Camargo Andrade e Frederick van Amstel.

Agradeço aos membros de minha banca de qualificação, Professora Doutora Cinthia Obladen de Almendra Freitas, Professor Doutor Gleison Santos, Professor Doutor Edson Emilio Scalabrin.

Um especial agradecimento à minha orientadora Professora Doutora Sheila Reinehr e à minha coorientadora Professora Doutora Andreia Malucelli, pelo apoio e pelo período de aprendizado ao longo desses anos.

Baseado em meus estudos, acredito ser melhor contemplar as próprias coisas e falar movido por elas, emitindo palavras adequadas aos fatos, de modo que, para onde quer que levem, o discurso siga esta espontaneidade. (Sêneca)

RESUMO

Estudo recente indica que 84% das empresas brasileiras de diversos portes não estão em conformidade legal com a Lei Geral de Proteção de Dados Pessoais (LGPD). A desconformidade afeta especialmente as *startups* de software, que possuem mais dificuldades em implementar adequação de proteção de dados que as grandes companhias. Empreendedores de s*tartups* têm a necessidade de implementar conformidade legal para evitar multas, que podem inviabilizar a empresa, ou para facilitar a inovação, ou para conquistar credibilidade perante o consumidor. Dado o contexto particular das *startups* de software, há a necessidade de práticas específicas que apoiem a conformidade legal de proteção de dados, mas até o momento inexistem estudos aprofundados sobre o tema ou métodos adequados às suas especificidades. Este estudo investiga as práticas de desenvolvimento de software em *startups*, focando na integração da conformidade com a LGPD. Foram identificados quatorze trabalhos que se aproximam do tema desta pesquisa, mas nenhum deles é adequado para apoiar *startups* nas atividades de desenvolvimento para implementação de conformidade com a LGPD. Utilizando o *Design Science Research Methodology* (DSRM), a tese propõe um método de tomada de decisão que auxilia *startups* a alinhar suas práticas de desenvolvimento com os requisitos da LGPD. Os resultados indicam que o artefato proposto não apenas facilita a tomada de decisão dos empreendedores de *startups* em relação à conformidade com a LGPD, mas também promove uma maior consciência sobre proteção de dados. Este trabalho contribui para a literatura em conformidade legal e engenharia de software, oferecendo um método aplicável ao contexto da LGPD.

Palavras-chaves: *startup*, conformidade legal, LGPD, Lei Geral de Proteção de Dados, engenharia de software, risco em privacidade.

ABSTRACT

A recent study indicates that 84% of Brazilian companies of various sizes are not legally compliant with the General Law of Data Protection (LGPD). Non-compliance primarily affects software startups, which have more difficulty implementing data protection adequacy than large companies. Entrepreneurs in startups need to implement legal compliance to avoid fines, which can render the company unviable, facilitate innovation, or gain credibility with the consumer. Given the particular context of software startups, there is a need for specific practices that support data protection legal compliance. Still, there are no in-depth studies on the topic or methods suited to their specificities to the best of our knowledge. This research investigates software development practices in startups, focusing on the integration of LGPD compliance. Fourteen works were identified that are close to the topic of this research. Still, none are suitable for supporting startups in development activities to implement compliance with the LGPD. Using the Design Science Research Methodology (DSRM), the thesis proposes a decision-making method that helps startups align their development practices with LGPD requirements. The results indicate that the proposed artifact facilitates startup entrepreneurs' decision-making regarding compliance with the LGPD and promotes greater awareness about data protection. This work contributes to legal compliance and software engineering literature, offering a method applicable to the LGPD context.

Keywords: startups, legal compliance, LGPD, General Data Protection Law, software engineering, privacy risk.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE EQUAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
DSRM	*Design Science Research Methodology*
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
SWEBOK	Software Engineering Body of Knowledge
TAM	Technology Acceptance Model
LINDDUN	Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, Non-compliance
CEP	Comitê de Ética e Pesquisa
TCLE	Termo de Consentimento Livre e Esclarecido

CAPÍTULO 1 - INTRODUÇÃO

A preocupação com a proteção dos direitos dos cidadãos tem suas origens na década de 1970, quando os Estados Unidos da América passaram a estabelecer regulamentos de privacidade de dados, com a edição de diversos atos normativos a partir de 1973, entre eles o *US Privacy Act* aprovado em 1974 (TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018). Mais recentemente, em 1995, a União Europeia adotou a Diretiva 95/46CE, que foi substituída pelo *General Data Protection Regulation* (GDPR)[1] aprovado em 2016 e em vigor desde maio de 2018.

O movimento regulatório da União Europeia foi fator de motivação para que a Lei nº 13.709 de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), fosse sancionada em agosto de 2018, com o Brasil se tornando a 128ª nação a ter uma normativa dessa natureza (MULHOLLAND e FRAJHOF, 2020). O motivador teve natureza econômica, uma vez que o novo modelo europeu de proteção de dados trouxe uma série de impactos nas atividades de empresas que queiram fazer negócios com a União Europeia (SOUZA; MAGRANI; CARNEIRO, 2020).

Os objetivos da União Europeia ao estabelecer o regulamento, conforme apresentado nos Considerados 2 e 6 do GDPR, foram, entre outros, os de contribuir para a convergência de economias de mercado e bem-estar das pessoas, dado que as novas tecnologias vêm transformando a economia e a vida em sociedade, razão pela qual as organizações devem contribuir para um elevado nível de proteção aos dados pessoais (UNIÃO EUROPEIA, 2016). De forma semelhante à motivação do GDPR expressa em seus considerandos, a lei brasileira traz a preocupação com a proteção de dados pessoais dos indivíduos, de um lado, e, de outro, com o exercício e o incremento das atividades econômicas (SAAD e HIUNES, 2020).

Há, assim, uma busca das autoridades estatais em proteger os titulares de dados, com a finalidade de estabelecer regras transparentes para o tratamento de dados pessoais, bem como ter formas de mitigar riscos de violação dos direitos

[1] Embora se tenha traduzido o termo para Regulamento Geral de Proteção de Dados (RGPD) em Portugal, o termo usado no Brasil é GDPR.

fundamentais dos cidadãos (VAINZOF, 2019). Essas normas mais recentes trazem também uma abordagem fundada no risco de violação de direitos fundamentais do indivíduo, em instrumentos técnicos e organizacionais que focam na demonstração do cumprimento de parâmetros legais e na responsabilidade dos agentes de tratamento (DONEDA, 2021).

O GDPR e a LGPD possuem racionalidades regulatórias convergentes, reflexo de um consenso transnacional a respeito de princípios básicos que regulam a temática da proteção de dados pessoais (BIONI e MENDES, 2019). Ambas as normas preveem uma série de sanções contra pessoas naturais ou pessoas jurídicas que violarem seus dispositivos, o que inclui multas severas. No Brasil, as sanções podem chegar a dois por cento do faturamento ou até R$ 50 milhões, conforme o artigo 52, II, da LGPD, podendo ser aplicadas de forma administrativa pela Autoridade Nacional de Proteção de Dados (ANPD) a todos os agentes de tratamento, quando comprovada a violação da lei.

A conformidade legal de proteção de dados, portanto, é uma necessidade que as empresas de qualquer magnitude precisam atender, para evitar que sofram com sanções em suas atividades. Porém, o cenário brasileiro é de ampla desconformidade com a LGPD. Relatório da empresa de consultoria ICTS Protiviti, divulgado no site LGPD Brasil[2] em maio de 2021, mostra que 84% de 508 empresas de diversos portes e segmentos pesquisadas não se encontram em conformidade com a lei brasileira.

Empresas de software estão no coração da LGPD, uma vez que é por meio de recursos computacionais que os dados são processados e armazenados nos mais diferentes tipos de sistemas, demandando que elas busquem adequação às normas de proteção de dados. A conformidade tem impacto nesse setor, por conta da obrigação de que os dispositivos legais de privacidade devem ser respeitados desde a concepção do projeto, nos termos do Artigo 46, §2º da LGPD (BRASIL, 2018).

No contexto da engenharia de software, em síntese, o GDPR e as leis de proteção de dados têm entre seus objetivos: (i) proteger indivíduos de ameaças como violações de dados por conta de ações de *hackers* ou de pessoas da própria organização que atuam como agentes de tratamento; e (ii) assegurar que os dados estão tratados em conformidade com os critérios estabelecidos por essas normas (MARTIN *et al.*, 2019). Para ser implementada, a conformidade legal de proteção de

[2] Site: https://www.lgpdbrasil.com.br/84-das-empresas-brasileiras-nao-estao-preparadas-para-a-lgpd/.

dados deve ser considerada na tomada de decisão desde o início do projeto de software. O GDPR traz no Artigo 25º previsão expressa que a proteção de dados tem de ser realizada desde a concepção e por padrão (UNIÃO EUROPEIA, 2016). De forma semelhante, a LGPD estabelece no Artigo 46, §2º, que as medidas de segurança de dados pessoais devem ser observadas desde a concepção do produto ou serviço (BRASIL, 2018).

Um dos obstáculos para a implementação da LGPD, em especial para empresas de pequeno porte, pode ser o custo. Estimativas apontavam que em 2020 projetos básicos de conformidade de LGPD, tanto jurídicos quanto de Tecnologia da Informação, poderiam variar entre R$ 25 mil e R$ 3 milhões, dependendo do porte e da complexidade das atividades das empresas[3].

Se para as grandes empresas já é um desafio, o processo de adequação legal de proteção de dados pode ser ainda mais desafiador para *startups* de software, que têm agora sobre si o custoso encargo da adequação legal de proteção de dados, que retira recursos de outras atividades produtivas, como o desenvolvimento de inovação, e gera barreiras de entrada em mercados, dificultando a concorrência (MARTIN *et al.*, 2019). Apesar de a implementação ser onerosa, entretanto, *startups* de software consideram que é necessário implementá-la, a fim de evitar multas que podem até mesmo inviabilizar o negócio (NORVAL *et al.*, 2021, MARTIN *et al.*, 2019).

Pesquisadores consideram o contexto das *startups* de software diferente dos demais tipos de companhias existentes. *Startups* de software podem ser compreendidas como equipes que desenvolvem um novo produto inovador, intensivo em software e orientado ao mercado (MELEGATI *et al.*, 2020), em um contexto de falta de recursos, alta reatividade ao ambiente, incerteza, pressão do tempo, equipe pequena, alto risco, entre outras características (GIARDINO *et al.*, 2014, PATERNOSTER *et al.*, 2014, UNTERKALMSTEINER *et al.*, 2016, MELEGATI *et al.* 2020). Podem ser consideradas também, empresas inovadoras com potencial de criar produtos que escalam rapidamente no mercado (TRIPATHI *et al.*, 2018). As *startups* de software, portanto, podem se beneficiar de abordagens de engenharia que levem em conta suas características singulares.

[3] Sato, L; Braguim, G. A Hora e a vez de aprovar o orçamento para adequação à lei geral de proteção de dados. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/313566/a-hora-e-a-vez-de-aprovar-o-orcamento-para-a-adequacao-a-lei-geral-de-protecao-de-dados

Estudos mostram que *startups* de software possuem desvantagens para atingir a conformidade de proteção de dados, quando comparadas com empresas maiores e já estabelecidas no mercado (BLEIER *et al.*, 2020). Além disso, há o desafio de elas desconhecerem como a conformidade legal em proteção de dados pode ser alcançada (NORVAL *et al.*, 2021).

Existem algumas abordagens ou métodos para lidar com a conformidade legal de proteção de dados no âmbito do GDPR, entre eles, encontrando-se os trabalhos de pesquisadores como Piras *et al.* (2019), Li *et al.* (2020), Johansen e Fischer-Hübner (2020) e Fähnrich e Kubach (2019), Matulevicius *et al.* (2020) e Tsohou *et al.* (2020). Esses trabalhos estão descritos na seção 2.3.4.

No âmbito das normas técnicas, o tema da Segurança de Informação, um dos aspectos de conformidade legal, vem sendo orientado pela ISO/IEC 27001:2022, que traz recomendações para a implementação de um Sistema de Gestão de Segurança da Informação; pela ISO/IEC 27002:2022, que apresenta um código de prática para controles de segurança da informação; pela ISO/IEC 27005:2022, que traz uma abordagem para gestão de risco de segurança da informação; e pela ISO/IEC 27701:2019, que propõe recomendações específicas sobre dados pessoais e estabelece diretrizes para um sistema de gerenciamento de privacidade.

Contudo, as abordagens existentes não conseguem apoiar as *startups* de software de forma adequada ao contexto em que operam. Dada a escassez de recursos materiais e humanos e por conta de estarem em busca de criar inovações orientadas ao mercado, que exige intensivo desenvolvimento de software (MELEGATI *et al.*, 2020), as *startups* de software concentram seus esforços em desenvolver o produto. Isso leva ao fato de que uma abordagem de conformidade legal de proteção de dados precisa levar em conta suas particularidades, que as diferenciam das demais empresas, como falta de recursos, alta reatividade ao ambiente, incerteza, pressão do tempo, equipe pequena e alto risco.

Esta pesquisa trata da dificuldade que *startups* possuem em desenvolver softwares em conformidade com a LGPD. *Startups* iniciam suas atividades de software sem se fundamentar em um corpo científico de conhecimento (PATERNOSTER *et al.*, 2014) e sem estabelecer práticas de engenharia de software padronizadas de forma consistente (TRIPATHI *et al.*, 2018).

O contexto de desenvolvimento de software das *startups*, segundo Coleman e O´Connor (2008), é único, o que dificulta o uso de metodologias prescritivas. Por essa

razão, há a necessidade de pesquisas que apoiem a atividade de engenharia de *startups* e que permitam contribuir para o processo de tomada de decisão, evitando escolhas que inviabilizem a criação de novos negócios (PATERNOSTER *et al.*, 2014).

Além disso, há evidências de que *startups* não sabem como realizar conformidade legal em proteção de dados nas atividades de engenharia de software (NORVAL *et al.*, 2021, Bleier et al., 2020). Entretanto, consideram-na necessária (NORVAL *et al.*, 2021) porque: (i) é preciso evitar multas (NORVAL *et al.*, 2021, MARTIN *et al.*, 2019); (ii) há o desejo de facilitar a inovação e conquistar a confiança do consumidor (BACHLECHNER; LIESHOUT; TIMAN, 2019).

Ao mesmo tempo que entendem ser relevante desenvolver softwares em adequação às normas de proteção de dados, as *startups* reconhecem que isso traz custos e absorve recursos que poderiam ser utilizados em outras atividades (BACHLECHNER; LIESHOUT; TIMAN, 2019, MARTIN *et al.*, 2019). Acrescente-se a esse contexto o estudo de Bleier, Goldfarb e Tucker (2020), que indica que *startups* estão em desvantagem para adotar conformidade legal no desenvolvimento de software, quando comparadas com grandes empresas já estabelecidas no mercado (BLEIER; GOLDFARB; TUCKER, 2020).

Não há atualmente abordagem ou método específico para tratar de adequação legal de dados abrangendo todos os aspectos de conformidade para o contexto de *startups*. Segundo Li *et al.* (2020), embora existam estudos que abordem implicações gerais de GDPR, há uma ausência de estudos aprofundados das práticas de conformidade e desafios em organizações de software, em geral, e de pequenas e médias empresas, em particular.

Existem algumas abordagens ou métodos para lidar com a conformidade legal de proteção de dados, contudo, nenhum deles leva em conta a complexidade do contexto das *startups* ou trata dos aspectos de adequação em sua integralidade. Além disso, a maioria carece de validação na indústria e apenas alguns deles, levam em conta avaliação de risco de violação de conformidade legal ou a visão dos *stakeholders* para tomada de decisão. A ausência de soluções testadas em contextos reais foi identificada em revisão sistemática de literatura de Ferreira (2020), que constatou, também, a falta de soluções adequadas para apoiar empresas na melhoria de conformidade com o GDPR.

Além da ausência de estudos sobre abordagens de conformidade adequadas ao contexto das *startups*, destaque-se, também, a falta de estudos aprofundados na

investigação de práticas de conformidades em pequenas e médias empresas (Li *et al.*, 2020). No mesmo sentido, segundo Bleier, Goldfarb e Tucker (2020), pouco se conhece sobre como questões envolvendo privacidade e regulamentações têm afetado novas empresas, quando comparadas com empresas estabelecidas.

No âmbito dos estudos de *startups*, Melegati *et al.* (2020) afirmam que as pesquisas ainda não estão maduras para lidar com problemas no contexto de empresas nascentes, que envolve inovação e direcionamento ao mercado, necessitando de aprofundamento.

Ao conseguir integrar conformidade legal de proteção de dados nas atividades de desenvolvimento de software, *startups* podem evitar sanções administrativas ou judiciais, bem como estabelecer uma boa imagem junto aos seus clientes, algo que, como já observado, são objetivos desejados (MARTIN e*t al.*, 2019, BACHLECHNER; LIESHOUT; TIMAN, 2019, NORVAL *et al.*, 2021). Podem, ainda, reduzir, gerenciar ao longo do tempo ou, mesmo, evitar, dívida técnica de segurança (RINDELL; HOLVITIE, 2019), que pode representar uma ameaça à conformidade com a LGPD.

Em síntese, o problema identificado é que *startups* possuem dificuldades em realizar conformidade legal de proteção de dados, os custos tendem a retirar recursos de atividades importantes para o negócio – como a inovação –, e a não adequação pode implicar em perda de credibilidade e sanções, como multas, que podem inviabilizar a existência dessas empresas.

Startups de software se beneficiariam de um método que as permitissem tomar decisões de engenharia levando em conta o risco de desconformidade legal com a LGPD e apresentassem um sistema de recomendação de ações a partir do risco identificado.

Do problema identificado, apresenta-se, portanto, a seguinte questão de pesquisa: **Como apoiar a tomada de decisão no processo de desenvolvimento de software sobre a conformidade com a LGPD em *startups*?**

1.1 Objetivos

1.1.1 Objetivo geral

O objetivo geral deste projeto de pesquisa é: **Propor um método de tomada de decisão apoiado em um conjunto de recomendações para *startups*, na**

implementação da conformidade com a LGPD durante o processo de desenvolvimento de software.

1.1.2 Objetivos específicos

São os objetivos específicos:

a) Investigar como *startups* lidam com atividades de proteção de dados pessoais ao longo do desenvolvimento de software.
b) Desenvolver um método de tomada de decisão e um conjunto de recomendações que apoiem *startups* na conformidade com a LGPD nas práticas de desenvolvimento de software.
c) Avaliar a abordagem proposta.

1.2 Delimitação de escopo

A pesquisa trata de conformidade legal no âmbito brasileiro, com fundamento na Lei nº. 13.709, mais conhecida como Lei Geral de Proteção de Dados. Embora seja reconhecido que a LGPD tem influência do GDPR da União Europeia e sejam marcos regulatórios convergentes, e que as pesquisas relativas ao tema de conformidade em proteção de dados sejam geralmente sobre o regulamento europeu, este trabalho insere-se no contexto da norma brasileira.

A proposta de abordagem para a tomada de decisão sobre a conformidade legal de proteção de dados no desenvolvimento de software trata apenas do contexto de desenvolvimento de software das *startups*, não se estendendo para micro, pequenas e médias empresas, tampouco para grandes organizações, embora não haja impeditivo para sua utilização nesses outros contextos.

A abordagem proposta foi avaliada com tomadores de decisão que integram equipes de *startups* em estágios iniciais de maturidade ou que estão em fase de crescimento, tendo como base as etapas do ciclo de vida nos termos estabelecidos por Crowne (2002). Ao final da avaliação, a abordagem foi validada, possibilitando seu uso por tomadores de decisão de *startups* e apoiando suas decisões no desenvolvimento do produto levando em conta a conformidade legal de proteção de dados.

1.3 Estrutura do documento da tese

O Capítulo 1 apresenta o contexto no qual está inserida a pesquisa, a motivação do trabalho e sua relevância para a comunidade científica e profissional no que tange à conformidade legal de proteção de dados em engenharia de software no contexto de *startups*.

O Capítulo 2 aprofunda o referencial teórico que inicialmente foi descrito no Capítulo 1, concentrando a atenção especialmente no contexto das startups e suas práticas de engenharia de software, na LGPD e suas relações com o desenvolvimento de software, bem como apresenta as pesquisas de conformidade legal de proteção de dados e os estudos relacionados ao tema deste trabalho.

O Capítulo 3 traz a estrutura da pesquisa, descrevendo-se a natureza da pesquisa e a estratégia que foi seguida para realizá-la.

O Capítulo 4 abrange o projeto e o desenvolvimento, demonstrando a construção do artefato, composto pelo método, tutorial, bem como resultado de avaliação de risco e recomendações.

O Capítulo 5 apresenta os dois ciclos de demonstração e avaliação, bem como traz a análise dos resultados da avaliação do artefato.

O Capítulo 6, por fim, abrange as conclusões do estudo, sua relevância, limitações e ameaças à validade, bem como contribuições de pesquisa e estudos futuros.

1.4 Considerações sobre o capítulo

Este capítulo introdutório apresentou a importância da conformidade legal em proteção de dados pessoais no mundo hoje, trazendo um breve relato da evolução do tema até o GDPR e a LGPD, esta última tema central deste trabalho.

A conformidade legal de proteção de dados imposta pela LGPD é um desafio para todas as empresas, em especial para *startups*, por conta não só das dificuldades intrínsecas ao contexto das empresas nascentes, mas também pela quantidade de prescrições trazidas pela norma. Muito além de um desafio, é, também, uma necessidade reconhecida pelas *startups*, seja por conta da possibilidade de penalizações mediante vultuosas multas que podem inviabilizar suas atividades, seja porque as empresas nascentes reconhecem na conformidade uma forma de obter credibilidade e atrair clientes.

Diante desse cenário, este capítulo apresenta a motivação e a lacuna existente na pesquisa de conformidade legal de proteção de dados na engenharia de software em um contexto de *startups*, bem como traz os objetivos, delimita o escopo, o problema de pesquisa e a estrutura do documento.

CAPÍTULO 2 - REVISÃO DE LITERATURA

A revisão de literatura é dividida em 03 (três) subseções. Primeiro apresenta-se o tema relativo às *startups* de software e seu contexto. Em seguida, é abordada a LGPD e suas relações com a engenharia de software. Por fim, aborda-se o tema da conformidade legal de proteção de dados em suas diferentes dimensões.

2.1 Startups de software

Nesta seção apresenta-se, primeiramente, a definição e o conceito de *startup* de software. Em seguida, abordam-se as práticas de engenharia de software ao longo do ciclo de vida das empresas nascentes e as revisões sistemáticas de literatura sobre o contexto das *startups* no âmbito da engenharia de software. Por fim, são feitas considerações sobre o tópico.

2.1.1 Definição e contexto

No âmbito do empreendedorismo, *startups* são entendidas como organizações temporárias que buscam um modelo de negócio que seja viável, escalável, recorrente e lucrativo (BLANK; DORF, 2014). No início da jornada, segundo Blank e Dorf (2014), o empreendedor procura testar hipóteses, de forma iterativa, com o objetivo de entender o mercado em que quer atuar e prospectar clientes. Ries (2012) considera *startup* como uma organização humana projetada para criar um produto ou serviço em condições de extrema incerteza.

No campo da engenharia de software, o termo *startup* de software foi empregado em 1994 por Carmel (1994), em estudo sobre empresas jovens de software que denominou de *startups* e em que afirmava que a equipe era um ativo importante delas. Wang (2019) afirma, entretanto, que o termo havia sido usado pela revista Forbes 1976 e pela *Business Week* em 1977, em ambos os casos no contexto de dados eletrônicos, alta tecnologia e rápido crescimento. Por essa razão, diz ele, *startups* de software são tão antigas quanto as demais *startups* (WANG, 2019).

Sutton (2000) caracteriza *startups* de software como empresas que possuem pouco ou nenhum histórico operacional, recursos limitados, influenciadas por múltiplos

atores, que desenvolvem tecnologias inovadoras, empregando técnicas de desenvolvimento de ponta, e atuam em mercados dinâmicos. Isso as diferencia das empresas estabelecidas, que possuiriam menos problemas de comunicação e coordenação, de base de produtos, de parceiros e de clientes estabelecidos, além de terem menor histórico e visão compartilhadas por seus membros (SUTTON, 2000).

Hilmola, Helo e Ojala (2003) sugerem que *startups* de software em sua maioria buscam desenvolver produtos de alta tecnologia. Coleman e O´Connor (2008) afirmam que *startups* de software desenvolvem software sem uso de metodologias prescritivas.

Estudo de Suominen *et al.* (2017) com 20 mil empresas finlandesas fundadas entre 2010 e 2013 mostra que há diferenças estatísticas significativas entre *startups* de software em relação às demais *startups*. De acordo com eles, *startups* de software têm desempenho médio melhor no que se refere a retorno de ativos, margem de lucro e índice de liquidez, enquanto outras *startups* possuem melhor desempenho em receita. Para Suominen *et al.* (2017), isso permite concluir que *startups* de software se diferenciam das demais.

Wang (2019), de outro lado, afirma que, como o software é atualmente onipresente no mundo dos negócios, existe uma linha tênue separando *startups* de software daquelas que atuam em outros ramos. Porém, Wang (2019) considera que o software acaba por desempenhar diferentes papéis em *startups* – desde facilitar processos de criação de entrega de valor a estar ligado profundamente ao núcleo de criação de valor de uma empresa iniciante –, de modo que a capacidade de inovação pode ser derivada de diferentes partes do modelo de negócio, podendo inclusive gerar inovações disruptivas, mas não sendo esta uma característica definidora da *startup* de software.

Giardino *et al.* (2014) consideram *startup* uma pequena empresa que busca novas oportunidades de fazer negócio e concentra suas atividades no enfrentamento de problemas em mercado altamente volátil, cuja solução não é bem conhecida. Na visão desses autores, portanto, não basta a empresa ser recém-criada, é necessário, ainda, que haja elementos de elevada incerteza e rápida evolução da companhia. Em outro estudo, Giardino, Wang e Abrahamsson (2014) apontam que *startups* podem falhar ao estabelecer estratégias de gestão inconsistentes com a execução de suas atividades.

Em mapeamento sistemático, Paternoster *et al.* (2014) identificaram temas que aparecem no contexto dos estudos sobre engenharia de software em *startups*, conforme apresentado na Tabela 2-1. Eles constataram também que não há uma definição padrão para *startup*, de modo que diversos autores trazem diferentes abordagens, o que torna desafiadora a tentativa de identificar um corpo sólido de conhecimento. A partir do estudo realizado, eles definem *startups* de software como empresas recém-criadas, orientadas a desenvolver produtos inovadores de alta tecnologia, a fim de expandir negócios em mercados de alta escalabilidade. Segundo os autores, *startups* de software enfrentam pressão do mercado e da concorrência, operando em um contexto que evolui muito rápido, de forma caótica e incerta, razão pela qual para sua sobrevivência é crucial que consigam se adaptar rapidamente às novas demandas do ambiente (PATERNOSTER *et al.*, 2014).

Tabela 2-1. Temas em *startups*.
(Adaptado de PATERNOSTER *ET AL.*, 2014)

TEMA	DESCRIÇÃO	FREQUÊNCIA
Falta de recursos	Recursos físicos, humanos e econômicos extremamente limitados	18
Alta reatividade	São rápidas em reagir às mudanças	17
Inovação	Como o ecossistema é altamente competitivo, necessitam de foco em segmentos altamente inovadores de mercado	15
Incerteza	Lidam com ecossistema altamente incerto no que tange ao mercado, características do produto, competição, pessoas e finanças	14
Rápido desenvolvimento	Quando bem-sucedidas, focam em crescer e escalar rapidamente	14
Pressão do tempo	O ambiente frequentemente força a lançar rápido e a trabalhar sob constante pressão	13
Dependência de uma terceira parte	Devido à falta de recursos para construir o produto, contam muito com soluções externas: APIs externas, software de código aberto, terceirização, entre outras	10
Equipe pequena	Começam com um reduzido número de indivíduos	9
Produto único	As atividades da companhia gravitam em torno de um único produto ou serviço	9
Baixa experiência da equipe	Uma parte considerável da equipe de desenvolvimento tem menos de cinco anos de experiência	8
Nova companhia	Foram criadas recentemente	7

Organização plana	São centradas na figura dos fundadores, com pessoas acumulando responsabilidades, e não necessitam de alto gerenciamento	5
Alto risco	A taxa de falha é extremamente alta	5
Não autossustentável	Especialmente nos estágios iniciais, necessitam de investimentos externos para custear suas atividades	3
Pouco histórico de funcionamento	A base da cultura organizacional não está presente inicialmente	3

Unterkalmsteiner *et al.* (2016) afirmam que *startups* são, por natureza, empreendimentos desafiadores, por serem empresas iniciantes que desenvolvem tecnologia de ponta e operam em mercados de elevada incerteza, tendo como principais desafios: (i) falta recursos; (ii) serem formadas por equipes com pouca experiência; (iii) dependerem de um único produto; (iv) operarem em condições de incerteza; (v) buscarem evoluir rapidamente; (vi) sofrerem pressão do tempo; (vii) dependerem de terceiros para sustentar o negócio; (viii) desenvolverem negócio de alto risco.

Giardino *et al.* (2015), de outro lado, definem *startups* como companhias recém-criadas que desejam crescer rapidamente em extrema incerteza e classificam os principais desafios de empresas iniciantes em quatro dimensões – de produto, finanças, mercado e equipe. Na visão deles, prosperar em ambiente de incerteza tecnológica e obter um primeiro cliente pagante são os desafios comuns de *startups*.

Atualmente, entretanto, há divergências sobre definição de *startup* de software, com um estudo que questiona as tentativas de se apresentar contextos, características ou uma definição. Em um contraponto a Paternoster *et al.* (2014), Klotins (2018) coloca em dúvida se há diferenças entre as características que são geralmente atribuídas para distinguir *startups* de organizações estabelecidas. Inconsistências na caracterização de *startups* por diversos autores foram também identificadas por Berg et al. (2018) em revisão sistemática de literatura.

Berg *et al.* (2018) usaram os mesmos conceitos-tema de Paternoster *et al.* (2014) para classificar a frequência deles em dois períodos – de 2013 a 2017 e de 1994-2013. Como se observa na Tabela 2-2, os temas relativos a *startups* mais mencionados foram mudando ao longo do tempo, inexistindo conceito único nos 22 artigos pesquisados no período de 2013 a 2017. Entre 1994 e 2013, os temas emergentes que apareciam com maior frequência relativos a startups eram inovação,

falta de recursos e alta reatividade, enquanto entre 2013 e 2017, os temas mais frequentes foram inovação, incerteza e equipe pequena.

Tabela 2-2. Temas em *startups* – 1994-2013 e 2013-2017 (BERGER *et al.*, 2018).

TEMA	FREQUÊNCIA 2013-2017	FREQUÊNCIA 1994-2013
Inovação	15	19
Incerteza	14	15
Equipe pequena	11	12
Falta de recursos	9	21
Pouco histórico de funcionamento	9	3
Pressão do tempo	7	17
Rápido desenvolvimento	5	16
Nova companhia	5	8
Alta reatividade	3	19
Alto risco	3	8
Dependência de uma terceira parte	2	12
Produto único	2	9
Não autossustentável	1	3
Baixa experiência da equipe	0	9
Organização plana	0	5

Em estudo de 2017, Klotins (2017) conceituou *startup* de software como pequenas organizações criadas com o objetivo de desenvolver produto ou serviço inovador, e apoiou-se em Sutton (2000) para diferenciá-las de pequenas e médias empresas, com base nos desafios que enfrentam e pelo contexto em que se inserem, de incerteza, falta de recursos, de evolução rápida, equipe imatura e pressão de tempo.

Em estudo de 2018, contudo, Klotins (2018) muda seu posicionamento e afirma que a maioria das características que autores como Paternoster *et al.* (2014) atribuem a *startups* tem pouco apoio empírico, enquanto outras são encontradas em organizações maiores, de tal modo que termos que caracterizam *startups* de software, bem como sua definição no contexto da engenharia de software necessitam de revisão. Para Klotins (2018), a maioria das pesquisas existentes parte da suposição de que *startups* de software são únicas e requerem abordagem especial de engenharia de software, o que seria justificado pela escassez de recursos das empresas iniciantes, bem como a pressão de tempo, pouco histórico operacional e foco em inovação (Klotins, 2018). Isso conduziu, segundo Klotins (2018), as pesquisas a explorarem o âmbito das *startups* de software negligenciando o potencial existente na transferência das melhores práticas de engenharia já implementadas em outros contextos.

Klotins (2018) afirma que desse fato decorre a questão se as *startups* são especiais e se devem usar práticas de engenharia diferente de pequenas e médias companhias, ou de outro tipo de organizações. Klotins (2018) defende que a rápida evolução de *startups* e os objetivos conflitantes das partes interessadas no sucesso do modelo de negócio podem estar resultando em complexidade adicional à engenharia de software, de modo que isso sugere que empresas nascentes deveriam buscar ser mais estruturadas para seguir as melhores práticas de engenharia de software de forma mais incisiva que outras formas de organizações.

Klotins (2018) afirma ainda que essa descoberta tem implicações em três direções potenciais referentes à *startups* de software. A primeira delas trata de questões referentes à rápida evolução de empresas *startups* – uma organização de poucas pessoas, que cresce para várias equipes trabalhando juntas em um curto espaço de tempo, o que conduz à evolução das práticas de comunicação e coordenação. Segundo Klotins (2018), práticas que são adequadas para poucos engenheiros de software, um número reduzido de clientes e um produto simples, não vão ter sucesso com equipes maiores, milhares de clientes e produto complexo, que podem requerer práticas orientadas a ambientes dinâmicos, como as práticas ágeis. Por essa razão, afirma ele, avaliar a necessidade, a seleção e a adoção de novas práticas torna-se um grande desafio (Klotins, 2018).

A segunda, trata das margens de erro menores que as *startups* têm, por conta de seu tamanho pequeno e da dependência de patrocinadores externos, diferentemente de organizações maiores, que podem compensar ineficiências com a realocação ou, mesmo, a introdução, de mais recursos. Os erros das empresas nascentes, avalia Klotins (2018), podem ser referentes às decisões de construção do produto, como quais recursos e qual nível de qualidade criar, bem como podem ser erros de decisões de processo, ao tratar de forma equivocada como empregar os recursos de modo eficiente. Empresas iniciantes possuem recursos escassos e a falta de uma rápida entrega de valor ao cliente pode significar a falência da companhia, razão pela qual há, para Klotins (2018), a necessidade de métodos de engenharia de software comprovados, bem como de melhoria contínua, de controle sobre o uso de recursos e melhor gerenciamento de riscos.

Por fim, a terceira trata do desalinhamento das partes interessadas, que, segundo Klotins (2018), pode ocorrer quando os patrocinadores e a equipe da *startup* possuem objetivos diferentes, como quando o interesse de investidores é maximizar

o retorno do capital investido e os integrantes da empresa é o de ser pioneira na criação de uma tecnologia. Isso traz aos engenheiros de software a necessidade de mediação e equilíbrio de interesses das diferentes partes interessadas como investidores, integrantes da *startup* e clientes (Klotins, 2018).

Em síntese, na visão de Klotins (2018), haveria não só potencial para revisão da definição de *startup* de software como abriria oportunidade de pesquisa que considere a perspectiva de acionistas na decisão sobre o produto, o fornecimento de apoio para engenharia de software em organizações de rápido crescimento, assim como a possibilidade de transferência de melhores práticas de engenharia de contextos já consolidados para o ambiente das *startups*.

Em contraposição a Klotins, Melegati *et al.* (2020) posicionam-se que *startups* se diferenciam das demais organizações, por entenderem que inovação e direcionamento ao mercado são elementos suficientes para caracterizá-las. Embora por si só esses dois elementos permitam caracterizar *startups*, Melegati *et al.* (2020) afirmam que foram fatores levemente abordados nos estudos de engenharia de software, necessitando de mais pesquisas para explorar novos caminhos com profundidade.

Melegati *et al.* (2020) defendem que uma *startup* de software pode ser definida como uma equipe que desenvolve um produto inovador, com uso intensivo de software e orientada ao mercado. Segundo eles, incerteza, pressão de tempo e necessidade de ser altamente reativa na busca de encontrar um mercado para o produto são características do contexto de *startups*, que requerem uma forma particular de lidar com a ideia que está sendo desenvolvida, de modo a diferenciá-las de outras organizações (MELEGATI *et al.*, 2020). Por essa razão, afirmam os autores, *startups* de software podem se beneficiar de práticas feitas sob medida para um processo inovador (MELEGATI *et al.*, 2020).

No mesmo sentido de Melegati *et al.* (2020), em estudo que investiga táticas de empreendedores que orientam atividades de engenharia de software, Nguyen-Duc, Kemell, Abrahamsson (2021) concluem que as abordagens de desenvolvimento existentes são limitadas no contexto das *startups*. Além de poderem ser consideradas diferentes de outras organizações, alguns pesquisadores identificam, ainda, que empreendedores de *startups* tomam decisões de forma diferente de empresas estabelecidas por lidarem com fenômenos relativamente imprevisíveis

(SARASVATHY, 2001, YRJÖNKOSKI; SUOMINEN, 2018, NGUYEN-DUC; KEMELL; ABRAHAMSSON, 2021).

Em estudo recente, Gandomani et al. (2024) afirmam que *startups* tendem a se concentrar no desenvolvimento do produto mínimo viável, o que torna desafiador o uso de métodos ágeis e exige uma adaptação personalizada dessas práticas. Segundo os pesquisadores, além do foco no desenvolvimento do produto mínimo viável, *startups* têm como características times pequenos e flexíveis, buscam induzir mudanças de forma eficaz, concentram-se na proposta de valor do negócio e focam na comunicação efetiva.

Em pesquisa realizada com 23 especialistas de 7 equipes de *startups*, Gandomani et al. (2024) desenvolveram orientações para o desenvolvimento de software ágil em empresas nascentes, entre elas, a ênfase na construção de cultura ágil e na adaptação de práticas conforme as capacidades e limitações da empresa.

Neste estudo posiciona-se em sentido semelhante à posição de Melegati *et al.* (2020), Giardino *et al.* (2014) e outros pesquisadores que consideram o contexto das *startups* diferente de outras organizações, por conta da incerteza, da pressão de tempo e da necessidade alta reatividade na procura por um mercado para o produto.

2.1.2 Práticas de engenharia de software ao longo do ciclo de vida da *startup*

Crowne (2002) apresenta o ciclo de vida em quatro fases para empresas nascentes de software: *startup*, estabilização, crescimento e maturidade. A primeira fase começa na concepção inicial e vai até o primeiro lançamento do produto. A segunda, estabilização, inicia no primeiro lançamento e termina quando a empresa obtém a estabilidade do produto para poder escalar. Na terceira fase, o foco é aquisição de novos clientes e conquistar participação de mercado. E, por fim, na quarta, a *startup* se torna uma empresa estabelecida.

De acordo com Crowne (2002), essa classificação permite identificar problemas característicos de engenharia de software de cada fase da *startup*. Klotins, Unterkalmsteiner e Gorschek (2017) consideram que a classificação de Crowne possibilita compreender também a mudança nos objetivos das *startups* ao longo de sua evolução. Segundo Klotins, Unterkalmsteiner e Gorschek (2017) nos estágios iniciais busca-se encontrar um problema relevante e criar uma solução viável, enquanto mais adiante o foco muda para questões de marketing e de melhoria de eficiência das operações e no estágio de maturidade os desafios estão mais ligados

ao gerenciamento de grandes equipes. Em caso de pivotagem em algum momento de sua trajetória, a *startup* pode ter que voltar a um estágio anterior no modelo de ciclo de vida (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2017).

Ao tratar de *startups* em seu estágio inicial, Besker *et al.* (2018) afirmam que, nas primeiras versões do software, as empresas nascentes testam e validam ideias para evitar que implementem funcionalidades desnecessárias que venham a ser descartadas pelo mercado – por essa razão, o desenvolvimento de um software com um *design* ideal é entendido como um luxo desnecessário e um desperdício de tempo e esforço (BESKER *et al.*, 2018).

A introdução de processos de engenharia de software – compreendidos como um conjunto de práticas, políticas, estruturas organizacionais, tecnologias e procedimentos com o fim de desenvolver software (FUGGETTA, 2000) – no estágio inicial de uma *startup*, enfrenta obstáculos complexos, dado que empresas nascentes são por natureza criativas e flexíveis e resistem a burocratizar o processo de construção de produto, por temerem perder as características que as definem (PATERNOSTER *et al.*, 2014).

Orientadas a produto, segundo Paternoster *et al.* (2014), elas concentram-se na produtividade de equipes, com fluxos de trabalho flexíveis, que as permitem alterar a direção de seus trabalhos conforme muda o ambiente do mercado, sem estabelecerem diretrizes rígidas. Os requisitos de produto, geralmente definidos na fase inicial, frequentemente são inventados, raramente documentados e, por vezes, são validados após serem colocados à disposição do mercado (PATERNOSTER *et al.*, 2014).

É na fase de *startup* também que, segundo Besker *et al.* (2018), começam os problemas com erros no código e o decorrente acúmulo de dívida técnica, com as *startups* procurando equilibrar os vários fatores que afetam a qualidade do produto. Besker *et al.* (2018) afirmam que o acúmulo de dívida técnica ocorre de forma imprudente nesta fase, mas que isso é necessário e valioso para reduzir risco, custo e atender de forma satisfatória os primeiros clientes. Advertem, ainda, que a falta de preocupação com o código pode ser prejudicial, levando a falhas de produto e interrupção do negócio, e impedindo a entrega do produto mínimo viável. Por essa razão, sugerem que haja a preocupação em lidar com a dívida técnica, aplicando técnicas de refatoração ainda nesse estágio (BESKER *et al.*, 2018).

Na fase de estabilização, o produto pode ainda não estar em condições confiáveis, afirma Crowne (2002), e neste momento o empreendedor pode precisar de mais recursos para melhorar o produto e escalar a operação. Problemas que não tenham sido resolvidos na primeira fase podem, segundo Crowne (2002), ter um impacto crescente nas atividades da *startup*. De acordo com Besker *et al.* (2018), nesta fase as empresas nascentes tendem a tomar decisões de projeto abaixo do ideal com o objetivo de que o produto seja entregue rapidamente ao mercado, a fim que obtenham feedback do usuário para continuar a evoluir.

Na fase de crescimento, o mercado fica atento para conhecer a estratégia de evolução da empresa e é nesta etapa também, que geralmente ocorre a abertura de capital do negócio (CROWNE, 2002). A pressão sobre a *startup* se altera, com a atenção se voltando para modificações do software a fim de atender as necessidades do cliente, introduzindo recursos, o que pode ocasionar novos problemas caso o projeto original tenha sido realizado com uma arquitetura inflexível (BESKER *et al.*, 2018).

Nesta fase os novos desenvolvedores contratados podem agravar os problemas existentes no código gerando nova dívida técnica, em ciclo vicioso, o que pode comprometer a cultura inicial da *startup* e o crescimento do modelo de negócio (BESKER *et al.*, 2018). É na etapa de crescimento também que o código precisa ser otimizado para se tornar escalável, com uma arquitetura de sistema que permita o gerenciamento dos diversos tipos de clientes atendidos, de modo a reduzir o custo de operação e manutenção, a fim de evitar a perda de produtividade (BESKER *et al.*, 2018).

Em estudo com quatro *startups* em crescimento, Pizzini *et al.* (2021) identificaram que nesta fase elas adotam práticas de qualidade limitadas. Segundo o estudo, elas tendem a ser reativas em relação à qualidade de software, resolvendo problemas na medida em que eles venham a impactar produto, negócio e cliente, ou quando a dívida técnica se torna difícil de ser gerenciada. Pizzini *et al.* (2021) afirmam que à medida em que as *startups* crescem, elas passam a adotar alguns comportamentos de empresas maduras, assim que obtêm mais recursos, iniciando um processo de mudança cultural em relação à qualidade.

Por fim, a *startup* chega à maturidade quando o tamanho de mercado, a participação e a taxa de crescimento estabilizam e os processos de desenvolvimento

e venda estão organizados e em pleno funcionamento (CROWNE, 2002). Nessa fase, *startups* se comportam como empresas maduras (BESKER *et al.*, 2018).

Identificar o estágio que uma *startup* está em seu ciclo de vida, portanto, permite compreender seus objetivos e desafios ao longo do processo de desenvolvimento (CROWNE, 2002, KLOTINS *et al.*, 2017 e BESKER *et al.*, 2018).

2.1.3 Revisões sistemáticas de literatura sobre *startups*

Ao longo dos últimos anos foram realizadas algumas revisões sistemáticas a respeito de práticas de engenharia de software em *startups*. Paternoster *et al.* (2014) concentram atenção principalmente nos aspectos organizacionais de *startups* que compõem o desenvolvimento de software. Klotins, Unterkalmsteiner e Gorschek (2015) fazem uma análise das áreas de conhecimento da Engenharia de Software empregadas em empresas iniciantes. Cavalcante *et al.* (2018) examinam aspectos técnicos, identificando práticas, técnicas e ferramentas que apoiam *startups* no desenvolvimento de software. Berg *et al.* (2019), por sua vez, abordam práticas de engenharia de software em *startups*, comparando dois períodos distintos, entre 1994 e 2013 e entre 2013 e 2017.

Os resultados desses mapeamentos encontram-se resumidos na Quadro 2-1.

Quadro 2-1. Mapeamentos sistemáticos de literatura. Fonte: o Autor.

MAPEAMENTO SISTEMÁTICO	QTDE. DE ESTUDOS	RESULTADOS	CONCLUSÕES
Paternoster *et al.* (2014)	43 estudos primários	19 deles (44%) concentram em fatores organizacionais; 16 (37%) são dedicados a desenvolvimento de software em *startups,* dos quais trazem fracas contribuições. Apenas 4 são contribuições inteiramente dedicas a práticas de engenharia de software em *startups*, porém três deles usam os mesmos dados.	Há uma falta de estudos primários relevantes sobre desenvolvimento de software em *startups*
Klotins, Unterkalmsteiner e Gorschek (2015)	14 estudos primários	Identificou 54 práticas de ES extraídas de 11 das 15 áreas do SWEBOK. Embora a maioria das áreas do SWEBOK seja incluída, somente 28 das 62 categorias foram cobertas pelas pesquisas.	Número pequeno de artigos abordam as principais áreas de conhecimento de ES nas *startups*, o que já havia sido identificado por Sutton et al (2000). Os estudos são insuficientes não criam corpo sólido de conhecimento em ES, sendo difícil transferir

			resultados deles para *startups*, por falta de rigor.
Cavalcante *et al.* (2018)	19 estudos primários	Identificou um total de 24 técnicas, 31 práticas e 37 ferramentas de engenharia de software usadas por *startups*.	O número de estudos que apresentam resultados transferíveis para a indústria ainda é baixo.
Berg *et al.* (2018)	74 estudos primários, dos quais 27 recentes	Identificou que a maioria dos estudos trata de processo, gerenciamento, construção, design e engenharia de requisitos.	Trabalhos futuros podem focar em modelos de evolução de *startups* e aspectos humanos, bem como a conceitos descritivos a respeito de *startups*.

Paternoster *et al.* (2014) realizaram mapeamento sistemático com 43 estudos primários, dos quais foram identificadas 213 práticas de trabalho e 90 de engenharia de software em *startups*, que foram categorizadas e analisadas, concluindo que: (i) o corpo de conhecimento era limitado a poucos estudos de alta qualidade; (ii) as práticas em empresas iniciantes são escolhidas a partir do contexto e adaptadas para serem úteis em um ambiente de restrições que caracteriza o contexto dessas companhias.

Das 243 práticas de trabalho identificadas por Paternoster *et al.* (2014), 90 delas dizem respeito a desenvolvimento de software, 70 são gerenciais ou organizacionais, 47 são de gerenciamento de processos e 6 são ferramentas ou tecnologias.

Paternoster *et al.* (2014) consideram as práticas de gerenciamento de processos as principais atividades de engenharia de software usadas para fazer a gestão do desenvolvimento de produtos em *startups*. Segundo eles, as metodologias ágeis são consideradas as mais viáveis para empresas iniciantes de software, por permitirem que o desenvolvimento prossiga alinhado à estratégia de negócios, com lançamentos rápidos de produto, abordagem iterativa e incremental e redução do tempo de espera entre a concepção da ideia e a implantação.

Paternoster *et al.* (2014) identificaram nos estudos, o uso de variantes de metodologias ágeis, como *Lean Startup* (em dois estudos), que defende o uso de produto mínimo viável (MVP), para testes rápidos iterativos, mensuração e aprendizado. Entretanto, os pesquisadores afirmam que *startups* não seguem metodologias específicas, mas escolhem práticas que sejam convenientes e adequadas às suas necessidades do momento (Paternoster *et al.*, 2014).

Paternoster *et al.* (2014) sugerem o uso do modelo Cynefin, de Kurtz e Snowden (2003), para explicar a orientação de *startups* em abordagens flexíveis e

reativas, por lidarem com domínios complexos e caóticos, o que necessitaria de métodos não rigorosos de controle de atividades, que estimulem o *feedback* do cliente, ampliem a quantidade de perspectivas e soluções disponíveis para tomadores de decisões. Na visão de Paternoster *et al.* (2014), é necessário que qualquer processo que seja adaptado para *startups* possibilite que a empresa transite em domínios complexos e caóticos. Portanto, afirmam eles, os engenheiros de software precisam de liberdade para escolher rapidamente atividades, permitindo que parem de imediato quando os resultados forem considerados errados, corrigindo a abordagem, aprendendo com os equívocos cometidos ao longo do processo, e buscando um equilíbrio entre flexibilidade e repetibilidade nos processos e na gestão de conhecimento (PATERNOSTER *et al.*, 2014).

Assim, no que tange às práticas de gerenciamento de processos, eles afirmam que a pesquisa identificou como úteis para *startups*: (i) metodologias leves para obter flexibilidade em escolher práticas sob medida e capacidade de reagir rápido para mudar o produto de acordo com a estratégia de negócio; (ii) práticas de lançamentos rápidos para construir um protótipo de modo evolutivo e aprender rápido com o *feedback* dos usuários, a fim de lidar com a incerteza de mercado (Paternoster *et al.*, 2014).

Sobre as 90 ocorrências de práticas de software em *startups*, conforme Tabela 2-3, o mapeamento sistemático de Paternoster *et al.* (2014) identificou que 32 (trinta e duas) delas eram de práticas de projeto e arquitetura, 23 (vinte e três) de práticas de garantia de qualidade, 21 (vinte e uma) de engenharia de requisitos, 14 (catorze) implementação, manutenção e entrega.

Tabela 2-3. Práticas de engenharia de software. (Paternoster et al., 2014).

PRÁTICAS DE ENGENHARIA DE SOFTWARE	FREQUÊNCIA
Projeto e arquitetura	32
Garantia de qualidade	23
Engenharia de requisitos	21
Implementação, manutenção e entrega	14
Total	**90**

Sobre engenharia de requisitos, Paternoster *et al.* (2014) constataram que estabelecer um processo é desafiador, uma vez que as práticas são reduzidas a poucas atividades básicas no contexto das *startups*, com um esforço em definir uma proposta de valor no início do ciclo de vida. Como os clientes não são bem conhecidos,

afirmam eles, os requisitos são guiados pelo mercado, o que, em alguns estudos traz grande dificuldade para obter e detalhar as especificações de requisitos funcionais e não funcionais, podendo os desenvolvedores utilizarem histórias de usuários e estimativa de esforço de cada história para identificá-los (Paternoster *et al.*, 2014). Isso porque, explicam os autores, mercados inexplorados e inovadores conduzem à necessidade de mudar os requisitos mais rapidamente, o que dificulta à equipe de desenvolvimento mantê-los de forma consistente ao longo do tempo.

Segundo Paternoster *et al.* (2014), em cinco dos estudos foi relatada a importância de envolver clientes no processo de obtenção e priorização de requisitos conforme suas necessidades primárias. Os pesquisadores avaliam que (i) dada a necessidade de ajustar o problema à solução proposta, é preciso descobrir as reais demandas dos clientes, com o objetivo de testar hipóteses para definir um conjunto mínimo de requisitos; e (ii) no futuro o desenvolvimento de software tende a trabalhar em uma profunda colaboração com clientes, o que pode resultar em mudanças no método de obtenção de requisitos (Paternoster *et al.*, 2014).

No que tange a práticas de *Design* e Arquitetura, Paternoster *et al.* (2014) afirmam que essa área é orientada por princípios simples, a fim de evitar as dificuldades que restrições arquiteturais podem apresentar na medida em que as *startups* crescem. Apesar de terem identificado nos estudos uma ausência de preocupação com a arquitetura e *design*, Paternoster *et al.* (2014) afirmam que devem ser suficientemente bons para evitar que causem problemas na obtenção de receita do produto, podendo ser corrigidos posteriormente, quando houver aumento de fluxo de caixa.

Nesse contexto, os pesquisadores encontraram o uso de padrões de projeto (*design patterns*) que permitem flexibilidade na refatoração do produto, assim como emprego de arquiteturas iniciais com modelos de alto nível, reuso de código com base em padrões da indústria ou de componentes de terceiros. De acordo com Paternoster *et al.* (2014), os estudos indicam que as dificuldades das *startups* aumentam quando a complexidade da base de clientes e dos produtos cresce, de modo que se torna necessária uma análise de decisões na fase inicial, a fim de evitar problemas antes da obtenção de receitas. A evolução do produto, afirmam eles, pode ser apoiada por recursos modulares e independentes, e, por essa razão, há a necessidade de se empregar práticas e estruturas de arquitetura que permitam uma fácil extensão do *design*, alinhando o produto às incertezas de mercado.

A respeito das práticas de implementação, manutenção e entrega, Paternoster *et al.* (2014) afirmam que *startups* utilizam métodos próprios que se adequam às suas necessidades circunstanciais, como rastreamento de *bugs*, métricas simples de código e sessões de programação em pares. Eles identificaram estudos que abordam programação em pares e padrões de codificação em fases mais adiantadas da *startup*, quando o produto vai se tornando mais complexo. Foi identificado também o uso de métodos próprios, adequados à necessidade do momento, para avaliação e métricas, bem como o benefício da refatoração constante do código (PATERNOSTER *et al.*, 2014).

Da análise feita sobre práticas de implementação, manutenção e entrega, Paternoster *et al.* (2014) consideram que as *startups* tendem a iniciar o desenvolvimento de produto de modo informal, relegando a introdução de práticas padronizadas apenas quando o projeto se torna maior. Ou seja, na fase inicial desenvolvem uma base de código simples, com foco somente nas funcionalidades que serão validadas com os clientes (PATERNOSTER *et al.*, 2014). Os pesquisadores sugerem ainda que, como a meta da *startup* orienta os esforços na refatoração e implementação, é preciso mais pesquisas para alinhar negócios e execução de práticas de desenvolvimento em empresas iniciantes.

Sobre práticas de garantia de qualidade, Paternoster *et al.* (2014) descobriram que testes tendem a ser caros e comprometer o tempo de lançamento de *startups*, enquanto a implementação de testes pode ser uma tarefa complexa que fica dificultada pela falta de experiência da equipe, causando baixa qualidade por conta da fraca gestão de software. Foram identificadas como práticas de qualidade adotadas por *startups*: (i) testes de usabilidade para buscar o encaixe entre produto e mercado; e (ii) terceirização de testes, a fim que a equipe de desenvolvimento permaneça com foco no desenvolvimento do produto (PATERNOSTER *et al.*, 2014).

No mapeamento sistemático, Paternoster *et al.* (2014) abordam também o contexto das *startups*, conforme já apresentado, e relatam como práticas gerenciais e organizacionais encontradas nos estudos: (i) empoderamento da equipe, com poder de influenciar no resultado do trabalho; (ii) uso de indicadores-chave de desempenho para análise de demanda de consumidores; (iii) plano de objetivos de curto e médio prazo, avaliando o tempo de ciclo de desenvolvido para buscar pontos de melhoria. Na visão de Paternoster *et al.* (2014), ao empoderar as pessoas, a *startup* consegue trabalhar de forma mais ágil e com menos burocracia, possibilitando aumentar o

comprometimento, a criatividade e a capacidade de adaptação. Eles avaliam, ainda, que a comunicação aberta é crucial para empresas nascentes lidarem com as práticas de engenharia de software e entenderem os desafios a serem superados, de modo que ferramentas e técnicas que encorajem o compartilhamento verbal de informações são recomendadas nas fases iniciais, mas tendem a se tornar um problema quando a empresa entra em crescimento (PATERNOSTER *et al.*, 2014).

No que se refere a ferramentas, o estudo identificou que há uma preferência por ferramentas que sejam fáceis de implantar – por exemplo, quadros brancos –, dada a necessidade de lidar com dados em constante mudança, em detrimento de soluções mais complexas que exijam treinamento e tenham alto custo para implementação (PATERNOSTER *et al.*, 2014). E no que tange a tecnologias, as *startups* buscam ferramentas, muitas vezes de código aberto, que possam alterar os produtos rapidamente, a fim de evitar conflitos com a direção do modelo de negócio: infraestruturas de uso geral, como sistemas de relatório e rastreamento de problemas, gerenciamento de configuração, planejamento, programação e notificação. Por fim, o Quadro 2-2 apresenta um resumo das perguntas de pesquisa e das respostas.

Quadro 2-2. Perguntas de pesquisa do mapeamento de Paternoster *et al.* (2014). Fonte: o Autor.

Mapeamento sistemático	Perguntas de Pesquisa	Respostas
Paternoster et al. (2014)	P1 Qual é o contexto que caracteriza o desenvolvimento de software em *startups*?	R1 Não há conceito único na literatura sobre o que é uma *startup*. As características contextuais relatadas com mais frequência são: escassez de recursos, alta reatividade e flexibilidade, pressão de tempo, condições incertas e crescimento rápido.
	P2 Até que ponto a pesquisa sobre *startups* fornece resultados confiáveis e transferíveis para a indústria?	R2 A análise de rigor e relevância indica que apenas nove dos estudos (21%) representa o estado da arte e fornece resultados transferíveis e confiáveis aos profissionais. Mais da metade dos estudos, 23 deles, (53%) tem relevância moderada no setor, mas baixo rigor científico.
	P3 Quais são as práticas de trabalho relatadas em associação com a engenharia de software em *startups*?	As práticas de desenvolvimento de software são adotadas apenas parcialmente e principalmente em um estágio avançado do ciclo de vida da startup. São preferidas metodologias leves que permitam as empresas escolher e adaptar práticas, a fim de facilitar a reatividade e possibilitar mudanças rápidas no produto.

Como se observa no Quadro 2-2, Paternoster et al. (2014) não identificaram um conceito único de *startup*, mas verificaram características de contexto mais frequentes, como escassez de recursos, reatividade e flexibilidade, condições de incerteza, pressão de tempo e rápido crescimento. Apenas parte dos estudos (21%)

apresentaram rigor e relevância e, no que tange às práticas de trabalho, Paternoster et al. (2014) elencaram um amplo conjunto de considerações conforme já foi relatado.

Eles observaram que metodologias ágeis e mais tradicionais têm dificuldade de serem adotadas devido à excessiva incerteza e à pressão de tempo, com as *startups* preferindo processos de natureza evolutiva, com o produto sendo criado por meio de interações e atualizações de um protótipo inicial que recebe *feedback* de clientes. Requisitos são dificilmente documentados, mas geralmente orientados ao mercado. Arquitetura e *design* são frequentemente substituídos por uso de estruturas conhecidas que facilitem a manutenção, com pouco esforço de documentação.

Segundo Paternoster *et al.* (2014), *startups* usam geralmente ferramentas simples para apoiar e rastrear a base de conhecimento, bem como gerenciar o fluxo de trabalho, podendo optar por soluções de código aberto que requerem pouco treinamento e manutenção. O teste utilizado é principalmente o de aceitação pelo cliente, grupos focais, ou, por vezes, terceiriza-se a atividade de teste. Práticas gerenciais e organizacionais são reduzidas ao essencial. Objetivos são focados em curto e médio prazo por causa da incerteza, e indicadores desempenho servem para identificar demandas de clientes.

Klotins, Unterkalmsteiner e Gorschek (2015) realizaram mapeamento sistemático em que procuram identificar e classificar as áreas de conhecimento exploradas por artigos sobre engenharia de software em *startups*, com o objetivo de analisar as práticas existentes e descobrir oportunidades de pesquisa. Conforme a Tabela 2-4, os autores do estudo identificaram 54 práticas em 14 estudos, nos quais 11 das 15 principais áreas de conhecimento do *Software Engineering Body of Knowledge* (SWEBOK) foram cobertas por algum tipo de pesquisa. Segundo eles, embora a maioria das áreas do SWEBOK seja incluída, somente 28 das 62 categorias foram cobertas pelas pesquisas. Por fim, concluíram que os estudos existentes não forneciam, no que tange à engenharia de software, suporte confiável para qualquer estágio de ciclo de vida de *startups*, por conta do baixo rigor das pesquisas realizadas até aquele momento (KLOTIN; UNTERKALMSTEINER; GORSCHEK, 2015).

Tabela 2-4. Estudos por área de conhecimento (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015).

ÁREA DE CONHECIMENTO	COBERTURA	CATEGORIAS COBERTAS
Engenharia de Requisitos de Software	6/8	Processos de requisitos Elicitação de requisitos Análise de requisitos Validação de requisitos

		Considerações práticas
Projeto de software	4/8	Fundamentos de Projeto de Software Questões Chave em Projeto de Software Design de Interface de Usuário Ferramentas de design de software
Construção de Software	3/5	Fundamentos de Construção de Software Gerenciamento de Construção Considerações Práticas
Teste de Software	2/6	Fundamentos de Teste de Software Processo de Teste
Manutenção de Software	1/5	Técnicas para Manutenção
Gerenciamento de Configuração de Software	3/7	Identificação de Configuração de Software Entrega e Gerenciamento de Liberação de Software Ferramentas de Gerenciamento de Configuração de Software
Gerenciamento da Engenharia de Software	3/7	Planejamento de Projeto de Software Promulgação de Projeto de Software Ferramentas de Gerenciamento de Engenharia de Software
Processo de Engenharia de Software	2/5	Técnicas de Mensuração de Processo de Software Ferramentas de Processo de Engenharia de Software
Métodos e Modelos de Engenharia de Software	2/4	Modelagem Métodos de Engenharia de Software
Qualidade de Software	1/4	Qualidade de Software
Prática Profissional de Engenharia de Software	2/3	Profissionalismo
Competências de Comunicação	-	-
Economia de Engenharia de Software	0/5	-
Fundamentos de Computação	0/17	-
Fundamentos de Engenharia	0/7	-

Em seu mapeamento sistemático, Klotins, Unterkalmsteiner e Gorschek (2015) também utilizaram o ciclo de vida de Crowne (2002) para analisar os artigos selecionados, cujo resumo dos resultados encontra-se no Quadro 2-3. Segundo os autores, na fase *Startup*, como a companhia busca construir a primeira versão de produto, é importante a compreensão e a comunicação das demandas do cliente, bem como a definição de um escopo de desenvolvimento. Nessa fase, afirmam os autores, a área de Engenharia de Requisitos contribui ao dar suporte ao entendimento das necessidades e restrições do software.

De outro lado, a área de Engenharia de Gerenciamento de Software apoia a definição e a avaliação do escopo, tendo em vista que *startups* em fase inicial

trabalham com recursos bastante limitados. Embora a experiência de interação seja considerada um diferencial relevante, não foi relatada nos estudos a presença de requisitos específicos de qualidade, o que indicaria uma falta de compreensão do papel deles no contexto das empresas iniciantes (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015). Diferentemente de o que ocorre com a Engenharia de Requisitos, que teve seis estudos identificados na fase inicial, o Gerenciamento da Engenharia de Software não teve estudos encontrados.

Quadro 2-3. Estudos por etapa do ciclo de vida da *startup*, com base em Klotins, Unterkalmsteiner e Gorshek (2015). Fonte: o Autor.

FASE DO CICLO DE VIDA	OBJETIVO	CATEGORIAS COBERTAS	
		DESCRIÇÃO	IDENTIFICADA NA REVISÃO SISTEMÁTICA
Inicialização	Construção da primeira versão do produto para um nicho de cliente	Engenharia de Requisitos (AC) Gerenciamento de Engenharia de Software (AC)	06 estudos Não
Estabilização	Melhoria do produto para que possa obter novos clientes sem sobrecarga	Projeto de Software (AC) Gerenciamento de Requisitos (Cat)	07 estudos Não
Crescimento	Expansão da equipe, transferência know-how e gerência do produto	Habilidades de Comunicação (Cat) Ciclo de Vida do Produto (Cat) Gerenciamento de Portfolio (Cat)	03 estudos Não Não
Maturidade	Introdução e melhoria de processos	Processo de Engenharia de Software (AC): Técnicas de Medição de Processo de Software (Cat) Ferramentas de Processo e Engenharia de Software (Cat)	01 estudo 01 estudo

Como na fase de Estabilização o objetivo é desenvolver um produto para aquisição de novos clientes sem que haja sobrecarga do sistema, a área de Projeto de Software apoia a melhoria da qualidade interna do produto (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015). Foram identificados por Klotins, Unterkalmsteiner e Gorschek (2015) sete estudos nessa área de conhecimento.

A categoria Gerenciamento de Requisitos, segundo os autores, é importante nesse estágio por conta da necessidade de manter a integridade de produto enquanto se adiciona novas funcionalidades. Porém, estudos a esse respeito não foram

encontrados na revisão sistemática (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015).

Na fase de Crescimento os desafios principais encontram-se na expansão da equipe, na garantia de transferência das práticas e *expertises* e na gerência do produto, o que conduz à aplicação da categoria Habilidades de Comunicação, para transferir conhecimento internamente – elementos identificados em três estudos que constam na revisão sistemática (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015). Segundo os pesquisadores, categorias da área de Economia e Engenharia de Software, como Ciclo de Vida do Produto e Gerenciamento de Portfolio, que abordam relações entre decisões técnicas de desenvolvimento e metas do negócio, não foram encontrados, o que revelaria uma lacuna importante para ser elaborada na construção de produtos viáveis.

Por fim, na fase de Maturidade, em que o produto está desenvolvido e estável, os processos cotidianos já são previsíveis e há a criação de novos produtos, uso de práticas da área de Processo de Engenharia de Software é adequado, pois tratam de introdução e melhoria de processo (KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015). Dentro dessa área, os pesquisadores afirmam que identificaram dois estudos nas categorias de Técnicas de Medição de Processo de Software e Ferramentas de Processo e Engenharia de Software.

Em sua revisão sistemática, Klotins, Unterkalmsteiner e Gorschek (2015) identificaram uma ausência de estudos relacionados a processos de requisitos, arquitetura de software e processos de engenharia de software. Apresenta-se no Quadro 2-4 um resumo das perguntas de pesquisa e respostas encontradas por Klotins, Unterkalmsteiner e Gorschek (2015). Em síntese, eles constatam que apenas 28 das 62 categorias do SWEBOK são abordadas, que há poucos estudos nas fases de crescimento e maturidade de ciclo de vida de *startups*, e que há pouco rigor nos estudos analisados.

Quadro 2-4. Perguntas de pesquisa de KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2015.

MAPEAMENTO SISTEMÁTICO	PERGUNTAS DE PESQUISA	RESPOSTAS
Klotins, Unterkalmsteiner e Gorschek (2015)	Q1 Qual é o estado da prática sobre utilização das áreas de conhecimento de ES em *startups*?	Das 15, 11 áreas do SWEBOK são abordadas, mas apenas 28 das 62 categorias são cobertas. Classificaram os achados com base no modelo de ciclo de vida de *startups* de Crowne (2002), ordenando os estudos por áreas e categorias.

	Q2 Qual é a relevância e o rigor das experiências de geração de relatórios de estudos de ES em startups?	A maioria dos estudos identificados foi realizada com empresas iniciantes em operação, o que os torna relevante. Porém, a maioria é de relatos de experiência e analisam apenas um caso. Análise realizada implica em baixo rigor dos estudos, não podendo ser generalizados e sendo de difícil transferência para outras *startups*.

Cavalcante *et al.* (2018) fizeram um mapeamento sistemático em que procuraram identificar técnicas, práticas e ferramentas usadas em desenvolvimento de software em *startups*. Após qualificação de estudos primários, de um total de 112 estudos, 19 foram selecionados para o mapeamento que encontrou 24 técnicas, 31 práticas e 37 ferramentas.

Das 24 técnicas, a que apresenta maior frequência, conforme apresentado na Tabela 2-5, é a de *Lean/Lean Startup*, com sete menções nos estudos analisados; seguida do Scrum (quatro menções); metodologias ágeis de forma geral, Kanban e cartões de história (três menções cada); eXtreme Programming (XP), *Planning Game*, *Backlog* e programação de pares (dois menções cada); e as demais citadas aparecem uma vez cada - *Join Application Design* (JAD), *Experiment Driven Development* (EDD), Teste A/B, *Feature Driven Development* (FDD), *Rational Unified Process* (RUP), Scrumban, logs e estatísticas e *Code Review*. Diferentes técnicas para construção de produto mínimo viável foram citadas, em um total de sete vezes.

Tabela 2-5. Métodos de gerenciamento (CAVALCANTE *ET AL.*, 2018).

TÉCNICAS	**FREQUÊNCIA**
Lean/Lean Startup	7
Técnicas para construção de Produto Mínimo Viável	7
Scrum	4
Metodologias ágeis, Kanban e cartões de estórias	3
Extreme Programming, Planning Game, Backlog e programação de pares	2
Outras	1
Total	**24**

No que se refere às 31 práticas, integração continua é mencionada cinco vezes e soluções comercial *off-the-shef* (COTs), *open source*, padrões de código/*design*/*frameworks*, refatoração de código e entregas contínuas (quatro vezes cada); teste de aceitação e reuso de software (três ocorrências cada); cliente no local de desenvolvimento e testes de integração (duas vezes cada), e as demais foram mencionadas uma vez cada – semana de trabalho de 40 horas, código pertence a todos, teste contínuo, *design* simples, lançamentos curtos, teste unitário, teste de

usabilidade, entrega manual, gerenciamento de requisitos, apresentação de materiais, backups diários em produção, reversão automática em produção em caso de falha, bug-tracking, capacitação dos membros da equipe, indicadores-chave de performance, controle de versão, prototipagem evolucionária, entrevistas, pesquisas de mercado, usuários de testes, comando e controle e incluir e capacitar.

Tabela 2-6. Mapeamento sistemático: Práticas (CAVALCANTE *ET AL*., 2018).

PRÁTICAS	FREQUÊNCIA
Integração contínua	5
Soluções comercial off-the-shef (COTs), Open Source, padrões de código/*design*/*frameworks*, refatoração de códigos e entregas contínuas	4
Teste de aceitação e reuso de software, três ocorrências cada, cliente no local de desenvolvimento e testes de integração	2
Outras	1
Total	**31**

E a respeito das 37 ferramentas utilizadas, conforme a Tabela 2-7, Google Analytics teve duas menções, com as demais sendo mencionadas apenas uma vez – Atlassian Jira, Axosoft OnTime, Target Proccess, Microsoft TFS, Rally Platform, Mingle, Version One, Blossom.io, Scrumwise, Base Camp, LeanKit, AgileZen, PlanBox, Kanbanize, ScrumWorksPro, BananaScrum, AgileFant, IceScrum, Xplanner, Trello, Asana, XPStoryStudio, JustInMind, Betalist.com, Mixpanel, Hadoop, Storm, Kafka, Flume, Hbase e AIMLBot e linguagens Haskell, C++, PHP, Python e .NET.

Tabela 2-7. Mapeamento sistemático (2018): Ferramentas (CAVALCANTE *ET AL*., 2018).

FERRAMENTAS	FREQUÊNCIA
Google Analytics	2
Outras	35
Total	**37**

Dos 19 artigos selecionados no mapeamento realizado por Cavalcante *et al.* (2018), sete foram classificados como de pesquisa de avaliação (metodologia é aplicada e avaliada), seis foram categorizados como de experiência (mostram como algo foi feito) e outros seis como filosóficos (procuram estruturar modelos conceituais). No que tange ao foco dos artigos, segundo Cavalcante *et al.* (2018), oito são de desenvolvimento de software, sete de gestão de processo, dois de instrumentos de apoio a atividades de desenvolvimento e dois de gestão organizacional. Cavalcante *et al.* (2018) afirmam ainda que os estudos demonstram haver uma diversidade de trabalhos sobre desenvolvimento de software em empresas iniciantes, sendo a maior parte dos artigos de lições aprendidas (12) e proposição de modelos (6), com um único

artigo tratando de método relacionado a construção de software ou gestão de processo.

Cavalcante *et al.* (2018) consideram que grande parte das técnicas, práticas e questões voltadas à capacitação de time encontradas contribuem para a agilidade que as empresas iniciantes necessitam, sendo o uso de alguma técnica, princípio ou métodos ágeis um ponto comum dos artigos. Eles reconhecem, entretanto, que há um número reduzido de estudos empíricos e sugerem que os dados coletados no estudo que fizeram serve de ponto de partida novas pesquisas no tema das *startups*. Na Tabela 12, apresenta-se um resumo da resposta à pergunta de pesquisa.

Tabela 2-8. Pergunta de pesquisa (CAVALCANTE *ET AL.*, 2018).

MAPEAMENTO SISTEMÁTICO	PERGUNTA DE PESQUISA	RESPOSTA
Cavalcante et al. (2018)	P1: Quais são as técnicas, práticas e ferramentas utilizadas para o desenvolvimento de software em startups?	Foram extraídas 24 técnicas, 31 práticas e 37 ferramentas. Lean/Lean startup são as técnicas mais mencionadas (sete vezes), integração contínua é a prática mais identificada (cinco vezes) e Google Analytics a ferramenta mais usada (duas vezes mencionada).

A revisão sistemática da literatura realizada por Berg *et al.* (2018) cobriu os mapeamentos realizados por Paternoster *et al.* (2014) e Klotins, Unterkalmsteiner e Gorschek (2015). Os autores analisaram outros 27 artigos publicados entre 2013 e 2017 e concluiram que houve uma evolução na qualidade dos estudos ao longo dos últimos cinco anos, o que permite identificar mudanças na direção da pesquisa na engenharia de software em *startups*.

Segundo eles, o contexto das empresas iniciantes aparece nos estudos como um fator relevante que dificulta os processos de engenharia de software, indicando também a razão pela qual no estágio inicial não seguem estritamente nenhuma metodologia ágil, optando pelo uso de algumas técnicas não sistematizadas (BERG *et al.*, 2018). Na avaliação de Berg *et al.* (2018) a revisão sistemática de literatura que realizaram constitui em uma fusão da literatura primária que cobre o campo da engenharia de software no contexto das *startups* entre 1994 e 2017, fornecendo uma visão abrangente para pesquisadores do tema.

O estudo de Berg *et al.* (2018) mostra que a frequência e a pertinência dos estudos aumentaram entre 2013 e 2017, em relação ao período anterior pesquisado, de 1994 a 2013, concluindo que: (i) a maior parte utiliza casos; e (ii) trazem lições

aprendidas. Os pesquisadores classificaram esses estudos também empregando as categorias do SWEBOK identificando a incidência de prática no que tange às áreas de conhecimento: (i) práticas de gerenciamento (16 estudos); (ii) processo de software (14); (iii) engenharia de requisitos (10); (iv) *design* de software e construção de software (9 cada); (v) prática profissional (8); (vi) métodos e modelos (7); (vii) qualidade e testes (6); (viii) gerenciamento de configuração (3); e (ix) manutenção (1). Ficaram ausentes seis das 15 áreas de conhecimento: (i) gerenciamento de configuração de software; (ii) economia de engenharia de software; (iii) manutenção de software; (iv) fundamentos de computação; (v) fundamentos matemáticos; e (vi) fundamentos de engenharia.

Em comparação com o mapeamento realizado por Klotins, Unterkalmsteiner e Gorschek (205), Berg *et al.* (2018) mostram que ocorreu uma significativa alteração nos rumos da pesquisa ao longo de cinco anos – enquanto entre 1994 e 2013 as áreas mais representadas eram *design* de software e engenharia de requisitos, entre 2013 e 2017, processo de engenharia de software e gerenciamento de software passaram a receber mais atenção.

Berg *et al.* (2018) fazem também uma comparação com o estudo de Paternoster *et al.* (2014), em relação ao tipo de contribuição dos artigos analisados, e concluem que, entre 1994 e 2013, as contribuições mais representativas foram de recomendações e modelos, enquanto, entre 2013 e 2017, apresentou-se maior número de lições aprendidas.

Por fim, a Tabela 2-9 traz as respostas às perguntas de pesquisa. Importante mencionar ainda que Berg *et al.* (2018) identificaram que embora os trabalhos pesquisados apresentem um conjunto inconsistente de temas para definir *startups*, trazem conceitos recorrentes que definem o contexto delas: inovação, falta de recursos, incerteza, pressão do tempo, equipe pequena, altamente reativa, de rápida evolução. Verificaram também que a transferência de resultados de um ambiente para outro somente é possível quando se leva em conta tamanho da equipe, orientação do produto, número de anos de atividade e fase de ciclo de vida, número de *startups* investigadas, localização delas, método de desenvolvimento (BERG *et al.*, 2018). Além disso, há necessidade de mais rigor na descrição de contexto de engenharia de software em *startups*, visto que dos 27 trabalhos primários analisados apenas 14 possuíam descrições de qualidade satisfatória.

Tabela 2-9. Pergunta de pesquisa (BERG *ET AL.*, 2018).

MAPEAMENTO SISTEMÁTICO	PERGUNTA DE PESQUISA	RESPOSTA
Berg *et al.* (2018)	P1: Como a pesquisa de startup de software mudou ao longo do tempo em termos de áreas de conhecimento focadas?	A pesquisa entre 2013 e 2017 tem um rigor maior que o do período de 1994-2013. Áreas mais encontradas entre 2013 e 2017: processo e gerenciamento de engenharia de software. Entre 1994 e 2013, foram: design e de requisitos de software. Áreas de modelos e métodos de engenharia de software, de qualidade de software e de testes tiveram pouca atenção dos pesquisadores durante o período de 1994 e 2017. Entre 2013 e 2017, gerenciamento de configuração e manutenção de software não foram pesquisados.
	P2: Qual é a força relativa das evidências empíricas relatadas?	Houve um aumento de rigor dos estudos primários entre 2013 e 2017 em relação ao período anterior de 1994 a 2013.
	P3: Em que contexto foi realizada a pesquisa de startup de software?	Os trabalhos apresentam uso inconsistente de conceitos temáticos que descrevem as startups. Transferência de resultados de um ambiente ao outro necessita levar em conta fatores de contexto. Necessidade de esforço maior para descrever o contexto da engenharia de software em *startups*.

As quatro revisões sistemáticas trazidas nesta seção permitem compreender o estado atual da pesquisa de práticas de engenharia de software em *startups*. Como se observa, as preocupações das pesquisas estão em torno de entender as práticas de engenharia de software empregadas por empresas nascentes, as áreas pesquisadas e o rigor dos estudos, bem como o desenvolvimento de pesquisas de *startups* em suas diferentes fases do ciclo de vida.

Práticas de engenharia de software para conformidade legal de proteção de dados estão ausentes nos mapeamentos sistemáticos.

2.2 LGPD e o contexto da engenharia de software

Esta seção inicia-se apresentando definições legais no âmbito da proteção de dados que serão usadas ao longo desta pesquisa. Em seguida apresentam-se a LGPD e suas implicações no que se refere à engenharia de software.

2.2.1 Definições em proteção de dados

Nesta seção são apresentados os conceitos da LGPD e, quando necessário, mencionam-se também aqueles do GDPR, que são utilizados ao longo deste trabalho.

O Artigo 5° da LGPD traz diversas definições que são úteis para o presente estudo. Dado pessoal, nos termos do Artigo 5º, I, da LGPD, é toda a informação que esteja relacionada a pessoa natural identificada ou identificável (BRASIL, 2018). Por essa definição fica esclarecido que a lei não trata de dados de pessoas jurídicas. Entretanto, importante mencionar que dados de pessoas jurídicas podem conter informações atribuíveis a pessoas naturais e esses dados, por essa razão, terão a proteção da lei.

Dado pessoal sensível, conforme o Artigo 5º, II, do referido texto legal, é informação pessoal que trate de origem racial ou étnica da pessoa, bem como de filiação a sindicato, organização de caráter religioso, filosófico ou político, ou, ainda, de saúde, vida sexual, dados genéticos ou biométricos (BRASIL, 2018).

As definições de dado pessoal e dado pessoal sensível são importantes porque a lei vai apresentar hipóteses diferentes de tratamento de dados para cada uma dessas categorias. As hipóteses para tratamento de dados pessoais estão estabelecidas no Artigo 7º da lei, enquanto as de dados pessoais estão no Artigo 11º. Dados pessoais sensíveis requerem especial atenção por seu conteúdo poder tornar vulnerável o seu titular a alguma forma de discriminação (BIONI, 2020).

Dano anonimizado, nos termos do Artigo 5º, III, da LGPD, é aquele relativo à pessoa que não pode ser identificada com o emprego de meios técnicos e razoáveis no momento de seu tratamento. O Artigo 12 da lei estabelece, ainda, que dados anonimizados não são considerados dados pessoais, desde que a anonimização não possa ser revertida, seja por meios próprios, seja com o emprego de esforços razoáveis, neste último caso levando-se em conta fatores objetivos como custo e tempo para a realização de processo de reversão dos dados anônimos, com base nas tecnologias disponíveis existentes.

Tratamento é qualquer operação efetuada com dados pessoais, que vai desde o mero acesso até a tratamentos complexos, como processamento por meios automatizados. Ao definir tratamento, a lei trouxe no Artigo 5º, X, um rol não exaustivo, elencando pelo menos 20 possibilidades: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação da informação, controle da informação, modificação, comunicação, transferência, difusão e extração (BRASIL, 2018).

No que se refere aos agentes relevantes no contexto da lei, seis são mencionados na LGPD: titular, controlador, operador, agente de tratamento, encarregado e autoridade nacional (BRASIL, 2018).

Titular, de acordo com o Artigo 5º, V, da LGPD, é a pessoa natural a quem é atribuído o dado, seja pessoal ou seja pessoal sensível (BRASIL, 2018).

Nos termos do Artigo 5º, VI, da lei, controlador é definido como aquela pessoa natural ou jurídica, seja de direito público ou privado, que toma as decisões sobre o tratamento de dados pessoais (BRASIL, 2018).

Operador, por sua vez, segundo o Artigo 5º, VII, da LGPD, é a pessoa natural ou jurídica, de direito público ou privado, que faz o tratamento de dados pessoais seguindo as instruções do controlador estabelecidas pelo controlador (BRASIL, 2018).

Quando a lei se refere aos agentes de tratamento, de acordo com o Artigo 5º, IX, da LGPD, ela está se referindo indiscriminadamente, tanto ao controlador, quanto ao operador (BRASIL, 2018).

Na prática, a diferença entre controladores e operadores pode não ser tão simples, requerendo uma análise caso a caso mais detalhada, de modo que a ANPD publicou um guia para dirimir eventuais dúvidas (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2021).

Encarregado, nos termos do Artigo 5º, VIII, da LGPD, é a pessoa indicada por um agente de tratamento para atuar como um canal de comunicação que medeia as relações entre controlador, titulares de dados e ANPD. A LGPD traz no Artigo 41 as responsabilidades do encarregado de proteção de dados.

Autoridade nacional, conforme o Artigo 5º, XIX, da lei, é a Autoridade Nacional de Proteção de Dados, o órgão da administração pública cuja responsabilidade é a de zelar, implementar e fiscalizar no território brasileiro o cumprimento da LGPD por todos os agentes de tratamento, sejam eles de direito público ou privado (BRASIL, 2018).

Outra definição de interesse para esta pesquisa, trazida pela LGPD no Artigo 5º, XVII, é a de relatório de impacto à proteção de dados, documento de responsabilidade controlador cujo teor “contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (BRASIL, 2018). A LGPD menciona ainda, no Artigo 10, que a ANPD pode requerer o relatório de impacto ao controlador, quando o tratamento tiver fundamento o legítimo interesse do controlador (BRASIL, 2018). Por fim, no Artigo 38, a LGPD

estabelece que a ANPD pode determinar a elaboração do relatório de impacto “inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial” (BRASIL, 2018).

Os conceitos aqui apresentados serão tratados ao longo deste estudo, tendo implicações para a conformidade legal de *startups* no desenvolvimento de software. Na próxima seção, apresenta-se o regime de proteção de dados no Brasil e suas implicações nas atividades de engenharia de software.

2.2.2 Convergências e divergências entre a LGPD e o GDPR

O GDPR substituiu a Diretiva de Proteção de Dados 95/46/CE, a fim de trazer uma abordagem mais consistente e uniformizando a regulação no âmbito da União Europeia (BIONI e MENDES, 2019). Diferentemente da diretiva, que tem caráter orientativo, a edição de um regulamento pela União Europeia tem eficácia imediata no âmbito interno dos países membros. O GDPR possui 173 considerandos (orientações interpretativas) e 99 artigos.

A LGPD, em contrapartida, foi sancionada sem que antes houvesse uma norma específica sobre proteção de dados, em que pese o Marco Legal da Internet trouxesse alguns dispositivos referentes ao tratamento de dados. Diferentemente do regulamento europeu, a lei brasileira não traz textos explicativos que permitam o aprofundamento de interpretação da norma, contendo 65 artigos.

A LGPD e o GDPR possuem convergências significativas em pelo menos três pontos importantes, no que se refere a princípios estabelecidos em ambas as normas, no modelo de proteção preventivo e na valorização do princípio de prestação de contas sobre a as atividades de conformidade (BIONI e MENDES, 2019). Ao longo dos anos houve um processo de construção internacional de consenso sobre os princípios básicos de conformidade legal, cuja função é impor limites ao tratamento de dados e trazer autonomia informativa ao titular do dado (BIONI e MENDES, 2019).

A LGPD traz no Artigo 6º, 11 princípios de tratamento de dados pessoais: (i) boa-fé; (ii) finalidade; (iii) adequação; (iv) necessidade; (v) livre acesso; (vi) qualidade dos dados; (vii) transparência; (viii) segurança; (ix) prevenção; (x) não discriminação; e (xi) responsabilização e prestação de contas (BRASIL, 2018).

O GDPR, por sua vez, apresenta no Artigo 5º, sete princípios: (i) licitude, lealdade e transparência; (ii) limitação das finalidades; (iii) minimização dos dados; (iv)

exatidão; (v) limitação da conservação; (vi) integridade e confidencialidade; (vii) responsabilidade.

Embora possuam nomenclaturas diferentes, os textos das normas guardam semelhanças. Ambos possuem o princípio da finalidade, transparência e responsabilidade.

Há outros princípios que, apesar de haver denominação diversa, apresentam correspondência conceitual. O princípio da adequação, da LGPD, corresponde ao princípio da minimização de dados, do GDPR, enquanto o princípio de qualidade dos dados, da LGPD, se assemelha ao princípio da exatidão, no GDPR. O da transparência da LGPD, tem semelhança com o princípio da licitude, lealdade e transparência do GDPR. O princípio da necessidade da LGPD, corresponde ao princípio da limitação da conservação, do GDPR. O princípio da segurança da LGPD, corresponde no GDPR ao princípio da integridade e confidencialidade. A responsabilidade e prestação de contas da LGPD guarda semelhança com o princípio da responsabilidade no GDPR.

Assim, apenas os princípios da boa-fé, da prevenção e o da não discriminação não possuem correspondência direta com os princípios estabelecidos no GDPR. Contudo, os Considerandos 71, 75 e 85 trazem chaves orientativas para se evitar discriminação de indivíduos a partir de tratamento de dados pessoais.

Pode se argumentar ainda, que há uma certa correspondência entre o princípio da boa-fé, da LGPD, com o princípio de licitude, lealdade e transparência, no GDPR, uma vez que este se refere ao dever de lealdade no tratamento de dados e o dispositivo da norma brasileira determina a boa fé no tratamento de dados pessoais. Essa visão é corroborada por Häuselmann e Custers (2024), que afirmam que o princípio da “licitude, lealdade e transparência”, do Artigo 5.1.a do GDPR, pode ser entendido como boa-fé e como forma de não trazer nenhum efeito prejudicial ao titular de dados.

Contudo, embora haja diálogo entre esses princípios, segundo Bioni e Mendes (2019), a boa-fé faz remissão a toda uma tradição do direito civil alemão, possibilitando controle de situações subjetivas a partir de parâmetros objetivos.

Essa convergência tem suas raízes nos princípios do *Fair Infomation Practice Principles*, que foram fonte de inspiração para diversas legislações, entre elas o GDPR e a LGPD (PALHARES, PRADO e VIDIGAL, 2021).

Há convergência também no que se refere ao exercício dos direitos dos titulares, previsto no GDPR no Capítulo 3 e no LGPD também no Capítulo 3. Em ambas as normas, são estabelecidos os direitos de acesso, notificação, retificação, portabilidade e cancelamento de dados pessoais (BIONI e MENDES, 2019).

Há, contudo, algumas divergências no tratamento dessa matéria pelas duas normas. Segundo Bioni e Mendes (2019) o GDPR, no Artigo 21, n. 2 e 3, apresenta uma abrangência maior do direito do titular de se opor ao tratamento de dados, ao estabelecer a possibilidade de oposição à comercialização direta de dados pessoais, previsão inexistente na lei brasileira.

A segunda divergência nessa matéria trata dos dispositivos sobre decisões automatizadas. Embora em ambas as normas estejam salvaguardados os direitos de explicação da decisão e a possibilidade de auditoria quando a decisão puder trazer potencial de discriminação, o GDPR, diferentemente da LGPD, prevê expressamente a possibilidade de revisão do processo decisório por pessoa natural (BIONI e MENDES, 2019). Embora na lei brasileira não haja essa previsão, Bioni e Mendes (2019) consideram que a interpretação da LGPD pode no futuro conduzir a um tratamento semelhante ao estabelecido pelo GDPR.

A LGPD traz no Artigo 21 um direito do titular de dados inexistente no GDPR, que trata da impossibilidade de uso de dados pessoais referentes ao exercício regular de direitos pelo titular em seu prejuízo. De outro lado, o GDPR traz no Artigo 17, o direito ao esquecimento, previsão inexistente na LGPD.

No que se refere ao modelo de proteção preventivo, tanto a LGPD quanto o GDPR preveem que o tratamento de dados pessoais pode ser realizado somente se houver uma hipótese legal de tratamento para tanto. A lei brasileira, no Artigo 7º, possui quatro bases legais a mais que o regulamento europeu apresenta no Artigo 6º, para o tratamento de dados pessoais: realização de estudos por órgão de pesquisa (Artigo 7º, IV), exercício regular de direitos em processo judicial (Artigo 7º, VI), tutela da saúde (Artigo 7º, VIII), proteção do crédito (Artigo 7º, X).

Ambas as normas estabelecem hipóteses de tratamento para dados que possuem maior sensibilidade. Na LGPD esses dados são categorizados como sensíveis e as bases legais estão inseridas no Artigo 11, enquanto no GDPR a nomenclatura utilizada é a de dados pessoais e o seu regramento está estabelecido no Artigo 9º. Embora os textos sejam diferentes há, em grande medida, convergência de significado entre eles. O Artigo 10° do GDPR traz uma previsão inexistente na

LGPD, relativa ao tratamento de dados pessoais relacionados com condenações penais e infrações, que só é permitido sob o controle de uma autoridade pública ou se autorizado pela União Europeia ou Estados-Membros.

No que se refere a segurança, ambos os diplomas legais estabelecem a necessidade de se estabelecer medidas técnicas e administrativas para a proteção de dados, inclusive desde a concepção e por padrão. O GDPR traz esse regramento no Artigo 25º e 32º, enquanto a LGPD traz dispositivos semelhantes a partir do Artigo 46.

Há semelhanças também na forma como ambas as normas tratam o tema da prestação de contas. Tanto a LGPD, em seu Artigo 38, quanto o GDPR trazem a previsão de realização de avaliação de impacto de proteção de dados, quando o tratamento puder acarretar dano a direitos fundamentais e liberdades civis. O regulamento europeu, entretanto, apresenta um detalhamento dos requisitos desse relatório, o que é inexistente na lei brasileira.

Ainda dentro do contexto da prestação de contas, ambas as normas determinam que os controladores de dados realizem o registro de todas as atividades de tratamento de dados que realizam. Novamente, o GDPR, no Artigo 30º, traz detalhes sobre quais informações devem fazer parte deste relatório, o que não ocorre na LGPD. Na visão de Bioni e Mendes (2019), o regulamento europeu traz um tratamento mais prescritivo que a LGPD, que não se ocupou de estabelecer procedimentos, relegando essa tarefa para a Autoridade Nacional de Proteção de Dados.

Por fim, importante mencionar ainda, um aspecto divergente em relação aos dois diplomas legais, referente ao uso de cookies e as hipóteses de tratamento que podem ser utilizadas para que seu uso seja lícito. Cookies são arquivos de texto que podem ser usados para facilitar a navegação de sites, os chamados cookies necessários, até para rastrear comportamentos e criar perfis de usuários (PALHARES, 2020).

Na LGPD, há a possibilidade de uso tanto da hipótese do consentimento, quanto da hipótese do legítimo interesse. Na União Europeia não é o GDPR que estabelece o regramento para uso de cookies, mas a Diretiva n° 2009/136/EC, também conhecida como Cookie Directive. A orientação dessa diretiva é a de que o uso de cookies deveria ser permitido apenas mediante o consentimento do titular, em

aviso que contenha informações claras e abrangentes, ficando de fora dessa obrigação aqueles cookies estritamente necessários para o fornecimento de serviços solicitado pelo titular do dado, ou quando necessário para a transmissão de comunicação pela Internet (PALHARES, 2020).

O nível de equivalência entre o GDPR e a LGPD ainda é uma questão em aberto. Os Artigos 33 e 34 da lei brasileira determinam que a Autoridade Nacional irá permitir a transferência internacional de dados levando em consideração as normas do país de destino, a natureza dos dados, os princípios gerais de proteção de dados e direitos dos titulares, a adoção de medidas de segurança, a existência de garantias judiciais e institucionais de respeito aos direitos de proteção de dados pessoais, entre outras circunstâncias. O GDPR traz também seu regramento a esse respeito a partir do Artigo 44º. A interoperabilidade entre os dois regimes regulatórios, entretanto, deverá levar em conta os aspectos normativos, o princípio da prestação de contas, os aspectos de corregulação, os arranjos institucionais dos países envolvidos, bem como a atuação das autoridades de proteção de dados (BIONI e Mendes, 2019).

2.2.3 A LGPD e suas implicações na engenharia de software

Ao longo desta seção o objetivo é identificar aspectos de conformidade legal que impactam no desenvolvimento de software.

A LGPD tem forte influência do GDPR (PALHARES, 2021a), o que confere ao Brasil o reconhecimento de ter uma norma rigorosa e equiparável à regulação estabelecida na União Europeia (VAINZOF, 2019). A lei brasileira apresenta 10 capítulos assim divididos: (i) Disposições Preliminares; (ii) Do Tratamento de Dados Pessoais; (iii) Dos Direitos do Titular; (iv) Do Tratamento de Dados Pessoais pelo Poder Público; (v) Da Transferência Internacional de Dados; (vi) Dos Agentes de Tratamento; (vii) Da Segurança e Boas Práticas; (viii) Da Fiscalização; (ix) Da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (x) Disposições Finais e Transitórias.

Nas disposições preliminares, a LGPD, no Artigo 1º, estabelece que o objetivo das disposições sobre o tratamento de dados, seja em meio físico ou digital, é o de proteger os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade do titular de dados.

A privacidade tem reconhecimento na Constituição Federal, no Artigo 5º, inciso X, em que trata do direito fundamental à intimidade e à vida privada, e no Artigo 5º,

inciso XII, ao tratar da inviolabilidade de dados. O conceito de privacidade no contexto atual de elevado impacto tecnológico, entretanto, vem sofrendo modificações, podendo ser compreendido como a possibilidade de conhecer, controlar e interromper fluxo de informações relativas a uma pessoa, o que conduz à ideia de o indivíduo ter o direito de controlar informações atribuídas à sua personalidade (SOUZA; MAGRANI; CARNEIRO, 2020). A LGPD, portanto, tem seu fundamento, segundo Souza, Magrani e Carneiro (2020, p. 51):

> A LGPD é fundada na autodeterminação informativa (artigo 2º, II), enquanto possibilidade de controlar os próprios dados e decidir acerca de seu uso; liberdade de expressão, de informação, de comunicação e de opinião (artigo 2º, III), respaldadas no uso seguro dos dados sob o controle de seu titular; inviolabilidade da intimidade, da honra e da imagem (artigo 2º, IV), à medida que a proteção de dados pessoais perpassa a visão objetiva de terceiros dos aspectos pessoais; e, nos direitos humanos, no livre desenvolvimento da personalidade, na dignidade e no exercício da cidadania pelas pessoas naturais (artigo 2º, VII).

A proteção de dados e a autodeterminação informativa, portanto, são praticamente sinônimos, e estão relacionadas ao direito do titular em determinar como suas informações são usadas por terceiros (SOUZA; MAGRANI; CARNEIRO, 2020).

Proteção de dados pessoais e desenvolvimento econômico, tecnológico e inovação não devem ser compreendidos como valores antagônicos, até porque esses temas são trazidos como fundamentos legais da LGPD, no Artigo 2º, inciso V. Ao conjugar os direitos dos titulares com o desenvolvimento e a inovação, a LGPD sugere uma correlação entre elas, que deve ser levada em conta no ambiente dos negócios (SOUZA; MAGRANI; CARNEIRO, 2020).

A primeira questão que se coloca trata-se de quando a lei é aplicável. O Artigo 3º da LGPD estabelece que ela incide: (i) em operações de tratamento realizadas no território nacional; (ii) quando, independentemente de onde estiver sediado o agente de tratamento, a atividade de tratamento tiver o objetivo de fornecer bens ou serviços em território nacional ou de tratar dados de indivíduos localizados no Brasil; (iii) ou quando os dados forem coletados no país.

A segunda questão é se há exceções para sua aplicação. As hipóteses de exceções de aplicação encontram-se no Artigo 4º da lei, entre elas, quando realizado por pessoa natural para fins particulares e não econômicos; quando exclusivamente para fins jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão penal.

Os aspectos referentes à aplicação e à exceção de aplicação da LGPD são relevantes para que desenvolvedores avaliem em que circunstâncias deverão levar em conta a conformidade de proteção de dados em suas atividades.

Um terceiro ponto a ser levado em consideração é que a LGPD, assim como o GDPR, é uma norma de base principiológica que orienta as atividades de tratamento de dados pessoais. No Artigo 6°, a lei brasileira determina que as atividades de tratamento precisam respeitar o princípio da boa-fé, além de dez outros: (i) finalidade; (ii) adequação; (ii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação; (x) responsabilização e prestação de contas.

Alguns estudos de engenharia de software no âmbito do GDPR (FELTUS *et al.* 2017, LI *et al.*, 2020) utilizam princípios do regulamento europeu para construir modelos ou artefatos de apoio a atividades de desenvolvedores para conformidade legal em segurança de privacidade. Abordagens como a de Li *et al.* (2020), que consideram a conformidade a partir dos princípios do GDPR com vistas a implementação de requisitos não-funcionais, entretanto, cumprem apenas parcialmente o propósito de adequação. Abordagens dessa natureza não são apropriadas porque a conformidade em proteção de dados necessita de cumprimento de requisitos funcionais e não funcionais (RINGMANN; LANGWEG; WALDVOGEL, 2018, KNEUPER, 2020).

Um quarto ponto a ser analisado trata-se das hipóteses que permitem o tratamento de dados pessoais. Esse tema é regulado no Capítulo II da LGPD, em que se apresenta não só quando os dados pessoais poderão ser tratados, mas também as prescrições a serem seguidas no término do tratamento.

A LGPD traz duas categorias de dados pessoais – dados pessoais, dados sensíveis – para os quais define diferentes conjuntos de hipóteses de tratamento de dados. Também chamadas de bases legais, as hipóteses de tratamento encontram-se descritas: (i) no Artigo 7º, as dez bases legais que fundamentam o tratamento de dados pessoais; (ii) no Artigo 11, as oito hipóteses de tratamento de dados pessoais sensíveis; (iii) no Artigo 14, as prescrições para o tratamento de dados de crianças e adolescentes.

As bases legais para dados pessoais que constam no Artigo 7º da LGPD são: (i) consentimento; (ii) cumprimento de obrigação legal; (iii) execução de políticas públicas; (iv) estudos de órgãos de pesquisa; (v) execução de contrato; (vi) exercício

regular de direitos; (vii) proteção da vida ou da incolumidade física; (viii) tutela da saúde; (ix) interesse legítimo; (x) proteção do crédito.

As hipóteses de tratamento para dados sensíveis, que constam no Artigo 11 da LGPD são: (i) consentimento; (ii) cumprimento de obrigação legal; (iii) execução de políticas públicas; (iv) estudos por órgãos de pesquisa, anonimizando os dados sempre que possível; (v) exercício regular de direitos, inclusive em contrato; (vi) proteção da vida ou da incolumidade física; (vii) tutela da saúde; (viii) prevenção a fraudes e segurança.

Além dessas duas categorias de dados, a LGPD traz normas adicionais no que tange a crianças e adolescentes. No caso de tratamento de dados pessoais de crianças, a lei estabelece que o controlador tem o dever de coletar o consentimento dos pais ou responsáveis, conforme o Artigo 14, §1º, necessitando ainda estabelecer medidas para comprovar a coleta do aceite, nos termos do Artigo 14, §5º. O objetivo desta norma, segundo Palhares, Prado e Vidigal (2021), foi o de coibir a coleta direta de dados de crianças sem que houvesse consentimento assistido, no intuito de afastar ilegalidades, uma vez que o menor tem capacidade reduzida quando em relação com adultos para entender o impacto de fornecimento de dados pessoais. Nesse sentido também, a regra do Artigo 14, §4º, que impacta diretamente em modelos de negócio, ao estabelecer que controladores devem requerer apenas as informações estritamente necessárias de crianças quando da participação de jogos, aplicações de internet ou outras atividades.

O tratamento de dados de crianças pode vir a sofrer modificações ao longo dos próximos anos, seja por conta do debate que vem sendo realizado no campo teórico (PALHARES; PRADO; VIDIGAL, 2021, VIDIGAL, 2021), seja por decisões judiciais ou eventuais alterações legislativas. Em estudo recente, Vidigal (2021) propõe que todas as demais bases legais possam ser utilizadas no tratamento de dados de crianças, com a hipótese de consentimento, tendo regramento especial a ser seguido nos termos do Artigo 14 da LGPD. Em 2023, a ANPD publicou enunciado em que afirma que o tratamento de dados de crianças e adolescentes podem ser realizados com fundamento nas hipóteses de tratamento previstas no Artigo 7º ou no Artigo 11, não

ficando restrito à base legal do consentimento, desde que observado o melhor interesse, a ser avaliado no caso concreto[4].

A base legal do consentimento tende a trazer questões de interesse para o campo da engenharia de software não somente por conta das regras estabelecidas para o tratamento de dados de criança. O Artigo 8º, a LGPD traz uma série de regras que devem ser seguidas quando for usada a hipótese do consentimento, que é definido, no Artigo 2º, XII, como manifestação livre, informada e inequívoca do titular dos dados em concordância com o tratamento que será realizado. O Artigo 8º da LGPD determina que o consentimento seja destacado das demais cláusulas contratuais quando fornecido por escrito, devendo ser informadas as finalidades específicas para os quais serão tratados. A lei estabelece ainda, que o controlador consiga provar o consentimento sempre que for necessário e, em caso de o titular retirá-lo, o que pode acontecer a qualquer tempo, este deve ser informado das consequências dessa retirada.

Para se notar as implicações do consentimento na atividade de engenharia de software, basta imaginar o exemplo de uma aplicação digital que colete o consentimento para tratamento de dados marketing – diversos cuidados terão de ser levados em consideração no desenvolvimento, seja em atividades como a função de coleta, que deverá ser clara, ostensiva, inequívoca, ao ser informada ao titular, seja em função da necessidade de um sistema que permita o arquivamento seguro dessas informações para eventual demonstração de conformidade perante à Autoridade Nacional de Proteção de Dados ou ao Poder Judiciário.

O quinto ponto que traz implicações para a engenharia de software se refere à própria operação de tratamento a ser realizada. Segundo Palhares, Prado e Vidigal (2021), não basta ao agente de tratamento definir qual base legal que o permite realizar uma determinada atividade. É necessário que o tratamento ocorra respeitando os princípios: (i) da boa-fé (tratamento justo ético); (ii) finalidade (fins legítimos, específicos, explícitos e informados ao titular); (iii) adequação (tratamento compatível com a finalidade informada ao titular); (iv) necessidade (uso do mínimo de dados necessários); (v) transparência (dever de prestar informações claras, precisas e

[4] ANPD. Enunciado CD/ANPD nº 1. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em: 22.08.2024.

acessíveis); (vi) responsabilização e prestação de contas (o agente necessita demonstrar que está em conformidade) (PALHARES; PRADO; VIDIGAL, 2021).

O sexto ponto de atenção está no Artigo 9º da LGPD, que estabelece o direito de o titular de ter acesso fácil, claro, adequado e ostensivo a respeito de informações sobre como o tratamento de seus dados é realizado, quais finalidades, sua forma e duração, além de ser informado sobre os seus direitos (previstos no Artigo 18 da lei), bem como sobre quem está realizando o tratamento de dados. O referido artigo concretiza o princípio da transparência e pode ter como consequência o uso de técnicas de experiência do usuário, para que as informações sejam prestadas de forma clara, adequada e ostensiva. No âmbito do GDPR, destaca-se estudo de Ataei, Degbelo e Kray (2018), que propõe uma interface de usuário que permite um maior senso de controle da privacidade no uso de dados de geolocalização.

O sétimo ponto refere-se às prescrições que devem ser seguidas no caso de o controlador utilizar a hipótese do legítimo interesse para o tratamento de dados. Previsto no Artigo 10 da LGPD, essa base legal somente pode fundamentar dados pessoais para finalidades legítimas, a partir de situações concretas, somente usando dados estritamente necessários e adotando medidas de transparência.

Neste caso as implicações para a engenharia de software podem ser: (i) necessidade de que o software a ser desenvolvido utilize somente o conjunto estritamente necessário de dados; (ii) adoção de medidas que deem transparência ao titular de dados sobre quais dados são usados, como e para que finalidades são tratados.

O oitavo ponto a ser analisado trata das prescrições sobre o término do tratamento de dados previstas nos Artigos 15 e 16 da LGPD. Ambos os artigos podem implicar em necessidades a serem levadas em consideração nas atividades de desenvolvimento de software, no que tange à eliminação, armazenamento ou anonimização de dados.

O Artigo 15 da lei determina as hipóteses de término de tratamento: (i) quando a finalidade é alcançada, ou os dados deixaram de ser necessários ou pertinentes para o objetivo desejado; (ii) ao fim do período de tratamento; (iii) comunicação do titular, o que inclui o exercício de revogação do consentimento; (iv) decisão da Autoridade Nacional de Proteção de Dados, em caso de violação da LGPD.

O Artigo 16 da LGPD determina que os dados pessoais sejam eliminados após o término do tratamento. Entretanto, o referido dispositivo autoriza que os dados

possam permanecer armazenados para atender as finalidades de: (i) cumprir obrigação legal ou regulatória; (ii) desenvolvimento de estudo por órgão de pesquisa; (iii) transferir a terceiro; (iv) uso exclusivo do controlador desde que os dados sejam passados por um processo de anonimização.

O nono ponto trata dos direitos dos titulares, previstos no Capítulo III da lei e dispostos nos Artigos 17 a 22. O Artigo 18 traz um rol de direitos que os titulares podem exercer em sua relação com o controlador de dados, solicitando, entre outras coisas: (i) a confirmação de existência de tratamento, (ii) o acesso aos dados; (iii) a correção de dados que estejam incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; (v) a portabilidade dados para uso com outro fornecedor; (vi) eliminação de dado pessoais tratados com fundamento no consentimento; (vii) informar a possibilidade de não fornecimento de consentimento e as consequências da negativa; (viii) revogação do consentimento.

A correção de dados incompletos, inexatos ou desatualizados, bem como a portabilidade, por exemplo, podem resultar em decisões de desenvolvimento de software para atingir a conformidade legal de proteção de dados.

O Artigo 19, da LGPD prescreve que as solicitações do titular de dados referentes à confirmação de existência de tratamento, bem como ao acesso dos dados devem ser respondidas de imediato quando em formato simplificado e por meio de documentação completa indicando origem dos dados, critérios usados e finalidade de tratamento em até quinze dias a partir da requisição. Já o Artigo 19, §1º estabelece que os dados devem ser armazenados em formato que facilite o direito de acesso previsto. Esse dispositivo pode ter algum impacto no desenvolvimento de software, de modo que a extração de dados possa ser facilitada.

O Artigo 20 estabelece que o titular tem direito de requerer que decisões automatizadas de dados pessoais sejam revisadas, quando isso puder afetar seus interesses, o que inclui decisões que façam a definição de seu perfil, seja pessoal, profissional, de consumo, crédito ou de aspectos relativos à sua personalidade. O parágrafo §1 do Artigo 20 determina que o controlador forneça ao titular, sempre que houver uma solicitação, informações claras e adequadas sobre critérios e procedimentos usados para a realização de decisões automatizadas.

No contexto da conformidade do GDPR na engenharia de software, Altorbaq, Blix e Sörman (2018) chamam a atenção para a necessidade de os controladores

cumprirem com suas obrigações perante os titulares, que devem ter mecanismos para fazerem valer os seus direitos, bem como compreenderem o que eles significam e quais riscos de violação existem.

Os capítulos IV e V da LGPD possuem, na visão do pesquisador, menor interesse para a presente pesquisa. O Capítulo IV da LGPD, entre os Artigos 23 e 32, traz regras para o tratamento de dados pessoais pelo poder público. Aqui destaque-se o disposto no Artigo 25, que menciona a necessidade de manter os dados em formato que garanta a interoperabilidade para uso compartilhado na execução de políticas públicas, o que implica em decisões de arquitetura para satisfazer a prescrição normativa.

O Capítulo V, entre os Artigos 33 e 36, apresenta as normas sobre transferências internacionais. Menção deve ser feita ao Artigo 33, que somente permite transferência internacional para países com nível de proteção semelhante ao da LGPD, bem como ao Artigo 34, que detalha o grau de proteção, levando em conta a adoção de medidas de segurança previstas na norma brasileira, entre outros pontos.

O décimo ponto a ser analisado está inserido no Capítulo VI, que, nos Artigos 37 a 45, apresenta deveres e responsabilidades dos agentes de tratamento e do encarregado de dados. As preocupações da LGPD com o impacto que de violações de dados pessoais são demonstradas ao tratar do relatório de impacto à proteção de dados, conforme já conceituado na Seção 2.2.1, e que é mencionado no Artigo 38 da lei.

Pelo referido dispositivo legal, controlador tem o dever de documentar em relatório de impacto à proteção de dados, quando exigido pela ANPD, os tipos de dados coletados, método de coleta e para garantir segurança de informação, bem como a avaliação feita sobre medidas de salvaguarda e mitigação de risco adotados.

Embora a LGPD não traga uma lista para operações de tratamento que sejam consideradas inerentemente de risco e que devam ser inseridas em um relatório de impacto, no âmbito do GDPR o *Working Party* 29, traz nove critérios que podem contribuir para a discussão no contexto da legislação brasileira (ARTICLE 29 WORKING PARTY, 2016): (i) avaliação ou *scoring*; (ii) decisões automatizadas com efeitos significativos sobre direitos; (iii) monitoramento sistemático; (iv) tratamento em larga escala; (v) uso de dados sensíveis ou de elevada criticidade; (vi) tratamento de dados de titulares em condição de vulnerabilidade; (vii) uso de tecnologia inovadora;

(viii) cruzamento ou combinação de bases de dados; (tratamento que possa impedir exercício de direito ou acesso a produtos e serviços.

Em análise desses nove critérios de atividade de risco, Palhares Prado e Vidigal (2021a) apresentam as considerações descritas no Quadro 2-5.

Quadro 2-5. Análise de critérios para avaliação de impacto da LGPD. Adaptado de PALHARES; PRADO; VIDIGAL, 2021.

CRITÉRIOS	ANÁLISE
Avaliação ou *scoring*	O tratamento é de risco, pois consiste na criação de perfis individualizados dos titulares de dados, que podem dar ensejo a decisões que afetam de maneira mais significativa a esfera de privacidade
Decisões automatizadas que afetem de modo significativo os titulares	O tratamento guarda risco, já que pode conduzir à exclusão ou discriminação indevida de indivíduos
Monitoramento sistemático	O tratamento importa em risco, pois pode envolver a coleta de dados em circunstâncias em que o titular não tem expectativa ou ciência de que isso ocorre ou, mesmo que tenha essa expectativa, não há como evitar
Utilização de dados sensíveis ou de alto impacto em direitos fundamentais	O tratamento revela risco aumentado, diante da importância e sensibilidade dos dados utilizados
Tratamento em ampla escala	O tratamento importa risco, considerado o elevado número de titulares envolvidos, volume dos dados tratados, tempo de duração e extensão geográfica da atividade
Combinação ou cruzamento de bases de dados	O tratamento é de risco, já que possibilita maior grau de utilização de dados para fins secundários, não originalmente traçados, em ameaça ao princípio da finalidade.
Tratamento de titulares vulneráveis	O tratamento é de risco, já que os titulares de dados figuram em situação de impotência face ao agente de tratamento, o que prejudica a capacidade de exercício de direitos e controle sobre o fluxo informacional.
Emprego de soluções tecnológicas ou organizacionais inovadoras	O emprego de nova tecnologia, ou de tecnologia conhecida para um novo propósito apresenta risco, pois pode envolver novas formas de coleta e utilização de dados pessoais, com impactos imprevisíveis aos titulares de dados
Tratamento que impeça exercício de direito ou obste acesso a serviço e produtos	O tratamento capaz de produzir os efeitos destacados detém riscos elevados, à medida em que geram consequências significativas na esfera de direitos e liberdades dos titulares de dados

Palhares, Prado e Vidigal (2021) consideram que é o risco da atividade de tratamento e não a base legal utilizada que determinam a exigência do relatório de impacto. Isso porque, conforme já observado na Seção 2.2.1, a própria definição do relatório de impacto à proteção de dados pessoais menciona que deverão estar descritos os “processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais” (Brasil, 2018).

Acrescente-se, o GDPR é omisso no que se refere à avaliação e gerenciamento de risco e à probabilidade, apresentando apenas elementos referentes ao impacto

sobre direitos (Gellert, 2018). Por essa razão, no âmbito europeu, documentos como o do *Working Party* 29, que comentam aspectos do GDPR adquirem relevância.

O décimo primeiro ponto a ser considerado está inserido no Capítulo VII, que trata de segurança e boas práticas, o que envolve segurança de informação e governança. A LGPD determina no Artigo 46 que os agentes de tratamento adotem "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" (Brasil, 2018).

A lei não especifica, entretanto, quais devem ser essas medidas, limitando a estabelecer: (i) no Artigo 46, §1º, que a ANPD pode apresentar padrões mínimos a serem adotados, levando em conta a natureza dos dados e do tratamento, o contexto da tecnologia, principalmente quando se tratar de dados sensíveis; e (ii) no Artigo 46, §2º, os procedimentos tomados para garantir a segurança devem ser observados "desde a fase de concepção do produto ou do serviço até a sua execução" (Brasil, 2018).

Jimene (2019, p. 333) afirma que por medidas técnicas entende-se "aquelas adotadas no âmbito da Tecnologia da Informação, com o uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação". Assim, portanto, estariam incluídas ferramentas de autenticação de acesso, mecanismos de segurança para softwares e hardwares, controle de tráfego de rede, criptografia, testes de vulnerabilidade, cópias de segurança, entre outras medidas (Jimene, 2019).

As medidas administrativas, de outro lado, são aquelas de gestão administrativa, o que inclui as relativas ao direito, como políticas corporativas, contratos e cláusulas de confidencialidade, avisos de privacidade, treinamento de colaboradores, entre outras (Jimene, 2019). Dado o caráter técnico e administrativo, Jimene (2019) considera que se deve avaliar riscos operacionais na implementação de controles, bem como adotar "processos internos, controles tecnológicos, políticas corporativas, regulamentos, contratos, que terão por missão precípua a proteção dos dados pessoais que estejam sob sua custódia" (Jimene, 2019, p. 334).

O Artigo 47 da LGPD determina que tanto o controlador quanto o operador devem garantir a segurança da informação em relação aos dados pessoais mesmo após o término do tratamento realizado. O tema segurança da informação atualmente é norteado pelas Normas Técnicas ISO/IEC 27001:2022, ISO/IEC 27002:2022 e

ISO/IEC 27701:2019. A primeira delas, apresenta os requisitos do Sistema de Gestão de Segurança da Informação, a segunda traz boas práticas para controle de segurança da informação, enquanto a terceira propõe recomendações específicas sobre dados pessoais e estabelece diretrizes para um sistema de gerenciamento de privacidade.

Em comentário às medidas de segurança, técnicas e administrativas mencionadas no Artigo 46 e sobre o dispositivo do Artigo 47 da LGPD, Jimene (2019) afirma que o objetivo delas é o mesmo que sustenta “os pilares da Segurança da Informação (confidencialidade, disponibilidade e integridade)” (Jimene, 2019, p. 345). Segurança da Informação, portanto, tem contribuição importante para a conformidade legal de proteção de dados.

O Artigo 49 da referida lei, por sua vez, determina que os sistemas usados para tratamento de dados sejam estruturados levando em conta requisitos de segurança, padrões de boas práticas e de governança. Jimene (2019) afirma que dado o caráter genérico e abrangente desse dispositivo da lei é necessário fazer uma interpretação restritiva, a fim que os “requisitos de segurança” sejam entendidos “a aptos proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito” (Jimene, 2019, p. 354). Além disso, segundo Jimene (2019), padrões de boas práticas e de governança podem ser entendidos aqueles mencionados das normas ISO já citadas, bem como métodos de *Privacy by Design* e instrumentos de governança corporativa.

O *Privacy by Design* apresenta princípios para uma organização desenvolver atividades que levem em consideração a privacidade desde o início do projeto bem como ao longo de todas suas etapas (Cavoukian et al. 2014). Os princípios do Privacy by Design propostos por Cavoukian (2009) são: (i) Proativo, não reativo; Preventivo, não corretivo; (ii) Privacidade como padrão; (iii) Privacidade incorporada ao design; (iv) Funcionalidade total - Soma positiva, não soma zero; (v) Segurança de ponta a ponta - Proteção do ciclo de vida; (vi) Visibilidade e Transparência; e (vii) Respeito pela privacidade do usuário. Há, entretanto, uma ausência de pesquisas consistentes e boas práticas validadas para a engenharia de software na área de *Privacy by Design* (Morales-Trujillo *et al.*, 2019).

Trabalho recente propõe um processo de desenvolvimento de software para auxiliar equipes na implementação dos sete princípios do *Privacy by Design*,

colocando a proteção de dados pessoais como requisito fundamental, desde as etapas iniciais do desenvolvimento. (ANDRADE, 2024). O estudo apresenta também um repositório de instâncias de padrões de privacidade, cujo objetivo é auxiliar profissionais de desenvolvimento de software a compreender padrões de privacidade, com base em exemplos concretos.

Por fim, no que tange a boas práticas e governança, o Artigo 50, §1º, da LGPD prescreve que ao estabelecer regras de boas práticas, os agentes de tratamento precisam levar em conta, “em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular”. Além disso, a norma determina no Artigo 50, §2º, a necessidade de, na aplicação dos princípios de segurança e de prevenção, o controlador deve avaliar estrutura, escala, volume de operações, sensibilidade dos dados, assim como probabilidade e gravidade dos danos que eventualmente poderiam atingir os titulares de dados.

Ambos os dispositivos trazem critérios para que agentes de tratamento possam avaliar o rigor das medidas a serem tomadas, que devem levar em conta critérios como probabilidade e gravidade do risco, probabilidade e gravidade do dano, sensibilidade dos dados tratados, natureza do tratamento, estrutura, escala e volume de operações.

Ao lado das nove operações de tratamento que são consideradas de risco e que condicionam a elaboração de relatório de impacto no GDPR, conforme o Working Party 29 (2016) e mencionados quando da análise do Artigo 38 da LGPD, os critérios estabelecidos no Artigo 50, §1º e §2º da lei podem ser relevantes para análise de risco em proteção de dados nas práticas de engenharia de software.

O Capítulo VIII, nos Artigos 52 a 54, traz as penalidades administrativas que podem ser aplicadas aos agentes de tratamento em caso de descumprimento da LGPD. Nesse capítulo encontra-se um dos principais motivos para empresas buscarem a conformidade legal em proteção de dados, que é o de evitar multas (NORVAL *et al.*, 2021, MARTIN *et al.*, 2019).

O Artigo 52 da lei prevê sanções que vão da mera advertência e prazo para adotar medidas corretivas, até multa de até 2% do faturamento, podendo atingir o valor máximo de R$ 50 milhões por infração, ou mesmo, a proibição parcial ou total do exercício de atividades relativas à proteção de dados. O Artigo 52, §1º, traz os

critérios para a aplicação de penalidades após processo administrativo (BRASIL, 2018):

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Alguns dos parâmetros elencados na LGPD para avaliar a aplicação de sanções podem impactar na tomada de decisão em engenharia de software, em especial: (i) gravidade e natureza das infrações dos direitos afetados; (ii) o nível do dano; (iii) implantação de práticas internas que minimizem o dano; (iv) implementação de boas práticas e governança; (v) implementação de medidas corretivas; (v) sanção proporcional à gravidade da falta.

Na visão deste pesquisador, os critérios estabelecidos na LGPD para avaliar as penalidades administrativas a serem aplicadas ao caso concreto são úteis ao processo de tomada de decisão de atividades de engenharia de software. Isso porque oferecem critérios que podem ser levados em conta ao estabelecer não só os riscos, mas por ser orientativo sobre quais medidas tomadas podem minimizar eventuais punições da ANPD.

O Artigo 52, §2º, da LGPD faz a ressalva, entretanto, de que as punições pela ANPD não são substitutivas de outras penalidades, sejam elas administrativas, civis

ou penais previstas no Código de Defesa do Consumidor ou em legislações específicas. Em análise do referido dispositivo, Alves (2019) explica se tratar de norma que determina “que eventual penalidade aplicada por violação de normas de proteção e dados não confere nenhum grau de isenção ou imunidade ao agente infrator, quando a mesma conduta também violar outros instrumentos legais do ordenamento jurídico” (Alves, 2019, p. 388).

O Capítulo IX, apresenta os dispositivos sobre a criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, temas que não requerem exame detalhado para fins desta pesquisa, à exceção do dispositivo do art. 55-J, XVIII. O referido artigo permite à ANPD editar normas e procedimentos simplificados para pequenas empresas e *startups*, o que deve ocorrer em algum momento em futuro próximo.

Por fim, o Capítulo X traz as disposições finais e transitórias da lei. Merece destaque o Artigo 63 da lei, que prevê a possibilidade de a ANPD estabelecer normas de adequação progressiva dos bancos de dados anteriores à vigência da LGPD, que teriam um prazo diferenciado para a adequação legal. No entanto, até o momento não houve regulamentação desse dispositivo pela ANPD.

2.2.4 A Resolução CD/ANPD nº 2 de 2022

Em 27 de janeiro de 2022, a Autoridade Nacional de Proteção de Dados aprovou a Resolução CD/ANPD nº 2, a fim de regular a LGPD para agentes tratamento de pequeno porte. O regulamento, em seu artigo 2º, define agentes de tratamento de pequeno porte vários agentes, entre eles, *startups*.

A Resolução CD/ANPD nº 2 apresenta em seu Artigo 2º, III, também, a definição de *startups*:

> organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021. (Brasil, 2022)

Note-se que o regulamento menciona que, para ser considerada *startup* e obter os benefícios de tratamento diferenciado destinado às empresas de pequeno porte, é preciso que a organização cumpra os requisitos que a Lei Complementar n° 182 de 2021 traz em seu Capítulo II. A referida lei apresenta, no Artigo 4º, os requisitos necessários para o enquadramento de empresas como *startups*:

> Art. 4º São enquadradas como startups as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.
>
> § 1º Para fins de aplicação desta Lei Complementar, são elegíveis para o enquadramento na modalidade de tratamento especial destinada ao fomento de startup o empresário individual, a empresa individual de responsabilidade limitada, as sociedades empresárias, as sociedades cooperativas e as sociedades simples:
>
> I - com receita bruta de até R$ 16.000.000,00 (dezesseis milhões de reais) no ano-calendário anterior ou de R$ 1.333.334,00 (um milhão, trezentos e trinta e três mil trezentos e trinta e quatro reais) multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 (doze) meses, independentemente da forma societária adotada;
>
> II - com até 10 (dez) anos de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Secretaria Especial da Receita Federal do Brasil do Ministério da Economia; e
>
> III - que atendam a um dos seguintes requisitos, no mínimo:
>
> a) declaração em seu ato constitutivo ou alterador e utilização de modelos de negócios inovadores para a geração de produtos ou serviços, nos termos do inciso IV do caput do art. 2º da Lei nº 10.973, de 2 de dezembro de 2004; ou
>
> b) enquadramento no regime especial Inova Simples, nos termos do art. 65-A da Lei Complementar nº 123, de 14 de dezembro de 2006. (Brasil, 2021)

Para fins de ser enquadrada como *startup* e poder receber tratamento diferenciado, portanto, a empresa precisa ter receita bruta até R$ 16 milhões por ano, ter até no máximo dez anos de inscrição no Cadastro Nacional de Pessoa Jurídica, além de atender ao menos um dos seguintes requisitos: (i) ter em seu ato constitutivo a declaração de que usa modelo de negócio inovador para a geração de produtos ou serviços; (ii) ou estar enquadrada no Inova Simples, o regime especial simplificado que facilita a abertura de negócios inovadores.

Uma vez cumprindo esses requisitos, e, portanto, sendo enquadrada como *startup*, a resolução permite que a empresa tenha os seguintes benefícios em relação à aplicação da LGPD:

I. Registro de atividades pode ser feito de forma simplificada.
II. Dispensa a obrigação de indicar o encarregado de dados, porém, deve oferecer um canal de comunicação com o titular de dados.

III. Pode estabelecer medidas administrativas e técnicas essenciais e necessárias, com requisitos mínimos de segurança de informação, desde que considere o nível de risco à privacidade dos titulares.

IV. Pode estabelecer política simplificada de segurança de informação que contemple requisitos essenciais e necessários para o tratamento de dados, a fim de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

V. Prazos administrativos da ANPD devem ser contados em dobro.

Importante mencionar que, conforme estabelece o art. 6º da Resolução nº 2 da ANPD, o regime mais benéfico do regulamento da ANPD não isenta os agentes de tratamento de pequeno porte das demais obrigações da LGPD.

Entretanto, os benefícios da Resolução AC/ADPD nº 2, conforme o Artigo 3º, não poderão ser concedidos: (i) em caso de realização de tratamento de dados de alto risco para os titulares; ou (ii) se a startup fizer parte de grupo econômico que em seu conjunto obtenha receita superior a R$ 16 milhões por ano.

A primeira hipótese é importante de ser examinada, porque a resolução traz definição de tratamento de alto risco no artigo 4º:

> Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
>
> I - critérios gerais:
>
> a) tratamento de dados pessoais em larga escala; ou
>
> b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
>
> II - critérios específicos:
>
> a) uso de tecnologias emergentes ou inovadoras;
>
> b) vigilância ou controle de zonas acessíveis ao público;
>
> c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
>
> d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

> § 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.
>
> § 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. (Brasil, 2022)

Ou seja, a *startup* perde os benefícios incluídos na Resolução nº 2, caso realize tratamento de dados pessoais em larga escala ou o tratamento possa afetar interesses e direitos dos titulares de forma significativa, e, ao mesmo tempo, se refira a uso de tecnologia inovadora, ou de vigilância e controle em área pública, ou seja, realizado tratamento automatizado de dados para definição de perfis, ou ainda, sejam usados dados pessoais sensíveis, de crianças ou de idosos.

Apesar de o regime diferenciado de tratamento de dados para agentes de pequeno porte reduzir algumas obrigações trazidas pela LGPD, a Resolução nº 2 permite a ANPD afastar a aplicação do regulamento, ao avaliar circunstâncias concretas, levando em conta a natureza, o volume das operações ou os riscos para os titulares.

Na próxima seção apresenta-se revisão de literatura referente ao tema de conformidade legal de proteção de dados.

2.3 Conformidade legal de proteção de dados

A maioria dos estudos de conformidade legal em proteção de dados na engenharia de software são realizados no âmbito do GDPR, o regulamento europeu aprovado em 2016 e que passou a vigorar a partir de maio de 2018. Nesse contexto, a privacidade tem sido compreendida como um espaço pessoal ou relacional, físico ou virtual, que quando violado resulta em alguma forma de dano físico, financeiro, reputacional ou psicológico (BACHLECHNER; LIESHOUT; TIMAN, 2019). A proteção de dados, então, tem sua atenção voltada para procedimentos, como análise de risco e comunicação aos titulares sobre os dados que estão sendo tratados (BACHLECHNER; LIESHOUT; TIMAN, 2019). Segundo Bachlechner, Lieshout e Timan (2019), o GDPR trata não somente de questões procedimentais acerca da proteção de dados, mas de aspectos como avaliação de risco, em que se requer

análise, identificação e tomada de medidas de privacidade necessárias, bem como avaliação de impacto de proteção de dados pessoais, que possam violar direitos fundamentais dos titulares.

Estudo de GELLERT (2018) demonstra que muitos dos elementos constitutivos da noção de risco estão consagrados no GDPR, em especial aqueles referentes ao impacto, mas não necessariamente os que tratam da probabilidade. Além disso, afirma GELLERT (2018), o GDPR é omisso a respeito da forma que se deve realizar a avaliação e o gerenciamento de risco.

Segundo Martin *et al.* (2019) as normas de proteção de dados atuais têm como primeira finalidade a segurança de Tecnologia de Informação, em segundo lugar, o controle dos processos de tratamento, em terceiro, garantir os direitos dos titulares e, por fim, estabelecer medidas organizacionais e de processamento. O GDPR e as leis dos Estados Nacionais europeus definem também regras para tratamento de dados pessoais, com a finalidade de proteger os titulares de duas ameaças – a primeira, violação de dados promovida por criminosos ou indivíduos desonestos que fazem parte da empresa controladora; a segunda, tratamento ilegal de dados realizado pela organização controladora (MARTIN *et al.*, 2019).

Andrade *et al.* (2023) investigaram, por meio de um estudo de caso múltiplo com cinco organizações, como organizações integram a proteção de dados pessoais em seus processos de desenvolvimento de software. A pesquisa identificou que as questões de proteção de dados são abordadas em estágios posteriores do processo de desenvolvimento. Essa descoberta tem relevância, uma vez que contradiz com o que determina a LGPD e o GDPR (ANDRADE *et al.*, 2023). Os pesquisadores sugerem que tal fato pode ser atribuído à falta de especialistas da área na composição de equipes de desenvolvimento e à ausência de incentivos para treinamento em proteção de dados.

Importante ponderar, entretanto, que requisitos não funcionais nem sempre são definidos em tempo de desenvolvimento. Viviani *et al.* (2023) realizaram pesquisa com 40 profissionais de desenvolvimento de software que identificou que requisitos não funcionais geralmente são definidos após a entrega de software. Além disso, segundo os pesquisadores, podem ser incertos e mudar com frequência, o que exige abordagens ágeis para evoluir a arquitetura de software, que deve levar em conta essa incerteza.

Outra descoberta relevante de Andrade *et al.* (2023) é que os desenvolvedores não diferenciam privacidade de segurança. No campo da conformidade de proteção de dados, entretanto, os conceitos são diversos. A segurança de informação faz parte da conformidade legal de proteção de dados. Há diversos requisitos de conformidade, entretanto, que não dizem respeito à segurança de informação, mas tratam de normas para assegurar o direito de privacidade e de proteção de dados.

Em linha complementar ao estudo de Andrade *et al.* (2023), pesquisa de Peixoto *et al.* (2023) indica que muitos desenvolvedores não possuem conhecimento suficiente para desenvolver softwares que assegurem a proteção de dados. De acordo com os estudos, desenvolvedores estão mais preocupados com segurança de informação que com outros aspectos de privacidade, utilizando estratégias para lidar com segurança de dados.

Breaux e Norton (2022) afirmam que falhas de conformidade resultam em erros técnicos de projeto e que há grande lacuna entre experiência técnica e a cultura de analistas jurídicos e engenheiros de software. Além disso, afirmam os pesquisadores, há prioridades concorrentes entre requisitos legais e objetivos de negócio, razão pela qual eles propõem que a conformidade legal seja uma atividade de design principal, em que advogados e engenheiros de software utilizem métodos e ferramentas adequados para preencher a lacuna cultural e de conhecimento.

Breaux e Norton (2022) propõem uma nova qualidade de software, que denominam como "*Legal Accountability*", e que pode ser avaliada conjuntamente com outras qualidades, como usabilidade, modificabilidade, desempenho e teste. A "*Legal Accountability*" abrangeria cinco propriedades: (i) rastreabilidade legal; (ii) integridade; (iii) validade; (iv) auditabilidade; e (v) continuidade.

Conformidade legal de proteção de dados pode, portanto, ser compreendida como um aspecto da qualidade do software.

Koolen et al. (2024) afirmam que medidas de segurança devem ser adaptadas e dimensionadas de acordo com o tamanho e o escopo das atividades da organização. Essas medidas, segundo os pesquisadores, devem resistir ao teste do tempo, de forma que um sistema não deve ser seguro apenas quando é colocado no mercado, mas deve persistir em segurança durante o seu ciclo de vida. Por essa razão, afirmam Koolen et al. (2024), é necessário revisar e atualizar de forma periódica as medidas de segurança. Conformidade legal de proteção de dados, portanto, pode ser

compreendida não só como um aspecto da qualidade do software, mas como algo a ser perseguido de forma contínua.

Alguns estudos sugerem uso de artefatos ou modelos para atender a aspectos de conformidade legal de proteção de dados. Pesquisa recente de Saraiva e Soares (2023), com 34 estudantes de graduação, analisou a possibilidade de uso de inventário de dados pessoais – documento em que se registra todas as operações de tratamento de dados realizado por uma organização – para a criação de histórias de usuários. Segundo Saraiva e Soares (2023), o experimento permitiu concluir que o inventário de dados pessoais pode ser usado na área de engenharia de requisitos como ferramenta para compreender e especificar um software, a fim de garantir aspectos de conformidade de proteção de dados.

Estudo de Olca *et al.* (2022) sugere um modelo para estabelecer preferências de privacidade dos dados pessoais, para garantir o processo de consentimento. Eles propõem um modelo genérico para consentimento que tem o objetivo de controlar e gerenciar o consentimento dado por um titular de dados.

Tsiodra *et al.* (2023) propõem uma estrutura de apoio à decisão de segurança cibernética que leva em consideração o custo de uma violação de segurança, para em seguida comparar estratégias de investimentos em medidas de mitigação. A proposta adota uma abordagem de fluxo de caixa descontado para modelar e avaliar o risco de ataques cibernéticos.

Esta seção é subdividida em quatro partes. A primeira traz revisão de literatura em conformidade legal de proteção de dados. A segunda apresenta como os estudos de engenharia de software tem abordado a análise de risco e a avaliação de impacto em proteção de dados. A terceira parte aborda aspectos referentes à conformidade legal e às relações entre os diferentes *stakeholders* e, por fim, a quarta apresenta os estudos relacionados à presente pesquisa.

2.3.1 Revisões de literatura em conformidade legal

Foram identificados oito estudos de revisão de literatura sobre conformidade em proteção de dados ou temas correlatos, como *Privacy by Design* que, como já apresentado na Seção 2.2.2, faz parte dos esforços de adequação legal.

Em estudo realizado com base em artigos anteriores à aprovação do GDPR, Akhigbe *et al.* (2019) fizeram mapeamento sistemático de literatura contendo 103 artigos, em que analisam métodos de modelagem para apoio em atividades de

conformidade de 60 leis e regulamentos de 14 países. Eles identificaram dois métodos de modelagem. O primeiro concentra a atenção na intencionalidade e nas prescrições da legislação, e o segundo é orientado a objetivos de privacidade, refletindo a estrutura das normas e as relações entre elas e os processos regulados. Segundo Akhigbe *et al.* (2019) este segundo método traz benefícios substanciais para todas as tarefas de conformidade.

Lenhard *et al.* (2017) realizaram revisão de literatura, utilizando 49 estudos primários, para mapear padrões de privacidade no âmbito do GDPR. Eles identificaram as contribuições existentes e classificaram os 148 padrões encontrados no contexto as questões de privacidade em engenharia de software. Concluíram que as descrições dos estudos são superficiais, trazendo obstáculos para avaliação de validade, e evidências empíricas escassas, com apenas 12 dos 49 artigos oferecendo dados empíricos substanciais, faltando abordagens com base em padrões, o que dificulta a adoção na indústria.

Aljohani *et al.* (2018) realizaram revisão sistemática de literatura sobre padrões de privacidade, identificando 19 estudos relevantes, e descobriram que quase não faziam referência a legislações de privacidade, cobrindo segurança, mas não a interface com o usuário.

Morales-Trujillo *et al.* (2019) realizaram revisão sistemática de literatura para identificar em que medida o *Privacy by Design* é aplicado no desenvolvimento de projetos de software, constatando falta de pesquisas sólidas, bem como ausência de boas práticas validadas na área.

Ferreira (2020) realizou revisão sistemática de literatura em que selecionou 51 artigos para compreender como a comunidade de pesquisa tem lidado com requisitos de segurança e privacidade no âmbito do GDPR e constatou que quase nenhuma das soluções propostas foram testadas e utilizadas no mundo real e a maioria delas se concentra em aspectos referentes a consentimento, *privacy by default*, sendo analisadas no contexto da Internet das Coisas e na área da saúde. Por essa razão, Ferreira (2020) afirma que há necessidade de mais soluções, testes e análises sobre conformidade em ambientes reais, bem como é preciso que as soluções integrem componentes sócio-técnicos para que seja possível o enfrentamento dos desafios do GDPR em suas dimensões de infraestruturas, atividades e processos.

Gharib, Giorgini e Mylopoulos (2020) realizaram revisão sistemática de literatura como base para criar uma ontologia de requisitos de privacidade que

contemplasse as pesquisas existentes no contexto do GPDR. O resultado é uma ontologia de conformidade legal para uso de desenvolvedores no âmbito regulatório da União Europeia.

Del-Real *et al.* (2024) realizou uma revisão sistemática de literatura, em que selecionaram 46 estudos, a fim de comparar definições relevantes de "*Security by Design*" e "*Privacy by Design*", identificando que as definições carecem de clareza e uniformidade. Segundo os pesquisadores, "*Privacy by Design*" é mais bem definido, e "*Security by Design*" tem abordagens variadas. Eles sugerem que pesquisas futuras devem esclarecer os valores específicos protegidos por "*Security by Design*".

Alguns estudos no âmbito do GDPR procuram facilitar a análise dos desafios de adequação legal. Feltus *et al.* (2017) propõem um modelo de privacidade para o GDPR a partir de uma revisão de literatura sobre privacidade, abrangendo as conexões entre companhias em um ecossistema empresarial. Eles observaram que a gestão da privacidade necessita de recursos específicos, como funcionários especializados, novas ferramentas e políticas. Grundstrom *et al.* (2019) identificam 13 desafios de conformidade no GDPR em relação especificamente a acesso a dados, classificando-os em quatro categorias – procedimento, proteção, privacidade e proliferação. E Tikkinen-Piri, Rohunen e Markkula (2017) comparam o GDPR com a Diretiva de Proteção de Dados 95/46/CE, que regulava o tema da proteção de dados e apresentam 12 orientações a respeito dos então novos requisitos de conformidade.

Alshammari e Simpson (2018) utilizam UML para representar atividades de processamento de dados com o objetivo de facilitar o raciocínio de conformidade de privacidade. E Alkubaisy e Mouratidis (2019) apresentam um *framework* para identificar e resolver conflitos entre requisitos de segurança e privacidade, sugerindo ferramentas para apoiar o desenvolvimento de requisitos.

Alguns estudos abordam aspectos referentes à segurança de informação. Silva e Barros (2017) apresentam um modelo de maturidade de desenvolvimento de software para segurança da informação com base na ISO/IEC 27001. Diamantopoulou *et al.* (2019), concluem que seguir a ISO/IEC 27001 cumpre apenas com parte dos requisitos do GDPR.

Há estudos que analisam pontos específicos do GDPR. Ataei, Degbelo e Kray (2018) propõe um conjunto de interface com usuários para gestão de configurações de privacidade em tecnologia de geolocalização. Vanberg e Ünver (2017), Hert *et al.* (2018) e Graef, Husovec e Purtova (2018) apresentam possibilidades e desafios de

implementação do direito à portabilidade no GDPR. Urquhart, Sailaja e McAuley (2018) analisa o direito de portabilidade no contexto da Internet das Coisas. Outros tratam do impacto do regulamento europeu em domínios definidos, como o de saúde (LOPES; OLIVEIRA, 2018) e de contabilidade (STANCIU; RÎNDASU, 2018).

No que tange às pesquisas sobre requisitos de privacidade, Ringmann, Langweg e Waldvogel (2018) identificam 74 requisitos técnicos genéricos no GDPR que podem ser usados em produtos de software, com o objetivo de atender princípios de *Privacy by Design*. Peixoto (2020) apresentam um método para especificação de requisitos de privacidade.

Kneuper (2020) constata que o GDPR conduz a requisitos funcionais, de qualidade e restrições que precisam ser levadas em consideração no desenvolvimento. Kneuper (2019) afirma também que a proteção de dados afeta principalmente o projeto e a análise de sistemas de software, desde o momento em que os dados são processados, até o processamento e os mecanismos de proteção utilizados.

Baldassarre *et al.* (2020a) apresentam uma ferramenta para apoiar desenvolvedores na integração de requisitos de privacidade e segurança. Baldassarre *et al.* (2020b) sugerem uma abordagem que leva em conta *privacy by design*, estratégias de projeto e padrão de privacidade, vulnerabilidades e contexto, com a finalidade de descobrir fragilidades de software.

Em relação a aspectos sobre o dever de informação a titulares de dados, Colesky e Caiza (2018) propõem padrões de privacidade e informação ao usuário para uso no GDPR, com o objetivo de orientar o desenvolvimento. Huth e Matthes (2019), de outro lado, constatam que as abordagens existentes de privacidade não fornecem apoio para direitos dos titulares nos moldes estabelecidos pelo GDPR.

Diversas pesquisas concentram a atenção nos desafios de aplicação de conformidade legal em proteção de dados em atividade de engenharia de software. Piras *et al.*, (2019) consideram um desafio aplicar o GDPR, dada sua extensão, complexidade e os diversos aspectos que abrange, não oferecendo detalhes às medidas de segurança técnicas e organizacionais que devem ser aplicadas para se obter a conformidade. Além disso, eles consideram a implementação cara e difícil, por conta de o regulamento europeu cobrir muitos aspectos de proteção de dados. Piras *et al.* (2019) afirmam, ainda, que existem ferramentas e protótipos para atendimento

de aspectos isolados do GDPR, mas destacam a inexistência de instrumento que possa apoiar todos os requisitos de conformidade.

Peixoto *et al.* (2020) concluem que desenvolvedores possuem conhecimento prático de privacidade, mas não conhecimento teórico, concentrando-se em segurança, o que pode comprometer a solução de problemas de privacidade. Na mesma linha, Alhazmi e Arachchilage (2020) constatam que desenvolvedores de software são pouco familiarizados com os princípios do GDPR, o que impede integrar conformidade legal.

Quando softwares são desenvolvidos de forma iterativa, como é o caso das *startups*, segundo alguns pesquisadores, as questões de conformidade podem ser pensadas de forma análoga à dívida técnica. Rindell e Holvitie (2019) trazem a ideia de dívida técnica para o campo dos estudos de segurança da informação, a fim de desenvolver um novo conceito, a dívida de segurança. De acordo com eles, quando há desenvolvimento iterativo de software, o projeto tende a evoluir ao longo do tempo, de modo que o ambiente técnico pode ser alterado significativamente, aumentando a demanda por avaliação e gestão de risco de segurança durante o processo. A dívida de segurança, assim, é uma forma de identificar riscos de segurança que podem ser priorizados e tratados ao longo do tempo, sem que permaneçam ocultos.

Grande parte dos estudos sobre conformidade de proteção de dados existentes no contexto das *startups* tratam das dificuldades que elas possuem de se adequar à legislação. Em pesquisa qualitativa, Norval *et al.* (2021) identificam uma desconexão entre abordagens de *startups* e a natureza dos requisitos do GDPR, argumentando a necessidade de mais estudos para garantir que tecnologias e práticas das empresas nascentes estejam alinhadas às obrigações regulatórias.

Estudo de Li *et al.* (2019) constatam que o escopo do GDPR é bastante abrangente para *startups* e que desenvolvedores geralmente precisam desempenhar diversas tarefas o que dificulta a compreensão do regulamento. Segundo Li *et al.* (2019), a falta de treinamento em GDPR é um fator adicional de complexidade para que se atinja a conformidade legal em proteção de dados.

No mesmo sentido, Bleier *et al.* (2020) afirmam que *startups* frequentemente estão em desvantagem na implementação de conformidade legal de proteção de dados quando comparadas com companhias estabelecidas. E Li *et al.* (2020) afirmam haver uma falta de estudos aprofundados sobre práticas de conformidade do GDPR

em organizações de software, especialmente sobre pequenas e médias empresas e sobre aquelas companhias que operam em integração contínua.

Brodin (2019) afirma que o fato de o GDPR requerer mudanças significativas em diversas áreas da organização, o que inclui controle de todos os processos de tratamento de dados pessoais, dificulta pequenas e médias empresas alcançarem a conformidade, até porque elas possuem menor padronização de processos. Em pesquisa sobre pequenas e médias empresas, Fähnrich e Kubach (2019) constataram ser necessário analisar todos os processos de negócio de modo separado para atender aos requisitos do GDPR, o que torna a tarefa complexa para companhias de menor porte.

Estudos realizados no âmbito do GDPR indicam a necessidade de abordagens de conformidade específicas para o contexto das s*tartups.* Nesse sentido, Norval *et al.* (2021) constatam que *startups* consideram o aconselhamento jurídico como uma forma eficaz de garantir a conformidade legal, uma vez que elas não entendem como a conformidade de proteção de dados pode ser realizada, em especial em relação às tecnologias emergentes que desenvolvem. As startups, portanto, precisam de uma abordagem razoável, que as permita conciliar a necessidade de rápida evolução com os requisitos do GDPR (NORVAL *et al.*, 2019).

Li *et al.* (2020) afirmam que, como o tempo para *startups* é valioso, desenvolvedores podem avaliar o risco de não conformidade, protelando decisões de desenvolvimento, por considerarem que a exposição potencial não é grave o suficiente para penalidades drásticas, podendo a adequação legal ser resolvida no futuro. Ou seja, *startups* podem acumular o que Rindell e Holvitie (2019) denominam, como já mencionado, de dívida de segurança, para decidir tratá-la em momento posterior. Segundo Li *et al.* (2020), o desenvolvimento contínuo de software pode contribuir para uma empresa responder rapidamente a um problema de privacidade, mas para que isso ocorra é preciso que o desafio seja apresentado como uma tarefa de trabalho que terá de ser em algum momento priorizada.

Angermeir *et al.* (2024) realizaram um estudo sobre conformidade de segurança contínua em que apresentam uma visão geral preliminar dos desafios na área. O estudo pondera que as atividades de conformidade tradicionais são lentas, trabalhosas e caras, o que as tornam inadequadas para o desenvolvimento e lançamento rápidos de software no mundo contemporâneo. Eles propõem uma definição de conformidade contínua de segurança levando em consideração a

execução contínua de atividades de conformidade, a adesão de fontes regulatórias de segurança relevantes e a necessidade de conformidade em todo o ciclo de vida do desenvolvimento.

Li *et al.* (2020), entretanto, diferentemente de outros pesquisadores (RINGMANN; LANGWEG; WALDVOGEL, 2018, KNEUPER, 2020) consideram a conformidade de proteção de dados uma questão de cumprimento de requisitos não funcionais, apresentam uma relação entre três princípios do GDPR (integridade e confidencialidade, minimização de dados, limitação de armazenamento) e uma lista de 19 requisitos não funcionais de privacidade.

Alguns pesquisadores mapearam também que a adequação legal à proteção de dados é desejável por *startups* por pelos três motivos. O primeiro deles, é a possiblidade de multas pesadas, em especial, em casos de descumprimento não intencional (NORVAL *et al.*, 2021). A esse respeito, Martin *et al.* (2019) afirmam que *startups* temem o novo cenário, que aumentou consideravelmente o valor das multas administrativas das agências reguladoras.

O segundo motivo é que clientes se preocupam cada vez mais com privacidade e segurança, dadas as crescentes ameaças que novas tecnologias podem trazer para os indivíduos, de modo que a proteção de dados deve continuar a ser um valor perseguido pelas novas gerações de *startups* de software (VAN LE; SUH, 2018). De outro lado, de acordo com Bachlechner Lieshout e Timan (2019), a privacidade vem sendo compreendida como um facilitador de inovação e um desejo dos consumidores, que cada vez buscam empresas que tenham credibilidade a respeito da forma como processam seus dados pessoais.

Há uma terceira razão para as startups desejarem implementar conformidade de proteção de dados – é uma questão de sobrevivência. Segundo Martin *et al.* (2019), elas temem, ainda, que caso sejam incapazes por qualquer motivo de se adequar à legislação precisem abandonar o desenvolvimento do produto.

2.3.2 Análise de risco e avaliação de impacto

O tema relatório de impacto tem sido bastante estudado no âmbito da União Europeia no campo da engenharia de software, compreendido como documento de apoio para implementação de medidas de segurança e privacidade (OETZEL; SPEIKERMANN, 2012, ESAYAS, 2014, JAMES, 2015, MEIS; HEISEL, 2015, DE; LE MÉTAYER, 2017, CORTINA et al., 2018, VEMOU; KARYDA, 2019).

Antes de o GDPR ser aprovado, o termo usado na União Europeia para as avaliações de impacto era *Privacy Impact Assessment* (PIA), ou Avaliação de Impacto em Privacidade, em tradução livre. Relatório do UK *Information Commissioner´s Office* de 2014 define o PIA como "uma ferramenta que pode ajudar as organizações a identificar a forma mais eficaz de cumprir com suas obrigações de proteção de dados e atender às expectativas individuais de privacidade" (tradução livre)"[5] (UK INFORMATION COMMISSIONER´S OFFICE, 2014, p. 3).

Contudo, após o GDPR ser aprovado em 2016, o termo utilizado foi alterado, uma vez que o regulamento europeu apresenta uma nova terminologia no artigo 35, passando a ser chamado de *Data Protecion Impact Assessment* (DPIA), ou Avaliação de Impacto sobre a Proteção de Dados, em tradução livre. O DPIA é descrito no artigo 35 da seguinte forma:

> 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação (UNIÃO EUROPEIA, 2016).

Conforme o artigo 35 do GDPR, um controlador deve realizar uma avaliação de impacto de proteção de dados previamente ao tratamento, sempre que a operação puder implicar risco para direitos fundamentais e liberdades dos titulares.

Segundo Easton (2016), embora o termo empregado no GDPR seja diferente de PIA, ambos possuem abordagens parecidas, devendo neles serem incluídas a descrição das operações e dos objetivos do tratamento, a avaliação de necessidade e proporcionalidade do tratamento, a avaliação de risco relativa à possibilidade de violação de direitos e liberdades, bem como as medidas de segurança para proteção e mitigação dos riscos identificados. A avaliação de impacto, portanto, é um método abrangente de análise de processos e contexto organizacionais, com o objetivo de identificar necessidades de um amplo espectro de partes interessadas (Easton, 2016).

Tanto a LGPD quanto o GDPR descrevem que o risco relevante para o objeto dessas normas de proteção de dados é aquele que pode causar dano a direitos fundamentais e liberdades civis. Para entender a dimensão de o que isso significa e

[5] No original: "*a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy*" (UK ICO, 2014, p. 3).

que implicações pode ter seja para o direito, seja para a engenharia de software, apresenta-se o conteúdo do Considerando 75 do GDPR:

> O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. (UNIÃO EUROPEIA, 2016)

A preocupação do regulamento europeu, portanto, é que o risco seja analisado com base na probabilidade e na gravidade de dano ao titular do dado – seja físico, material ou imaterial. O GDPR preocupa-se também com possibilidades de discriminação, roubo de identidade, prejuízos financeiros, de reputação, bem como de perdas de confidencialidade, em especial quando se trata de dados sensíveis e titulares de dados vulneráveis, como crianças.

A análise de riscos de privacidade, como parte integrante da avaliação de impacto, tem parâmetros definidos no Considerando 76, do GDPR, que recomenda sejam levados em conta o contexto, a natureza, o âmbito e as finalidades de tratamento de dados.

Já no âmbito brasileiro a LGPD, estabelece no artigo 50, a necessidade de, ao se desenvolver boas práticas de governança, serem considerados aspectos referentes a natureza, escopo, finalidade de dados e operações de tratamento, bem como a probabilidade e gravidade dos riscos e benefícios do tratamento dos dados do titular.

Uma definição de risco de privacidade útil para o presente estudo é a da *Commission Nationale de l'Informatique et des Libertes* (CNIL, 2018, p. 6):

> “um cenário hipotético que descreve um evento temido e todas as ameaças que permitiriam que ocorresse. Mais especificamente, descreve:
> - como as fontes de risco (por exemplo: um funcionário subornado por um concorrente)
> - poderiam explorar as vulnerabilidades de recursos de suporte (por exemplo: o sistema de gerenciamento de arquivos que permite a manipulação de dados);
> - em um contexto de ameaças (por exemplo: uso indevido ao enviar e-mails);
> - e permitir que eventos temidos ocorressem (por exemplo: acesso ilegítimo a dados pessoais);
> - em dados pessoais (por exemplo: arquivo do cliente);
> - gerando impactos na privacidade dos titulares dos dados (por exemplo: solicitações indesejadas, sentimentos de invasão de privacidade, problemas pessoais ou profissionais) 6 (CNIL, 2018, p. 6) (tradução nossa).

A definição de risco em privacidade da CNIL (2018) envolve aspectos relativos à avaliação de impacto, o que demonstra a forte conexão entre o DPIA e a análise de risco de privacidade.

Pesquisadores indicam que não parece correto considerar a avaliação de impacto como uma análise de risco estritamente de segurança de tecnologia da informação. Estudo de Abu-Nimeh e Mead (2010) constatou que os métodos de avaliação de risco de segurança não eram uma alternativa para análise de risco de privacidade, porque a primeira identifica ameaças ao sistema, enquanto a segunda trata das características e da sensibilidade dos dados inseridos nos sistemas.

Para James (2015), a conformidade legal de proteção de dados é um desafio contínuo para empresas, mas especialmente para *startups*, já que empresas nascentes precisam ser criativas e inovadoras e, ainda, proteger os dados pessoais de seus clientes. Por essa razão, há a necessidade de avaliar riscos envolvidos no tratamento de dados pessoais, incluindo a conformidade legal nas atividades de desenvolvimento de software (James, 2015).

Em um cenário regulatório anterior ao GDPR, Oetzel e Speikermann (2012) propuseram uma abordagem para a elaboração de avaliações de impacto de privacidade. Esayas (2014) apresentou uma abordagem para gerenciar riscos de conformidade legal, que permite um alinhamento entre o que uma organização considera um risco aceitável e o que seja também aceitável do ponto de vista legal

---

[6]: No original: a hypothetical scenario that describes a feared event and all the threats that would allow this to occur. More specifically, it describes: - how risk sources (e.g.: an employee bribed by a competitor) - could exploit the vulnerabilities of supporting assets (e.g.: the file management system that allows the manipulation of data) - in a context of threats (e.g.: misuse by sending emails) - and allow feared events to occur (e.g.: illegitimate access to personal data) - on personal data (e.g.: customer file) - thus generating impacts on the privacy of data subjects (e.g.: unwanted solicitations, feelings of invasion of privacy, personal or professional problems) (CNIL, 2018, p. 6)

dessa mesma organização. Meis e Heisel (2015) propuseram um método com apoio de ferramentas a fim de reduzir o esforço para obtenção de informações para a condução da avaliação de impacto sobre a privacidade (PIA).

Já no âmbito da vigência do GDPR, estudos têm analisado os desafios e propostos métodos para ou Avaliação de Impacto sobre a Proteção de Dados e para análises de risco. Sion *et al.* (2019) identificaram a existência de conflito entre o raciocínio jurídico que conduz os referidos relatórios e as abordagens de engenharia de software para modelagem de ameaças e identificação de requisitos e riscos de privacidade. As atividades de engenharia, segundo eles, são geralmente realizadas de forma isolada, afetando não só a implementação de conformidade, como a capacidade de evolução do sistema e arquitetura do software.

Estudo realizado por De e Le Métayer (2017) avalia como melhorar a relação custo-eficácia de avaliações de impacto de privacidade a partir de uma abordagem sistemática para arquitetura que busca integrar privacidade desde o início do projeto. Vemou e Karyda (2019) propõem um processo de avaliação de impacto derivado de métodos existentes, com uma estrutura que envolve 17 critérios, que vão desde a análise da necessidade de realizar um DPIA com base no artigo 35 do GDPR, até a revisão periódica do documento.

De e Le Métayer (2016) consideram a análise de risco em privacidade o núcleo da avaliação de impacto em privacidade e sugerem um método extensivo para desenvolver análise de risco em privacidade. Na visão deles, privacidade é um conceito mais complexo que segurança, multifacetado, que, por meio de normas tem o objetivo de proteção do indivíduo. Por essa razão, o método que propõem leva em conta fatores que impactam riscos de privacidade, analisando probabilidade e gravidade para potenciais danos à privacidade.

Ahmadian *et al.* (2018) propõem um método para apoiar a avaliação de impacto, com base em análises de privacidade e segurança para a fase inicial do desenvolvimento de sistemas, utilizando controles técnicos e organizacionais presentes na ISO/IEC 27001, para estabelecer recomendações com o objetivo de ou mitigar riscos. O método de Ahmadian *et al.* (2018) não avalia probabilidades específicas de ocorrência de eventos de violação de privacidade, por considerarem que o risco no domínio da privacidade relaciona-se com as emoções humanas, de modo que, quando um direito como a privacidade está ameaçado, os riscos devem ter seu impacto potencial avaliado e serem mitigados.

Alshammari e Simpson (2018a, 2018b) também propõem uma avaliação de risco para ser integrada a uma avaliação de impacto de privacidade. A avaliação proposta por Alshammari e Simpson (2018a, 2018b) tem a vantagem de não reduzir a proteção de privacidade a conceitos como anonimato, pseudo-anonimato e desvinculação, ao tratar de um conjunto de objetivos que considere aspectos legais, organizacionais, sociais e técnicos. A avaliação leva em conta o ciclo de vida dos dados, representando os processos em oito estágios – desde a iniciação, coleta retenção e acesso, até revisão, uso, divulgação e eliminação – que são usados como fonte para a representação de dados pessoais e as atividades de processo vinculadas, bem como atores e funções envolvidos em cada etapa.

Cortina *et al.* (2018) também apresentam uma abordagem para determinar risco de processamento de dados pessoais no GDPR, a fim de apoiar avaliação de impacto de proteção de dados. Enquanto Ali-Eldin, Zuiderwijk e Janssen (2018) propõem um modelo de avaliação para minimizar riscos em estruturas de dados abertos. E Wagner e Boiten (2018) sugerem um método para quantificar risco de privacidade que leva em conta escala da violação, sensibilidade dos dados, expectativa dos indivíduos, dano (financeiro, reputacional, discriminatório, entre outros), probabilidade de ataque e de impacto no titular do dado.

Sion *et al.* (2019) apresentam um modelo de avaliação de risco de privacidade que leva em conta riscos técnicos, organizacionais e do titular dos dados, bem como a probabilidade de incidentes. Sion *et al.* (2019) consideram também a capacidade das fontes de risco causarem um incidente de violação de dados, bem como as medidas para evitar que a ameaça de segurança se realize.

Alva e Young (2019) comparam métodos de avaliação de impacto de proteção de dados e sugerem que a Norma ISO/IEC 29134:2017, documento técnico que trata de avaliação de impacto de privacidade, oferece a melhor estrutura tanto em termos de conteúdo quanto de processo.

Gumusel *et al.* (2024) realizaram estudo em que buscaram entender como profissionais jurídicos lidam com relatos de incidentes de segurança, por meio de experimento em que fizeram 33 entrevistas semiestruturadas com profissionais da área jurídica. O estudo concentrou atenção na avaliação de risco de privacidade e de conformidade legal de proteção de dados em respostas a incidentes, identificando que atualmente as ferramentas de apoio à análise de risco em incidentes de segurança são deficientes e que fatores contextuais, como as características dos dados, a forma

de tratamento e a finalidade dos dados, impactam de forma significativa na avaliação de risco.

Segundo Gumusel *et al.* (2024) o estudo identifica a necessidade de criação de ferramentas que permitam que os usuários entendam a relação entre riscos potenciais de privacidade associados a artigos relevantes de lei e regulamentos, bem como que entendam os riscos de privacidade associados a dados técnicos, de modo que possam tomar medidas mitigatórias para os problemas identificados. Eles identificaram também a necessidade de treinamento multidisciplinar, por conta das questões técnicas e jurídicas necessárias para o cumprimento das normas de proteção de dados.

No âmbito das *startups* de software, não parece razoável a este pesquisador utilizar metodologias que partam de relatórios de impacto para então buscar a conformidade legal em proteção de dados. Isso porque, com recursos escassos e pressionada pelo tempo, a preocupação central da *startup* está em encontrar um modelo de negócio para atender um nicho de mercado (PATERNOSTER *et al.*, 2014, MELEGATI *et al.*, 2020).

Entretanto, a análise de risco em relação à privacidade e outros direitos fundamentais do titular em relação aos dados tratados pela *startup*, na visão deste pesquisador, é um importante instrumento para orientar a tomada de decisão de conformidade legal de proteção de dados na engenharia de software. Por meio dela, a equipe da *startup* pode optar pelo melhor momento de implementar aspectos de conformidade legal de proteção de dados no desenvolvimento do produto, gerenciando, assim, o risco de conformidade legal ao longo do ciclo de vida da empresa nascente.

No próximo tópico apresentam-se estudos que mostram a importância de envolver os *stakeholders* no processo de tomada de decisão para a implementação de conformidade legal de proteção de dados na engenharia de software.

2.3.3 S*takeholders*, conformidade legal e *startups*

Estudos do âmbito da engenharia de software sugerem que a diferença de pontos-de-vista tende a ter impacto na implementação de conformidade de proteção de dados (SENARATH; ARACHCHILAGE, 2018, PEIXOTO *et al.*, 2020, ALHAZMI; ARACHCHILAGE, 2020, LI *et al*., 2020).

Por *stakeholder*, entende-se uma “pessoa ou organização que influencia os requisitos de um sistema ou que é impactada por esse sistema” (GLINZ; WIERINGA, 2007, p. 19). Para que *stakeholders* estejam mais propensos a levar em conta diferentes percepções sobre o desenvolvimento de software, é necessário que a tomada de decisão seja conjunta e colaborativa (LIU *et al.*, 2011). O trabalho colaborativo é sugerido também por Machiridza (2016) como forma de evitar conflitos causados pelas diferentes expectativas de *stakeholders*.

Nos estudos de *startups*, Klotins (2018) afirma que a rápida evolução das empresas nascentes e os objetivos conflitantes entre os *stakeholders* adiciona complexidade extra à engenharia de software, o que sugere a necessidade de seguirem práticas que melhorem o uso de recursos e o gerenciamento de riscos, bem como o alinhamento de interesses dos diferentes *stakeholders*, entre eles, investidores. Segundo Gopagoni e Sabella (2020), engenheiros de software de *startups* precisam equilibrar as metas das partes interessadas, como governo, comunidade, usuários, clientes.

Poucos são os estudos que levam em conta os diversos *stakeholders* na implementação de conformidade legal de proteção de dados na engenharia de software. Em estudo sobre expectativa de privacidade, Senarath e Arachchilage (2018) descobriram que o ponto de vista de desenvolvedores é significativamente diferente das expectativas reais dos usuários. Isso conduz os desenvolvedores a desconsiderarem as expectativas dos usuários ao tomarem suas decisões de privacidade em seus projetos (SENARATH; ARACHCHILAGE, 2018).

Como já mencionado na Seção 2.3.1, a falta de conhecimento prático de privacidade pode causar problemas (PEIXOTO *et al.*, 2020), além do que desenvolvedores de software são pouco familiarizados com normas de proteção de dados, o que dificulta a implementação de conformidade legal (ALHAZMI; ARACHCHILAGE, 2020).

Por conta de questões como essas, Li *et al.* (2020), afirmam ser necessário reduzir a distância entre gerentes e desenvolvedores, a fim de garantir que a conformidade de proteção de dados seja alcançada. Segundo eles, desenvolvedores e gerentes precisam ter o mesmo nível de urgência em relação às atividades que envolvam a adequação legal. Li *et al.* (2020) asseveram que todos os indivíduos de uma organização precisam estar em conformidade com o GDPR, não sendo algo que

possa ocorrer somente a partir de uma perspectiva organizacional, a fim de garantir a adequação legal no longo prazo.

Por essa razão, um método de tomada de decisão em conformidade legal de proteção de dados que possibilite aos diferentes *stakeholders* de *startups* alinharem seu entendimento sobre o tema pode fortalecer o processo de adequação em uma perspectiva mais ampla no nível da organização.

2.3.4 Estudos relacionados

Durante a pesquisa de revisão de literatura identificaram-se abordagens de conformidade legal em proteção de dados, todas ou no âmbito do GDPR ou sobre segurança de informação de forma genérica, que podem ser consideradas como mais próximas ao tema desta pesquisa. Para mostrar a diferença entre elas e a presente proposta foram estabelecidos alguns critérios a serem utilizados para analisá-las. Os critérios empregados foram: (i) contexto de *startups*; (ii) análise de risco em privacidade; (iii) conformidade legal; (iv) alinhamento de *stakeholders*, (v) validação na indústria.

O critério “contexto de *startups*” é introduzido por conta dos aspectos que o tornam único, conforme apresentado na Seção 2.1.1 e em que é caracterizado pela incerteza, pressão de tempo e da necessidade de alta reatividade na procura por um mercado para o produto (MELEGATI *et al.*, 2020, GIARDINO *et al.*, 2014).

O critério análise de risco em privacidade é utilizado pela relevância que possui em relação ao tema de conformidade legal em proteção de dados, conforme apresentado na Seção 2.3.2. Além disso, a Seção 2.2.2 bem como a Seção 2.3.2 apresentam a importância de avaliar o impacto de eventual violação de dados pessoais, seja para a tomada de decisão de mitigação de riscos, seja para a implementação de boas práticas, seja para a aplicação de penalidades. A análise de risco, em especial para encontrar formas repetíveis de tomar decisão sobre proteção de dados, tem inclusive sido entendida como uma importante linha de pesquisa na área de conformidade legal de proteção de dados pessoais (LI *et al.*, 2020).

O critério conformidade legal foi escolhido pela própria natureza deste trabalho, que trata de adequação de proteção de dados e é subdividido em dois subcritérios – requisitos não funcionais (RNF) e requisitos funcionais (RF). Essa subdivisão é relevante por que parte dos trabalhos consideram a conformidade de proteção de dados um aspecto apenas relativo a requisitos não-funcionais (LI *et al.*, 2020), o que,

como apresentado na Seção 2.3.1 é equivocado, uma vez que há a necessidade de se levar em conta também requisitos funcionais para se alcançar a adequação legal.

O critério de alinhamento de *stakeholders* diz respeito à possibilidade de a abordagem impactar a organização como um todo, ao permitir que diferentes *stakeholders* compartilhem entendimento sobre conformidade de dados (SENARATH e ARACHCHILAGE, 2018, LI *et al.*, 2020).

Por fim, o critério de validação na indústria trata da avaliar se a abordagem foi testada empiricamente em um contexto real na indústria de software.

A partir desses critérios, foram analisadas 15 abordagens, conforme apresentado no Quadro 2-6.

Quadro 2-6. Abordagens de conformidade legal em proteção de dados. Fonte: o Autor.

Autor	**Análise de risco de privacidade**	**Conformidade legal**		**Contexto de *startups***	**Alinhamento de *stakeholders***	**Validação na indústria**
		RNF	**RF**			
Massey *et al.* (2010)		**X**	**X**			**X**
Ataei, Degbelo e Kray (2018)			**X**			
Ayala Rivera e Pasquale (2018)		**X**	**X**		**X**	
Piras *et al.* (2019)	**X**	**X**	**X**			
Salnitri et al. (2019)		**X**				**X**
Fähnrich e Kubach (2019)	**X**	**X**				**X**
Barbosa et al. (2019)	**X**	**X**				**X**
Brodin (2019)		**X**	**X**			**X**
Li *et al.* (2020)		**X**		**X**		**X**
Wuyts, Sion e Joosen (2020)	**X**	**X**			**X**	
Tsohou *et al.* (2020)		**X**	**X**		**X**	**X**
Matulevicius et al. (2020)		**X**	**X**			**X**
Peixoto (2020)	**X**	**X**			**X**	
Shaked e Reich (2021)		**X**				
Ayala-Rivera *et al.* (2024)		**X**	**X**			

Massey *et al.* (2010) apresentam uma avaliação de requisitos para conformidade legal de segurança nos termos estabelecidos pelo *Health Insurance Portability and Accountability Act* of 1996, em um sistema de registros eletrônicos de saúde. A avaliação de requisitos é para um diploma legal específico e para uso em

sistemas pré-existentes, muito diferente daquele que é objeto de análise deste trabalho. Além disso, não é adequado ao contexto das *startups*, não se preocupando com a adequação em ambientes de incerteza, pressão de tempo e alta reatividade com vistas a descobrir um nicho de mercado para um produto. O método de Massey *et al.* (2010) não leva em conta análise de risco de privacidade. A avaliação de requisito proposta foi aplicada uma única vez, sem a pesquisa trazer informações sobre os resultados obtidos.

Ataei, Degbelo e Kray (2018) apresentam um conjunto de diretrizes para lidar com conformidade com o GDPR de interface com o usuário para serviços georreferenciados, baseados em localização, com foco em notificação, consentimento e controle sobre o tratamento de dados dos titulares. O foco do estudo é bastante específico, tratando de requisitos funcionais orientados à transparência com os titulares de dados, não abordando o contexto das *startups* e análise de risco. Não houve validação na indústria.

Ayala-Rivera e Pasquale (2018) sugerem uma abordagem de seis etapas para elicitação de requisitos em conformidade com o GDPR. A abordagem procura atender apenas princípios do GDPR e envolve colaboradores da área jurídica e de desenvolvimento, no processo de identificação de problemas de conformidade e elicitação de novos requisitos. O método requer alto nível de conhecimento de conformidade legal. Além disso, não leva em conta análise de risco de privacidade e não aborda o contexto de incerteza, pressão de tempo e alta reatividade em que se inserem *startups*. Abordagem não validada na indústria.

Piras *et al.* (2019) propõem um projeto de plataforma de governança de privacidade que possibilita integrar diversas ferramentas de apoio ao cumprimento ao GDPR. O projeto não foi testado nem validado na indústria. Não leva em consideração o contexto de *startups*.

Salnitri *et al.* (2019) propõem um método de engenharia de requisitos que oferece suporte à especificação de requisitos, com ênfase em segurança, privacidade e confiança. O método trata apenas de requisitos não funcionais de segurança e privacidade, sem abordar conformidade legal, para contextos genéricos da indústria. Não leva em conta o contexto das *startups*, nem avaliação de risco de privacidade.

Fähnrich e Kubach (2019) propõem um método apoiado por ferramenta de software para adequação ao GDPR com vistas a atender a pequenas e médias empresas. Contudo, a ferramenta trata apenas de requisitos não funcionais de

segurança, além de exigir extensa documentação, o que conflita com as práticas de engenharia de software em *startups* (Paternoster et al., 2014). O método foi elaborado para uso em sistemas pré-existentes, não tratando do contexto de escassez, pressão, incerteza e reatividade das *startups*.

Barbosa, Brito e Almeida (2019) sugerem um método de desenvolvimento de software para aumentar a cultura de proteção de dados e a consciência do tema privacidade no GDPR. O método não é adequado para o contexto das *startups*, pois necessita de ampla documentação dos sistemas utilizados e conjuntos de dados (Paternoster et al., 2014), para então identificar risco e demandas de segurança. Além disso, trata apenas de requisitos não funcionais de segurança. O modelo de análise de risco usado lida somente com questões referentes a desenvolvimento de software, não trazendo clareza sobre as implicações da violação de dados para os direitos dos titulares de dados, o que é essencial em uma abordagem de conformidade.

Brodin (2019) propõe um *framework* para apoiar pequenas e médias empresas a se adaptarem ao GDPR. O *framework* sugere de forma genérica a atualização e criação de rotinas para processamento de dados pessoais e para evitar violação de dados pessoais, atualização de políticas e criação de modelos para rotinas e políticas, porém não prescreve análise de risco de privacidade. Brodin (2019) não considera em sua proposta o contexto de *startups*, em que há escassez de recursos, pressão de tempo incerteza e elevada reatividade ao ambiente, nem os diversos *stakeholders*.

Li *et al.* (2020) realizaram um estudo longitudinal com uma *startup* por 20 meses, sobre as práticas e desafios de conformidade do GDPR e desenvolveram, a partir da metodologia *Design Science Research*, dois artefatos para tentar solucionar o problema – um conjunto de requisitos não funcionais derivados de três princípios do GDPR e uma ferramenta automatizada e personalizada que verifica se esses requisitos pré-estabelecidos foram observados – e concluíram que alguns dispositivos podem ser parcialmente operacionalizados e testados de forma automatizada, a fim de melhorar as práticas de conformidade.

O estudo, entretanto, trata apenas de três princípios do GDPR – integridade e confidencialidade, minimização de dados e limitação de armazenamento – para gerar uma lista de requisitos não funcionais, atendendo apenas alguns dos dispositivos do regulamento europeu. A proposta não trata de tomada de decisão, nem leva em conta análise de risco de privacidade ou as relações entre *stakeholders*.

Wuyts, Sion e Joosen (2020) propõem o LINDDUN GO, um *kit* de ferramentas de apoio, que utiliza cartões para modelar ameaças de segurança em privacidade a partir de princípios de *privacy by design*. O LINDDUN GO é baseado no LINDDUN (Deng *et al.*, 2011), uma estrutura para modelagem de ameaças de privacidade cujo objetivo é apoiar a elucidação e a mitigação de ameaças de segurança em arquitetura de software. Embora o LINDDUN GO, e mesmo o LINDDUN, contribuam para análise de risco e apoie a elucidação e a mitigação de ameaças de privacidade, tratam apenas de aspectos de arquitetura, não lidando com questões de conformidade legal de proteção de dados em sua integralidade.

Apesar de ágil, o LINDDUN GO não foi projetado para atender os desafios do contexto de *startups*, mas para dar respostas rápidas sobre ameaças de segurança. O método não foi validado em um caso real na indústria. Além disso, embora possa ser usado para avaliação de risco, não trata de conformidade legal de proteção de dados, nem de análise de risco privacidade orientado para questões de violação de direitos fundamentais.

Tsohou *et al.* (2020) apresentam processo de elicitação e análise de requisitos de privacidade para apoiar conformidade com o GDPR. O processo é realizado com base em análise de dados obtidos com clientes e colaboradores de diferentes áreas. O método é complexo, inadequado para o contexto de *startups*, não só pela dificuldade de implementação, mas porque elas geralmente desconhecem os clientes em estágios iniciais (GIARDINO *et al.*, 2014). O método não leva em conta a análise de risco de privacidade dos dados tratados.

Matulevicius *et al.* (2020) sugerem um modelo para conformidade organizacional com o GDPR para sistemas pré-existentes de organizações que construíram seus sistemas antes da entrada em vigor do regulamento europeu. O modelo não leva em conta contexto de alta reatividade de *startups* na busca de mercado. O modelo busca fazer um diagnóstico de conformidade de uma organização e a partir da comparação com o modelo de conformidade com o GDPR avaliar o que é preciso ser feito para se adequar ao regulamento europeu. Contudo, não analisa riscos de privacidade nem busca o alinhamento de *stakeholders*.

Peixoto (2020) propõe um método para especificação de requisitos não funcionais de privacidade para uso em desenvolvimento ágil. A abordagem não leva em conta conformidade legal, em especial requisitos funcionais. Embora preveja avaliação de risco, não leva em conta análise de risco de privacidade com base a

possibilidade de violação de direitos dos titulares. Apesar de o método de especificação ser orientado para desenvolvimento ágil, não é abordado o contexto de *startups*, cujas decisões referentes a requisitos são geralmente *ad hoc* (GIRARDINO *et al.*, 2014, PATERNOSTER *et al.*, 2014) O método não foi testado em um caso real na indústria.

De forma semelhante a Salnitri *et al.* (2019), Shaked e Reich (2021) apresentam um método segurança cibernética, que não trata de conformidade, nem de outros tópicos de interesse do presente estudo.

Ayala-Rivera *et al.* (2024) propõem uma abordagem semiautomatizada para apoiar organizações a respeitarem princípios de proteção de dados no GDPR, pela qual engenheiros utilizam diagramas e selecionam controles de segurança e privacidade provenientes de um catálogo, a serem incluídos no projeto do software.

Os controles do catálogo tiveram sua utilidade em relação ao GDPR avaliada por um único especialista e não foram testados na indústria. Além disso, a proposta não analisa risco e não foi projetada para atender o contexto das *startups*, inclusive requer a existência prévia de um dicionário de dados existente na organização, bem como de engenheiros e especialistas que já tenham realizado mapeamento de atividades de tratamento de dados.

2.4 Considerações sobre o capítulo

A revisão de literatura iniciou conceituando e apresentando o particular contexto em que as *startups* de software estão inseridas. Estabelecido o contexto, apresentou-se a classificação do ciclo de vida das *startups* de software (CROWNE, 2002) e os objetivos e desafios em casa fase (CROWNE, 2002; PATERNOSTER *et al.*, 2014, KLOTINS; UNTERKALMSTEINER; GORSCHEK, 2017, BESKER *et al.*, 2018).

Em seguida, foram apresentadas quatro revisões sistemáticas de literatura sobre práticas de engenharia de software e *startups*, identificando o estado da arte da pesquisa, bem como o estado da prática de engenharia de software em empresas nascentes. Constatou-se a inexistência de práticas relativas à conformidade legal de proteção de dados nos mapeamentos sistemáticos.

Realizada a revisão de literatura sobre engenharia de software e *startups*, apresentaram-se definições de proteção de dados presente na LGPD. Em seguida,

foi feita uma análise do texto legal, com base em pesquisadores da área jurídica e de engenharia de software, e suas implicações em relação à engenharia de software.

Um outro aspecto considerado na análise trata da relevância que a LGPD traz para a análise de risco em privacidade, que precisa levar em consideração de outros pontos além da natureza do dado, como o impacto que o tratamento de dados pode ter em direitos fundamentais e liberdades civis dos titulares. Além disso, a LGPD estabelece que as penalidades administrativas devem levar em conta a gravidade e natureza das infrações dos direitos afetados, o nível do dano, a implantação de práticas internas que minimizem o dano; a implementação de boas práticas e governança, a implementação de medidas corretivas. Esses critérios, na visão deste pesquisador, são importantes para a tomada de decisão de *startups* de software, que, dado o contexto de escassez de recursos, precisam avaliar quais aspectos de conformidade priorizar, a partir da avaliação da natureza de seu modelo de negócio.

Analisada a LGPD e suas implicações com a engenharia de software, adentrou-se no tópico de conformidade legal e proteção de dados, primeiramente apresentando a revisão de literatura sobre o tema, depois abordando-se os temas de análise de risco e avaliação de impacto, bem como os de stakeholders, terminando com a apresentação de estudos relacionados.

Depois de apresentar revisão de literatura sobre relatório de impacto e análise de risco, abordou-se a necessidade de uma percepção comum entre os *stakeholders* sobre conformidade legal de proteção de dados

Por fim, foram analisados 15 estudos cujas abordagens podem ser consideradas próximas a esta pesquisa. Da análise, ficou evidenciado que nenhum dos estudos relacionados é adequado para apoiar *startups* na tomada de decisão de conformidade legal de proteção de dados nas atividades de software, havendo espaço para a proposição de um método de tomada de decisão e um sistema de recomendações que apoiem startups na implementação conformidade legal em LGPD nas práticas de desenvolvimento de software.

CAPÍTULO 3 - ESTRUTURAÇÃO DA PESQUISA

Este Capítulo apresenta a estrutura e os procedimentos operacionais da pesquisa. Na Seção 3.1 são abordados os métodos empregados ao longo do presente trabalho, enquanto na Seção 3.2 é apresentada a estratégia de pesquisa com os detalhes de cada etapa. A Seção, 3.3 traz as considerações finais da estruturação da pesquisa.

3.1 Método de Pesquisa[7]

Devido às características da pesquisa, que visa a produção de um artefato de processo a ser utilizado por *startups*, optou-se pela utilização do método *Design Science Research Methodology* (DSRM). No contexto desta pesquisa o artefato refere-se ao método de tomada de decisão e ao conjunto de recomendações que apoiam *startups* na conformidade com a LGPD nas práticas de desenvolvimento de software.

DSRM é um método utilizado na área de tecnologia da informação desde o começo da década de 1990, que, a partir de princípios, práticas e procedimentos, possibilita a criação de artefatos para resolver problemas no mundo real (PEFFERS *et al.*, 2007). A elaboração do artefato, segundo Peffers *et al.* (2007) é um processo de descoberta fundado em base teórica e em conhecimentos pré-existentes, com o objetivo de resolver um problema proposto.

Peffers *et al.* (2007) estabelecem que o DSRM é constituído de seis atividades, conforme representado na Figura 3-1:

(i) identificação do problema e motivação;
(ii) definição de objetivos para a solução;
(iii) projeto e desenvolvimento;
(iv) demonstração;
(v) avaliação; e
(vi) comunicação.

[7] Este projeto envolve seres humanos e foi aprovado pelo Comitê de Ética em Pesquisa (CEP) da PUCPR em 24/05/2022 sob o parecer número 5.427.429.

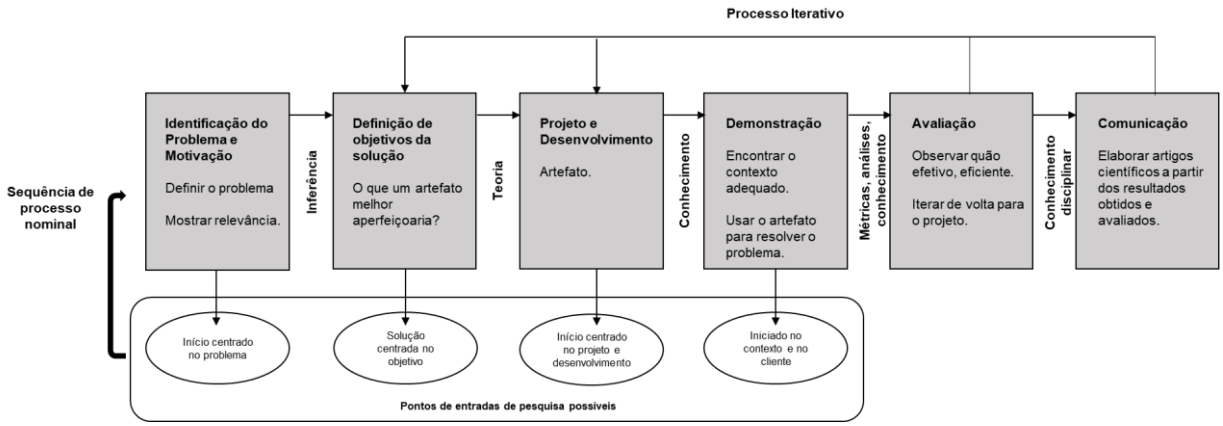

Figura 3-1 .Método de Pesquisa DSRM. Adaptado de PEFFERS et al., 2007.

A atividade da primeira etapa é o momento em que se define o problema de pesquisa e se apresenta a justificativa da importância de sua solução. É a partir da definição do problema que irá ser desenvolvido o artefato que irá contribuir para solucioná-lo. Segundo Peffers *et al.* (2007), para realizar esta tarefa é preciso compreender o problema que se propõe a resolver e qual a importância de se encontrar uma solução.

Na segunda atividade busca-se a definição dos objetivos a serem atingidos com a solução do problema. Eles podem ser, afirma Peffers *et al.* (2007), quantitativos ou qualitativos, e devem ser inseridos a partir do problema definido.

Na terceira etapa, de projeto e desenvolvimento, apresenta-se o artefato, que pode ser um modelo, um método, um construto, enfim, um objeto elaborado para uma contribuição de pesquisa (Peffers *et al.*, 2007). Para desenvolver esta fase, segundo Peffers *et al.* (2007), é preciso definir a função do artefato, sua estrutura, bem como elaborar o artefato concreto que será utilizado.

A quarta atividade é a de demonstração, em que se apresenta o uso do artefato para a solução de uma ou mais partes do problema. Nesta etapa, conforme Peffers *et al.* (2007), demonstra-se o uso do artefato para a solução do problema por meio de experimentação, provas de conceito, simulação etc.

A quinta etapa refere-se à atividade de avaliação, em que se analisa o desempenho do artefato para a solução do problema. Peffers *et al.* (2007) afirmam que a avaliação pode ser feita conforme a natureza do problema e do artefato, incluindo qualquer evidência empírica que seja adequada. Ao fim desta fase, segundo

eles, é possível decidir se há necessidade de se retornar à terceira etapa a fim de melhorar o artefato ou se já é possível prosseguir para a etapa seguinte.

A sexta atividade é a de comunicação. Nela, de acordo com Peffers *et al.* (2007), informa-se os resultados da investigação realizada, comunicando-se o problema e a importância dele, o artefato e sua utilidade e originalidade, o rigor do projeto e a eficácia dele para outros pesquisadores e públicos de interesse.

Embora o processo de DSRM seja sequencial, segundo Peffers *et al.* (2007), ele pode ser iniciado a partir de qualquer atividade, com abordagens centradas, por exemplo, no problema começando pela fase 1, abordagens centradas nos objetivos pela etapa 2 e aquelas orientadas ao projeto e no desenvolvimento pela etapa 3.

Para avaliar o artefato proposto, na etapa de demonstração irá se utilizar um roteiro de entrevista com objetivo de aferir a utilidade e aceitação da proposta de pesquisa, usando como fundamento o modelo de aceitação de tecnologia (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008).

3.2 Estratégia de pesquisa

Apresenta-se aqui a estratégia de pesquisa que está sendo utilizada neste trabalho nos termos propostos por Peffers (2007) para o DSRM. A pesquisa tem como ponto de partida o problema identificado, conforme representado na Figura 3-2.

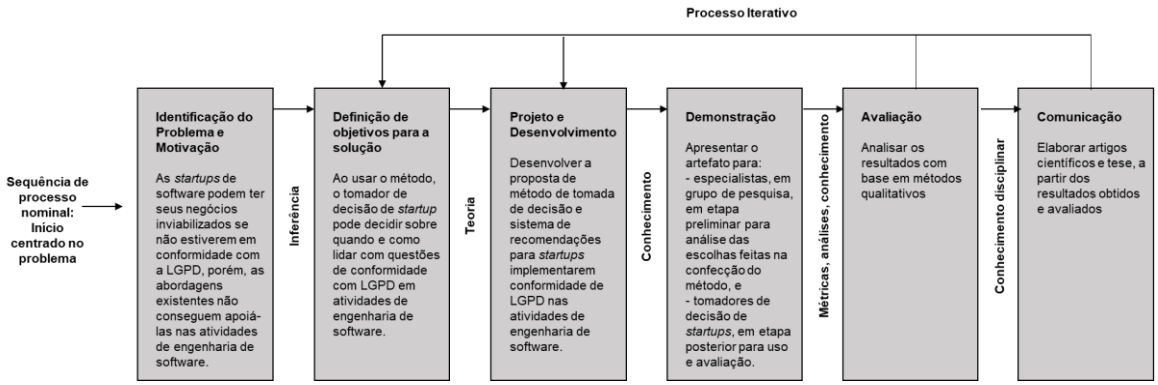

Figura 3-2. Método de Pesquisa, adaptado de Peffers *et al.* (2007). Fonte: o Autor.

As próximas seções descrevem as etapas de identificação do problema e motivação, seguindo de objetivos para a solução, projeto e desenvolvimento, demonstração, avaliação e, por fim, comunicação.

3.2.1 Identificação do Problema e Motivação

Esta pesquisa iniciou a partir de uma análise exploratória para identificar trabalhos em duas frentes: (i) abordagens de conformidade legal em proteção de dados na engenharia de software; e (ii) práticas de engenharia de software em *startups*. Para ambas as frentes foram consultadas as bases da IEEE Xplore, Scopus, Springer Link, Science Direct e Engineering Village. O procedimento utilizado para as quatro *strings* de busca selecionadas para abordagens de conformidade legal em proteção de dados na engenharia de software é ilustrado na Figura 3-3:

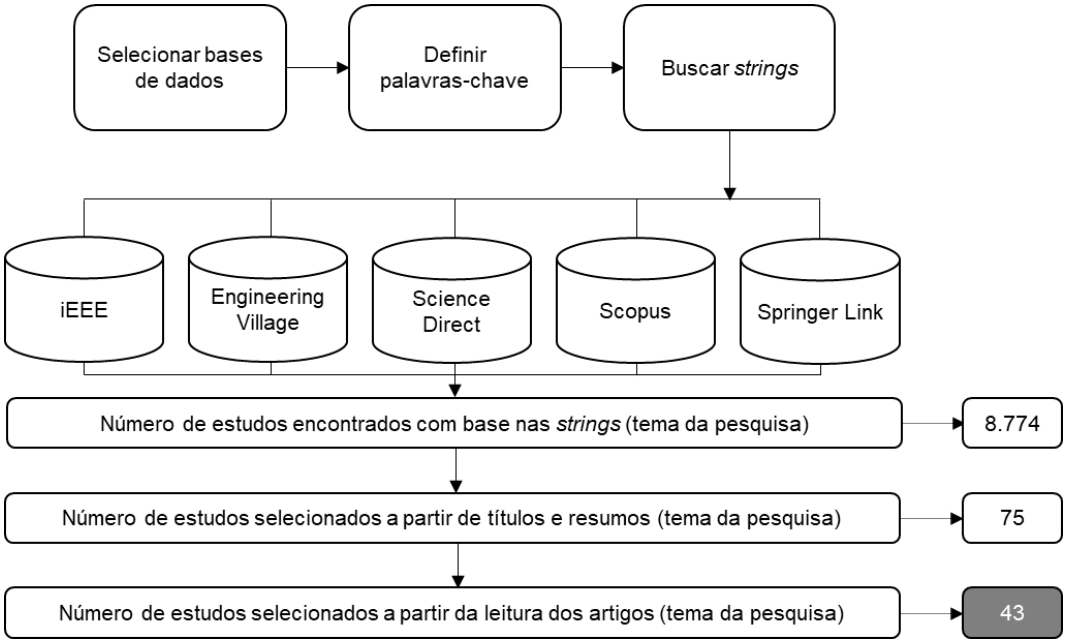

Figura 3-3. Procedimento para análise exploratória da literatura. Fonte: o Autor.

Para analisar abordagens de conformidade legal em proteção de dados na engenharia de software foram utilizadas quatro *strings* de busca nas bases mencionadas:

I. "(*startup or start-up*) AND (GDPR OR *privacy* OR *data protection*) AND (*software engineering* OR *software development* OR *software development process* OR *software development method*)";

II. "(GDPR OR *privacy* OR *data protection*) AND (*software engineering* OR *software development* OR *software development process* OR *software development method*)";

III. “(*startup or start-up*) AND (LGPD OR *privacy* OR *data protection*) AND (*software engineering* OR *software development* OR *software development process* OR *software development method*)”;

IV. “(LGPD OR *privacy* OR *data protection*) AND (*software engineering* OR *software development* OR *software development process* OR *software development method*)”.

A consulta foi realizada em 30/06/2021 para as duas primeiras *strings* e em 06/08/2021 para as duas últimas *strings*, nas cinco bases de dados já mencionadas.

A primeira *string* retornou 896 artigos, conforme apresentado na Tabela 3-1, dos quais nove foram selecionados a partir da leitura de títulos e resumos. Porém, após realizada a leitura completa, nenhum deles foi selecionado, por não se tratar do tema da pesquisa.

Tabela 3-1. Resultados da busca pela *string* 1. Fonte: o Autor.

***String*: (startup or start-up) AND (GDPR OR privacy OR data protection) AND (software engineering OR software development OR software development process OR software development method)**			
Nome da base	**Retornou**	**Títulos e Resumos**	**Aceitos**
IEEE	1	0	0
Engineering Village	65	1	0
Science Direct	271	2	0
Scopus	4	0	0
Springer	555	6	0
Total	896	9	0

A segunda *string* retornou 7.541 artigos, dos quais, após lidos títulos e resumos, foram selecionados 62, conforme representado na Tabela 3-2. Após analisados os 62 artigos, foram selecionados 39 para leitura e análise.

Tabela 3-2. Resultados da busca pela string 2. Fonte: o Autor.

String: (GDPR OR privacy OR data protection) AND (software engineering OR software development OR software development process OR software development method)			
Nome da base	**Retornou**	**Títulos e Resumos**	**Aceitos**
IEEE	1718	12	5
Engineering Village	1263	25	21
Science Direct	3006	12	3
Scopus	1013	6	3
Springer	511	7	7
	7541	62	39

As duas últimas *strings* trazem o termo LGPD no lugar de GDPR. A terceira *string* retornou um total de 333 artigos, porém após feita a leitura dos títulos e resumos nenhum deles foi selecionado por não se tratar do tema da pesquisa.

Tabela 3-3. Resultados da busca pela *string* 1. Fonte: o Autor.

***String*: (startup or start-up) AND (LGPD OR privacy OR data protection) AND (software engineering OR software development OR software development process OR software development method)**			
Nome da base	**Retornou**	**Títulos e Resumos**	**Aceitos**
IEEE	1	0	0
Engineering Village	53	0	0
Science Direct	275	0	0
Scopus	4	0	0
Springer	0	0	0
Total	333	0	0

A quarta *string* retornou um total de 3.455 artigos, dos quais quatro foram destacados a partir de leitura de títulos e resumos. Três deles tratam do âmbito do GDPR, dois dos quais já haviam sido previamente selecionados na consulta da segunda *string*. O quarto artigo trata de proteção de dados em geral, apenas citando a existência da LGPD.

Tabela 3-4. Resultados da busca pela *string* 3. Fonte: o Autor.

String: (LGPD OR privacy OR data protection) AND (software engineering OR software development OR software development process OR software development method)			
Nome da base	**Retornou**	**Títulos e Resumos**	**Aceitos**
IEEE	399	1	1
Engineering Village	1260	0	0
Science Direct	1671	1	1
Scopus	125	1	1
Springer	1	1	1
	3455	4	4

Dos artigos selecionados, foram identificados 14 estudos que tratam de abordagens de conformidade legal em proteção de dados, todos no contexto do GDPR, que podem ser considerados mais próximos ao tema do presente trabalho. A fim de demonstrar a diferença entre eles e a presente pesquisa, foram utilizados cinco critérios, conforme apresentado na Seção 2.3.4: (i) contexto de *startups*; (ii) análise de risco em privacidade; (iii) conformidade legal; (iv) alinhamento de *stakeholders*, (v) validação na indústria.

Para caracterizar o contexto das práticas em engenharia de software em *startups* foi utilizada a seguinte *string*: (“*startup”* OR *“start-up”)* AND “software engineering”. A consulta foi realizada em 30 de julho de 2019 e selecionando-se um total de 147 artigos lidos. Posteriormente foi feito *snowballing* a partir das revisões sistemáticas de literatura encontradas e novas pesquisas para atualizar os dados da consulta original, incluindo-se mais 71 artigos lidos. Posteriormente, em agosto de 2021, a busca foi refeita para pesquisar trabalhos mais recentes. Dos artigos lidos, 26

foram selecionados e serviram para definir o contexto de *startups* de software. Nenhum dos artigos tratava de conformidade legal em proteção de dados. O procedimento é apresentado na figura a seguir:

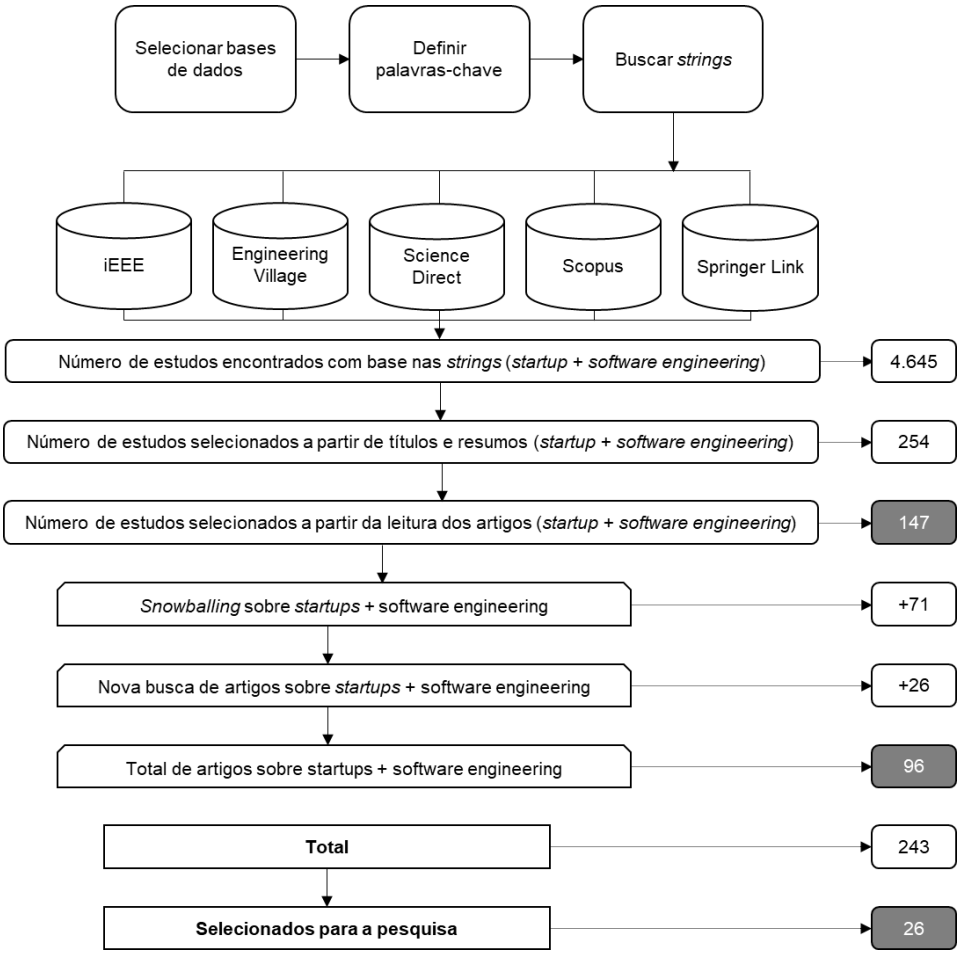

Figura 3-4. Procedimento para análise exploratória. Fonte: o Autor.

Em síntese, de um lado, a análise dos estudos selecionados traz evidências de que inexiste abordagem de engenharia de software para conformidade em LGPD no contexto de *startups*. De outro, a revisão de literatura identificou que *startups* possuem um contexto singular, e não sabem como realizar conformidade legal em proteção de dados (NORVAL *et al.*, 2021), têm dificuldade de implementá-la (BLEIER *et al.*, 2020), embora entendam-na como onerosa (MARTIN *et al.*, 2019), porém necessária, já que a não adequação pode ter como consequências a perda de credibilidade e sanções, como multas, que podem inviabilizar a existência dessas empresas (MARTIN *et al.*, 2019, BACHLECHNER; LIESHOUT; TIMAN, 2019, NORVAL *et al.*, 2021).

3.2.2 Definição dos objetivos para a solução

A revisão de literatura identificou a necessidade de *startups* introduzirem práticas de conformidade de proteção de dados no desenvolvimento de software (Martin et al., 2019, BACHLECHNER; LIESHOUT; TIMAN, 2019, BLEIER *et al.*, 2020, NORVAL *et al.*, 2021).

Nesse contexto, conforme já apresentado, a presente pesquisa traz como objetivo geral: propor um método de tomada de decisão apoiado em um conjunto de recomendações para *startups*, na implementação da conformidade com a LGPD durante o processo de desenvolvimento de software.

Para atingir esse objetivo, tem-se como objetivos específicos:

(a) Investigar como *startups* lidam com atividades de proteção de dados pessoais ao longo do desenvolvimento de software.

(b) Desenvolver um método de tomada de decisão e um conjunto de recomendações que apoiem *startups* na conformidade com a LGPD nas práticas de desenvolvimento de software.

(c) Avaliar a abordagem.

Como esta etapa trata de definição de objetivos da solução – ou seja, o que o artefato vai aperfeiçoar – estabelece-se como objetivo que, ao usar o método, o tomador de decisão de *startup* pode decidir sobre quando e como lidar com questões de conformidade em LGPD em atividades de engenharia de software.

3.2.3 Projeto e desenvolvimento

Na revisão de literatura foi identificado o contexto específico de engenharia de software em que as *startups* operam (MELEGATI *et al.* 2020), bem como foram apresentados os pontos de atenção para o desenvolvimento de software com base no texto da legislação. Além disso, foi possível também identificar estudos no âmbito do GDPR, normas técnicas e padrões que podem auxiliar o desenvolvimento da abordagem.

Foram analisados também ao todo 814 resumos de decisões administrativas de autoridades nacionais de proteção de dados de países pertencentes à União

Europeia, cadastradas no site CMS Law GDPR *Enforcement Tracker*, (banco de dados de um escritório de advocacia presente em mais de 40 países) [8].

Com base nesse corpo de conhecimento foi desenvolvida uma abordagem para o contexto das *startups*, de apoio para a tomada de decisão de desenvolvimento de software em conformidade com a LGPD. A proposta, com seu artefato, é apresentada no Capítulo 4.

3.2.4 Demonstração

A etapa de demonstração iniciou com a definição do escopo: analisar o método proposto, a partir da percepção de utilidade, facilidade e intenção de uso futuro de praticantes e tomadores de decisão de *startups*, nos termos sugeridos pelo *Technology Acceptance Model* (TAM 3) (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008).

Em seguida, foram realizadas sessões de avaliação do artefato junto ao Grupo de Pesquisa de Engenharia de Software do PPGIA-PUCPR, que reúne desenvolvedores de software, pesquisadores de engenharia de software e profissionais da indústria. Os apontamentos trazidos serviram para definir o conjunto de pontos a serem tratados no método. Nas análises, foi levado em consideração que o artefato seria usado por tomadores de decisão de *startups*, e que, portanto, precisava ser leve e didático. Isso porque tomadores de decisão de *startups* geralmente possuem poucos conhecimentos de conformidade de LGPD.

Com o artefato pronto, na fase de planejamento, foram definidos os tomadores de decisão de *startups* do primeiro ciclo, o modo como seriam coletados os dados e o instrumento de avaliação.

Na fase seguinte, de execução, foram realizados os procedimentos de coleta de dados da avaliação empírica, que aconteceram em dois momentos, conforme detalhado no Capítulo 5 – Demonstração e Avaliação.

Foram conduzidos dois ciclos de sessões online de demonstração. Em cada um deles, o pesquisador explicou o procedimento para que os tomadores de decisão aplicassem o método. O pesquisador comunicou que no corpo do texto do método havia um link com um tutorial. Comunicou também que, ao finalizarem, avisassem

[8] CMS LAW GDPR ENFORCEMENT TRACKER. Disponível em: https://www.enforcementtracker.com/. Acesso: em 13 jul. 2024.

para que o pesquisador gerasse o relatório, com o resultado da avaliação de risco e o conjunto de recomendações para mitigar os riscos de conformidade.

Explicou, ainda, que, após receberem relatório, deveriam preencher o questionário de avaliação de uso da ferramenta, uso futuro dos artefatos (o que já constitui parte da atividade seguinte, de avaliação). O pesquisador acompanhou todas as sessões com os tomadores de decisão de *startups*, para caso de dúvidas. Para a avaliação foi utilizado o *Technology Acceptance Model* (TAM 3) (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008).

Uma vez aceita a participação, os tomadores de decisão realizaram a leitura e deram o aceite no Termo de Consentimento Livre e Esclarecido (TCLE). Em seguida, leram a proposta de abordagem e a aplicaram. Quando terminaram, o pesquisador apresentou a eles o relatório gerado com base nas respostas que deram, que trazia uma avaliação de risco e um conjunto de recomendações.

Por fim, em cada um dos dois momentos, os tomadores de decisão preencheram um formulário para avaliação dos resultados, a fim de verificar a utilidade, a aceitação e a possibilidade de uso futuro dos artefatos (TAM3).

No primeiro ciclo, o artefato gerado foi apresentado a 24 tomadores de decisão de 21 startups. Após a análise das respostas foram realizadas alterações no tutorial do artefato, assim como foram feitas ligeiras modificações na parte explicativa de algumas questões. E, então, repetiu-se o procedimento de coleta de dados em avaliação empírica com mais 22 tomadores de decisão de 17 startups.

O instrumento de avaliação foi composto de: termo de consentimento, explicação da abordagem, aplicação do método, e questionário de avaliação.

3.2.5 Avaliação

Após a coleta de dados nos dois ciclos os resultados foram avaliados, utilizando codificação provisória (SALDAÑA, 2013) para as questões abertas, a fim de realizar investigação exploratória para avaliação da abordagem proposta, bem como foi usado um questionário, a fim de aferir a utilidade, facilidade de uso e intenção de uso futuro do método, bem como limitações e sugestões de aprimoramento, a partir do uso do modelo TAM3 (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008).

3.2.6 Comunicação

Na atividade de comunicação é descrita a avaliação da abordagem utilizada, sua utilidade e eficácia para resolver problemas de tomada de decisão de engenharia de software levando em consideração a necessidade de conformidade com a LGPD. Espera-se que a abordagem proposta seja útil para *startups* apoiarem suas atividades de desenvolvimento em conformidade legal de proteção de dados. A avaliação da abordagem será comunicada a *startups*, bem como é comunicada nesta tese e artigos futuros.

3.3 Considerações sobre o capítulo

Foi apresentada neste capítulo a estrutura da pesquisa da tese de doutorado. Primeiro, detalharam-se os métodos escolhidos para o desenvolvimento da pesquisa: o DSRM e suas etapas, os procedimentos de revisão de literatura e método de avaliação do artefato que será elaborado. Em seguida, apresentaram-se os passos dados para a realização do trabalho.

CAPÍTULO 4 - MÉTODO PROPOSTO

O método proposto tem como premissa que um nível baixo de conformidade gera um alto risco. Assim, quanto maior o risco, maiores podem ser as consequências sobre os direitos dos titulares de dados (GELLERT, 2018). Ao utilizar o método, o tomador de decisão de *startup* consegue avaliar o nível de risco de conformidade em diferentes aspectos, podendo implementar as medidas sugeridas, a fim de mitigar esse risco.

4.1 Bases conceituais do método proposto

Esta sessão detalha as bases conceituais do método proposto, que são resumidas a seguir no Quadro 4-1:

Quadro 4-1. Bases Conceituais. Fonte: o Autor.

Aspecto	Bases conceituais
Ciclo de Vida dos Dados	Artigos 15, I, II, 16, e 46 da LGPD CNIL (2015, 2018) Normas ISO/IEC 27.001 e ISO/IEC 27.002 Wuyts, Sion e Joosen (2020), Li et al. (2020), Open Worldwide Application Security Project (2022) 100 decisões administrativas de autoridades de proteção de dados de países da União Europeia, identificadas no CMS Law GDPR Enforcement Tracker *Recommendations for a methodology of the assessment of severity of personal data breaches* (*European Union Agency for Cybersecurity*, 2013)
Desenvolvimento	Artigo 46 da LGPD Normas ISO/IEC 27.001 e ISO/IEC 27.002 CNIL (2015, 2018)
Conformidade de Tratamento	Artigos 6º, I, II, III, IV, V, IX, e 50, §1º, da LGPD Wuyts, Sion e Joosen (2020), Li et al. (2020) 520 decisões administrativas de autoridades de proteção de dados de países da União Europeia, identificadas no CMS Law GDPR Enforcement Tracker 7 decisões administrativas da Autoridade Nacional de Proteção de Dados 137 decisões judiciais brasileiras, catalogadas no Painel LGPD nos Tribunais - 2022 Resolução CD/ANPD nº 2 *Recommendations for a methodology of the assessment of severity of personal data breaches* (*European Union Agency for Cybersecurity*, 2013)
Direitos dos Titulares de Dados	Artigos 8º, 9º, 18 e 19 da LGPD Artigos 12º, 13º, 14º, 15º, 16º, 17º, 18º, 19º, 20º do GDPR 194 decisões administrativas de autoridades de proteção de dados de países da União Europeia, identificadas no CMS Law GDPR Enforcement Tracker 137 decisões judiciais brasileiras, catalogadas no Painel LGPD nos Tribunais – 2022

Para a construção do método de apoio à tomada de decisão com base em riscos de conformidade em LGPD, tem-se como ponto inicial parte das orientações de

processo de avaliação de riscos, nos termos da ISO/IEC 27.005 e da ISO/IEC 31.000. Ambos os documentos estabelecem etapas de identificação, análise e avalição de riscos. Essas etapas foram usadas para estruturar a construção do método com base em risco.

Foram utilizados também para a construção do método o texto da LGPD e do GDPR, a revisão de literatura do Capítulo 2, bem como foram analisados 814 resumos de decisões administrativas de autoridades nacionais de proteção de dados de países pertencentes à União Europeia, cadastradas no site *CMS Law GDPR Enforcement Tracker*.

Segundo as normas ISO/IEC 27.005 e da ISO/IEC 31.000, na etapa de identificação busca-se descrever os eventos de risco, com os ativos envolvidos e as consequências potenciais, bem como apresentar ameaças, vulnerabilidades e controles existentes. Na etapa de análise, são designados valores estimados para consequências e probabilidades de um risco, para que se possa aferir o risco. Por fim, na etapa de avaliação, é avaliado o nível de exposição ao risco existente, de modo que, a partir disso, o tomador de decisão possa decidir o que fazer (ou não fazer) em relação a ele.

Para os fins deste trabalho, foram usadas somente orientações necessárias para a construção do método, concentrando a atenção no objetivo de apoiar *startups* na implementação da conformidade com a LGPD durante o processo de desenvolvimento de software.

A perspectiva aqui adotada difere daquelas que buscam a análise de eventos de violações de segurança de informação. Abordagens em segurança de informação orientam-se a evitar violações de confidencialidade, integridade e disponibilidade dos dados. A abordagem objeto desta tese, diferentemente, trata, por óbvio dos aspectos de segurança de informação, mas lida também com outras de questões de conformidade em LGPD que tenham algum impacto em atividades de engenharia de software.

A LGPD é uma norma que, como já evidenciado no Capítulo 2 – Revisão de Literatura, abrange tanto a segurança de informação – mais especificamente segurança de dados pessoais –, como outros aspectos. A norma estabelece, entre outras obrigações, o dever de o tratamento respeitar os princípios inscritos no Artigo 6º da lei, bem como a necessidade de cumprir com as solicitações dos titulares no que tange aos direitos elencados nos Artigos 18 e 19 da LGPD.

Há também outros deveres inscritos na lei, como os de elaborar o registro de operações de tratamento de todos os dados pessoais que tratarem (Artigo 37[9]), o de indicar um encarregado de dados[10] (Artigo 41[11]); o de tratar dados somente com base em uma hipótese legal de tratamento de dados (Artigo 7º, Artigo 11 e Artigo 23). Contudo, esses deveres são obrigações jurídicas que não interferem diretamente em atividades de engenharia de software.

As obrigações referentes aos princípios de tratamento de dados e aos direitos dos titulares, de outro lado, possuem impacto em decisões de engenharia de software.

No que tange ao tratamento, as atividades de engenharia precisam respeitar os princípios de tratamento que são elencados no Artigo 6º da LGPD. Como já mencionado, tratamento é, por definição legal, qualquer operação que seja realizada com dados pessoais. Segundo o Artigo 5º, X, isso abrange operações como: coleta e recepção; acesso e utilização; transferência, reprodução, transmissão, distribuição, difusão e comunicação; arquivamento e armazenamento; eliminação ou extração; modificação; processamento, classificação, avaliação ou controle da informação. Ou seja, tratamento é um termo que abrange desde operações muito simples, como coleta ou acesso até atividades complexas, como processamento, classificação e avaliação de informações.

A LGPD obriga que o tratamento de dados seja realizado obedecendo os princípios da boa-fé, para propósitos legítimos, específicos e informados ao titular. O tratamento precisa também ser compatível com as finalidades informadas ao titular, devendo utilizar o mínimo necessário de dados pessoais. Além disso, o tratamento precisa ser realizado de forma transparente, com dados corretos e atualizados, não podendo ser realizado para finalidades discriminatórias ilícitas ou abusivas.

Nesse contexto, as atividades de engenharia precisam ser levadas em conta respeitando essas obrigações de conformidade legal de tratamento de dados.

No que se refere aos direitos dos titulares, decisões de engenharia de software permitem facilitar que os titulares tenham suas solicitações cumpridas pelos agentes de tratamento. A LGPD determina no Artigo 18 que o controlador tem o dever de,

---

[9] LGPD, Artigo 37: “O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.”

[10] Nos termos do Artigo 5º, VIII: “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).”

[11] LGPD, Artigo 41. “O controlador deverá indicar encarregado pelo tratamento de dados pessoais.”

quando solicitado pelo titular de dados: confirmar a existência de tratamento de dados do titular; permitir o acesso ao dados; permitir a correção de dados; cumprir com a obrigação de anonimização, bloqueio ou eliminação de dados, quando necessário; cumprir com a obrigação de portabilidade dados para que o titular possa usar por outro fornecedor; cessar o tratamento e eliminar dados quando necessário; informar outros agentes de dados para que realizem a correção, eliminação, anonimização ou bloqueio de dados, quando necessário. Essas obrigações também devem ser pelos operadores de dados, que devem repetir as operações feitas pelo controlador, a fim de resguardar os direitos dos titulares de dados.

Decisões de engenharia podem facilitar que agentes de tratamento cumpram com essas obrigações, a fim de garantir que as solicitações dos direitos dos titulares sejam cumpridas.

A abordagem aqui apresentada, portanto, leva em conta riscos de conformidade de LGPD que podem ser mitigados por decisões de engenharia de software. Leva em consideração também o contexto das *startups*, abordado no Capítulo 2 – Revisão de Literatura.

4.2 Como o método funciona

O método é composto por três partes: (i) Preparação; (ii) Avaliação; e, (iii) Resultado, conforme a Figura 4-1:

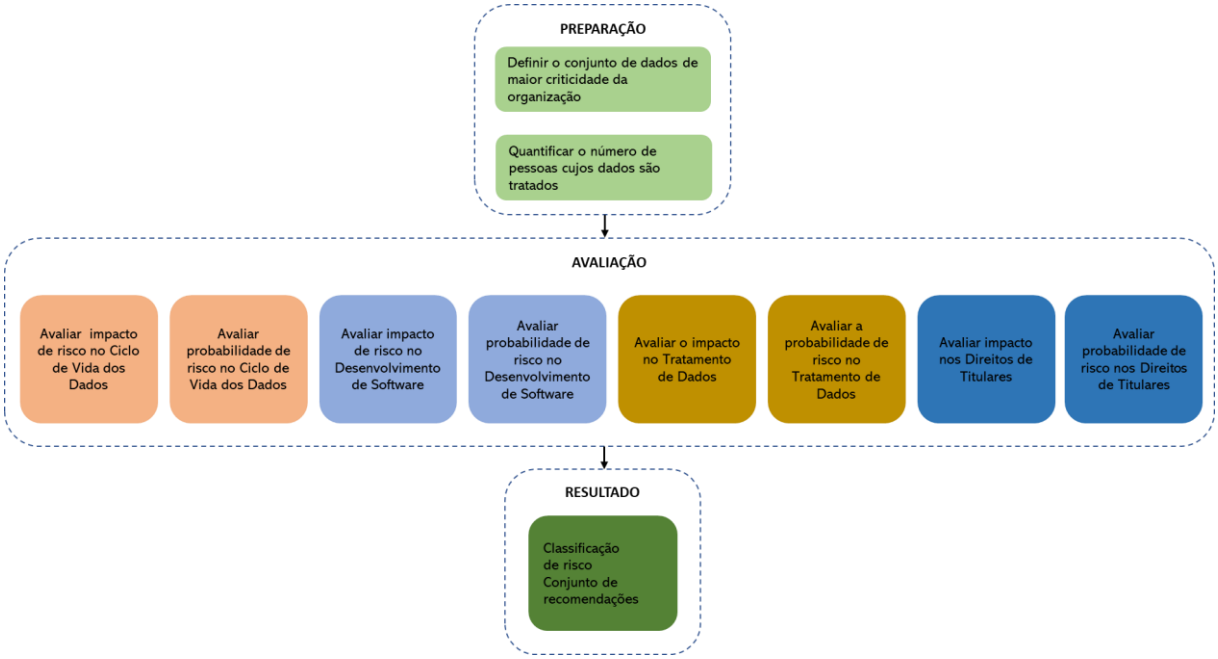

Figura 4-1. Método proposto. Fonte: o Autor.

A etapa de **Preparação** consiste em o tomador de decisão definir o conjunto de dados de maior criticidade da *startup*, bem como informar o número de pessoas que têm seus dados tratados em seu sistema.

Na etapa de **Avaliação**, o tomador de decisão avalia quatro aspectos:

(i) Ciclo de Vida dos Dados;

(ii) Desenvolvimento;

(iii) Conformidade de Tratamento; e,

(iv) Direitos dos Titulares.

Essa avaliação considera impacto e probabilidade para cada um dos quatro aspectos apresentados.

Em **Ciclo de Vida dos Dados** são tratadas questões referentes à segurança da informação dos dados pessoais, nos diferentes momentos em que é usado pela *startup*:

(i) coleta e acesso;

(ii) armazenamento;

(iii) compartilhamento; e,

(iv) retenção e eliminação.

No aspecto **Desenvolvimento** são tratados pontos que dizem respeito ao desenvolvimento de software seguro, lidando, portanto, também com questões referentes à segurança da informação.

Em **Conformidade de Tratamento** apresenta-se de questões referentes às obrigações exigidas pela LGPD, para que o tratamento de dados seja lícito, e de questões sobre atividades que são inerentemente de alto risco e podem trazer impactos mais severos aos direitos dos titulares de dados.

Em **Direitos dos Titulares** são apresentados pontos que devem ser levados em consideração quando do desenvolvimento de software pela *startup*, a fim de facilitar que os titulares tenham suas solicitações feitas à organização, bem como seus direitos garantidos.

A etapa **Resultado** consiste na geração de um relatório em que é apresentada uma classificação de risco e um conjunto de recomendações para que a *startup* possa mitigar riscos de conformidade com a LGPD.

As etapas de **Preparação e Avaliação** foram desenvolvidas utilizando o aplicativo web Qualtrics, próprio para questionário. Após o aceite no Termo de Consentimento Livre e Esclarecido (TCLE) para participação na pesquisa, e a

inserção de nome completo, nome da *startup*, e-mail e telefone (este último opcional), o tomador de decisão deve responder 42 questões, distribuídas conforme a Tabela 4-1:

Tabela 4-1. Distribuição de questões do método. Fonte: o Autor.

Questões do método por etapa, aspecto avaliado e número de questões		
Etapa	**Aspecto**	**Número de questões**
Preparação	-	3
Avaliação	Ciclo de Vida dos dados	17
Avaliação	Desenvolvimento	4
Avaliação	Conformidade de Tratamento	10
Avaliação	Direitos dos Titulares	8
Total		**42**

As questões da etapa de Preparação são de múltipla escolha e definem o conjunto de dados utilizados (duas questões) e a quantidade de pessoas cujos dados são tratados (uma questão).

Para definir o conjunto de dados, o tomador de decisão deve abrir um tutorial que possui tabelas com quatro categorias de dados (dados simples, dados de comportamento, dados financeiros e dados sensíveis) e analisar as opções apresentadas, com base em uma escala de impacto que vai de 1 (menor impacto) a 4 (maior impacto). Após a análise, o tomador de decisão deve escolher a categoria (uma questão) e a opção (uma questão) que representem o seu conjunto de dados de maior impacto. Para o segundo ciclo, esse tutorial, recebeu mais cinco slides, a fim de trazer mais orientações sobre a LGPD, conforme pode ser analisado no Apêndice D.

Embora sistemas operem geralmente com o tratamento de diversos conjuntos de dados, o método utiliza apenas o conjunto de dados de maior impacto, ou seja, de maior criticidade para a *startup*. Assim, simplifica-se a avaliação, de forma que a empresa terá, ao fim da aplicação do método, um resultado que corresponde ao seu maior risco de conformidade, podendo, portanto, tomar as ações para mitigá-los, quando julgar necessário.

Respondidas as duas questões sobre a natureza do conjunto de dados, o tomador de decisão define a quantidade de pessoas cujos dados estão sendo tratados, optando por uma das seguintes opções: (i) Até 99 pessoas; (ii) Maior igual a 100 pessoas.

Em seguida, o tomador de decisão deve responder as demais 39 questões para os quatro aspectos. Essas questões possuem três respostas possíveis: (i) Sim; (ii) Não; (iii) Não sei informar.

Após o tomador de decisão finalizar o uso do método, o pesquisador exporta o arquivo .CSV e em seguida o importa para o Excel para a geração do relatório. Um exemplo de resultado gerado a partir do uso do método é apresentado na Figura 4-2:

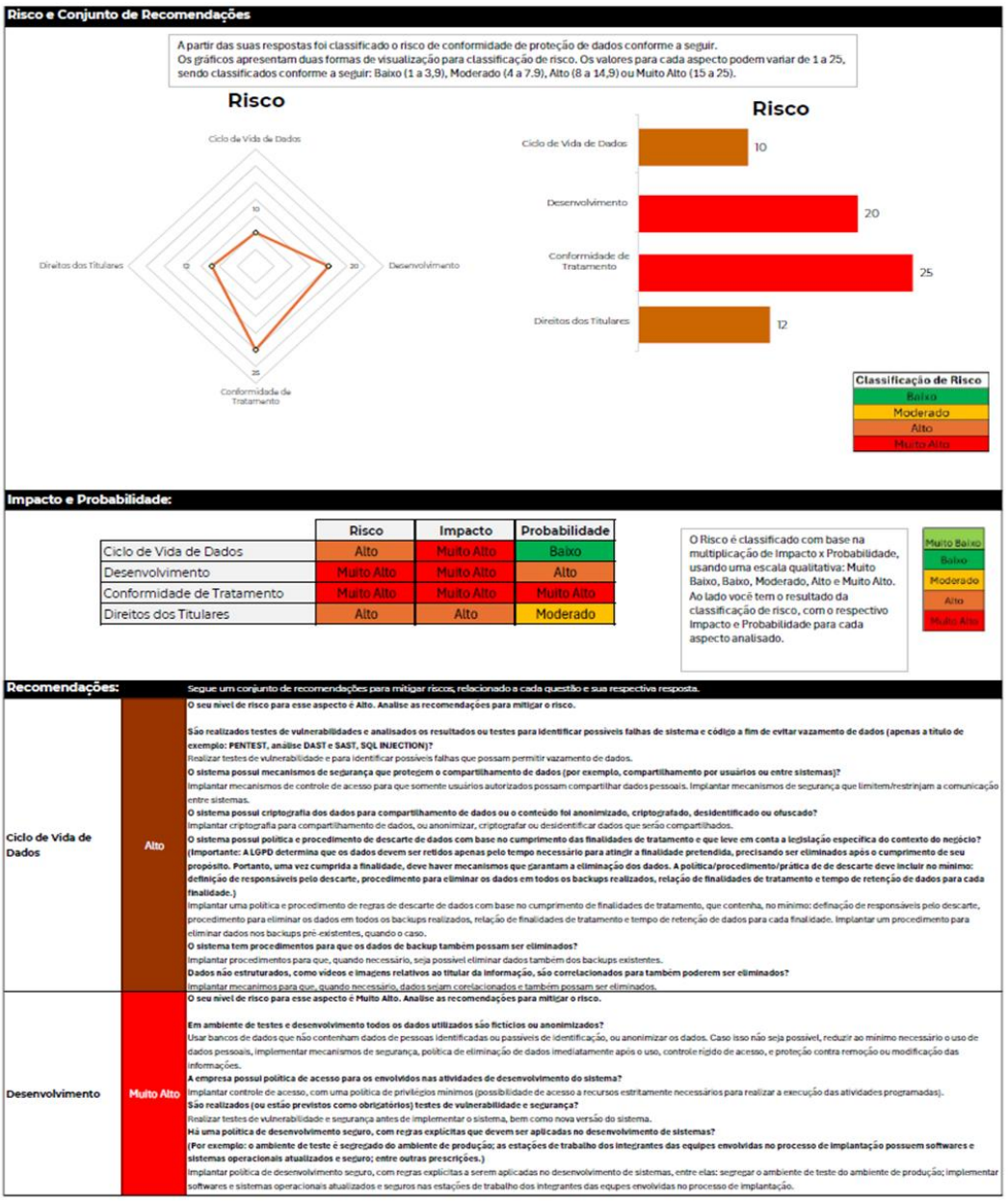

Figura 4-2. Exemplo de resultado gerado após uso do método. Fonte: o Autor.

O resultado gerado apresenta na parte superior um gráfico de teia de aranha e uma classificação de risco para os quatro aspectos, que varia de 1 a 25, classificados conforme a Tabela 4-2:

Tabela 4-2. Classificação de Risco. Fonte: o Autor.

Valor	Classificação de Risco
De 1 a 3,9	Baixo
De 4 a 7,9	Moderado
De 8 a 14,9	Alto
De 15 a 25	Muito Alto

Na parte intermediária, o resultado da classificação de risco é decomposto em impacto e probabilidade para cada um dos quatro aspectos analisados. Impacto e probabilidade podem variar em uma escala conforme a Tabela 4-3:

Tabela 4-3. Classificação de Impacto e Probabilidade. Fonte: o Autor.

Valor	Classificação de Risco
De 1 a 1,4	Muito Baixo
De 1,5 a 2,4	Baixo
De 2,5 a 3,4	Moderado
De 3,5 a 4,4	Alto
De 4,5 a 5	Muito Alto

Na parte inferior do resultado são apresentadas as recomendações para mitigação de riscos, segmentadas para cada aspecto e nível de risco identificado.

Com o resultado, portanto, o tomador de decisão consegue avaliar, de forma global, os riscos mais severos para cada aspecto de conformidade analisado e possui um respectivo conjunto de recomendações para cada ponto de risco identificado, que poderá utilizar quando entender mais adequado ao negócio.

A seguir apresenta-se como o método foi construído.

4.3 Descrição do funcionamento do método

4.3.1 Identificação dos ativos

Para fins de identificação dos riscos, o primeiro ponto a ser definido trata de quais ativos farão parte da análise.

O método proposto nesta tese estabelece que o tomador de decisão deve identificar o conjunto de dados utilizado pela *startup* que possa gerar as consequências mais severas para o negócio, e submetê-los à aplicação do método.

Portanto, a *startup* não precisa identificar suas mais diversas operações de tratamento de dados, bastando, apenas, delimitar o escopo de análise para o conjunto

de informações pessoais de maior impacto. Embora essa análise simplifique o que acontece na realidade – pois a *startup* geralmente vai realizar diversos tratamentos de dados pessoais, para diversas finalidades –, concentrar a atenção somente no conjunto mais relevante de dados permite conhecer o maior risco, de forma ágil, facilitando a avaliação e o uso do método.

Supondo que o tomador de decisão entenda que há outros conjuntos de dados igualmente relevantes e que deveriam ser avaliados, basta repetir a análise para esse novo conjunto de dados, de modo que a simplificação apresentada não se constitui em obstáculo para análises mais detalhadas.

4.3.2 Identificação de riscos

Uma vez identificado o ativo, é necessário deliminar os eventos de risco. Conforme já apresentado, risco pode ser compreendido como um cenário hipotético que descreve um evento temido e as ameaças que podem possibilitar sua ocorrência (CNIL, 2018). No caso do risco de desconformidade com a LGPD, os eventos de risco são as violações de dispositivos legais.

Além de se configurarem como violação de dispositivos da LGPD, os riscos podem ter como consequência violações mais amplas de direitos no caso concreto, como violação da privacidade e da intimidade, discriminação, dano patrimonial ou moral, impedimento de exercício de direitos, entre outras possibilidades. As ameaças, por sua vez, se constituem em tudo o que pode contribuir para que as violações legais se concretizem.

Nesse contexto, foi realizado um exame do texto da LGPD, a fim de identificar eventos de risco que de alguma forma podem ter influência no âmbito da engenharia de software – seja para aumentar o risco, seja para mitigá-lo. No Quadro 4-2, estão listados os eventos de risco e um resumo de sua descrição na LGPD.

Quadro 4-2. Eventos de risco de conformidade em LGPD. Fonte: o Autor.

Evento	Descrição
Violação do Art. 46, LGPD	Descumprimento dos deveres de segurança e prevenção nos termos do art. 46 da LGPD, que obriga empregar medidas técnicas “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”
Violação dos Art. 15, I, II, e Art. 16, LGPD	Descumprimento de regras de eliminação de dados após a finalidade do tratamento ser atingida, ou o período de tratamento ter acabado

Violação do Art. 6º, I, II, III;V; IX	Tratamento em desconformidade legal no que se refere à finalidade, adequação, necessidade, qualidade de dados e não discriminação
Violação dos Art. 9º, 18 e 19, LGPD	Descumprimento dos dispositivos que garantem direitos dos titulares
Violação dos art. 8º, §1º, §2º, §4º, 5º §6º, art. 18, VIII, IX, LGPD	Descumprimento das regras de consentimento

A LGPD apresenta no Artigo 46 o dever de implementação de medidas técnicas que sejam aptas a proteger dados pessoais de violações referentes “a acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação” (Brasil, 2018).

Os deveres de conformidade em LGPD, contudo, como já observado, não se restringem à proteção de dados com o fim de evitar violações de segurança. O Artigo 15, I, II e o Artigo 16 prescrevem a necessidade de cumprimento de regras em relação à retenção e eliminação de dados. O Artigo 6º, I, II, III, V, IX da lei, por sua vez, traz princípios que devem ser seguidos para que o tratamento de dados seja considerado em conformidade com a LGPD.

Além disso, de outro lado, os artigos 9º, 18 e 19 da LGPD trazem dispositivos referentes aos deveres de transparência e de atendimento às solicitações dos titulares de dados. Por fim, o Artigo 8º, §1º, §2º, §4º, 5º §6º, e o artigo. 18, VIII, IX, da LGPD, apresentam regras a serem seguidas para evitar desconformidade quando há a coleta de consentimento de titulares para a realização de um tratamento de dados pessoais previamente determinado e informado.

Após identificar os eventos de violação de conformidade da LGPD que estão relacionados às atividades de engenharia de software, eles foram divididos em quatro aspectos para a realização da análise de risco: (i) Ciclo de Vida dos Dados; (ii) Desenvolvimento; (iii) Conformidade de Tratamento; e (iv) Direitos dos Titulares.

O aspecto Ciclo de Vida dos Dados trata de eventos de violação de segurança dos dados pessoais, ao longo de toda a trajetória dos dados na organização. Abrange desde a coleta e o acesso, até o armazenamento, compartilhamento e eliminação dos dados.

O aspecto Desenvolvimento trata de eventos de risco de segurança que possam ocorrer durante as atividades de desenvolvimento de software. Neste aspecto, estão incluídas tanto as atividades realizadas antes de o produto ser disponibilizado aos usuários, quanto as que são efetuadas após a disponibilização, em novas versões de software.

O aspecto Conformidade de Tratamento refere-se às atividades de tratamento que podem violar a LGPD e, por consequência, infringir direitos dos titulares de dados. Este aspecto trata de violações a princípios de tratamento de dados previstos na legislação, bem como de atividades de tratamento que possuem alto risco, por conta da própria natureza da operação.

Por fim, o aspecto Direitos dos Titulares trata das atividades de engenharia que possam causar, ou facilitar, o descumprimento de obrigações em relação aos direitos dos titulares garantidos pela LGPD, nos Artigos 18 e 19.

Como já mencionado, os eventos de risco de conformidade em LGPD são violações de dispositivos legais. Esses eventos, quando ocorrem, geram consequências que podem, além de violar o direito de proteção de dados, resultar em impactos sobre outros direitos do titular de dados, como invasão da privacidade e da intimidade, discriminação, dano patrimonial ou moral, entre outros.

Esse conjunto de violações – do próprio direito à proteção de dados, e de outros direitos fundamentais e liberdades – por sua vez, pode ter consequências diversas, como: (i) sanções administrativas da ANPD; (ii) condenações judiciais, por conta de ações movidas por titulares de dados, Ministério Público ou outras organizações; (iii) dano reputacional; (iv) prejuízo comercial, por causa de comprometimento de operações, perda de clientes ou recusa de investidores. O Quadro 4-3 relaciona os quatro aspectos com os eventos de risco e as consequências possíveis:

Quadro 4-3. Eventos de risco e consequências e aspectos de análise. Fonte: o Autor.

Aspecto	Evento	Consequência/dano
Ciclo de Vida dos Dados (Coleta, Armazenamento, Acesso, Compartilhamento, Retenção e Eliminação)	Violação do Art. 46, LGPD Violação dos Art. 15, I, II, e Art. 16, LGPD	Impacto sobre Direitos Fundamentais e liberdades que podem acarretar: Sanção da ANPD Condenações judiciais Dano reputacional Prejuízo comercial
Desenvolvimento	Violação do Art. 46, LGPD	
Conformidade de Tratamento	Violação do Art. 6º, I, II, III;V; IX	
Direitos dos Titulares	Violação dos Art. 9º, 18 e 19, LGPD Descumprimento das regras de consentimento	

Uma vez estabelecidos os aspectos e seus respectivos eventos de risco, bem como as consequências que podem advir da violação dos preceitos legais, passa-se para a etapa de análise de risco.

4.3.3 Análise de risco

Nesta etapa são estabelecidos valores para impacto das consequências e probabilidades dos cenários de risco. Apresenta-se para cada aspecto analisado: as justificativas para: (i) estimar o impacto das consequências; (ii) estimar a probabilidade de ocorrência de eventos; (iii) estabelecer pesos para cenários de risco, quando necessário.

Os valores para impacto e probabilidade foram estabelecidos em uma escala qualitativa, de 1 a 5, em que o valor 1 é o menor e o valor 5, o maior. Optou-se por uma escala qualitativa porque até o momento, no cenário brasileiro, há pouca informação consolidada sobre valores de indenizações judiciais ou multas administrativas com base na LGPD.

A seguir, apresenta-se a classificação utilizada para impacto e probabilidade:

Tabela 4-4. Classificação de Impacto e Probabilidade. Fonte: o Autor.

Valor	Classificação de Risco
1	Muito Baixo
2	Baixo
3	Moderado
4	Alto
5	Muito Alto

No que se refere à Probabilidade, os valores resultantes do cálculo podem apresentar casas decimais, por conta do número de questões consideradas no formulário. Por exemplo, Ciclo de Vida dos Dados possui 17 questões para a avaliação de probabilidade. Como para questão é atribuído o valor de 1/17avos, o resultado terá casas decimais. Quando isso ocorrer, o valor será arredondado seguindo a regra matemática padrão.

Importante mencionar também que, para o cálculo de probabilidade, foi analisado, para cada aspecto, se havia a necessidade de estabelecer pesos para as questões. Essa análise foi feita como base no cenário de risco e no artigo de lei a que se referiam as questões. Para justificar a inclusão de pesos para as questões, quando necessário, houve necessidade de se recorrer ao direito comparado do contexto do GDPR, uma vez que as decisões no Brasil, sejam administrativas, da ANPD, sejam judiciais, dos Tribunais, ainda são escassas.

A seguir apresenta-se como foi construído o aspecto Ciclo de Vida dos Dados e, em seguida, Desenvolvimento. Na sequência, descreve-se como foi estruturado o

aspecto Conformidade de Tratamento, e, então, Direitos dos Titulares. Por fim, apresenta-se um quadro sintético para resumir a forma como impacto e probabilidade são avaliadas em cada aspecto.

4.3.3.1 Ciclo de Vida dos Dados

Para estimar consequências e probabilidade no **Ciclo de Vida dos Dados**, preliminarmente é necessário relembrar que este aspecto trata de eventos de violação aos artigos 15, I, II, 16, e 46 da LGPD. Como já descrito, são dispositivos legais que dizem respeito à segurança de informação durante o tratamento dos dados (Artigo 46, LGPD) e a questões referentes à retenção e eliminação dos dados (Artigos 15, I, II, 16, LGPD).

A importância do artigo 46 da lei para a avaliação de risco no Ciclo de Vida dos Dados fica mais clara ao se analisar o texto do dispositivo:

> 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. (Brasil, 2018)

O dispositivo trata de pontos que no âmbito da segurança de informação se referem à violação de dados. Há, inclusive, equivalência entre o texto da lei com princípios de segurança de informação. Para efeitos de comparação, note-se que a *Commission Nationale Informatique & Libertés*, a agência francesa de proteção de dados, em dois de seus documentos considera violação de dados como (CNIL, 2015, 2018):

(i) Acesso ilegítimo a dados pessoais, ou seja, violação de confidencialidade;

(ii) Alteração indesejada de dados pessoais, ou seja, violação de integridade;

(iii) Desaparecimento de dados pessoais, ou seja, violação de disponibilidade.

Quando se compara o texto do Artigo 46 da LGPD com as definições de violação de dados estabelecida pela CNIL nota-se que há uma correlação entre eles, conforme apresentado no Quadro 4-4:

Quadro 4-4. O Artigo 46 da LGPD e as violações de dados da CNIL. Fonte: o Autor.

Artigo 46 da LGPD (Brasil, 2018)	CNIL (2015, 2018)
Acesso não autorizado, situações acidentais ou ilícitas de comunicação	Violação de confidencialidade
Situações acidentais ou ilícitas de alteração	Violação de Integridade
Situações acidentais ou ilícitas de destruição, perda	Violação de Disponibilidade

Portanto, é possível afirmar que grande parte do dispositivo do artigo 46 estabelece a necessidade de adoção de medidas técnicas e administrativas que impeçam a violação de dados. Somente a parte final do referido dispositivo menciona a questão do tratamento inadequado ou ilícito. Esse ponto, entretanto, é analisado no aspecto de Conformidade de Tratamento.

Por essa razão, quando se trata de analisar os riscos no Ciclo de Vida dos Dados, busca-se compreender como os dados pessoais podem permanecer seguros ao longo das atividades de coleta, armazenamento, acesso, compartilhamento, e retenção e eliminação.

Para analisar a probabilidade de o evento de risco ocorrer ao longo desses sub-aspectos do Ciclo de Vida dos Dados, como se trata de aspectos de segurança, utilizaram-se como referência as Normas ISO/IEC 27.001 e ISO/IEC 27.002, bem como dois artigos que foram selecionados durante a etapa de revisão de literatura – Wuyts, Sion e Joosen (2020) e Li et al. (2020) –, o Projeto Aberto de Segurança em Aplicações Web (*Open Worldwide Application Security Project*, 2022), além do texto dos artigos 15 e 16, bem como o já citado artigo 46, da LGPD.

Esses conteúdos foram utilizados para elaborar 17 questões para aferição de probabilidade, bem como um conjunto de recomendações correspondente para mitigar os riscos. O questionário completo encontra-se no Apêndice A. O Quadro 4-5 apresenta alguns exemplos de questões:

Quadro 4-5. Exemplo de Questões – Ciclo de Vida de Dados, Probabilidade. Fonte: o Autor.

I. Em relação às atividades de Coleta e Acesso:	**Referência**	**Tratamento**
Os usuários são autenticados de forma segura (apenas a título de exemplo: certificação digital, autenticação multifator)?	ISO/IEC 27001, 8.5	Usar procedimentos de autenticação seguros (por exemplo: certificação digital, autenticação multifator)
II. Em relação às atividades de Armazenamento:		
O sistema registra o rastreamento de usuários que fizeram alterações nos dados relevantes da aplicação?	ISO/IEC 27001, 8.15	Implantar rastreamento de usuários que fizeram alterações em dados armazenados.

III. Em relação às atividades de Compartilhamento:		
O sistema possibilita que somente usuários autorizados possam compartilhar dados?	ISO/IEC 27001, 8.2, 8.3	Implantar controle de acesso para que somente usuários autorizados possam compartilhar dados.
IV. Em relação às atividades de Retenção e Eliminação: (4Q)		
O sistema tem procedimentos para que os dados de backup também possam ser eliminados?		Implantar procedimentos para que, quando necessário, seja possível eliminar dados também dos backups existentes.

As questões percorrem todo o ciclo de vida dos dados e foram divididas, apenas para fins didáticos de apresentação aos tomadores de decisão, em quatro partes: (i) coleta e acesso, (ii) armazenamento, (iii) compartilhamento, (iv) retenção e eliminação.

Em todas as questões, as respostas dadas com “Não” ou “Não sei informar” pontuam, com valor 1. As respostas com “Sim, não pontuam – ou seja, o valor atribuído a elas é zero.

O valor da probabilidade foi normalizado para uma escala de 1 a 5, conforme a Equação 4-1.

Equação 4-1. Cálculo da probabilidade para o Ciclo de Vida dos Dados. Fonte: o Autor.

$$P = 1+(\sum Q/17) \cdot 4$$

P: Probabilidade
∑Q: Somatório de questões cuja resposta foi “Não” ou “Não sei informar”

O valor de probabilidade levará em conta as respostas dadas com “Não” ou “Não sei informar” no conjunto das 17 questões, multiplicado por 4 e, então, somado 1. Caso todas as respostas sejam “Sim”, o valor para Probabilidade será 1. Afinal, não existe Probabilidade zero para um evento de risco. Sempre haverá uma probabilidade residual.

Não foram estabelecidos pesos diferentes para as questões. Essa medida teve como base, em primeiro lugar, a análise de 100 resumos de decisões administrativas de autoridades nacionais europeias, proferidas entre 4 de outubro de 2022 a 13 de

novembro de 2023 e, que tratam de falhas em medidas técnicas e organizacionais para a proteção de dados pessoais. Pela análise das decisões, identificadas no *CMS Law GDPR Enforcement Tracker*, não foi possível identificar quais falhas de segurança são mais recorrentes e justificariam um peso maior.

Em segundo lugar, muitas das vulnerabilidades de segurança, caso ocorram individualmente podem ter como resultado uma violação que atinge os dados e desencadear consequências relativas a todo esse conjunto de dados. Ou seja, uma única vulnerabilidade pode ter consequência no todo. Nesse sentido, isso é muito diferente do que ocorre com os aspectos de Conformidade de Tratamento e Direito dos Titulares, em que os diferentes cenários de risco para vão ter consequências distintas, trazendo diferentes probabilidades de ocorrência para cada um deles, o que será detalhado mais adiante.

Para analisar o Impacto do evento de risco no Ciclo de Vida dos Dados, utiliza-se a classificação de dados pessoais apresentada pela *European Union Agency for Cybersecurity – Enisa* (2013), no documento *Recommendations for a methodology of the assessment of severity of personal data breaches*. O documento traz um método para que organizações possam avaliar quando devem informar às autoridades a ocorrência de uma violação de dados pessoais.

Como somente violações de dados que possam causar danos relevantes a direitos dos titulares devem ser informadas, a Enisa estabeleceu uma fórmula para que as organizações avaliem se devem ou não comunicar um incidente. A fórmula envolve impacto dos dados violados, número de titulares afetados, entre outras características.

Um dos tópicos apresentados na fórmula utilizadas pela Enisa, e que foi adaptado para este trabalho, é uma classificação de impacto de dados que abrange quatro categorias: (i) dados simples; (ii) dados comportamentais; (iii) dados financeiros; (iv) dados sensíveis. Com base nessas categorias, estabelece uma gradação de criticidade dos dados, com valores de 1 a 4. A Tabela 4-5 apresenta essas categorias de dados, descrições para cada uma das gradações de criticidade dos dados e o valor atribuído para cada delas.

Para compor a análise de impacto em relação aos dados, cuja escala é de 1 a 5, a Enisa estabelece ainda que, quando o volume de pessoas que tiveram seus dados violados é superior a 100, acrescenta-se “mais um” ao resultado da classificação de impacto dos dados.

Para o âmbito da LGPD, a classificação é adequada, porque, assim como no contexto europeu, a norma brasileira estabelece, no Artigo 48, que o controlador deve comunicar à ANPD e ao titular o incidente de segurança que possa acarretar risco ou dano relevante às pessoas afetadas.

Tabela 4-5. Categorias de dados pessoais. Fonte: o Autor, adaptado de Enisa (2013).

Categorias de Dados		Valor
Dados Simples	**Exemplo: dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.**	
	Pontuação básica: quando a violação envolve ‘’dados simples’’ e a empresa não tem conhecimento de quaisquer circunstâncias consideradas agravantes.	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de “dados simples” e/ou as características do controlador são tais que certos perfis do indivíduo podem ser habilitados ou podem ser feitas suposições sobre o status social/financeiro do indivíduo.	**2**
	A pontuação pode ser de 2, por exemplo, quando os “dados simples” e/ou as características do controlador podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas.	**3**
	A pontuação pode ser aumentada em 3, p. e., quando devido a certas características do indivíduo (grupos vulneráveis, menores etc), as informações podem ser críticas para sua segurança pessoal ou condições físicas/psicológicas.	**4**
Dados de comportamento	**Exemplo. localização, dados de trânsito, dados sobre preferências e hábitos pessoais etc.**	
	Pontuação básica: quando a violação envolve ‘’dados comportamentais’’ e a empresa não tem conhecimento de circunstâncias agravantes ou atenuantes.	**2**
	A pontuação pode ser diminuída em 1, e. quando a natureza do conjunto de dados não fornece informações substanciais sobre as informações comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de “dados comportamentais” e/ou as características do controlador são tais que pode ser criado um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos.	**3**
	A pontuação pode ser aumentada em 2, por exemplo, se um perfil baseado em dados confidenciais do indivíduo puder ser criado.	**4**
Dados financeiro	**Dado de renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.**	
	Pontuação básica: quando a violação envolve ‘’dados financeiros’’ e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes.	**3**
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobre as informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem maiores detalhes).	**1**
	A pontuação pode ser diminuída em 1, por exemplo, quando o conjunto de dados específico inclui algumas informações financeiras, mas ainda não fornece informações significativas sobre a situação/status financeiro do indivíduo (por exemplo, números simples de contas bancárias sem mais detalhes).	**2**
	A pontuação pode ser aumentada em 1, por exemplo, quando, devido à natureza e/ou volume do conjunto de dados específico, informações financeiras completas (por exemplo, cartão de crédito) são divulgadas, que poderiam permitir fraudes ou um perfil social/financeiro detalhado ser criado.	**4**
Dados Sensíveis	**Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.**	
	Pontuação básica: quando a violação envolve “dados sensíveis” e a empresa não está ciente de nenhum fator de redução.	**4**

	A pontuação pode ser diminuída em 3, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobre os dados sensíveis do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	**1**
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza dos dados pode levar a suposições gerais.	**2**
	A pontuação pode ser diminuída em 1, por exemplo, quando a natureza dos dados pode levar a suposições sobre informações confidenciais.	**3**

Além disso, a classificação de impacto sobre direitos de titulares proposta pela Enisa não é somente relevante para eventos de violação de dados, mas também para análise de impacto em eventos de risco referentes ao Artigo 46 da LGPD.

Por essas razões, é utilizada no presente trabalho. A classificação de impacto da Enisa é adequada para aferir impacto tanto Ciclo de Vida dos Dados como também, como se verá adiante, é apropriada na análise de impacto relativa ao aspecto Desenvolvimento.

4.3.3.2 Desenvolvimento

O aspecto **Desenvolvimento** trata das questões referentes às atividades de desenvolvimento de software, seja antes de o sistema ser disponibilizado aos usuários, seja após, quando do oferecimento de novas versões.

O evento de risco neste aspecto também foi considerado aquele referente à violação de dados, conforme o artigo 46 da LGPD.

Por essa razão, no que tange à análise de probabilidade de ocorrência do evento de risco, foram abordados aspectos relativos à segurança, nos termos da ISO/IEC 27.001 e ISO/IEC 27.002, que serviram de subsídios para quatro questões, bem como para medidas mitigatórias do risco identificado.

O questionário completo encontra-se no Apêndice A. O Quadro 4-6 apresenta um exemplo de questão.

Quadro 4-6. Exemplo de Questões – Desenvolvimento - Probabilidade. Fonte: o Autor.

Em relação às atividades de Desenvolvimento:	**Referência**	**Tratamento**
Em ambiente de testes e desenvolvimento todos os dados utilizados são fictícios ou anonimizados?	ISO/IEC 27001, 8.33	Usar bancos de dados que não contenham dados de pessoas identificadas ou passíveis de identificação, ou anonimizar os dados. Caso isso não seja possível, reduzir ao mínimo necessário o uso de dados pessoais, implementar mecanismos de segurança, política de eliminação de

	dados imediatamente após o uso, controle rígido de acesso, e proteção contra remoção ou modificação das informações.

Em todas as questões, as respostas dadas com “Não” ou “Não sei informar” pontuam, com valor 1. As respostas com “Sim, não pontuam – ou seja, o valor atribuído a elas é zero. Para realizar o cálculo da probabilidade na escala qualitativa de 1 a 5 estabelecida, soma-se as respostas, conforme Equação 4-2, ou seja, o valor de probabilidade levará em conta as respostas dadas com “Não” ou “Não sei informar” somado 1.

Equação 4-2. Cálculo da probabilidade para os itens de Desenvolvimento. Fonte: o Autor.

$$P = 1 + \sum Q$$

P: Probabilidade

∑Q: Somatório de questões cuja resposta foi “Não” ou “Não sei informar”

Da mesma forma que em Ciclo de Vida dos Dados, para Desenvolvimento não foram atribuídos diferentes pesos para as questões. Os dois aspectos possuem natureza semelhante, ambos têm o impacto derivado dos conjuntos de dados e levam em conta o cenário de risco do Artigo 46 da LGPD, que trata de violação de dados. As razões para não se atribuir pesos, portanto, são as mesmas já apresentadas na seção anterior.

Na mesma linha, em relação à análise de impacto, utilizam-se os mesmos critérios usados no aspecto Ciclo de Vida dos Dados. Isso porque a preocupação nas atividades de desenvolvimento é essencialmente com eventos de risco de violação de dados, o que torna adequado aferir o impacto com base nos critérios propostos pela Enisa.

4.3.3.3 Conformidade de Tratamento

O aspecto **Conformidade de Tratamento** diz respeito à forma como os ativos de dados analisados são tratados, ou seja, aborda as características inerentes ao

tratamento que, quando em desconformidade, geram risco de dano a direitos dos titulares.

Os eventos de risco para este aspecto se referem à violação de parte dos princípios de tratamento de dados que estão elencados no Artigo 6º da LGPD: (i) finalidade[12] (Artigo 6º, I, LGPD); (ii) adequação[13] (Artigo 6º, II, LGPD); (iii) necessidade[14] (Artigo 6º, III, LGPD); (iv) qualidade dos dados[15] (Artigo 6º, V, LGPD); e (v) não discriminação[16] (Artigo 6º, IX, LGPD). A violação desses princípios pode causar danos aos direitos fundamentais e liberdades dos titulares de dados, pois podem ter seus dados tratados de forma que não atendem às suas expectativas, de forma abusiva, ilícita ou discriminatória.

Para a análise de probabilidade foram estabelecidas quatro questões que tratam controles e procedimentos que reduzem a possibilidade de violação de princípios de tratamento de dados. As questões tiveram como fundamento, além dos princípios elencados no Artigo 6º da LGPD, dois artigos que fazem parte da revisão bibliográfica (Li et al., 2020; Wuyts, Sion e Joosen, 2020). No Quadro 4-7, apresentam-se as questões, as referências de fundamento e as medidas de tratamento sugeridas.

Quadro 4-7. Questões – Conformidade de Tratamento - Probabilidade. Fonte: o Autor.

Questão	Referência	Peso	Tratamento
O sistema possui controles que garantam que os dados coletados e armazenados em servidor são usados apenas para atingir propósitos pré-estabelecidos, legítimos (não ilegais e não abusivos, ou seja, de forma a não prejudicar indevidamente), específicos e informados para o titular dos dados?	Brasil, 2018 (art. 6º, I, LGPD), Li et al., 2020	1	Estabelecer uma correlação clara entre dados coletados e finalidade e para qual são utilizados, e informá-la ao titular do dado (por meio, por exemplo, de aviso de privacidade).

[12] Artigo 6º (...): “I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;” (Brasil, 2018)

[13] Artigo 6º (...): “II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (Brasil, 2018)

[14] Artigo 6º (...): “III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;” (Brasil, 2018)

[15] Artigo 6º (...): “V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;” (Brasil, 2018)

[16] Artigo 6º (...): “IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;” (Brasil, 2018)

Há procedimento que garanta que o sistema armazena e trata somente o mínimo necessário de dados para os propósitos previamente definidos?	Brasil, 2018 (art. 6º, II, III, LGPD), Li et al., 2020	5	A LGPD determina que o tratamento precisa ser adequado com as finalidades informadas. Portanto, há a necessidade de corrigir casos de incompatibilidade. Eliminar dados que não são utilizados para finalidades previamente informadas.
Há mecanismos que garantam que os dados usados, ao longo do ciclo de vida (da coleta até sua eliminação), são exatos, atualizados, relevantes e necessários, para o cumprimento do propósito do tratamento?	Brasil, 2018 (art. 6º, V, LGPD)	1	Criar mecanismos que facilitem a atualização dos dados ao longo de todo o fluxo de informação.
O sistema possui controles que garantem que o tratamento não causa prejuízos nem discriminação dos titulares de dados?	Brasil, 2018 (art. 6º, IX, LGPD). Wuyts, Sion e Joosen, 2020	3	Realizar relatório de impacto para avaliar potencial discriminação ou prejuízo para o titular do dado.

Em todas as questões, as respostas dadas com “Não” ou “Não sei informar” pontuam. As respostas com “Sim, não pontuam. Para realizar o cálculo da probabilidade na escala qualitativa de 1 a 5 estabelecida, calcula-se a média ponderada considerando-se os pesos, conforme Equação 4-3. Ou seja, o valor de probabilidade levará em conta as respostas dadas com “Não” ou “Não sei informar” somado mais 1.

Equação 4-3. Cálculo da Probabilidade para Conformidade de Tratamento. Fonte: o Autor.

$$P = 1+(Q1+5\cdot Q2+Q3+3\cdot Q4)\cdot 2/5$$

P: Probabilidade
Q: Questão: Quando resposta for “Não” ou “Não sei informar”

Como se observa na fórmula de cálculo utilizada, foram estabelecidos pesos diferentes para as questões. Essa medida teve como base a análise de 520 resumos de decisões administrativas de autoridades nacionais europeias, proferidas entre 3 de novembro de 2023 e 21 de março de 2019, que tratam de inconformidade de tratamento de dados pessoais com base nos princípios de tratamento.

A partir da análise dos resumos de decisões encontradas no *CMS*[17] *Law GDPR Enforcement Tracker* identificou-se os princípios do GDPR com maior incidência e buscou-se os seus equivalentes na LGPD. Da análise das 520 decisões, foi identificado que diversos princípios podiam aparecer em uma mesma decisão. Por esse motivo, a soma dos resultados da coluna Decisões é 658, já que algumas delas utilizaram mais de um princípio. Assim, foram atribuídos pesos às questões com base no princípio a que elas se referem.

A Tabela 4-6 apresenta a síntese da análise realizada com: (i) o aspecto a que se refere o princípio; (ii) o princípio identificado no GDPR; (iii) seu correspondente na LGPD; (iv) o número de vezes que aparece em decisões; (v) o percentual em relação ao total de decisões (520); e (vi) o peso atribuído.

Tabela 4-6. Pesos para questões de Conformidade de Tratamento. Fonte: o Autor.

Aspecto	Princípio no GDPR	Princípio na LGPD	Decisões	Percentual	Peso
Conformidade de Tratamento	Licitude, Lealdade e Transparência (Art. 5º, 1, a)	Transparência e Não Discriminação (art. 6º,VI, e IX)	123	24%	3
Conformidade de Tratamento	Limitação de finalidades (Art. 5º, 1, b)	Finalidade (art. 6º, I)	42	8%	1
Conformidade de Tratamento	Minimização dos dados (Art. 5º, 1, c)	Adequação e Necessidade (art. 6º, II, III)	282	54%	5
Conformidade de Tratamento	Exatidão (Art. 5º, 1, d)	Qualidade dos dados (art. 6º, V)	22	4%	1
Ciclo de Vida dos Dados	Limitação da conservação (Art. 5º, 1, e)	Retenção/Descarte (Art. 15)	42	8%	-
Ciclo de Vida dos Dados	Integridade e Confidencialidade (Art. 5º, 1, f)	Prevenção e Segurança (art. 6º, VII e VIII)	114	22%	-
-	Responsabilidade (art. 5º, 2)	Responsabilização e prestação de contas (art. 6º, X)	33	6%	-

Note-se que alguns dos princípios identificados não fazem parte da análise do aspecto Conformidade de Tratamento. Limitação da Conservação e Integridade e Confidencialidade, que correspondem a questões de retenção e descarte (Artigo 15, LGPD) e Prevenção e Segurança (Artigo 6º, VII, VIII, LGPD) que são analisados no aspecto Ciclo de Vida dos Dados. Além disso, o princípio Responsabilidade, que corresponde à Responsabilização e Prestação de Contas (Artigo 6º, X, LGPD), traz

[17] CMS é um escritório de advocacia presente em mais de 40 países.

uma obrigação mais geral, ao determinar o dever de o agente de tratamento em poder comprovar que age em conformidade com a norma de proteção de dados.

Em relação aos princípios que são analisados no aspecto Conformidade de Tratamento, do total de 520 decisões, 54% estão relacionadas ao princípio de Minimização dos Dados (Artigo 5º, 1 c) no GPDR, cujos correspondentes são Adequação e Necessidade (Artigo 6º II e III) na LGPD, e que são tratados em uma única questão, com peso 5. O princípio Licitude, Lealdade e Transparência, nas decisões analisadas correspondem aos princípios de Transparência e de Não-Discriminação (Artigo 6º, VI e IX), aparecem em 123 decisões, 24% do total. As decisões apontam especialmente violações relativas a tratamento ilícito discriminatório, de forma que foi atribuído peso 3 à questão que trata a esse respeito.

Foram identificadas também 42 decisões referentes ao princípio Limitação de Finalidades (Artigo 5º, 1 b) do GDPR, que tem correspondência com o princípio da Finalidade (Artigo 6º, I) da LGPD. E outras 22 decisões sobre o princípio da Exatidão (Artigo 5º, 1, d), do GDPR, que corresponde ao princípio da Qualidade Dados (Artigo 6º, V) da LGPD. Para cada um desses princípios foi apresentada uma questão, com peso 1.

A lógica de atribuir pesos foi a de que a maior incidência de decisões em relação ao princípio relacionado permite inferir que a violação daquele dispositivo pode resultar mais facilmente em algum tipo de sanção, influindo na probabilidade de o risco se concretizar.

Foram utilizadas decisões do contexto do GDPR porque ainda são muito escassas as decisões referentes à LGPD no Brasil, seja no âmbito administrativo, seja no âmbito judicial.

A ANPD proferiu sete decisões até o momento, um conjunto de dados muito restritivo para permitir inferências. Nenhuma delas referente à conformidade de tratamento de dados pessoais. Apenas uma delas trata do setor privado, a primeira decisão da autarquia, proferida no ano de 2023, em que a empresa foi condenada à pena de multa máxima, mas não teve como base questões relativas à conformidade de tratamento [18].

[18] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 1/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em 27.7.2024.

Os demais processos administrativos foram todos em relação a órgãos públicos. Decisão do Relatório de Instrução nº 2/2023/FIS/CGF/ANPD indicou como fundamento violação aos Artigos 48 e 49 da LGPD, por ausência de comunicação de incidente de segurança e insuficiência de sistema de segurança para tratamento de dados pessoais[19]. A Decisão do Relatório de Instrução nº 3/2023/FIS/CGF/ANPD arquivou o processo por não configuração de violações[20].

A Decisão do Relatório de Instrução nº 4/2023/FIS/CGF/ANPD teve por base violação aos Artigos 48 e 49 da LGPD por falta de comunicação ao titular de dados sobre incidente de segurança em prazo razoável e por ausência de sistemas de tratamento de dados que atendessem aos requisitos de segurança e boas práticas de governança.

A Decisão do Relatório de Instrução nº 1/2024/FIS/CGF/ANPD apontou violação ao Artigo 48 da LGPD, por ausência de publicização de incidente de segurança de dados[21]. A Decisão do Relatório de Instrução nº 2/2024/FIS/CGF/ANPD teve por fundamento violação aos Artigos 37, 38 e 48 da LGPD, por ausência de registro de operações de tratamento de dados, não apresentação de relatório de impacto de proteção de dados e falta de comunicação adequada de incidente de segurança[22].

A Decisão do Relatório de Instrução nº 3/2024/FIS/CGF apresentou como fundamentos violação aos Artigos 48 e 49 da LGPD, por ausência de comunicação individualizada em caso de vazamento de dados e por ausência de medidas técnicas e administrativas adequadas[23].

---

[19] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 2/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf. Acesso em 27.7.2024.

[20] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 3/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4504630_relatorio_3.pdf. Acesso em 27.7.2024.

[21] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 1/2024/FIS/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-de-instrucao-1_2024.pdf. Acesso em 27.7.2024.

[22] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 2/2024/FIS/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-instrucao-2-2024_sec-educacao-gdf.pdf. Acesso em 27.7.2024.

[23] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Instrução nº 3/2024/FIS/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf. Acesso em 27.7.2024..

No âmbito judicial, foi analisado o levantamento Painel dos Tribunais[24] de 2022, elaborado pela Jusbrasil, no qual cerca de 50 pesquisadores catalogaram 274 decisões que aplicavam a LGPD, das quais 137 foram consideradas mais relevantes por envolver diretamente a norma de proteção de dados. Segundo o estudo, a LGPD é geralmente aplicada em situações de reforço a outras normas, como o Código de Defesa do Consumidor ou o Marco Civil da Internet.

As 137 decisões foram lidas, identificando-se que duas delas trataram diretamente de conformidade de tratamento. A primeira delas, invocou como fundamento o tratamento de dados em excesso ((TJ-SP - AC: 10091179520218260637 SP 1009117-95.2021.8.26.0637, Relator: Ricardo Pessoa de Mello Belli, Data de Julgamento: 30/05/2022, 19ª Câmara de Direito Privado, Data de Publicação: 01/06/2022). A segunda, tratou da falta de informação explícita sobre a finalidade do tratamento (TJ-AP - RI: 00343984820198030001 AP, Relator: MÁRIO MAZUREK, Data de Julgamento: 01/04/2021, Turma recursal). Um conjunto, portanto, muito reduzido de decisões que permitissem estabelecer, por meio delas próprias, um sistema de pesos para a realização da análise de riscos de conformidade de proteção de dados.

Além disso, o GDPR e a LGPD possuem muitas semelhanças, conforme foi apresentado no tópico 2.2.2 desta pesquisa. Como a LGPD e o GDPR possuem dispositivos e contextos semelhantes, como há ainda pouco conteúdo decisório no âmbito legal e regulatório brasileiro, justifica-se a análise das decisões administrativas das autoridades nacionais da União Europeia, para a atribuição de pesos a questões de conformidade de tratamento de dados.

Para a análise de impacto foi levada em consideração a perspectiva do tratamento inerentemente de alto risco, com base na Resolução CD/ANPD nº 2. Como já mencionado na seção 2.3.2, a forma como os dados são tratados pode ter consequências para os direitos dos titulares de dados, o que levou tanto no âmbito.

No GDPR são estabelecidos nove critérios para identificar tratamentos inerentemente de riscos. A LGPD, de outro lado, possui outros parâmetros. Como abordado na seção 2.2.4, a Resolução CD/ANPD nº 2 traz critérios sobre tratamento

[24] JUSBRASIL. Painel LGPD nos Tribunais. Disponível em: https://painel.jusbrasil.com.br/2022. Acesso em 05.08.2023.

de alto risco, em seu artigo 4º[25]. Os parâmetros lá estabelecidos, junto com a quantidade de titulares cujos dados são tratados, são utilizados para analisar o impacto em relação ao aspecto de conformidade de tratamento, conforme Tabela 4-7.

Tabela 4-7. Critérios de Impacto – Conformidade de Tratamento. Fonte: o Autor.

Critério	Valor
Quando há pelo menos um dos critérios gerais: - O tratamento é realizado em larga escala - O tratamento afeta significativamente interesses e direitos fundamentais das pessoas	2
Quando há pelo menos um dos critérios específicos: - O tratamento é feito com uso de tecnologias emergentes ou inovadoras (IA, IoT, blockchain, realidade virtual, metaverso etc.) - O tratamento de dados é de vigilância, monitoramento por vídeo ou controle de zonas de acesso ao público - As decisões são tomadas unicamente com base em tratamento automatizado de dados pessoais, como, por exemplo, aquelas destinadas a criar perfil pessoal, profissional, de saúde, de consumo e de crédito ou de aspectos da personalidade do titular - Uso de dados pessoais sensíveis, ou de dados pessoais de crianças, adolescentes e idosos.	2
O tratamento não envolve nenhuma das alternativas anteriores	1
O número de pessoas que estão tendo seus dados tratados é maior ou igual a 100	1

Assim, estabeleceu-se que quando há pelo menos um dos critérios gerais – ou seja, tratamento de dados pessoais em larga escala, ou tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares – a pontuação de impacto é 2. Se tiver os dois critérios, a pontuação continua sendo 2.

Da mesma forma, a pontuação é 2 também atribuída quando há pelo menos um dos critérios específicos – uso de tecnologia inovadora, vigilância ou controle de

[25] Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
I - critérios gerais:
a) tratamento de dados pessoais em larga escala; ou
b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
II - critérios específicos:
a) uso de tecnologias emergentes ou inovadoras;
b) vigilância ou controle de zonas acessíveis ao público;
c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

zonas acessíveis ao público, decisões com base em tratamento automatizado de dados pessoais, uso de dados sensíveis ou de crianças, adolescentes e idosos. Mesmo que o caso avaliado possua os quatro critérios, a pontuação atribuída continua sendo 2.

Essa forma de cálculo é justificada porque a ANPD considera alto risco quando estão presentes um critério geral e um específico. Não importa se o caso concreto possui dois critérios gerais e nenhum específico. Não importa se o caso concreto possui 4 critérios específicos e nenhum geral. Em ambos os casos não será de alto risco, nos termos estabelecidos pela ANPD.

Além disso, conforme a Tabela 4-4, o valor 4 é considerado como alto risco. Pelos parâmetros adotados, portanto, havendo um critério geral e um específico, o resultado deve corresponder a alto risco, de forma adequada à escala qualitativa pré-existente.

Por fim, para completar a escala de impacto, que varia de 1 a 5, atribui-se a quantidade de pessoas como parâmetro. Considera-se que um volume maior de titulares de dados que tenham seus dados tratados aumenta o risco. Por essa razão, quando houver 100 pessoas ou mais, soma-se 1 na escala de impacto, nos mesmos moldes já apresentados para Ciclo de Vida dos Dados e Desenvolvimento, com fundamento na classificação feita pela Enisa.

Nos termos do Artigo 50, §1º, LGPD, as sanções administrativas por violação da lei são aplicadas com base, entre outros critérios, na gravidade e na natureza das infrações e dos direitos pessoais afetados, bem como no grau do dano. Uma grande quantidade de titulares afetados tende a ampliar o grau do dano, ao atingir muitas pessoas. Além disso, ações judiciais individuais por conta de violação legal no tratamento de dados pessoais ampliam o risco de prejuízos financeiros, especialmente quando há um grande volume de titulares afetados com potencial de ajuizamento de demandas. A seguir, descreve-se os parâmetros de análise para o aspecto Direitos dos Titulares.

4.3.3.4 Direitos dos Titulares

Decisões de engenharia de software podem facilitar, dificultar ou, até mesmo, violar a conformidade em relação aos direitos dos titulares de dados pessoais. Facilitam, por exemplo, quando o sistema criado permite que ocorra o cumprimento das normas de conformidades estabelecidas na LGPD sem alto custo operacional.

O aspecto Direitos dos Titulares refere-se a eventos de risco que podem: (i) violar o direito do titular em acesso a seus dados e outros direitos a eles conectados, nos termos do artigo 18[26] e 19[27] da LGPD; (ii) violar o direito a garantia de acesso à informação sobre como seus são tratados[28]; (iii) violar as regras que garantem o direito de retirada de consentimento e deveres da organização em relação a prova de que o consentimento foi dado em conformidade com a LGPD[29].

O impacto que eventos de violação de conformidade podem ter em relação ao cumprimento de normas de direitos dos titulares está ligado à capacidade de atendimento às solicitações de titulares de dados. Isso depende de quatro fatores: (i)

---

[26] LGPD, 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, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; 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. (...) § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional (BRASIL, 2018).

[27] Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, 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 finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. § 2º As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; ouII - sob forma impressa. § 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 (BRASIL, 2018).

[28] LGPD, 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: (...) (BRASIL, 2018).

[29] 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. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados 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.§ 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 específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

quantidade de titulares de dados pessoais; (ii) existência de procedimento estabelecido para atendimento de solicitações; (iii) existência de pessoa responsável designada para responder solicitações; e (iv) existência de conhecimento sobre os deveres da organização a respeito dos direitos dos titulares. A partir desses critérios o cálculo é apresentado no Quadro 4-8.

Quadro 4-8. Direitos dos Titulares – Cálculo do Impacto. Fonte: o Autor.

Critério	Cálculo do impacto
Quantidade de titulares de dados cujos dados são tratados	Até 99 pessoas, o valor é 1; quando for 100 pessoas ou mais, 2
Existência de procedimento estabelecido para atendimento de solicitações	Quando há procedimento, o valor é zero; quando não existe, 1
Existência de pessoa responsável designada para responder solicitações	Quando há responsável, o valor é zero; quando não existe, 1
Existência de conhecimento sobre os deveres da organização a respeito dos direitos dos titulares	Quando há conhecimento na organização, o valor é zero; quando não existe, 1

A partir dos critérios estabelecidos, os valores de impacto vão de 1 a 5. Note-se que a quantidade de pessoas tem uma fórmula de cálculo ligeiramente diversa dos outros aspectos já apresentados. Isso ocorre porque o valor mínimo sempre será 1. Assim, no caso de haver menos de 99 pessoas tendo seus dados tratados pela *startup*, em um cenário em que há conhecimento sobre os deveres da organização a respeito dos direitos dos titulares, procedimento previamente estabelecido, e responsável designado por responder solicitações, o risco será muito baixo, com valor 1 atribuído para impacto.

Os critérios escolhidos para a análise de impacto levam em conta que as dificuldades de uma *startup* em atender às solicitações de titulares de dados aumentam na medida em que cresce o número de pessoas cujos dados são coletados, inexiste procedimento e conhecimento na organização, bem como quando não há responsável designado.

Para a análise de probabilidade foram estabelecidas cinco questões que tratam controles e procedimentos que reduzem a possibilidade de violação de direitos dos titulares de dados pessoais. As questões tiveram como fundamento os artigos 8º, 9º, 18 e 19 da LGPD, conforme apresenta-se no Quadro 4-9.

Quadro 4-9. Questões – Direitos dos Titulares – Cálculo da Probabilidade. Fonte: o Autor.

Questão	Referência	Peso	Tratamento
O sistema foi projetado de modo a garantir aos titulares mecanismos de informação sobre como seus dados são tratados: (a) aviso/política de privacidade; e (b) canal de comunicação que permita o titular, mediante requisição, exercer seus direitos em relação a seus dados pessoais (Por exemplo: formulário, sistema próprio, sistema de terceiros, e-mail, etc)?	Brasil, 2018 (LGPD, art. 18, caput, art. 19). Brasil, 2018 (LGPD, art. 9 º, art. 18, VII)	5	Disponibilizar aviso/política de privacidade para informar ao titular como os dados dele estão sendo tratados. E/ou disponibilizar canal de comunicação para que o titular possa exercer seus direitos.
O sistema permite facilmente: (a) extrair dados do titular para entregá-los a ele, em caso de requisição, inclusive cópia integral dos dados ou em formato lido por computador; (b) responder pedido do titular, informando como os dados são tratados, para quais finalidades, duração do tratamento e com quem são compartilhados?	Brasil, 2018 (LGPD, art. 9º, art. 18, II, V, art. 19, §1º, §3º).	5	Criar mecanismos para extração de dados do sistema, de forma a facilitar a entrega de dados para o titular, em formatos lidos por computador.
O sistema permite a correção de dados incompletos, inexatos ou desatualizados, diretamente pelo titular ou mediante requisição ao responsável, com possibilidade de verificação do histórico de alterações realizadas e de quem as realizou?	Brasil, 2018 (LGPD, art. 18, III, LGPD)	1	Criar mecanismos para a correção de dados no sistema.
O sistema possui um procedimento que garanta a eliminação, ou a anonimização, ou bloqueio de dados, (com possibilidade de verificação de histórico de realização do procedimento) quando eles: (a) não forem mais necessários; (b) tenham alcançado a sua finalidade de tratamento; (c) quando o titular retirar o consentimento (em casos que os dados sejam tratados mediante consentimento prévio, como no caso de uso de cookies para marketing ou rastreamento de comportamento); ou (d) quando o titular solicitar que cesse o envio de correspondência de marketing?	Brasil, 2018 (LGPD, art. 8º, §1º, §2º, §4º, §5º, §6º, art. 15, art. 18, IV; art. 8º, §5º, art. 18, VIII, IX, LGPD)	3	Criar mecanismos que permitam a eliminação, anonimização ou bloqueio de dados.
O responsável pelo sistema tem um procedimento para informar outros agentes de tratamento com quem tenha compartilhado dados, para que repitam procedimento de correção, eliminação, anonimização ou bloqueio de dados, quando tenha sido requerido pelo titular?	Brasil, 2018 (art. 6º, IX, LGPD). Brasil, 2018 (LGPD, art. 18, §6º)	1	Criar procedimento para informar outros agentes de tratamento, quando for necessário que também corrijam, eliminem, anonimizem ou bloqueiem

	dados, conforme requerido pelo titular de dados.

Em todas as questões, as respostas dadas com “Não” ou “Não sei informar” pontuam. As respostas com “Sim”, não pontuam. Para realizar o cálculo da probabilidade na escala qualitativa de 1 a 5 estabelecida, aplica-se a média ponderada, conforme a Equação 4-4, ou seja, o valor de probabilidade levará em conta as respostas dadas com “Não” ou “Não sei informar” somado mais 1.

Equação 4-4. Cálculo da Probabilidade para Direitos dos Titulares. Fonte: o Autor.

$$P = 1+(5\cdot Q1+5\cdot Q2+Q3+3\cdot Q4+Q5)\cdot 4/15$$

P: Probabilidade

Q: Questão: Quando resposta for “Não” ou “Não sei informar”

Como se observa na fórmula de cálculo utilizada, foram estabelecidos pesos diferentes para as questões. Essa medida teve como base a análise de 194 resumos de decisões administrativas de autoridades nacionais europeias, proferidas entre 18 de setembro de 2023 e 25 de outubro de 2018, que tratam de violações de direitos dos titulares de dados no âmbito do GDPR.

A partir da análise dos resumos de decisões encontradas no *CMS Law GDPR Enforcement Tracker*, identificaram-se as violações de direitos dos titulares com maior incidência e buscou-se os seus equivalentes na LGPD. Assim, foram atribuídos pesos às questões com base no princípio a que elas se referem.

A Tabela 4-8 apresenta a síntese da análise realizada com: (i) o conjunto de direitos do titular a que se refere a decisão no GDPR; (ii) os seus correspondentes na LGPD; (iv) o número de vezes em que um dos direitos do respectivo conjunto aparece em decisões; (v) o percentual em relação ao total das 192 decisões e (vi) o peso atribuído.

Como já mencionado, os dispositivos referentes a direitos dos titulares foram agrupados em conjuntos que podem ser relacionados a atividades no campo da

engenharia de software, utilizando-os para questões referentes a práticas e procedimentos que reduzem a probabilidade de riscos se concretizarem.

Tabela 4-8. Pesos para questões de Direitos dos Titulares. Fonte: o Autor.

Direitos dos titulares - GDPR	Direitos dos titulares – LGPD	Decisões	Percentual	Peso
Transparência das informações e das comunicações para exercício de direitos (GDPR, art. 12º, 1, 2, 3, 4, 5, 6, 7, 8; 15º, 2), Informação e acesso a dados pessoais (Artigo 13º, 1, 2, 3, 4, Artigo 14º, 1, 2, 3, 4, 5)	Direito de informação: aviso de privacidade e canal de comunicação com o titular (LGPD, art. 9º, 18, VII, 19)	101	52,6%	5
Direito de acesso do titular dos dados (Artigo 15º, 1, 3, 4) e Direito de portabilidade dos dados (Artigo 20º, 1, 2, 3, 4)	Direito de acesso e portabilidade (LGPD, art. 18, II, V, art. 19, §1º, §3º)	104	54,2%	5
Direito de Retificação (Artigo 16º)	Direito de correção de dados incompletos, inexatos ou desatualizados (LGPD, art. 18, III)	2	1%	1
Direito ao apagamento dos dados (Artigo 17º, 1, 2, 3), Direito à limitação do tratamento (Artigo 18º, 1, 2, 3)	Direito de eliminação, anonimização ou bloqueio de dados (LGPD, art. 8º, §1º, §2º, §4º, §5º, §6º, art. 15, art. 18, IV; art. 8º, §5º, art. 18, VIII, IX, LGPD)	48	25%	3
Obrigação de notificação da retificação, apagamento ou limitação do tratamento (Artigo 19º)	Direito de que as solicitações do titular sobre correção, eliminação, anonimização ou bloqueio de dados se estendam para os demais agentes com quem se compartilha dados (LGPD, art. 18, §6º)	0	0	1

Na classificação das decisões foram utilizados dois critérios. O primeiro, diz respeito a decisões que são fundamentadas em mais de um conjunto de direitos. Quando isso ocorreu, como a decisão tinha mais de um fundamento pertencente a diversos conjuntos de direitos, ela foi computada para cada um deles. Assim, quando os fundamentos de uma decisão foram, por exemplo, o direito de apagamento previsto no Artigo 17 e o direito de portabilidade do Artigo 15 do GDPR, essa decisão foi computada para ambos.

De outro lado, o segundo critério estabelece que decisões que tenham mais de um fundamento no mesmo conjunto de direitos relacionados, era computada uma única vez para aquele agrupamento. Portanto, quando os fundamentos de uma decisão foram, por exemplo, direito de transparência (GDPR, Artigo 12º) e direito de

acesso (GDPR, Artigo 13º), ela foi computada uma única vez para esse conjunto de direitos.

De forma similar ao que ocorre no aspecto Conformidade de Tratamento, o conteúdo decisório no âmbito brasileiro é muito restrito. No que se refere às decisões judiciais, o Painel LGPD nos Tribunais, de 2022, elaborado pela Jusbrasil, registrou 137 decisões judiciais em que a LGPD foi uma questão central analisada. Dessas decisões, nove trataram de direitos dos titulares de dados. Apenas os acórdãos de duas apelações, entretanto, estão relacionados diretamente ao tema direitos dos titulares. Foram elas:

- A primeira decisão condenou em indenização por danos morais no valor de R$ 10.000,00, por conta de não eliminação de dados pessoais (TJ-SP - AC: 10947304520218260100 SP 1094730-45.2021.8.26.0100, Relator: Berenice Marcondes Cesar, Data de Julgamento: 16/08/2022, 28ª Câmara de Direito Privado, Data de Publicação: 19/08/2022).
- A segunda, impondo indenização por danos de R$ 3.000,00 por compartilhamento comercial de dados sem autorização (TJ-SP - AC: 10095075120218260577 SP 1009507-51.2021.8.26.0577, Relator: Pedro Kodama, Data de Julgamento: 01/06/2022, 37ª Câmara de Direito Privado, Data de Publicação: 01/06/2022).

Esses dados demonstram que a judicialização da LGPD ainda é um fenômeno recente, trazendo dados limitados para oferecer subsídios ao método proposto.

4.3.3.5 Síntese de impacto e probabilidade nos quatro aspectos

A fim de se ter uma percepção global sobre o método proposto, apresenta-se no Quadro 4-10, a síntese dos cálculos para cada um dos aspectos.

Nele são apresentados: os quatro aspectos que estão sendo tratados neste trabalho, a fórmula do cálculo de impacto e a fórmula de cálculo da probabilidade. A partir das respostas às 42 questões propostas, o método permite que o tomador de decisão avalie o risco de conformidade de LGPD para cada um dos quatro aspectos, e obtenha um conjunto de recomendações, que são descritos na próxima seção.

Pretende-se que este instrumento apoie a *startup* na sua tomada de decisão sobre os riscos que envolvem a Lei.

Quadro 4-10. Síntese de Impacto e Probabilidade para os quatro aspectos. Fonte: o Autor.

Aspecto	Impacto (1 a 5)	Probabilidade (1 a 5)
Ciclo de Vida dos Dados	Definição do principal conjunto de dados, com base em quatro categorias (Simples, de Comportamento, Financeiros, Sensíveis): Varia de 1 a 4, com base na criticidade do conjunto de dados Definição de número de pessoas com dados tratados: Varia de 0, quando até 99 pessoas; a 1, quando 100 ou mais pessoas Quantidade de questões: 3	P=1+(∑Q/17)*4 P: Probabilidade Q: Somatório de questões cuja resposta foi “Não” ou “Não sei informar” Quantidade de questões: 17
Desenvolvimento	Idem a Ciclo de Vida dos Dados	P=1+∑Q P: Probabilidade Q: Somatório de questões cuja resposta foi “Não” ou “Não sei informar” Quantidade de questões: 4
Conformidade de Tratamento	Quando há um critério geral de alto risco (tratamento em larga escala ou que afete significativamente interesses e direitos), atribui-se o valor 2. Quando há um critério específico de alto risco (tratamento com tecnologia emergente ou inovadora; monitoramento em zona de acesso público; decisão com base em tratamento automatizado; ou dados de crianças, adolescentes ou idosos), atribui-se o valor 2. Se o tratamento não envolve nenhuma das alternativas anteriores, o valor é 1. Varia de 0, quando até 99 pessoas; a 1, quando 100 ou mais pessoas Quantidade de questões: 6	P=1+(Q1+Q2*5+Q3+Q4*3)*2/5 P: Probabilidade Q: Questão: Quando resposta for “Não” ou “Não sei informar” Quantidade de questões: 4
Direitos dos Titulares	Quando há procedimento, o valor é zero; quando não existe, 1 Quando há responsável, o valor é zero; quando não existe, 1 Quando há conhecimento na organização, o valor é zero; quando não existe, 1 Até 99 pessoas, o valor é 1; quando for 100 pessoas ou mais, 2 Quantidade de questões: 3	P=1+(Q1*5+Q2*5+Q3+Q4*3+Q5)*4 /15 P: Probabilidade Q: Questão: Quando resposta for “Não” ou “Não sei informar” Quantidade de questões: 5

4.3.4 Avaliação e tratamento de risco

Nesta etapa apresenta-se a forma pela qual são classificados os riscos, que servem para serem comparados com o resultado da avaliação realizada pelo tomador de decisão. Ao responder as questões apresentadas no método, o tomador de decisão completa a avaliação, sendo gerado um resultado que apresenta a atribuição de risco para cada um dos quatro aspectos, bem como traz o nível de impacto e de probabilidade. Para mitigar os riscos identificados, apresenta-se um conjunto de recomendações, a fim que se possa tratar os riscos identificados.

Como já observado, impacto e probabilidade são avaliados em uma escala Likert de cinco pontos. Para construir a classificação de nível de risco, esses dois parâmetros são multiplicados, portanto podendo variar de 1 a 25.

A partir do valor aferido, o método classifica o risco, conforme a Tabela 4-9.

Tabela 4-9. Classificação dos Níveis de Risco. Fonte: o Autor.

Valor	Classificação de Risco
De 1 a 3	Baixo
De 4 a 6	Moderado
De 8 a 12	Alto
De 15 a25	Muito Alto

A partir desses parâmetros, a avaliação de risco tem como resultado apresentado ao tomador de decisão, conforme já mostrado na Figura 4-2: (i) dois gráficos com a classificação de risco para os quatro aspectos; (ii) o resultado da avaliação de impacto e probabilidade também para os quatro aspectos; (iii) conjunto de recomendações para mitigação dos riscos encontrados, para cada aspecto analisado.

As recomendações estão relacionadas a não conformidades identificadas a partir das respostas dadas pelos tomadores decisão. Para toda a questão cuja resposta indicar um risco de conformidade, há uma recomendação de tratamento correspondente.

A relação completa encontra-se no Apêndice B – Questões e Recomendações para Tratamento de Riscos. O referido apêndice traz as questões, as indicações dos documentos ou artigos de lei de referência para a construção das questões, os pesos utilizados (quando o caso) e o tratamento sugerido.

O tratamento sugerido para cada aspecto é o que irá compor o conjunto de recomendações apresentado no resultado da aplicação do método. Para todos os

aspectos são trazidas recomendações para reduzir a probabilidade de desconformidade. Em relação ao impacto, entretanto, são apresentadas recomendações para Conformidade de Tratamento e Direitos dos Titulares.

Os aspectos Ciclo de Vida dos Dados e Desenvolvimento possuem recomendações para tratamento de risco somente para as questões referentes à probabilidade porque a forma de cálculo de impacto para esses dois aspectos não requer, por si, algum modo específico de tratamento. O impacto, nestes casos, refere-se às características e ao volume dos dados, o que por si só não requer uma medida específica de tratamento.

Para os aspectos Conformidade de Tratamento e Direitos dos Titulares, entretanto, há recomendações tanto para questões sobre impacto quanto para aquelas sobre probabilidade. No caso de Conformidade de Tratamento, o conteúdo das assertivas sobre impacto referem-se à identificação de tratamento inerentemente de alto risco, o que, quando identificado sugere a necessidade de elaboração de relatório de impacto, a fim de mitigar os riscos detectados. No caso de Direitos dos Titulares, o impacto está ligado à capacidade de resposta aos titulares de dados. Assim, medidas que possam tornar mais eficiente a performance de atendimento permite mitigar consequências neste aspecto.

Quando o empreendedor aplica o método, o resultado é apresentado na forma de relatório com a classificação de risco e as recomendações para mitigá-los. Ao aplicar o método, o tomador de decisão, portanto, pode avaliar por meio de gráficos os riscos de conformidade em LGPD que a *startup* possui, bem como quais ações podem reduzi-los. Isso possibilita, caso o tomador de decisão julgue necessário, o estabelecimento de prioridades das atividades de desenvolvimento de software a serem adotadas, seja no âmbito do desenvolvimento de funcionalidades atinentes ao negócio, seja para mitigar riscos de conformidade com a LGPD.

4.4 Considerações sobre o capítulo

Foi apresentado neste capítulo o método proposto, explicando-se sua aplicação, os aspectos analisados, bem como a justificativa das escolhas. Ao aplica-lo, o tomador de decisão consegue analisar os riscos de conformidade com a LGPD para os quais está exposto e compreender que medidas serão necessárias para mitigá-los, podendo avaliar, dentro de seu rol de prioridades, o melhor momento para implementá-las.

CAPÍTULO 5 - DEMONSTRAÇÃO E AVALIAÇÃO

Preliminarmente, antes de o artefato ter sido apresentado a tomadores de decisão de *startups*, ele foi debatido em sessões do Grupo de Pesquisa de Engenharia de Software do PPGIA-PUCPR. O grupo reúne desenvolvedores de software, pesquisadores de engenharia de software e profissionais da indústria.

Tanto a estrutura do método quanto o conteúdo das questões foram discutidos no grupo. A proposta inicial da qualificação ainda não tinha a configuração atual. A partir da revisão de literatura a versão inicial do artefato tinha 76 questões.

Com o debate no grupo, foram levantadas questões referentes ao contexto das *startups*, em especial às necessidades de o método ser leve e didático, para empresas com recursos e conhecimentos escassos (Paternoster *et al.*, 2014, Berg *et al.*, 2018). Essas discussões subsidiaram as mudanças no artefato, com as questões sendo analisadas e reelaboradas a partir das percepções do grupo. Após algumas iterações, chegou-se à versão atual, que possui 42 pontos para avaliação do tomador de decisão.

O artefato gerado, então, foi apresentado em dois ciclos de avaliação para um total de 46 tomadores de decisão de 38 *startups*. No primeiro ciclo, o artefato foi apresentado a 24 tomadores de decisão de 21 *startups*. Após a análise da avaliação feita pelos empreendedores, foram realizadas alterações no tutorial do artefato, bem como ligeiras modificações na parte explicativa de algumas questões, e, então, repetiu-se o procedimento de coleta de dados em avaliação empírica com mais 22 tomadores de decisão de 17 *startups*.

As *startups* foram selecionadas por meio de contato com a aceleradora Hotmilk, da PUC-PR, agências de fomento (Agência Curitiba, Sebrae-PR, Sebrae São José dos Pinhais, Sebrae Ponta Grossa), Aldeia Coworking, investidores anjo e profissionais da área de inovação e do meio acadêmico, que indicaram empresas que poderiam ter interesse em participar da pesquisa. A partir das indicações feitas, o pesquisador entrou em contato com os tomadores de decisão, certificou-se de que se tratava de empreendedores de *startups* de software, e, então, marcou sessões de demonstração.

As sessões duraram em média cerca de 40 minutos. O pesquisador acompanhou todas elas e explicou aos participantes que eles deveriam responder o formulário elaborado no Qualtrics, que faz parte do artefato, e que, em seguida seria gerado relatório com o resultado da avaliação de risco e o conjunto de recomendações. Caso necessitassem, podiam tirar dúvidas com o pesquisador.

Após terminarem de preencher o método, novo *link* era encaminhado a eles, para, então, fazerem a avaliação do uso do método. Foi utilizado o Technology Acceptance Model 3 (TAM-3), que se encontra no Apêndice C, avaliando-se três categorias – Facilidade de Uso, Utilidade e Uso Futuro –, conforme Quadro 5-1.

Quadro 5-1. Technology Acceptance Model 3 (TAM-3). Fonte: o Autor.

Categoria	**Assertivas**
Facilidade de uso	- O método e as recomendações são claros e compreensíveis para mim. Interagir com o método e as recomendações e interpretá-los não requer muito esforço. cognitivo (mental) para mim. - Acho fácil aprender como usar o método e as recomendações. - Acho fácil o uso do método e das recomendações para fazer o que eu quero.
Utilidade	- O uso do método e das recomendações melhorou meu desempenho para cumprir com a LGPD. - O uso do método e das recomendações pode aumentar minha eficácia para cumprir com a LGPD. - Eu considero que o método e as recomendações são úteis para cumprir com a LGPD.
Uso futuro	- Levando em consideração que eu tenha domínio para escolher uma abordagem para conformidade de LGPD, eu prevejo que irei usar o método e as recomendações propostas.

Para cada assertiva, o tomador de decisão poderia marcar uma das seguintes cinco opções: Discordo integralmente, Discordo parcialmente, Não concordo nem discordo, Concordo parcialmente, Concordo integralmente. Ao fim de analisar cada categoria, os empreendedores podiam realizar comentários a respeito daquele tema analisado.

A resposta à pergunta era obrigatória. Contudo, os empreendedores, poderiam, caso desejassem, responder que nada mais tinham a acrescentar. Os resultados das avaliações feitas pelos tomadores de decisão, para cada ciclo, são descritos neste capítulo, nas seções, 5.1.2 e 5.2.2, e as análises dos resultados, nas seções 5.1.3 e 5.2.3.

Os 46 tomadores de decisão tiveram seus nomes removidos e são mencionados por ordem de aplicação do método, pelo código que começa com #E01 e vai até #E46, preservando a confidencialidade de suas identidades.

A seguir apresentam-se o perfil das *startups*, os resultados da avaliação e as análises dos resultados do primeiro ciclo de demonstração e avaliação. Na sequência, apresentam-se os resultados da demonstração e avaliação do segundo ciclo, já trazendo comparações com o primeiro ciclo realizado.

5.1 Primeiro ciclo de demonstração e avaliação

A coleta de informações do primeiro ciclo de demonstração e avaliação ocorreu entre 24 de junho e 1º de julho de 2024. A seguir apresenta-se o perfil das *startups* e dos domadores de decisão, para após trazer os resultados das avaliações que fizeram sobre o uso do artefato.

5.1.1 Perfil das *startups* e dos tomadores de decisão

No primeiro ciclo, o artefato foi demonstrado para uma *startup* em estágio inicial, três em estágio de teste de protótipo, e 17 em fase de crescimento. Em três casos, as avaliações ocorreram para dois tomadores de decisão de uma mesma *startup*. Portanto, o artefato foi demonstrado para 21 *startups*, mas para 24 tomadores de decisão, conforme apresentado na Tabela 5-1.

Tabela 5-1. Primeiro ciclo: Estágio da *Startup*. Fonte: o Autor.

Estágio da *startup*	**Qtde. de *startups***
Inicial	1
Testando protótipo (com ao menos um cliente)	3
Em crescimento (com mais de um cliente recorrente)	17
Total	**21**

Em relação ao setor de atuação, cinco das *startups* são da área financeira, duas são plataformas de gestão, duas atuam no setor jurídico e outras duas no comércio e varejo. As demais são de setores variados conforme a Tabela 5-2.

Tabela 5-2. Primeiro ciclo: Setor de Atuação. Fonte: o Autor.

Setor de Atuação	**Qtde. de *startups***
Financeiro	5
Jurídico	2
Plataforma de gestão	2

Comércio e Varejo	2
Saúde	1
Contabilidade	1
Sustentabilidade	1
Serviços	1
Vendas	1
Comunicação omnichanel	1
Educação	1
Recursos humanos	1
Tecnologia de Saneamento	1
Imobiliário	1
Total	**21**

A quantidade de clientes das *startups* também apresentou ampla variação. Duas empresas não possuem clientes, quatro delas têm até dez clientes, nove possuem entre 13 e 50 clientes. Outras quatro delas têm entre 112 e 200 clientes. Apenas uma possui 3000 clientes.

Uma única startup assinalou ter mais 100.000 clientes. Este último caso, entretanto, não se trata de clientes recorrentes, o que poderia colocar em dúvida se de fato a empresa era uma *startup*, mesmo que classificada como em crescimento, dado o volume. O número de clientes refere-se a pessoas que utilizaram a plataforma para recursos em multas de trânsito, constituindo-se, portanto, de transações únicas. A Tabela 5-3 apresenta o número de clientes por *startup* de forma detalhada.

Tabela 5-3. Primeiro ciclo: Número de clientes. Fonte: o Autor.

Número de clientes	**Qtde. de *startups***
Zero	2
3	1
5	1
8	1
10	1
13	1
15	2
20	1
30	2
32	1
36	1
43	1
112	1
135	1
170	1
200	1
3000	1
100.000	1
Total	**21**

Em relação ao número de pessoas trabalhando na empresa (funcionários e sócios), 12 delas possuem menos de 10 pessoas e sete entre 12 e 50. Uma das startups tem 70 pessoas na atividade da empresa e outra, 73, conforme apresentado na Tabela 5-4.

Tabela 5-4. Primeiro ciclo: Pessoas trabalhando na *startup*. Fonte: o Autor.

Número de pessoas	Qtde. de *startups*
2	2
3	3
6	1
7	1
8	3
10	2
12	1
19	2
20	1
29	1
30	1
50	1
70	1
73	1
Total	**21**

Por fim, em relação ao tempo de atuação da *startup*, nove delas operam há 24 meses ou menos. Sete delas, há mais de 24 meses e até 60 meses. As demais cinco *startups* atuantes estão no mercado entre 92 meses e 108 meses. A Tabela 5-5 detalha o tempo de atuação das *startups* no mercado.

Tabela 5-5. Primeiro ciclo: Tempo de atuação. Fonte: o Autor.

Tempo de Atuação	Qtde. de *startups*
6 meses	1
8 meses	1
12 meses	1
16 meses	1
24 meses	5
30 meses	1
36 meses	3
48 meses	1
60 meses	1
54 meses	1
92 meses	1
96 meses	2
108 meses	2
Total	**21**

Como se observa pelos dados, as *startups* apresentaram perfis bastante variados em relação a tempo de atuação no mercado, a quantidade de pessoas

trabalhando e ao número de clientes. Embora cinco delas operem na área de finanças, duas no setor jurídico e outras duas na área de comércio e varejo, há uma variação grande em relação ao campo de atuação de cada uma. De outro lado, a maioria delas estão no estágio de crescimento, sendo apenas quatro delas estando em fase inicial ou de protótipo.

Em relação ao perfil dos tomadores de decisão, nove declararam ser diretores executivos de suas *startups*, sete, diretores de tecnologia, três, diretores da área comercial. Quatro deles se definiram apenas como sócios do empreendimento. Um, por fim, declarou ser diretor jurídico da empresa, conforme apresentado na Tabela 5-6.

Tabela 5-6 Primeiro ciclo: Cargo. Fonte: o Autor.

Área Cargo	Qtde. de pessoas
Sócio	4
Diretor executivo	9
Diretor de tecnologia	7
Diretor comercial	3
Diretor jurídico	1
Total	**24**

No que diz respeito ao grau de escolaridade, seis deles possuem graduação em ensino superior, 11, especialização e seis deles, mestrado. Um deles tem o ensino médio completo e, nenhum, doutorado, conforme Tabela 5-7.

Tabela 5-7. Primeiro ciclo: Grau de Instrução. Fonte: o Autor.

Grau de instrução	Qtde. de pessoas
Ensino médio	1
Ensino superior	6
Especialização	11
Mestrado	6
Doutorado	-
Total	**24**

A média de idade dos tomadores de decisão é de 38 anos. Os mais novos têm 26 e o mais velho 61 anos. São oito entre 26 e 30 anos, sete entre 33 e 40 anos, seis entre 41 e 49 anos e três com mais de 50 anos.

No que tange à área de formação, conforme apresentado na Tabela 5-8, oito são da área de engenharia de computação, análise de sistemas, TI ou informática. Três da engenharia mecânica, um da mecatrônica, um da engenharia civil e outro da robótica. Um dos tomadores de decisão, além de ciências da computação, cursou também publicidade. Três graduaram em administração de empresas. Dois são

bacharéis em contabilidade, um deles com graduação também em administração e o outro em Tecnologia da Informação. Três são bacharéis de direito, um deles também com formação em Negócios Imobiliários.

Tabela 5-8. Primeiro ciclo: Área de formação. Fonte: o Autor.

Área deformação	Qtde. de pessoas
Engenharia da Computação, Análise de Sistemas/TI/Bacharel em Informática	8
Administração de Empresas	3
Engenharia Mecânica	3
Direito	2
Contabilidade e Administração de Empresas	1
Contabilidade e Tecnologia da Informação	1
Ciências da Computação e Publicidade	1
Engenharia Robótica	1
Engenharia Mecatrônica	1
Engenharia Civil	1
Direito e Negócios Imobiliários	1
Nenhuma área de formação	1
Total	**24**

Além disso, a maior parte dedica-se em tempo integral às *startups*. Dos 24 empreendedores, 20 deles dedicam 40 horas ou mais por semana para suas *startups*, e um deles dedica 20 horas semanais. Três dos empreendedores dedicam 8 horas semanais.

Em síntese, do perfil dos tomadores de decisão, portanto, depreende-se que há, no geral, um elevado grau de escolaridade. O fato de pelo menos 16 deles possuem conhecimentos técnicos em áreas de engenharia e três na área de direito pode favorecer o entendimento de questões ligadas à conformidade em LGPD. Isso porque questões referentes a aspectos técnicos de segurança de informação podem ser de mais fácil compreensão para engenheiros, enquanto termos e definições que possuam conotação jurídica podem ser mais facilmente compreendidos por bacharéis em direito.

5.1.2 Resultado da avaliação

Em relação à **Facilidade de Uso**, os tomadores de decisão avaliaram quatro assertivas. A primeira delas foi: “O método e as recomendações são claros e compreensíveis para mim.” O resultado é apresentado na Figura 5-1.

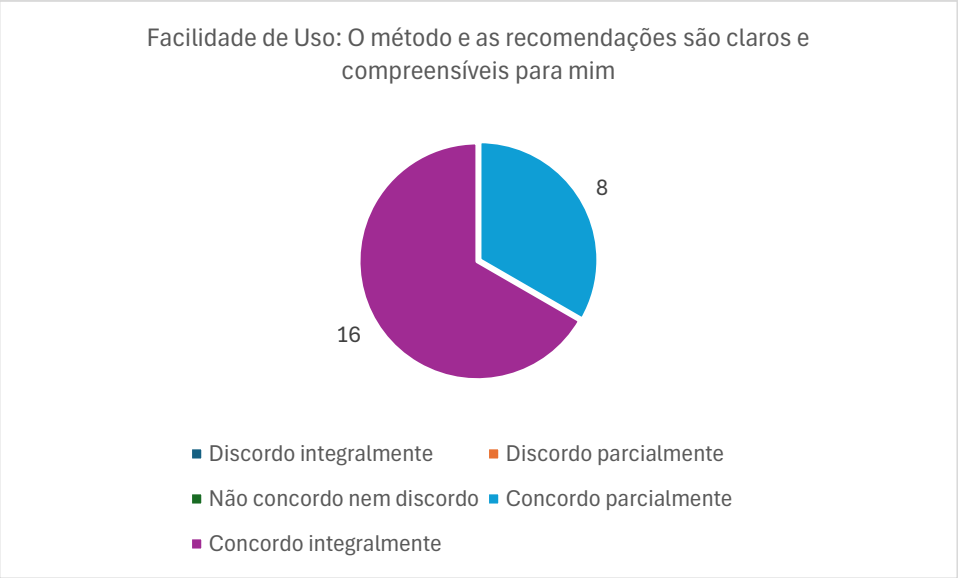

Figura 5-1. Primeiro ciclo, Facilidade de Uso: Compreensão do artefato. Fonte: o Autor.

Do total, 16 tomadores de decisão declararam concordar integralmente que o método e as recomendações são compreensíveis e oito concordaram parcialmente com a assertiva.

A segunda assertiva tratou do esforço cognitivo para interagir com o artefato, tendo o resultado apresentado na Figura 5-2.

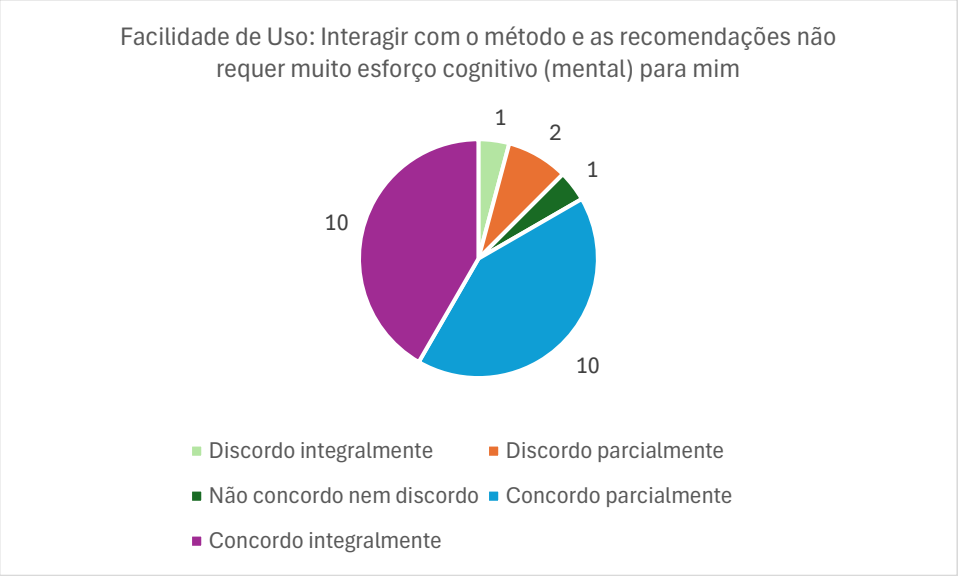

Figura 5-2 .Primeiro ciclo, Facilidade de Uso: Esforço cognitivo. Fonte: o Autor.

Dez empreendedores concordaram integralmente com a assertiva de que o método não requer muito esforço cognitivo e outros dez concordaram parcialmente com a assertiva. Um dos tomadores de decisão não concordou nem discordou, dois discordaram parcialmente e um discordou integralmente.

A terceira assertiva tratou da facilidade de aprender a usar o método e as recomendações. O resultado segue na Figura 5-3.

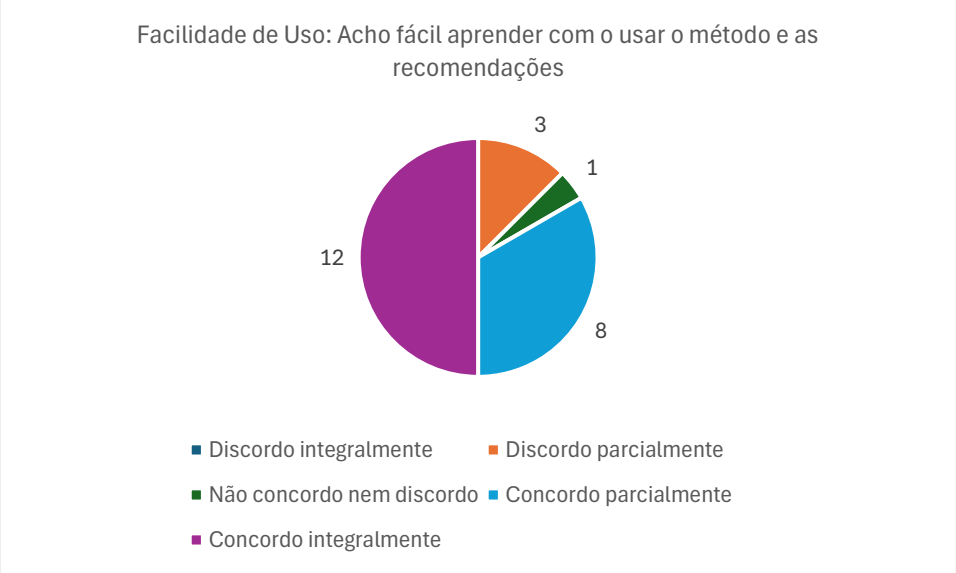

Figura 5-3. Primeiro ciclo, Facilidade de Uso: Aprender a usar o artefato. Fonte: o Autor.

Em relação à facilidade de aprender a usar o método e as recomendações, 12 tomadores de decisão declararam concordar integralmente, oito, parcialmente, um não concordou nem discordou e três discordaram parcialmente.

A quarta e última assertiva trata da facilidade de uso do método e das recomendações para se fazer o que quer – no caso, aplicar o método e chegar no resultado. A Figura 5-4 apresenta o resultado para esse ponto.

A esse respeito, 14 empreendedores concordaram integralmente com a assertiva de que o método e as recomendações são de fácil aplicação. Oito dos tomadores de decisão concordaram parcialmente e dois discordaram parcialmente.

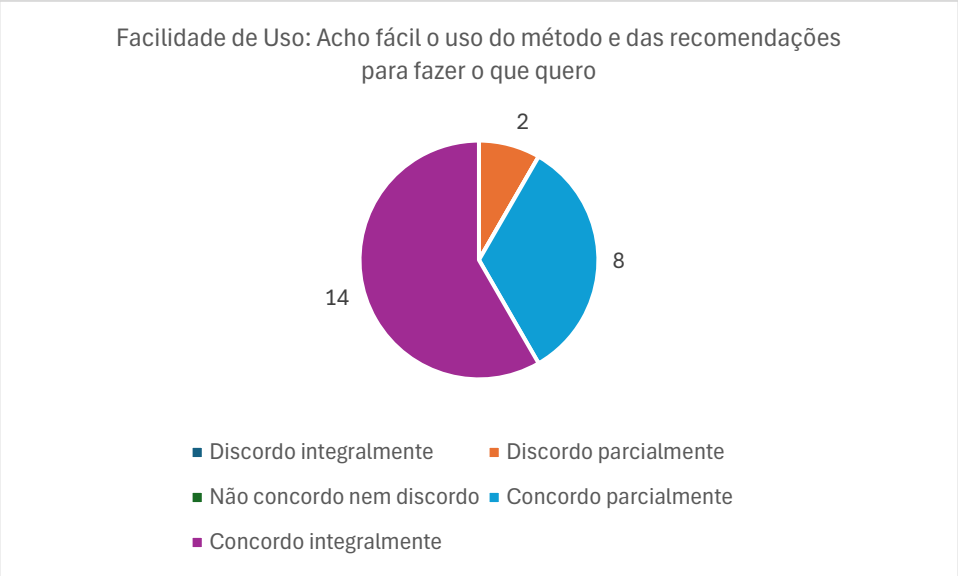

Figura 5-4. Primeiro ciclo, Facilidade de Uso: Facilidade de usar para se fazer o que quer. Fonte: o Autor.

Os comentários dos empreendedores para a categoria Facilidade de Uso foram codificados utilizando codificação provisória, estabelecendo-se códigos para cada manifestação dos tomadores de decisão. A Tabela 5-9 apresenta os códigos identificados, a quantidade de vezes em que ele aparece nos formulários respondidos e algumas das citações dos respondentes, a título de exemplo.

Como se observa, 13 citações dos tomadores de decisão demonstram a facilidade de uso – dez delas tratando diretamente da fácil usabilidade (#E02, #E06, #E7, #E08, #E09, #E010, #E14, #E18. #E19, #E21) e três delas da clareza textual (#E13, #E15, #E17). Esses dados estão alinhados com as avaliações feitas para a categoria Facilidade de Uso, conforme figuras acima.

De outro lado, houve 12 manifestações que demonstram possibilidade de melhoria no que se refere à usabilidade. Esses comentários foram levados em consideração para melhorar a compreensão do método, conforme descrito na seção 5.2.

Quatro dos tomadores de decisão apontaram que o método exige a necessidade de conhecimento técnico (#E03, #E11, #E19, #E24), um afirmou que o método poderia ser mais fácil (#E23) e outro que a linguagem deveria ser mais clara (#E04). Houve também quem sugerisse a necessidade de mais tempo para a aplicação do método (#E16), bem como de apresentação de exemplos (#E05) ou trazer mais explicações (#E06).

Além disso, um empreendedor (#E02) sugeriu incluir outras opções de resposta, como “parcialmente ou possivelmente” para que as questões ficassem adequadas a situações em que parte do enunciado era atendido.

Dois empreendedores (#E01, #E17) consideraram que o questionário trazia complexidade de interpretação para empresas que prestam serviços a outras empresas (*business-to-business* – B2B).

Tabela 5-9. Primeiro ciclo, Facilidade de Uso: Comentários. Fonte: o Autor.

Códigos	Qtde. de citações	Exemplos de códigos
Facilidade de uso	10	“É bem fácil entender o que é mencionado e recomendado.” (#E18) “Mesmo não sendo minha área de atuação, consegui compreender e utilizar a ferramenta com as explicações contidas no documento.” (#E09)
Necessidade de conhecimento técnico	4	“Não tenho o conhecimento técnico, uma vez que a atividade é performada pelo meu sócio.” (#E03)
Texto claro	3	“Achei as questões claras e objetivas” (#E15)
É complexo para empresas B2B	2	“(...) no entanto, a LGPD se torna um pouco confusa e requer uma interpretação específica de cada caso de empresa, no nosso caso o dado mais sensível que temos é o que nossos clientes armazenam em cadastro referente aos seus clientes, por exemplo, um cliente nosso pode ter salvado uma senha bancária do seu cliente sem nosso conhecimento e sem nosso controle.” (#E17)
Usar exemplos em perguntas	1	“A utilização de exemplos facilitou a compreensão das respostas. Recomendo usar em outras perguntas também.” (#E05)
Trazer mais explicações	1	“Interpretar as recomendações depende do quão familiarizado o respondente está com relação ao assunto, alguns pontos poderiam ter uma explicação adicional, caso necessário.” (#E6)
Necessidade de usar linguagem mais clara	1	“Considerar o baixo conhecimento do "intrevistado". Ele poderá responder aleatoriamente pois não conhece da temática. Talvez usar linguagem mais clara.” (#E04)
Dificuldade de compreensão no início do teste	1	“Acredito que o início poderia ser mais lógico, pois se não entender bem o conjunto de dados pode influenciar o resultado” (#E20)
Método poderia ser mais fácil	1	“Poderia ser mais fácil” (#E23)
Deve ser aplicado com mais tempo	1	“Certas perguntas envolvem uma vista mais detalhada. Acredito que se aplicado com mais tempo e provisão do time possa ser solucionado.” (#E16)
Deve incluir opções como parcialmente ou possivelmente para as questões	1	Fácil de Usar, porém acredito que algumas questões precisam de uma opção "parcialmente" ou "possivelmente" (#E02)

Em relação à categoria **Utilidade**, os tomadores de decisão avaliaram três assertivas. A primeira: “O uso do método e das recomendações melhorou meu desempenho para cumprir com a LGPD.” O resultado é apresentado na Figura 5-5.

Dos 24 empreendedores, 13 declararam concordar integralmente que o uso de artefato melhorou o desempenho para cumprir com a LGPD e 7 concordaram parcialmente com a assertiva. Os outros quatro declaram não concordar nem discordar da afirmação.

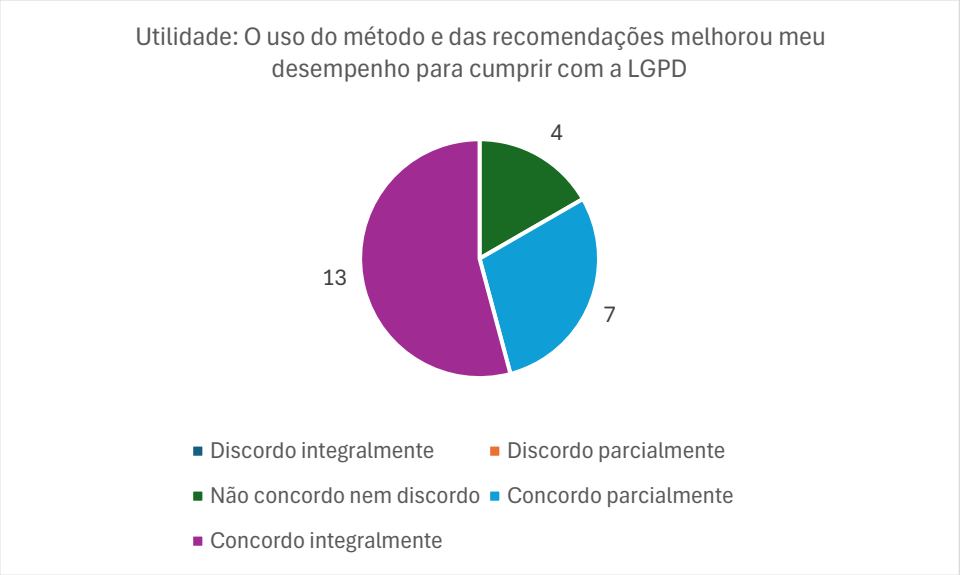

Figura 5-5. Primeiro ciclo, Utilidade: Melhoria de desempenho. Fonte: o Autor.

A segunda assertiva trata de o uso do método e as recomendações poderem aumentar a eficácia no cumprimento com a LGPD. O resultado das avaliações é apresentado na Figura 5-6.

Quinze empreendedores concordaram integralmente que o uso do método e das recomendações pode aumentar a eficácia no cumprimento da LGPD e outros sete, parcialmente. Dois tomadores de decisão indicaram não concordar nem discordar da assertiva.

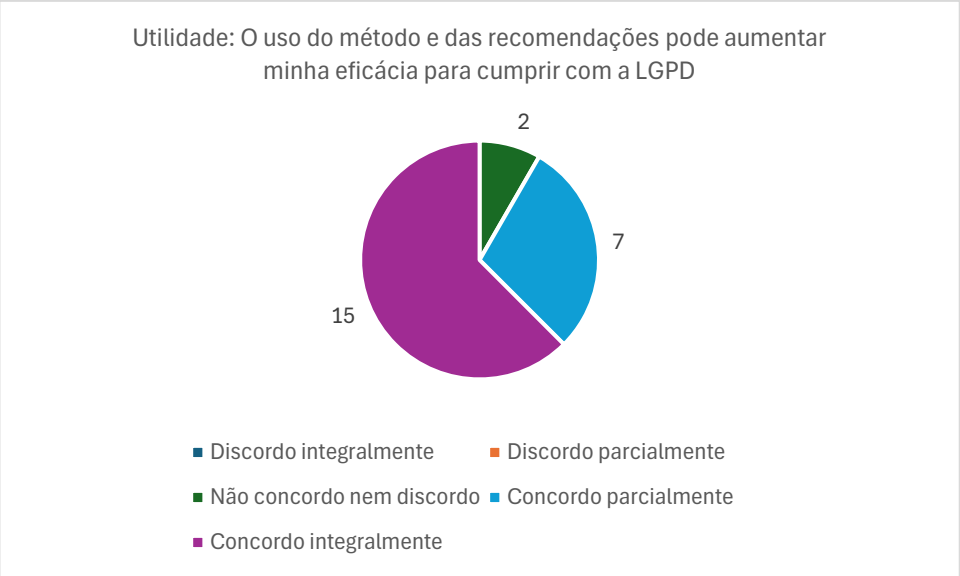

Figura 5-6. Primeiro ciclo, Utilidade: Aumento de eficácia para cumprir a LGPD. Fonte: o Autor.

A terceira e última assertiva referente a este ponto tratou da utilidade do método e das recomendações para cumprir com a LGPD. O resultado é apresentado na Figura 5-7. Dezoito empreendedores concordaram integralmente que o método e as recomendações são úteis para cumprir com a LGPD e cinco indicaram concordar parcialmente com a assertiva. Um dos tomadores de decisão declarou não concordar nem discordar da afirmação.

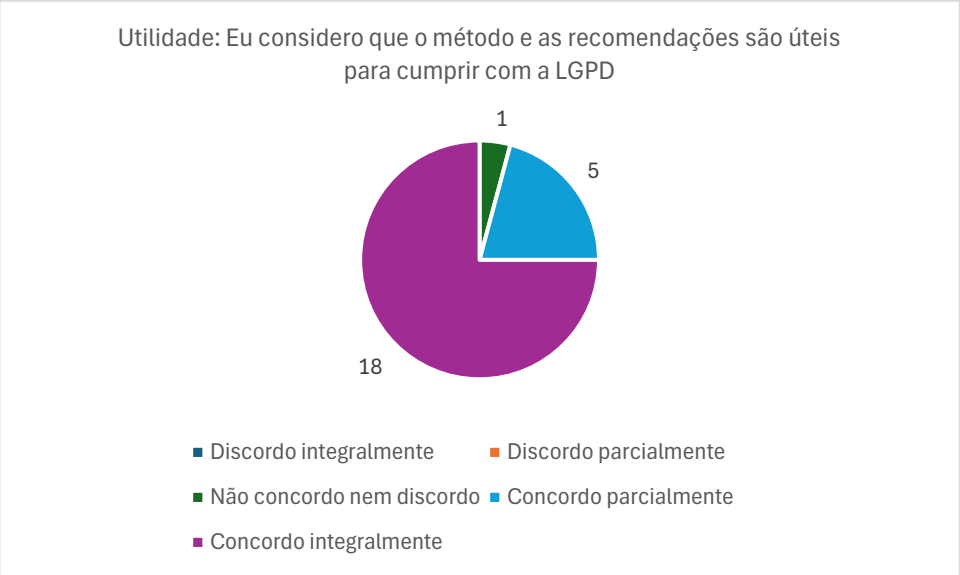

Figura 5-7. Primeiro ciclo - Utilidade: Útil para cumprir a LGPD. Fonte: o Autor.

Da mesma forma que para Facilidade de Uso, os comentários para a categoria Utilidade foram codificados utilizando codificação provisória, estabelecendo-se códigos para as manifestações dos tomadores de decisão. Os comentários e a codificação realizada encontram-se no Apêndice D e um resumo, para fins análise, é apresentado na Tabela 5-10.

Dos comentários dos tomadores de decisão, 10 menções tratam diretamente da utilidade do método (#E04, #E05, #E06, #E08, #E09, #E010, #E15, #E18, #E20, #E24). Outras cinco citações tratam da utilidade, mas de forma indireta: (i) uma informa que facilita o conhecimento e mapeamento de riscos (Facilita conhecimento e mapeamento de riscos (#E02); (iii) outra, que o método traz clareza sobre a implementação da LGPD (#E19); (iv) um empreendedor afirma que serve como ferramenta de avaliação de nível de conhecimento e de envolvimento dos diretores da empresa (#E22); e (v) outro declara ser muito útil para a governança corporativa. (#E3)

Há ainda quatro menções que se referem à clareza ou à praticidade do método (#E7, #E13, #E14, #E21).

De outro lado, quatro manifestações trazem pontos para reflexão sobre melhoramentos do método. Duas delas sugerem incorporar ao método explicação sobre como realizar as recomendações (#E12, #E16). Outra informa que há dificuldade em integrar as recomendações no cotidiano da startup (#E02) e uma quarta, já observada na categoria Facilidade de Uso, trata da complexidade em relação às empresas B2B (#E17).

Em que pese haja possibilidade de tornar mais aplicáveis as recomendações em versões posteriores do método, essa sugestão não foi incorporada para o segundo ciclo. E no que se refere ao contexto das empresas B2B, como já mencionado na categoria Facilidade de Uso, foram realizadas algumas alterações meramente informativas, a fim de esclarecer a aplicação do método.

Tabela 5-10. Primeiro ciclo, Utilidade: Comentários. Fonte: o Autor.

Código	Qtde. de citações	Exemplos de citações
Utilidade para cumprir com a LGPD	10	"O resultado é um material muito rico para entender onde estamos e ajustar para cumprir com a LGPD." (#0E6) "O mapa de risco com as recomendações será muito útil na geração de plano de ação para melhorias e correção de meus softwares" (#E09)
Sugere incorporar ao método explicação sobre como realizar as recomendações	2	Uma sugestão seria incorporar os como realizar as recomendações. (#E12)
Há dificuldade em integrar as recomendações no cotidiano da *startup*	1	"Minha maior dificuldade é conseguir aplicar as recomendações e integrá-las no dia a dia da *startup*. Essa parte pode ser mais explorada, além das recomendações quebrar em mais partes para explicar os próximos passos." (#E02)
É complexo para empresas B2B	1	"Como comentado anteriormente, existe uma dificuldade do nosso lado de executar algumas ações sugeridas, visto que somos a plataforma que armazena os dados de clientes dos nossos clientes" (#E17)
Facilita conhecimento e mapeamento de riscos	1	"Acredito que o método facilite o Conhecimento e o Mapeamento dos possíveis riscos envolvidos no Tratamento de Dados de outras pessoas." (#E02)
Método traz clareza sobre a implementação de LGPD	1	"Acho que a simplicidade das recomendações e a divisão dos critérios ligados à LGPD trazem uma clareza sobre onde focar e que caminho seguir." (#E19)
Método rápido e prático	1	"Super prático e rápido." (#E14)
Método prático e de fácil aplicação	1	"Achei bem prático e bem aplicável." (#E21)
Método satisfatório	1	"O método aplicado foi satisfatório (....)" (#E07)
Texto claro	1	"Textos claros" (#E13)
Método faz sentido para estágio inicial de startups	1	"As perguntas evidenciam algumas dúvidas que tínhamos lá no início do processo, tivemos direcionamento jurídico que permitiu estar num cenário mais aderente a LGPD, porém para casos insipientes, sistemas que estão iniciando, faz muito sentido." (#E01)
Muito útil para a governança corporativa	1	"Muito útil para cumprimento da LGPD e governança corporativa" (#E3)
Serve como guia de implementação, ferramenta de avaliação de nível de conhecimento e de envolvimento dos diretores da empresa	1	"Serve também como guia de implementação, como ferramenta de avaliaçãoo de nível de conhecimento e envolvimento dos CLevel's da empresa" (#E22)
Terá uso futuro	1	"(...) como meu negócio te várias versões de dados, vamos aprimorar novas aplicações como reteste, porque a empresa usa muitas dinâmicas de coleta de dados." (#E07)
Ainda não analisou com profundidade	1	"Ainda não analisei e apliquei o que recebi de análise, então é muito cedo para falar" (#E11)

Em relação à última categoria avaliada, **Uso Futuro**, foi avaliada a seguinte e única assertiva: “Levando em consideração que eu tenha domínio para escolher uma abordagem para conformidade de LGPD, eu prevejo que irei usar o método e as recomendações propostas”. A Figura 5-8 apresenta os resultados. Em relação à categoria Uso Futuro, 11 dos empreendedores concordam integralmente com a utilização do método e das recomendações futuramente e outros 11 declararam concordar parcialmente. Dois indicaram não concordar nem discordar com a assertiva.

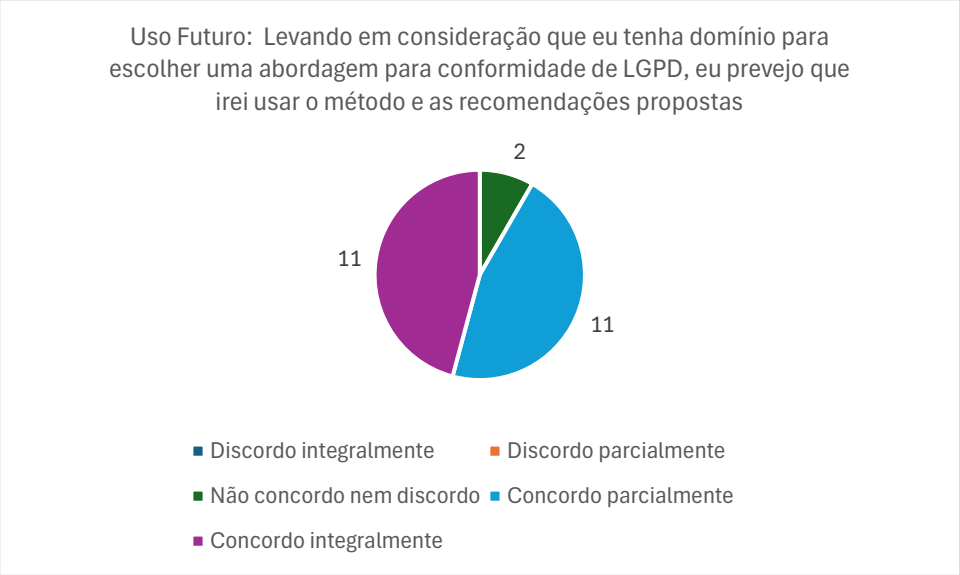

Figura 5-8. Segundo ciclo, Uso Futuro. Fonte: o Autor.

Da mesma forma que para as categorias Facilidade de Uso e Utilidade, os comentários para Uso Futuro foram codificados usando codificação provisória, estabelecendo-se códigos para as manifestações dos tomadores de decisão, que podem ser encontrados em sua totalidade no Apêndice D. Um resumo, para fins análise, é apresentado na Tabela 5-11.

Em relação a essa categoria, foram codificadas sete menções diretas nos comentários indicando o uso futuro do método (#E08, #E09, #E10, #E11, #E14, #E15, #E21). Há menções que indicam facilidade de uso – “texto claro”, “método bem elaborado” (E#03, E#07). Há também menções que indicam utilidade – “muito útil para cumprir com a LGPD” (E#06), “o método contribui de modo inicial” (#E24). Dois empreendedores, ainda, informaram que irão usar as recomendações (#E17, #E18).

Tabela 5-11. Primeiro ciclo, Uso Futuro: Comentários. Fonte: o Autor.

Código	Qtde. de citações	Exemplos de citações
Terá uso futuro	7	“Irei utilizar o método futuramente após implementar as melhorias.” (#E16) “Vou analisar sim o método e recomendações para o futuro” (#E11)
Irá usar as recomendações	2	“Irei utilizar as recomendações propostas para melhorar a conformidade com a LGPD.” (#E18)
Sugere incorporar ao método explicação sobre como realizar as recomendações	2	“Uma sugestão seria incorporar os como realizar as recomendações.” (#E12)
Precisa garantir a perenidade do negócio em primeiro lugar, por conta dos recursos escassos	2	“Acredito que startups no início da vida não tenham braço para priorizar e implementar boas práticas de LGPD. Apesar de perceber o benefício do método e das recomendações, não sei quando a adequação à LGPD será uma prioridade para mim.” (#E19)
Necessidade de conhecimento técnico para aplicação	2	“Não consigo sem ajuda técnica/especializada, e somente com o método, resolver na totalidade os assuntos sobre LGPD da minha startup.” (#E04)
Apresenta muitas recomendações, o que traz apreensão sobre a capacidade de aplicá-las	1	“São muitas as adequações e isso me deixou apreensiva sobre a capacidade de aplicá-las.” (#E05)
Necessidade de aplicar conforme o contexto da *startup*	1	“Necessário haver um recorte de acordo com o contexto ou nicho para maior aderência da solução/método proposto.” (#E01)
Traz os pontos para cumprimento e melhoria da governança	1	“Precisamos passar por cada um dos pontos para cumprimento e melhoria da governança de dados” (#E03)
O método é uma oportunidade de negócio	1	“Acredito que seja uma oportunidade de negócios, uma vez que as *startups* não possuem tangibilidade na aplicabilidade da LGPD.” (#E20)
Texto claro	1	“Textos claros” (#E13)
Muito útil para cumprir com a LGPD	1	O material servirá como uma excelente base e referência importantíssima (...).” (#E06)
Necessidade de uso de outras fontes para atender a LGPD em pontos mais específicos	1	“(...), porém eventualmente será necessário investigar em outras fontes quanto ao atendimento das conformidades, para refinamento, talvez em um aspecto mais específico.” (#E06)
Método bem elaborado	1	“Dinâmica bem elaborada (...).” (#E07)
Necessidade de o método atender às diversas categorias de dados utilizados	1	“(...), mas por se tratar de uma Fintech, utilizamos várias interfaces de uso de dados sensíveis, por esse motivo, em variações e escala, o estudo tem que convergir ao tipo de utilização e fins de dados.” (#E07)
O método contribui de modo inicial	1	“Ajuda de modo inicial e direcional (...).” (#E24)
Necessidade de aplicação a todo o time	1	“(...) mas precisaria ser aplicado ao time inteiro, para poder parametrizar respostas. Para alguns agentes seria necessário entrevista/formação prévia para ter acurácia nas respostas.” (#E24)

Além das 13 menções positivas em relação ao método, um comentário de um dos tomadores de decisão foi de que o método por si mesmo é uma oportunidade de negócio.

Os comentários apresentam também preocupações dos empreendedores com o contexto da empresa, como aqueles que se referem à necessidade de conhecimento técnico para a aplicação (E#04, E#24), ou da necessidade de garantir a perenidade do negócio em primeiro lugar, por conta dos recursos escassos (#E16, #E19).

Outras menções que indicam dificuldades para uso futuro, dizem respeito à necessidade de: (i) aplicar conforme o contexto da *startup*, que pode variar caso a caso (#E01); (ii) uso de outras fontes para atende a LGPD em pontos mais específicos (#E06); (iii) o método atender às diversas categorias de dados utilizados (#E07).

Da mesma forma que ocorreu em categorias anteriores, há duas menções que apresentam a sugestão de incorporar ao método explicação sobre como realizar as recomendações (#E02, #E12). Se implementadas, essas sugestões devem levar em conta o comentário de outro empreendedor que mencionou que o método apresenta muitas recomendações, trazendo apreensão sobre a capacidade de aplicá-las.

Uma vez descritos os resultados da avaliação sobre Facilidade de Uso, Utilidade e Uso Futuro, passa-se a análise dos resultados.

5.1.3 Análise do primeiro ciclo – Facilidade de Uso

O **primeiro ponto** a ser considerado em relação à Facilidade de Uso, é que o resultado da avaliação permite concluir que o método é claro para a maioria dos tomadores de decisão que o aplicaram. Dos empreendedores consultados, 16 deles concordaram integramente com a assertiva de que o método e as recomendações são claros e compreensíveis, e oito concordaram parcialmente.

O método e as recomendações foram considerados fáceis de aplicar para se chegar ao resultado pretendido pela maioria dos tomadores de decisão. Quatorze deles, conforme Figura 5-4, concordaram integralmente com essa afirmação e oito parcialmente.

Dois empreendedores, entretanto, discordaram parcialmente. Um deles comentou que o método poderia ser mais fácil de usar (#E23). E o outro indicou que, embora o método fosse fácil, haveria a necessidade de incluir opções como “parcialmente” ou “possivelmente” para as questões (#E02).

Esse é um importante ponto a ser levado em consideração, a fim de que o método seja melhorado. A sugestão, entretanto, não foi objeto de melhoria para o segundo ciclo e pode constar como ponto de aperfeiçoamento em versões futuras do método.

O **segundo ponto** a ser analisado é que, apesar de a maioria dos tomadores de decisão considerarem o método claro e fácil para se atingir ao resultado desejado, os resultados indicaram uma necessidade de melhorar a usabilidade do método, no que tange ao esforço cognitivo para utilizá-lo e à facilidade de aprendê-lo.

Dez empreendedores indicaram concordar integralmente que a interação não requer muito esforço cognitivo e outros dez concordaram parcialmente. Dos dez empreendedores que informaram concordar parcialmente, cinco deles, em seus comentários, declararam haver necessidade de conhecimento técnico para a aplicação do método.

Portanto, um ponto a ser melhorado é o de aprimorar a usabilidade do método, a fim que traga mais informações técnicas, para reduzir o esforço cognitivo de uso do método. Isso foi feito parcialmente para o segundo ciclo, ao ampliar a quantidade de informações no Tutorial, que passou de 6 para 11 slides. Mas há, entretanto, espaço para novas melhorias.

O **terceiro ponto** a ser levado em consideração é que, a introdução de informações técnicas, se bem implementada, pode influenciar positivamente também na facilidade para aprendizagem do método. Pois, quando avaliada a facilidade em aprender como usar como usar o método, 12 empreendedores concordaram integralmente que era uma tarefa fácil e 8, parcialmente. Contudo um não concordou nem discordou e outros três discordaram parcialmente. Os resultados indicam que há espaço para tornar o método mais fácil de aprender, algo que se tentou melhorar, ao ampliar a quantidade de informações no tutorial.

O **quarto ponto** a ser analisado trata de parte das respostas dadas à assertiva de que a interação com o método e as recomendações não requer muito esforço cognitivo. Um dos tomadores de decisão indicou não concordar nem discordar, outros dois discordaram parcialmente e um último discordou totalmente da afirmação.

Três dos comentários apresentados por esses quatro empreendedores, porém, não contribuem significativamente para a análise. O tomador de decisão que discordou totalmente (#E07) apenas elogiou o método, afirmando ser “simples, fácil e assertivo” e aquele que não concordou nem discordou comentou que os textos eram

claros (#E13). Um dos empreendedores que discordou parcialmente disse somente que o método poderia ser mais fácil (#E23).

De outro lado, o tomador de decisão remanescente, que discordou parcialmente, comentou que o início poderia ser “mais lógico” (#E20), pois teve dificuldade em entender como escolher o conjunto de dados e essa falta de compreensão pode influenciar o resultado.

Embora seja apresentado um passo a passo para a definição do conjunto de dados no tutorial e no corpo do texto do método, esse ponto pode ser melhorado. Não foi aperfeiçoado, entretanto, para o segundo ciclo, mas pode constar em aperfeiçoamentos futuros do método.

O **sexto ponto** de análise refere-se a dois empreendedores (#E01, #E17) que consideraram que o questionário trazia complexidade de interpretação para empresas que prestam serviços a outras empresas (*business-to-business* – B2B). Embora o questionário seja perfeitamente possível de se responder para empresas B2B, esse ponto foi alvo de melhoria no que se refere ao aspecto conformidade de tratamento, alterando-se ligeiramente o questionário para trazer explicações e remeter ao Tutorial, que foi modificado para apresentar algumas informações para empresas B2B.

5.1.4 Análise do primeiro ciclo - Utilidade

Em relação à categoria Utilidade, o **primeiro ponto** a ser considerado se refere à avaliação dos empreendedores de que o método e as recomendações são úteis para cumprir com a LGPD. Como já mencionado no tópico 5.1.2, nos comentários foram apresentadas dez menções diretas sobre a utilidade do método, sete tratam da utilidade forma indireta, além de haver quatro menções que o qualificam como rápido, prático, satisfatório ou claro.

Dezoito tomadores de decisão declararam concordar integralmente que o método e as recomendações são úteis para cumprir com a legislação, cinco concordaram parcialmente e somente um não concordou nem discordou. O empreendedor que declarou não concordar nem discordar (#E12) sugeriu, no espaço para comentários, que seria útil trazer mais informações sobre como implementar as recomendações apresentadas.

Esse parece ser um ponto de melhoria que pode trazer maior utilidade ao método, e que foi indicado também por um segundo tomador de decisão. Um dos empreendedores, que concordou integralmente a respeito da utilidade do método para

cumprir com a LGPD, também comunicou a necessidade de explicar melhor como implementar as recomendações. Entretanto, não houve alteração nesse sentido para o segundo ciclo, de forma que esse ponto pode ser aprimorado futuramente.

O **segundo ponto** de reflexão trata da percepção dos tomadores de decisão de que o método e as recomendações podem aumentar a eficácia para cumprir com a LGPD. Quinze dos empreendedores declararam concordar integralmente com o aumento de eficácia e sete parcialmente. Além disso, o tomador de decisão que informou não concordar nem discordar (#E14), comunicou, no campo de comentário, que achou o método “super prático e rápido”.

As razões para considerarem o método útil para aumentar a eficácia pode ser encontrada em parte dos comentários. Dos cinco empreendedores que declararam concordar parcialmente, dois informaram no campo de comentário que o método é “útil na geração de plano de ação para melhorias e correção de software”, ou que traz clareza sobre implementação da LGPD.

O **terceiro ponto** de reflexão diz respeito à percepção de grande parte dos empreendedores de que o método e as recomendações melhoraram o desempenho para cumprir com a LGPD – 13 deles concordaram integralmente e sete parcialmente com essa assertiva.

Dos sete tomadores de decisão que concordaram parcialmente, nenhum trouxe comentários negativos sobre a assertiva referente à melhoria de desempenho por conta do uso do método e das recomendações. Três comentários são relevantes, contudo, para compreender como o método pode estar associado à melhoria de desempenho. Um deles (#E20) considerou que o resultado foi o esperado e que acredita que outras *startups* podem se beneficiar.

Os outros dois fizeram comentários semelhantes entre si. Um deles informou que considera que o método facilita o conhecimento e o mapeamento de riscos (#E02), servindo como guia de boas práticas e que a dificuldade agora é conseguir aplicar as recomendações e integrá-las no cotidiano da empresa – “essa parte pode ser mais explorada, além das recomendações quebrar em mais partes para explicar os próximos passos”. O outro tomador de decisão (#E09) comentou que o método contribui para ter orientação sobre tomada de decisões e que com um plano de ação o método pode ser bastante efetivo.

Ambas as manifestações demonstram a utilidade do método e uma preocupação em como colocar as recomendações na prática. Isso, como já mencionado, é um ponto de melhoria a ser implementado futuramente.

Dos quatro que não concordaram nem discordaram a respeito de o método melhorar o desempenho no cumprimento da LGPD, um não deixou comentário (#E23) e outro (#E11) considerou muito cedo para fazer essa avaliação, uma vez que ainda não analisou e aplicou as recomendações. Um terceiro empreendedor (#E01) informou que o método evidenciou dúvidas que tiveram no início da jornada como *startup*, mas que para empresas que estão iniciando é útil.

O último deles (#E17) não fez comentários que pudessem ser relacionados à melhoria no desempenho para cumprir com a LGPD, apenas mencionando que algumas ações sugeridas teriam dificuldade de ser executadas por serem uma empresa B2B. Esse ponto, como já mencionado, identifica um problema de compreensão do questionário, pois o método abarca também companhias que atendem outras empresas, razão pela qual se procurou aprimorar o tutorial para o segundo ciclo.

O **quarto ponto**, por fim, a ser analisado, trata da análise dos comentários sobre a utilidade do método. Analisando os códigos é possível observar algumas razões apresentadas pelos empreendedores para considerarem o método útil: ser rápido, prático e de fácil aplicação, servir como guia de boas práticas e de ações a serem tomadas, e ser útil para a governança corporativa, facilitar o conhecimento e o mapeamento de riscos, trazer clareza sobre a implementação da LGPD, servir como ferramenta de avaliação de conhecimento e de envolvimento dos diretores.

5.1.5 Análise do primeiro ciclo – Uso Futuro

Em relação à categoria Uso Futuro, **o primeiro ponto** a ser considerado é que 11 dos tomadores de decisão afirmaram concordar integralmente com a assertiva de que irão usar o método e as recomendações propostas em momento futuro. Outros 11 declararam concordar parcialmente e dois afirmaram não concordar nem discordar da assertiva.

Embora onze tomadores de decisão tenham concordado parcialmente com a assertiva, dois deles (#E8, #E11) se manifestaram no campo de comentários no sentido de que irão usar o método e as recomendações no futuro. Além disso, um terceiro (#E18), embora não deixe explícito que irá usar o método futuramente,

comentou que irá usar as recomendações propostas para melhorar a conformidade com a LGPD.

Esses resultados indicam que, para parte dos empreendedores, o método possui potencial de uso futuro.

O **segundo ponto** a ser analisado trata da percepção de parte dos empreendedores de que o método teria dificuldade de atender contextos diversos de *startups*. Três dos tomadores de decisão que concordaram parcialmente ponderaram que haveria a necessidade de atender especificidades de suas *startups*. Um deles (#E01) afirmou que haveria necessidade de um recorte de acordo com o contexto ou nicho, para maior aderência do método. Outro (#E07) declarou que a dinâmica é bem elaborada, mas para o contexto de sua *startup* do setor financeiro haveria necessidade de o método “convergir ao tipo de utilização e fins de dados”. Por fim, um terceiro (#E06) manifestou-se no sentido de que o método possui uma base de referência importante, mas seria necessário outras fontes para atender aspectos específicos de conformidade com a LGPD.

As objeções levantadas demonstram a necessidade de aprimoração a comunicação do método. Embora necessite de alguns pontos de melhoria, o método, no que se refere à proposta – de contribuir para a tomada de decisão em relação à conformidade de LGPD –, é abrangente, podendo ser utilizado por *startups* de quaisquer áreas. Contudo, uma melhor comunicação pode alterar a percepção de que contextos diferentes, conforme exposto por #E01 e por #E07, necessitariam de ajustes no método.

A manifestação de #E06 indica a necessidade de recorrer a outras fontes para se adequar à LGPD em pontos específicos da lei. De fato, o método traz recomendações bastante gerais, para que cada empresa, dentro de sua especificidade busque caminhos de implementação de conformidade com a LGPD, podendo haver a necessidade de busca de mais conhecimentos. Importante mencionar, contudo, que o método trata apenas de aspectos de engenharia de software e suas relações com a conformidade com a LGPD. Outros aspectos específicos não fazem parte do escopo, como aqueles estritamente jurídicos, entre eles, por exemplo, a obrigação de manter um registro de operações de tratamento de dados, nos termos do Artigo 37 da LGPD.

Nesse sentido, uma comunicação mais assertiva aos tomadores de decisão, em relação às limitações do método para atender estritamente a atividades de engenharia parece ser necessária.

O **terceiro ponto**, trata da sugestão de #E12, de que se deveria incorporar nas recomendações mais informações sobre como cumpri-las. Se essa sugestão for implementada, talvez minimize a percepção da necessidade de busca de mais conhecimentos para a implementação de conformidade, conforme exposto por #E06.

Contudo, deve-se levar em conta o comentário de outro empreendedor que mencionou que o método apresenta muitas recomendações, trazendo apreensão sobre a capacidade de aplicá-las. Esse é um ponto, como já mencionado anteriormente, a ser melhorado futuramente.

O **quarto ponto** trata da necessidade de conhecimento técnico para cumprir com a conformidade com LGPD. Um dos tomadores de decisão (#E04) informou não conseguir usar o método sem ajuda técnica e outro (#E24) declarou que seria necessário formação prévia para algumas pessoas da equipe dele que viessem a aplicar o método, para que se tivesse acurácia nas respostas. Esses comentários evidenciam um ponto de melhoria que já foi identificado, o de que é necessário trazer mais conhecimento técnico, para que aqueles que não o possuem possam consultar e aplicar o método com facilidade.

O **quinto ponto** refere-se à análise dos tomadores de decisão que indicaram não concordar nem discordar sobre a assertiva de Uso Futuro. Um deles (#E23) não deixou comentário, mas #E16 declarou que, embora reconheça o risco para o negócio, há a necessidade de assegurar a perenidade do negócio em primeiro lugar, por conta dos recursos escassos.

O comentário evidencia algo que já identificado na revisão de literatura, quando analisado o contexto das *startups*. Empresas dessa natureza operam em um ambiente de falta de recursos, incerteza e pressão do tempo (MELEGATI *et al.* 2020). Empreendedores de *startups* reconhecem a importância da conformidade em proteção de dados, mas consideram que isso traz custos e absorve recursos que podem ser usados em outras atividades (BACHLECHNER; LIESHOUT; TIMAN, 2019, MARTIN *et al.*, 2019).

O **sexto ponto**, por fim, refere-se à análise da codificação provisória realizada que indica a validação do método para uso futuro, como observado no tópico 5.1.2, houve 13 menções positivas em relação método, além de um dos comentários, de

#E20, ser de que o método, por si só é uma oportunidade de negócio. Finalizada a análise do primeiro ciclo de demonstração, passa-se a seguir para a descrição da demonstração, avaliação e análise de resultados do segundo ciclo.

5.2 Segundo ciclo de demonstração e avaliação

Para a realização do segundo ciclo de demonstração foram realizadas quatro alterações no formulário do método e introduzidos cinco novos slides no Tutorial.

No primeiro ciclo, o Tutorial apresentava apenas as categorias de dados pessoais, para que os tomadores de decisão pudessem definir o conjunto de dados que seria usado na aplicação do método.

Para o segundo ciclo, o Tutorial, além das informações que já constavam, passou a trazer algumas explicações sobre conceitos básicos da LGPD – dados pessoais, dados pessoais sensíveis e tratamento de dados –, e alguns esclarecimentos sobre como a lei também é aplicável para empresas B2B e as implicações disso para o uso do método, nas seções de Conformidade de Tratamento e de Direitos dos Titulares.

O texto do formulário do método foi alterado em quatro pontos, para refletir as mudanças realizadas no Tutorial. A alteração no Bloco 1, em que se apresenta a introdução, trouxe uma breve explicação do conteúdo do Tutorial. A mudança no Bloco 2, em que se define o conjunto de dados, alterou o texto apenas para deixar claro que as instruções para a definição das categorias de dados começam a partir do slide 5 do Tutorial.

No Bloco 5, sobre Conformidade de Tratamento, foi introduzida uma frase recomendando as empresas B2B a consultarem o slide 4 do Tutorial, que apresenta orientações para que os tomadores de decisão tenham clareza sobre como responder as questões. Da mesma forma, foi incluído no Bloco 6 uma frase que recomenda que os empreendedores acessarem o slide 4 do Tutorial, a fim que recebam esclarecimentos sobre como responder a seção de Direitos dos Titulares.

Como se observa, as alterações realizadas foram apenas para trazer mais entendimento sobre o conteúdo da LGPD, bem como para esclarecer sobre o impacto da lei em relação às empresas B2B.

As seções de demonstração e avaliação do segundo ciclo ocorreu entre 4 e 26 de julho. A seguir apresenta-se o perfil das startups e tomadores de decisão do segundo ciclo e, depois, o resultado da avaliação.

5.2.1 Perfil de startups e tomadores de decisão

No segundo ciclo, o artefato foi demonstrado para uma *startup* em estágio inicial, nove em estágio de teste de protótipo, e 12 em fase de crescimento. Em quatro casos, as demonstrações ocorreram para dois tomadores de decisão de uma mesma *startup*. Assim, o artefato foi demonstrado para 22 tomadores de decisão de 17 *startups*, conforme Tabela 5-12.

Tabela 5-12. Segundo ciclo: Estágio da *Startup*. Fonte: o Autor.

Estágio da *startup*	**Qtde. de *startups***
Inicial	1
Testando protótipo (com ao menos um cliente)	6
Em crescimento (com mais de um cliente recorrente)	10
Total	**17**

Nesta nova etapa, participaram empreendedores de três *startups* da área de saúde, três da área jurídica, três de comércio e varejo, e duas do setor financeiro, além de outras nove, de setores variados, conforme se observa na Tabela 5-13.

Tabela 5-13. Segundo ciclo: Setor de Atuação. Fonte: o Autor.

Setor de Atuação	**Qtde. de *startups***
Saúde	3
Jurídico	3
Comércio e Varejo	3
Financeiro	2
SaaS – Algoritmo preditivo	1
SaaS – Transcrição e tradução de áudio e vídeo	1
Marketing	1
Educação	1
Moda	1
Sustentabilidade	1
Total	**17**

Em relação ao número de clientes, sete *startups* possuem entre zero e quinze clientes. Cinco delas têm entre 80 e 200 clientes. As demais possuem 500, 1.000, 1.800, 20.000 e 300.000. A empresa que tem mais de 20.000 clientes tem como modelo de negócio gestão do ciclo de vida de contratos e a 300.000 é uma *startup* em crescimento da área do varejo. A seguir a Tabela 5-14 detalha o número de clientes por quantidade de empresas nascentes.

Tabela 5-14. Segundo ciclo: Número de clientes. Fonte: o Autor.

Número de clientes	Qtde. de *startups*
Zero	1
1	1
3	1
5	1
10	1
15	2
80	1
120	1
150	1
180	1
200	1
500	1
1000	1
1800	1
20000	1
300000	1
Total	**17**

No que se refere ao número de pessoas trabalhando na *startup* (funcionários e sócios), 10 delas possuem menos de 10 pessoas e seis entre 11 e 50. Uma das empresas, que atua no varejo, tem 200 pessoas atuando. A Tabela 5-15 a seguir apresenta os dados de forma detalhada.

Tabela 5-15. Segundo ciclo: Pessoas trabalhando na *startup*. Fonte: o Autor.

Número de pessoas	Qtde. de *startups*
2	1
4	3
5	2
6	1
7	1
9	1
10	1
11	1
12	2
16	1
22	1
50	1
200	1
Total	**17**

Em relação ao tempo de atuação da *startup*, por fim, oito estão em operação há 24 meses ou menos. Seis delas operam há mais de 24 meses e até 60 meses. Uma das *startups* atua há 72 meses e as outras duas, há 84 meses. A Tabela 5-16 detalha o tempo de atuação das empresas no mercado.

Tabela 5-16. Segundo ciclo: Tempo de atuação. Fonte: o Autor.

Tempo de Atuação	Qtde. de *startups*
5 meses	1
10 meses	1
12 meses	4
24 meses	2
30 meses	1
48 meses	3
54 meses	1
60 meses	1
72 meses	1
84 meses	2
Total	**17**

Como se observa, a maior parte das startups que avaliaram o artefato estão em estágio de crescimento. Praticamente a metade do total (9 das 17) são dos setores de saúde, jurídico e de comércio e varejo, enquanto as demais são de diversas áreas. Além disso, o perfil delas é bastante variado em relação ao tempo de atuação no mercado, à quantidade de pessoas trabalhando, e ao número de clientes. A amostra do segundo ciclo, portanto, também possui startups bastante heterogêneas entre si, cenário semelhante ao do primeiro ciclo.

No que tange ao perfil dos tomadores de decisão, conforme apresentado na Tabela 5-17, nove indicaram ocupar posição de diretor executivo, oito, de diretor de tecnologia, dois de diretor da área comercial. Por fim, três dos tomadores de decisão declararam ser sócios do empreendimento.

Tabela 5-17 Segundo ciclo: Cargo. Fonte: o Autor.

Cargo	Qtde. de pessoas
Sócio	3
Diretor executivo	9
Diretor de tecnologia	8
Diretor comercial	2
Total	**22**

Todos os empreendedores possuem ensino superior, sete deles com especialização, seis com mestrado e dois com doutorado, conforme Tabela 5-18.

Tabela 5-18 Segundo ciclo: Grau de Instrução. Fonte: o Autor.

Grau de instrução	Qtde. de pessoas
Ensino médio	-
Ensino superior	7
Especialização	7
Mestrado	6
Doutorado	2
Total	**22**

No que se refere à idade dos tomadores de decisão, a média é de 35 anos. O mais novo tem 21 e o mais velho 55 anos. São cinco entre 25 e 30 anos, 13 entre 31 e 40 anos, e três acima de 40 anos, conforme apresentado na tabela abaixo.

No que se refere à área de formação dos empreendedores, nove são da área de engenharia de computação, ciência da computação, engenharia de software e Tecnologia da Informação. Um dos empreendedores tem formação em sistemas de informação e marketing e outro em engenharia elétrica. Três graduaram-se em Direito, com dois deles tendo outras formações – um em gestão e outro em Tecnologia da Informação. Os demais possuem formação, conforme Tabela 5-19, em diversas áreas do conhecimento.

Tabela 5-19 Segundo ciclo: Área de formação. Fonte: o Autor.

Área deformação	Qtde. de pessoas
Engenharia da Computação/Tecnologia da Informação/Ciência da Computação/Engenharia de Software	9
Sistema de Informação e Marketing	1
Engenharia Elétrica	1
Física	1
Medicina	1
Arquitetura e Urbanismo	1
Administração	1
Direito e Tecnologia da informação	1
Direito e Gestão	1
Direito	1
Gestão e Vendas	1
Filosofia e Moda	1
Jornalismo	1
Relações Internacionais	1
Total	**22**

Por fim, no que se refere ao tempo de dedicação, 15 dos empreendedores trabalham em tempo integral nas *startups*. Dos demais, três dedicam cerca de trinta horas semanais, outro trabalha 20 horas e os três restantes se ocupam por 10 horas ou menos com atividades de suas empresas.

5.2.2 Resultado da avaliação

Em relação à Facilidade de Uso, os tomadores de decisão avaliaram quatro assertivas. A primeira: “O método e as recomendações são claros e compreensíveis para mim.” Na Figura 5-9 é apresentado o resultado.

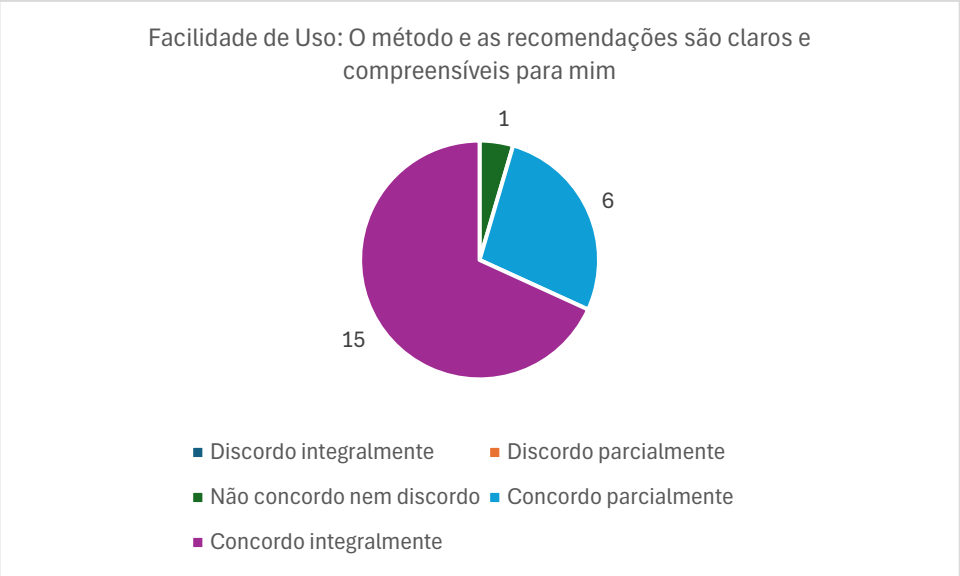

Figura 5-9. Segundo ciclo, Facilidade de Uso: Compreensão do artefato. Fonte: o Autor.

Do total de empreendedores, 15 indicaram concordar integralmente que o método e as recomendações são compreensíveis, seis declararam concordar parcialmente com a assertiva e um informou que não concorda nem discorda.

A segunda assertiva se referiu ao esforço cognitivo para interagir com o artefato. O resultado é apresentado na Figura 5-10.

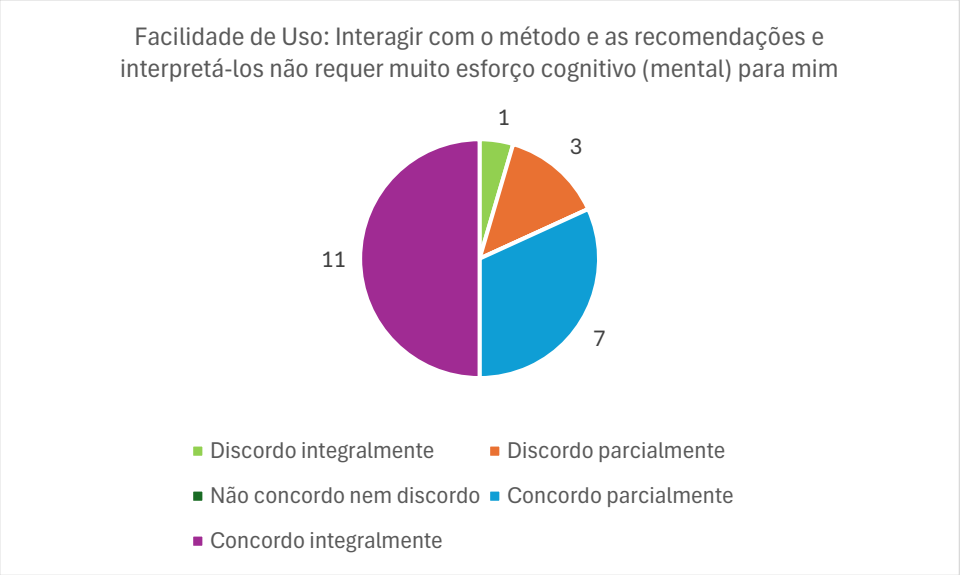

Figura 5-10.Segundo ciclo, Facilidade de Uso: Esforço cognitivo. Fonte: o Autor.

Onze empreendedores declararam concordar integralmente com a assertiva de que o método não requer muito esforço cognitivo e outros sete informaram concordar

parcialmente com a afirmação. Três dos tomadores de decisão indicou não concordar nem discordar, e o remanescente informou discordar integralmente.

A terceira assertiva tratou da facilidade do empreendedor em aprender a usar o método e as recomendações. O resultado é apresentado na Figura 5-11.

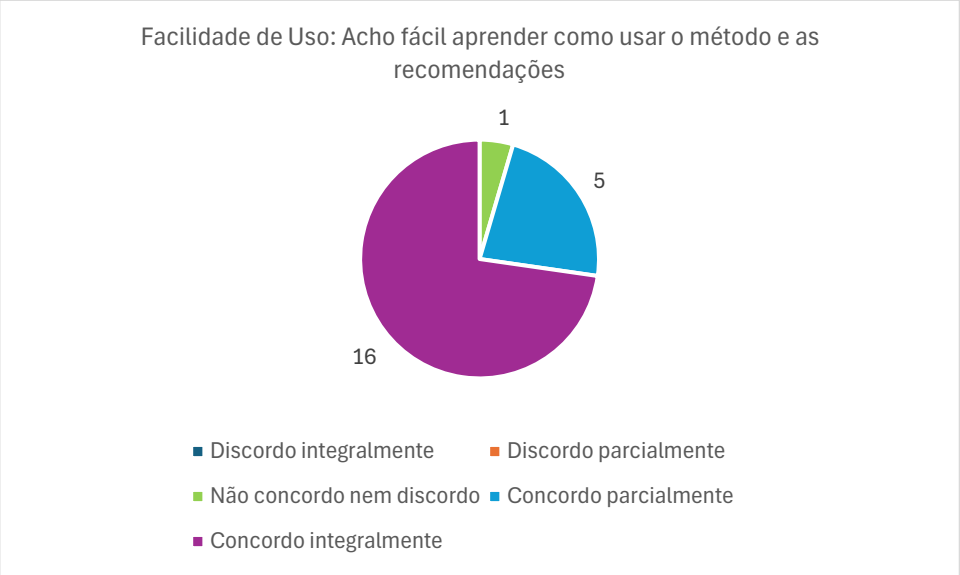

Figura 5-11 .Segundo ciclo, Facilidade de Uso: Aprender a usar o artefato. Fonte: o Autor.

No que tange à facilidade de aprender a usar o método e as recomendações, 16 tomadores de decisão informaram concordar integralmente, cinco, parcialmente, e um não concordou nem discordou.

Em relação à facilidade de uso do método, a quarta e última assertiva tratou da facilidade de utilizar o método e as recomendações para se fazer o que se quer. A Figura 5-12 apresenta o resultado da avaliação dos tomadores de decisão.

Como se observa, 15 tomadores de decisão informaram concordar integralmente com a afirmação de que o método e as recomendações são fáceis de se usar para se chegar ao resultado pretendido. Cinco deles indicaram concordar parcialmente e dois não concordaram nem discordaram da assertiva.

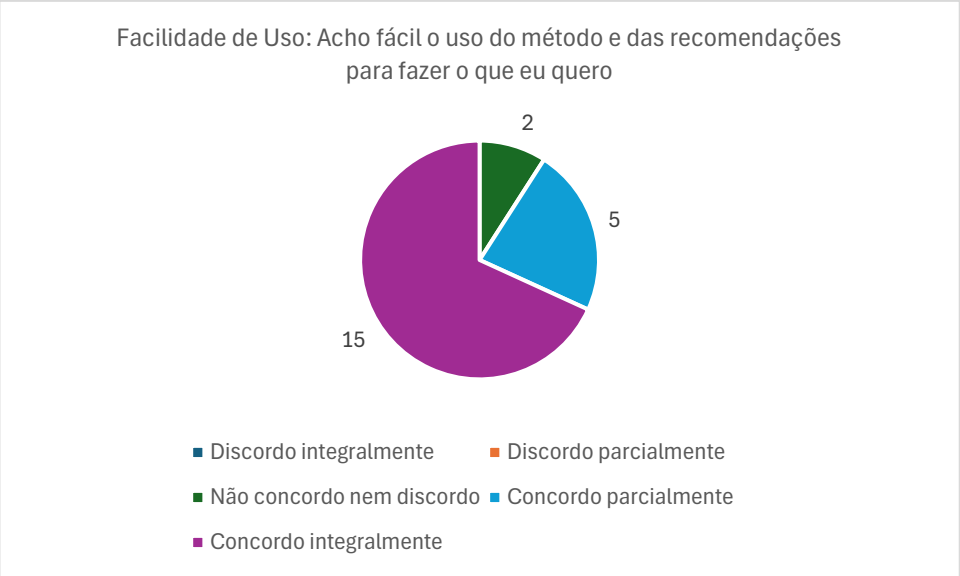

Figura 5-12 .Segundo ciclo, Facilidade de Uso: Facilidade de usar para se fazer o que quer. Fonte: o Autor.

Da mesma forma que no primeiro ciclo, os comentários para a categoria Facilidade de Uso foram codificados utilizando codificação provisória, para cada manifestação dos empreendedores. A resposta à pergunta era obrigatória. Os empreendedores, entretanto, poderiam, caso desejassem, responder que nada mais tinham a declarar. A Tabela 5-20 apresenta a síntese da codificação realizada para o bloco Facilidade de Uso.

Tabela 5-20 Segundo ciclo, Facilidade de Uso: Comentários. Fonte: o Autor.

Códigos	Qtde. de citações	Exemplos de citações
Facilidade de uso	8	“Muito acessível e de fácil entendimento.” (#E31) “Método tranquilo de aplicar.” (#E33)
Texto claro	6	“As proposições são muito claras.” (#E30)
Sugere incluir os artigos da LGPD junto com as recomendações	1	“Interessante incluir artigo da lei conforme recomendação.” (#E41)
Usar exemplos em perguntas	1	“Talvez mais exemplos ajudariam a entender melhor a pergunta.” (#E45)
Precisa trazer mais explicações	1	“Apenas alguns ajustes como esclarecimentos de pequenas dúvidas se faz necessário.” (#E36)
Disponibilizar o tutorial com antecedência facilitaria a aplicação	1	“Se o tutorial for disponibilizado com antecedência facilita a interação e execução.” (#E32)
Deve incluir opção "não se aplica" para as respostas	1	“Fácil de usar e responder as perguntas, entretanto faltou a alternativa de: não se aplica. Já que muitas das perguntas não fazem sentido no nosso caso.” (#E34)
Dificuldade para entender as questões sobre tratamento de dados	1	“Gostei! Senti dificuldade para entender e compreender os questionamentos referentes ao tratamento de dados.” (#E25)

Como se observa, ao menos 14 citações foram integralmente positivas, referentes à facilidade de uso e à clareza do texto. A maioria das demais apresenta sugestões de melhoria, como incluir os artigos da LGPD nas recomendações, usar exemplos nas perguntas, trazer mais explicações, disponibilização de tutorial com antes de aplicar o método, incluir a opção “não se aplica” para as respostas. Em uma única citação (#E25), apesar de o empreendedor ter informado gostar do método, ele comunicou ter sentido dificuldade para entender e compreender os questionamentos referentes ao aspecto de Conformidade de Tratamento.

Em relação à Utilidade, os empreendedores avaliaram três assertivas. A primeira delas foi: “O uso do método e das recomendações melhorou meu desempenho para cumprir com a LGPD.” A Figura 5-13 apresentada o resultado dessa primeira afirmação.

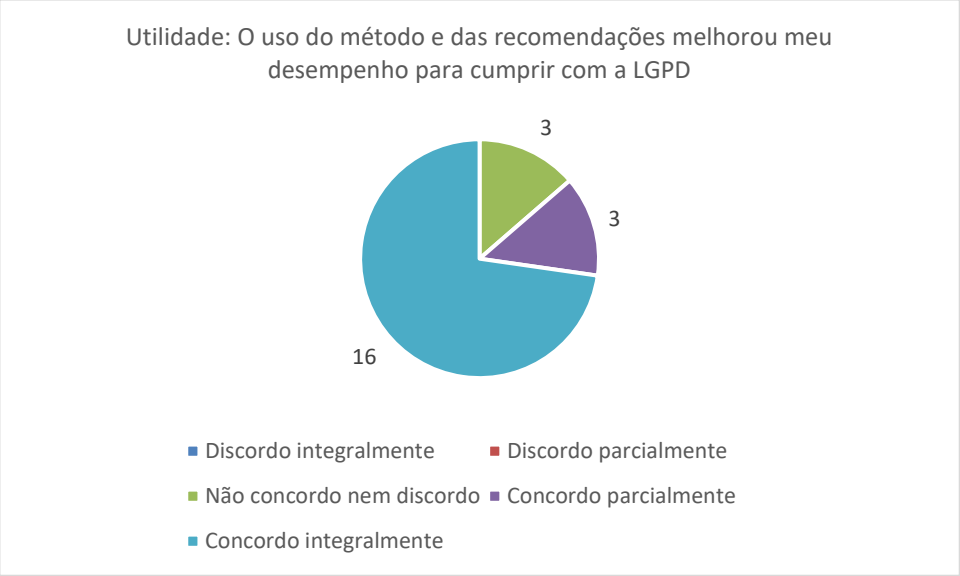

Figura 5-13. Segundo ciclo, Utilidade: Melhoria de desempenho. Fonte: o Autor.

Do total de tomadores de decisão, 16 declararam concordar integralmente que o uso de artefato melhorou o desempenho para cumprir com a LGPD, três concordaram parcialmente com a assertiva e três não concordaram nem discordaram.

A segunda assertiva refere-se ao uso do método e das recomendações possibilitarem aumentar a eficácia no cumprimento com a LGPD. A seguir, a Figura 5-14 apresenta o resultado das avaliações nos tomadores de decisão.

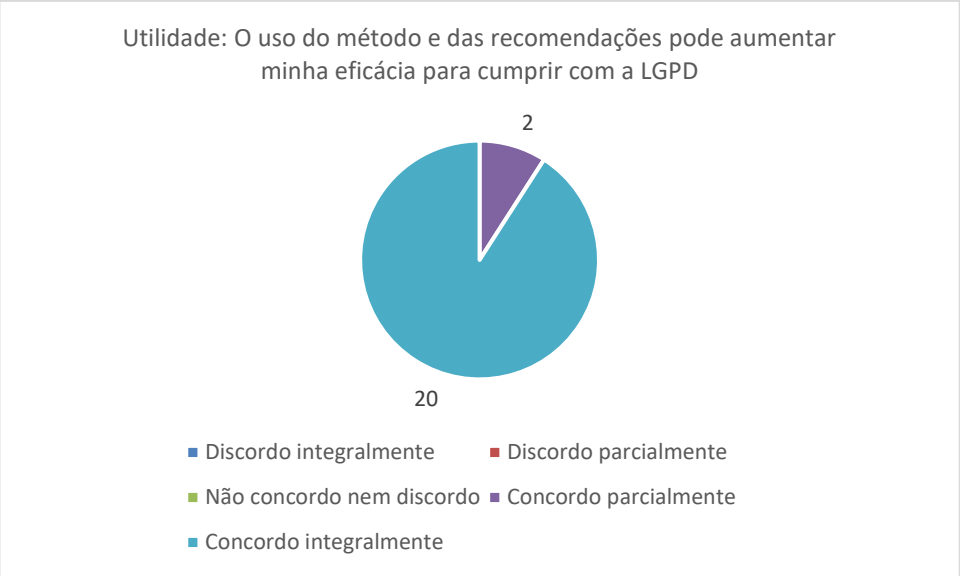

Figura 5-14. Segundo ciclo, Utilidade: Aumento de eficácia para cumprir a LGPD. Fonte: o Autor.

O resultado da avaliação indicou que 20 tomadores de decisão concordaram integralmente que o uso do método e das recomendações pode aumentar a eficácia no cumprimento da LGPD. Os outros dois empreendedores informaram concordar parcialmente com a assertiva.

A terceira e última assertiva sobre Utilidade tratou do proveito do método e das recomendações para cumpri com a LGPD. O resultado é apresentado na Figura 5-15.

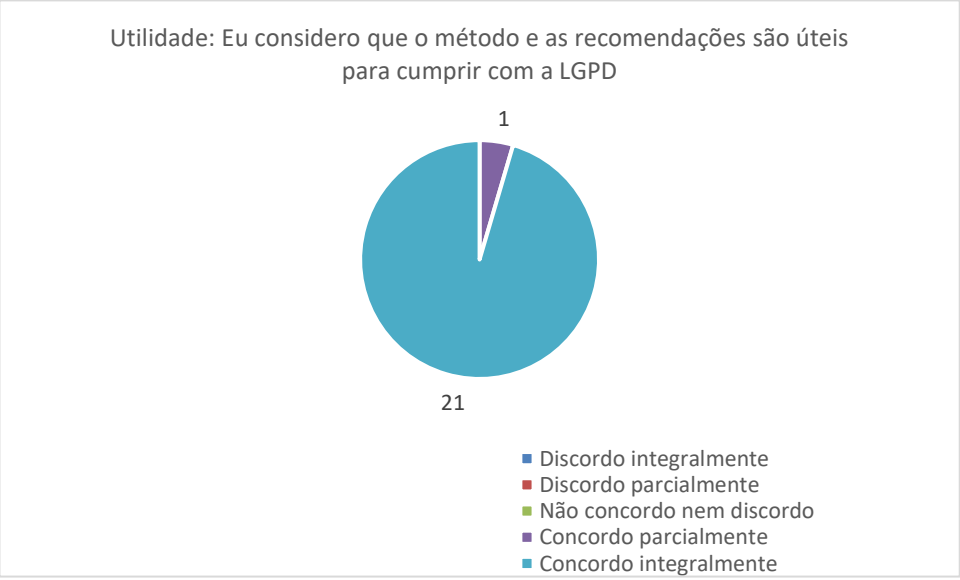

Figura 5-15. Segundo ciclo, Utilidade: Útil para cumprir com a LGPD. Fonte: o Autor.

Vinte e um empreendedores concordaram integralmente que o método e as recomendações são úteis para cumprir com a LGPD. O remanescente indicou concordar parcialmente com a assertiva.

Da mesma forma que para Facilidade de Uso, os comentários para a categoria Utilidade foram codificados utilizando codificação provisória. A codificação realizada é apresentada na Tabela 5-21.

Tabela 5-21 Segundo ciclo, Utilidade: Comentários. Fonte: o Autor.

Código	Qtde. de citações	Exemplos de citações
Utilidade para cumprir com a LGPD	11	"Claramente estar alinhado ao método levaria a uma maturidade elevada de segurança da informação e LGPD" (#E27) "Achei útil pois evidenciou diversas questões importantes que ainda não estavam no radar, especialmente sobe a dinamicidade e o ciclo dos dados." (#E30)
Causa reflexões positivas	1	"Acredito que causa reflexões positivas para mais rapidamente endereçar as ações com base em causas raízes." (#E32)
Traz uma visão geral sobre conformidade em LGPD	1	"Ótimo para gerar uma visão geral das necessidades que temos que cumprir." (#E33)
Forma simples para identificar lacunas de conformidade com a LGPD e relatório detalhado	1	"É uma forma simples e inteligível de identificar potenciais furos da cumplicidade da LGPD e o relatório é bem detalhado quanto às possíveis formas de mitigação." (#E35)
Falta de imposição de multa faz com que as empresas não cumpram a legislação	1	"Seria mais fácil justificar a dedicação de tempo para a aplicação das recomendações se houvesse vislumbre de que a ANPD impusesse multas às empresas que não cumprem a legislação, no sentido de haver uma redução de risco efetiva (sem a atuação da ANPD o risco parece mais teórico do que prático)." (#E44)
Necessidade de os empreendedores agirem conforme as recomendações	1	Entrega em uma análise rápida e superficial os principais pontos de atenção para a empresa tomar medidas. Porém é necessário seguimento por parte dos idealizadores das empresas que estão auxiliando no estudo. (#E29)

A tabela mostra que foram identificadas 14 citações positivas, entre empreendedores que indicaram utilidade do método, ou que o consideraram útil para causar reflexões positivas, para trazer um panorama sobre conformidade de LGPD ou para identificar lacunas de conformidade. Seis tomadores de decisão não deixaram comentários.

Um empreendedor (#E44) afirmou que a falta de atuação da ANPD na imposição de multas reduz o risco efetivo de não cumprimento com a LGPD. Outro tomador de decisão (#E29) declarou que embora o método entregue uma análise rápida dos principais pontos de atenção é preciso que os empreendedores deem seguimento às recomendações.

Em relação à Uso Futuro, última categoria avaliada, os tomadores de decisão tiveram de analisar uma única assertiva: “Levando em consideração que eu tenha domínio para escolher uma abordagem para conformidade de LGPD, eu prevejo que irei usar o método e as recomendações propostas”. O resultado é apresentado na Figura 5-16.

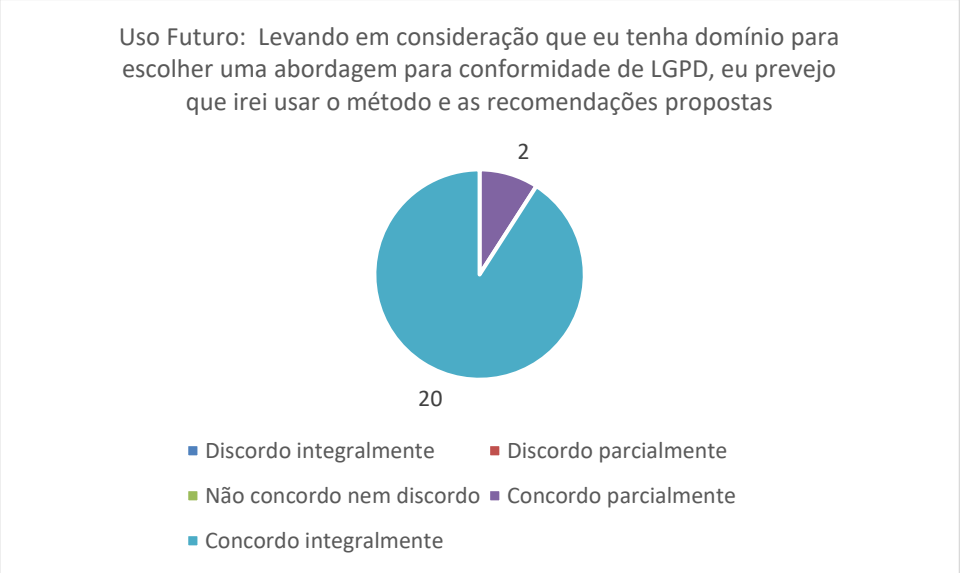

Figura 5-16. Segundo ciclo, Uso Futuro. Fonte: o Autor.

Em relação à possibilidade de usar futuramente o método e as recomendações propostas, 20 empreendedores informaram concordar integralmente. Os outros dois declaram concordar parcialmente com a assertiva.

Da mesma forma que para Facilidade de Uso e para Utilidade, os comentários para a categoria Utilidade foram codificados utilizando codificação provisória conforme a Tabela 5-22.

Tabela 5-22 Segundo ciclo, Uso Futuro: Comentários. Fonte: o Autor.

Código	Qtde. de citação	Exemplos de citações
Terá uso futuro	9	“Gostaria de usar futuramente com o time” (#E32) “Certamente vamos usar para gerar e priorizar nosso backlog de segurança da informação” (#E33)
Uso do método para identificar vulnerabilidades e as considerações para minimizar o risco	1	Provavelmente usaríamos o método pensando em novas features, aplicando o método para compreender onde existiria vulnerabilidade, e utilizando as considerações para minimizar os riscos (#E46)
A implementação das recomendações aumenta a maturidade da conformidade com a LGPD	1	“Seguir e implementar aumenta a maturidade” (#E27)
Deve incluir opção "cumpro parcialmente" para as respostas	1	“Se eu puder indicar uma resposta para algumas perguntas seria: (Cumpro parcialmente)” (#E39)
O método é aplicável para diversas áreas da empresa	1	“O método é aplicável para diversas áreas da empresa, como RH, Plataforma, novos produtos.” (#E31)
Facilidade de leitura do relatório	1	“Considerando a facilidade de leitura do relatório, será de extrema utilidade para que a gente possa reavaliar em quais aspectos a nossa aplicação pode não estar em conformidade com a LGPD e melhorar estas situações.” (#E35)
Dará seguimento do relatório junto ao departamento jurídico	1	“Sim, já vou passar para o time jurídico analisar.” (#E42)
Útil para incluir no roteiro ações a serem realizadas para manter a segurança de dados	1	“Me dá um roadmap de o que priorizar para arrumar.” (#E45)

Todas as citações dos empreendedores para uso futuro do método foram positivas. Nove delas apontam diretamente para uso futuro. Outras mostram a percepção dos tomadores da decisão sobre a utilidade, como no caso de #E45, que considera o método bom para estabelecer prioridades, e de #E35, que entende que permite a realização de aspectos que podem não estar em conformidade.

Há também quem considere o método de utilidade para aplicação em diversas áreas da empresa (#E31) ou para o desenvolvimento de novas funcionalidades (#E46), a fim de evitar vulnerabilidades em relação à LGPD. Além disso, dois tomadores de decisão informaram que iriam dar seguimento com as recomendações (#E27 e #E42).

Importante, ainda, mencionar o comentário de #E39, que sugere incluir a opção “cumpro parcialmente”, o que deve ser avaliado em momento futuro.

Dos dois empreendedores que declararam concordar parcialmente com a assertiva de uso futuro, apenas um publicou comentário, (#E32) no sentido de que gostaria de usar o método futuramente com a equipe. Sete empreendedores não incluíram comentários. Apresentados os resultados, passa-se à análise do segundo ciclo.

5.2.3 Análise do segundo ciclo – Facilidade de Uso

Para a análise deste novo ciclo, para fins de comparação, leva-se em conta os resultados da avaliação da primeira demonstração. Leva-se em consideração também as modificações realizadas no método e no Tutorial, bem como os resultados da aplicação do método para os 22 empreendedores que participaram do segundo ciclo.

Em relação à Facilidade de Uso, em que pese que o segundo ciclo teve dois respondentes a menos que o primeiro, os resultados foram relativamente parecidos.

A Tabela 5-23 apresenta os resultados para a primeira assertiva, que trata da clareza e da facilidade de compreensão do método e das recomendações, para os dois ciclos.

Tabela 5-23 Comparativo, Facilidade de Uso: Compreensão do artefato. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	16	15
Concordo parcialmente	8	6
Não concordo nem discordo	0	1
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

As variações numéricas entre os ciclos não são significativas. O empreendedor que participou da segunda rodada e que afirmou não concordar nem discordar da afirmativa (#E45), sugere que mais exemplos poderiam ajudar a melhorar o entendimento. Dos seis empreendedores que concordaram parcialmente na segunda rodada, é importante destacar os comentários, dois deles sugeriram que haveria a necessidade ou de trazer mais esclarecimentos para as questões (#E36) ou disponibilizar com antecedência o Tutorial (#E32).

Assim, como **primeiro ponto** de análise, esses comentários, em conjunto com o resultado da avaliação da segunda rodada sugerem que embora a maioria dos

empreendedores considere o método e as recomendações de fácil compreensão, continua havendo espaço para aprimoramento. As alterações realizadas no Tutorial e no texto de parte do método podem não ter surtido efeito para aumentar a clareza e a facilidade de compreensão do método.

Portanto, a necessidade de melhorar a usabilidade do método, já identificada no primeiro ciclo, permanece.

Em relação à segunda afirmação avaliada sobre Facilidade de Uso – “interagir com o método e as recomendações não requer muito esforço cognitivo para mim” – do resultado comparativo é apresentado na Tabela 5-24.

Tabela 5-24 Comparativo, Facilidade de Uso: Esforço cognitivo. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	10	11
Concordo parcialmente	10	7
Não concordo nem discordo	1	0
Discordo parcialmente	2	3
Discordo integralmente	1	1
Total	24	22

Os resultados aferidos entre os dois ciclos são muito parecidos. Em relação aos comentários da segunda rodada para a categoria Facilidade de Uso, e que podem estar relacionados a questões de esforço cognitivo, destaca-se a dificuldade de entender questionamentos sobre tratamento de dados (#E25), e a necessidade de se incluir a opção “não se aplica”, para poder atender particularidades de uma maior gama de empresas (#E27, #E34).

O **terceiro ponto** de análise, portanto, trata da necessidade de se incluir a opção “não se aplica” ao método, em desenvolvimento futuro.

A terceira assertiva avaliada foi referente à facilidade para se aprender a usar o método e as recomendações, cujo resultado comparativo apresenta-se na Tabela 5-25.

Tabela 5-25 Comparativo, Facilidade de Uso: Aprender a usar o artefato. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	12	16
Concordo parcialmente	8	5
Não concordo nem discordo	1	1
Discordo parcialmente	3	0
Discordo integralmente	0	0
Total	24	22

A avaliação da facilidade de uso do segundo ciclo apresentou resultado melhor que o da primeira rodada. Embora o Tutorial tenha sido ampliado, trazendo um pouco mais de informações técnicas, o resultado sugere, como **quarto ponto** de reflexão, que ainda há espaço para aprimoramento no que tange à facilidade se aprender a usar o método e as recomendações.

O último ponto analisado na categoria Facilidade de Uso, facilidade de utilizar o método e as recomendações para se atingir ao resultado desejado. A comparação é feita na Tabela 5-26.

Tabela 5-26 Comparativo, Facilidade de Uso: Facilidade de usar para se fazer o que quer. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	14	15
Concordo parcialmente	8	5
Não concordo nem discordo	2	2
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

As variações numéricas entre os ciclos mais uma vez não são significativas. A maioria dos tomadores de decisão considerou o método claro e fácil para se atingir ao resultado desejado no segundo ciclo. Mas, dado o resultado, com cinco empreendedores concordando parcialmente e dois não concordando nem discordado da assertiva, como **quinto ponto** de análise, permanece a necessidade de melhoria de usabilidade.

5.2.4 Análise do segundo ciclo – Utilidade

Em relação à Utilidade, o **primeiro ponto** a ser analisado é que houve melhora de avaliação em todas as três assertivas, em menor ou maior grau. A primeira questão tratou de avaliar se o método ajudou na melhoria de desempenho para o cumprimento da LGPD e, no comparativo o segundo ciclo apresentou resultado ligeiramente melhor que o primeiro.

Tabela 5-27 Comparativo, Utilidade: Melhoria de desempenho. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	13	16
Concordo parcialmente	7	3
Não concordo nem discordo	4	3
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

O **segundo ponto** de análise referente à Utilidade é sobre a segunda assertiva, que tratou do aumento da eficácia. O resultado do segundo ciclo foi melhor que o do primeiro, como se observa na Tabela 5-28.

Tabela 5-28 Comparativo, Utilidade: Aumento de eficácia para cumprir com a LGPD. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	15	20
Concordo parcialmente	7	2
Não concordo nem discordo	2	0
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

No segundo ciclo, quase a totalidade dos empreendedores declarou concordar integralmente que o método aumenta a eficácia do cumprimento da LGPD, com somente dois dos 22 declarando concordar parcialmente com a assertiva.

O **terceiro ponto** analisado indicou uma melhoria da percepção da utilidade do método, de acordo com o resultado apresentado a seguir na Tabela 5-29

Tabela 5-29 Comparativo, Utilidade: Útil para cumprir com a LGPD. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	18	21
Concordo parcialmente	5	1
Não concordo nem discordo	1	0
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

A avaliação dos empreendedores, com 21 dos 22 concordando integralmente que o método é útil para cumprir a LGPD e um único afirmando que é parcialmente útil, valida a utilidade do artefato.

O **quarto ponto** de análise trata do resultado dos comentários. Dos 16 deles publicados pelos tomadores de decisão, 14 trouxeram citações positivas que reforçam a validação da utilidade do artefato.

Os dois comentários remanescentes tratam de temas que não minimizam a utilidade do método. Um dos empreendedores (#E29) apenas manifestou a preocupação de que há a necessidade de realizar a implementação das recomendações e o outro refletiu sobre a falta de atuação da ANPD (#E44), o que, na visão dele tornaria o risco efetivo menor na imposição de multas.

O **quinto ponto** a ser mencionado é que embora não tenha ocorrido comentários sobre trazer mais informações para facilitar a implementação, esse é um tópico que deve ser registrado para aprimoramento futuro, dado o potencial de aumento de utilidade para tomadores de decisão.

O **sexto ponto** de análise trata dos motivos apresentados pelos empreendedores nos comentários para justificar a utilidade do método: estar alinhado ao método conduz à maturidade de proteção de dados (#E27); traz clareza sobre questões que não eram conhecidas (#E30); útil para inclusão na lista de ações a serem realizadas a fim de manter a segurança e a conformidade com a LGPD (#E31, #E32, #E35); contribui para relembrar atividades necessárias e reforçar o que já foi implementado (#E39); traz recomendações alinhadas à necessidades (#E40); é útil pela agilidade para se adaptar à LGPD (#E46). Essas justificativas se somam às já apresentadas no tópico 5.1.3, quando da análise do primeiro ciclo, permitindo inferir que o método e as recomendações, além de facilitar a tomada de decisão sobre conformidade com a LGPD, propicia maior consciência sobre questões referentes à proteção de dados.

5.2.5 Análise do segundo ciclo – Uso Futuro

Por fim, em relação à categoria Uso Futuro, o **primeiro ponto** de análise trata do aumento mais significativo ocorrido na comparação entre os ciclos, com 20 empreendedores da segunda rodada afirmando concordar integralmente com a assertiva sobre usar o método futuramente, em contraponto aos 11 da primeira. A Tabela 5-30 compara os resultados dos dois ciclos.

Tabela 5-30 Comparativo, Uso Futuro. Fonte: o Autor.

Avaliação	Primeiro ciclo	Segundo ciclo
Concordo integralmente	11	20
Concordo parcialmente	11	2
Não concordo nem discordo	2	0
Discordo parcialmente	0	0
Discordo integralmente	0	0
Total	24	22

Como se observa, o resultado valida o artefato em relação a uso futuro. Essa afirmação, é reforçada também pelos 15 comentários realizados pelos tomadores de decisão, que, como já apresentada em tópico anterior, indicaram positivamente uso futuro.

O **segundo ponto** a ser analisado, é que alguns dos comentários a respeito do uso futuro tratam da utilidade do método: bom para estabelecer prioridades (#E45); permite implementar aspectos que estejam em desconformidade (#E35); utilidade para aplicação em diversas áreas da empresa (#E31); para o desenvolvimento de novas funcionalidades de software, a fim de evitar vulnerabilidades em relação à LGPD (#E46).

O **terceiro ponto**, por fim, trata da sugestão de ser incluída a opção “cumpro parcialmente”, a fim de possibilitar uma alternativa intermediária, entre as opções “sim” e “não”. Esse ponto será indicado para aprimoramento futuro.

5.3 Síntese das análises de primeiro e segundo ciclo

Em síntese, as análises conjuntas do primeiro e do segundo ciclo de demonstração e avaliação:

- Validam a Facilidade de Uso do método, mas indicam espaço para aprimoramentos. As melhorias a serem consideradas são tanto de ordem de entendimento técnico, quanto de ordem estrutura do artefato. Em relação ao entendimento técnico, são pontos aprimoramento trazer mais informações didáticas sobre o funcionamento da LGPD, apresentar exemplos junto às questões, melhorar a usabilidade, de forma específica, do passo inicial do método, que trata da definição do conjunto de dados. Em relação à estrutura do artefato, é necessário avaliar a inclusão das opções “não se aplica” e “cumpro parcialmente. Essas melhorias podem reduzir o esforço cognitivo na aplicação do método, bem como torná-lo mais fácil de usar e de aprender.
- Validam a Utilidade do método. O artefato é considerado por parte dos empreendedores como rápido, prático e de fácil aplicação, podendo servir como guia de boas práticas e útil para a governança corporativa, facilitando o mapeamento de riscos e trazendo clareza sobre a implementação da LGPD. Há a possibilidade, contudo, de tornar mais robusto no que se refere à utilidade, ao aprofundar as informações que são apresentadas no conjunto de recomendações.
- Validam o Uso Futuro do método. Houve um aumento significativo de percepção de uso futuro no segundo ciclo, em relação ao primeiro, validando o artefato para uso futuro.

- Permitem concluir que o método e as recomendações facilitam a tomada de decisão em relação à conformidade com a LGPD, bem como promove maior consciência e cultura sobre proteção de dados.

5.4 Discussão

Neste tópico discute-se os resultados da pesquisa, levando-se em consideração a revisão de literatura realizada, as normas e documentos técnicos utilizados, as decisões administrativas e judiciais e as normas legais e regulamentares nos âmbitos europeu e brasileiro analisadas, o método proposto, os resultados coletados e suas análises em dois ciclos de demonstração e avaliação.

O método proposto diferencia-se das propostas apresentadas na Seção 2.3.4 por ser o único que leva em conta o contexto das *startups* sob uma perspectiva de avaliação de risco, considerando em sua totalidade os aspectos de conformidade presentes na LGPD que impactam em decisões pertinentes ao campo da engenharia de software. A conformidade com a LGPD, no método proposto, envolve tanto requisitos não funcionais, como segurança, como requisitos funcionais necessários ao cumprimento da legislação. Além disso, não requer amplo conhecimento técnico especializado, podendo ser utilizado de forma rápida por tomadores de decisão de *startups*.

É uma abordagem única, cujo conjunto de características não está presente nos 15 estudos relacionados, como apresentado na Seção 2.3.4. O mais recente desses estudos de Ayala-Rivera *et al.* (2024), apresenta um catálogo de controles com base em normas técnicas, sem, contudo, lidar com questões referentes a risco de conformidade. Tal proposta não é fácil de aplicar sem conhecimento especializado e tampouco foi projetada para uso específico de *startups*. Isso é um obstáculo, pois desenvolvedores de software geralmente não possuem conhecimento suficiente de conformidade de proteção de dados (PEIXOTO *et al.*, 2023), o que pode ser um problema mais severo quando se trata de equipes pequenas em *startups*. Não é adequado para o contexto de *startups*, que, como visto, é caracterizado pela incerteza, pressão de tempo e da necessidade de alta reatividade na procura por um mercado para o produto (MELEGATI *et al.*, 2020). *Startups* tendem a focar seus recursos no desenvolvimento do produto mínimo viável, adaptando métodos ágeis, para uso de seus times pequenos e flexíveis (JAVDANI GANDOMANI *et al.*, 2024)

De forma similar, outras propostas analisadas na Seção 2.3.4, como a de Ayla-Rivera e Pasquale (2018), a de Barbosa, Brito e Almeida (2019) e Tsohou *et al.* (2020), são inadequadas por, entre outras razões, serem complexas e requererem dos praticantes um alto nível de conhecimento em conformidade legal de proteção de dados.

Ainda que o método aqui proposto possa necessitar de melhorias de usabilidade, as evidências coletadas indicam a facilidade de uso, a utilidade e a perspectiva de uso futuro por parte dos tomadores de decisão. O método foi validado para o contexto das *startups*, suprindo lacunas de conhecimento da área de proteção de dados, tanto em sua aplicação, quanto em relação s medidas de mitigação de riscos de desconformidade, ao trazer um conjunto de recomendações para apoiar atividades de adequação à LGPD.

A falta de conhecimento especializado e a escassez de recursos circunstâncias pressionam as *startups* em ter de fazer escolhas difíceis. Tomadores de decisão possuem prioridades concorrentes – requisitos de objetivo do negócio e requisitos legais – que precisam ser ponderados de forma fundamentada (BREAUX e NORTON, 2022). Nesse sentido, a abordagem aqui apresentada é adequada.

O método proposto nesta pesquisa estabelece cenários de risco com base numa análise pormenorizadas dos artigos da LGPD, conforme apresentado na Seção 2.2, de modo a tratar de forma abrangente os mais diversos aspectos que possam ser impactados por decisões de engenharia de software. Além disso, os cenários de risco foram avaliados com base em centenas de decisões administrativas de autoridades de proteção de dados de países da União Europeia, a fim de que se pudesse ter parâmetros razoáveis para a ponderação da severidade dos riscos.

Em que pese a maioria dos estudos sejam do âmbito do GDPR, ainda assim, não foram identificados nos trabalhos relacionados estudos que tenham a mesma abrangência, nem que correlacionem dispositivos regulamentares de forma sistemática a cenários de risco. Nenhum dos estudos relacionados possui tais características. Ataei, Degbelo e Kray (2018), Ayala-Rivera e Pasquale (2018), Salnitri *et al.* (2019), Fähnrich e Kubach (2019), Li *et al.* (2020) e Wuyts, Sion e Joosen (2020), a título de exemplos, tratam apenas de alguns aspectos do GPDR. Outros, como Brodin (2019), Tsohou et al. (2022), Matulevicius et al. (2020) e Shaked e Reich (2021), tampouco tratam de análise de risco.

Outro aspecto relevante é a dificuldade de desenvolvedores diferenciarem conformidade legal de proteção de dados pessoais de segurança (ANDRADE *et al.*, 2023; Del-Real *et al.*, 2024). Essa distinção é importante porque a conformidade legal de proteção de dados trata de questões mais amplas, conforme mencionado em diversos momentos nesse trabalho.

É possível que a dificuldade na diferenciação desses conceitos faça algumas propostas concentrarem sua atenção em aspectos de segurança de informação, como as de Salnitri *et al.* (2019), Fähnrich e Kubach (2019) e Shaked e Reich (2021), o que as tornam de alcance limitado.

Importante mencionar também que esta pesquisa está inserida em um contexto de discussão sobre qualidade de software. *Startups*, mesmo quando em crescimento, possuem dificuldades em adotar práticas de qualidade de software (PIZZINI *et al.*, 2021). Empresas nascentes geralmente, até por conta da necessidade de sobrevivência, estão preocupadas com questões que venham a causar impacto no produto, em clientes e no negócio, mas deixam outros pontos, como a conformidade de proteção de dados em segundo plano.

A conformidade de proteção de dados, ou “Legal Accountability”, como propõem Breaux e Norton (2022), é um aspecto de qualidade. Mas é um aspecto que geralmente acaba sendo relegado para ser resolvido em momento posterior ao lançamento do produto (ANDRADE *et al*., 2023), seja porque a conformidade de proteção de dados concorre com requisitos de objetivo de negócio (BREAUX e NORTON, 2022), seja por falta de conhecimento técnico especializado das equipes de desenvolvimento (ANDRADE *et al*., 2023).

Isso não quer dizer que *startups* não se preocupem com conformidade de proteção de dados. Este estudo apresenta evidências no Capítulo 5 de que os empreendedores consideram importante a conformidade legal de proteção de dados. O problema, como já mencionado, é que *startups*, embora considerem necessária a conformidade para evitar custos de multas e indenizações (NORVAL *et al.*, 2021, MARTIN *et al.*, 2019) e para facilitar a inovação e conquistar a confiança de consumidores (BACHLECHNER; LIESHOUT; TIMAN, 2019), possuem dificuldades em implementar ações de adequação, por falta de conhecimento (PEIXOTO *et al.,* 2023; Norval *et al.*, 2021).

O método proposto supre essa lacuna ao possibilitar uma avaliação de risco fundamentada na literatura, nas normas e documentos técnicos e na análise de

centena de decisões administrativas de autoridades nacionais de proteção de dados da União Europeia, mesmo que empreendedores possuam poucos conhecimentos sobre a LGPD.

5.5 Considerações sobre o capítulo

O capítulo apresentou o perfil das *startups* e dos tomadores de decisão que participaram das sessões de demonstração e avaliação em dois ciclos. O primeiro ciclo contou com a participação de 24 tomadores de decisão de 21 empresas.

A partir da análise dos dados do primeiro ciclo foram realizadas algumas alterações no Tutorial, introduzindo-se mais informações em cinco slides adicionais. Foram realizadas também alterações no texto do método para atender às mudanças feitas no tutorial. Em seguida realizou um segundo ciclo de demonstração e avaliação, em que participaram 22 empreendedores de 17 *startups*. Os resultados das avaliações dos dois ciclos foram apresentados, comparados e sintetizados. Por fim, apresentou a discussão sobre os resultados de pesquisa.

CAPÍTULO 6 - CONCLUSÃO

Este capítulo apresenta as considerações finais sobre a pesquisa, ressaltando a relevância do estudo na Seção 8.1, as limitações e ameaça à validade na Seção 8.2, as contribuições na Seção 8.3 e os trabalhos futuros na Seção 8.4.

6.1 Relevância do estudo

Startups necessitam de práticas específicas que apoiem a conformidade de proteção de dados na engenharia de software, por conta do contexto das empresas nascentes, em especial, relativo entre outros fatores à pressão de tempo e de falta de recursos, mas há dificuldades em encontrar modelos que facilitem a implementação. Não estar em conformidade com a LGPD pode acarretar sanções administrativas da ANPD, como multas, pagamento de indenizações por conta de ações judiciais, e prejuízos reputacionais.

A LGPD, assim como o GDPR, é uma legislação cuja implementação de conformidade deve ser realizada com base no risco de violação de direitos, identificado no contexto de cada organização. Compreender os riscos de conformidade com a legislação é uma tarefa complexa, dado que, como mostrado neste estudo, o cumprimento exige não somente atender a questões de segurança de dados. Mas se refere, também, à necessidade de realizar tratamento em conformidade com princípios da LGPD, bem como de avaliar o risco inerente nas atividades que utilizam os dados. Além disso, é preciso levar em consideração que os sistemas desenvolvidos precisam estar preparados para cumprir com obrigações a respeito dos direitos dos titulares de dados, que podem, a depender das circunstâncias, exigir, a exclusão, a alteração, e o acesso de informações, entre outras requisições.

A fim de preencher essa lacuna, no âmbito do GDPR as propostas existentes ou não levam em conta a totalidade dos aspectos de conformidade, ou não consideram o contexto específico das *startups*, ou não tratam dos riscos, ou não foram validadas na indústria. Assim, é relevante buscar um método que possibilite *startups* avaliarem seus riscos de conformidade com a LGPD e obter um conjunto de

recomendações para que possam estabelecer suas prioridades nas atividades de engenharia que precisam realizar.

A relevância desta pesquisa está em oferecer um método de tomada de decisão que permite empreendedores de *startup* aferirem o risco de conformidade com a LGPD em quatro aspectos – no ciclo de vida dos dados, no desenvolvimento, no tratamento dos dados e no atendimento de direito dos titulares. A partir dos riscos identificados, o método oferece a eles um conjunto de recomendações relativo a atividades de engenharia de software, para que orientem suas ações de conformidade com a legislação. Assim, podem gerenciar suas prioridades e escolher o melhor momento, dentro de sua estratégia de negócio, para implementar aspectos relativos à LGPD.

6.2 Limitações e ameaças à validade

Ameaças à validade de constructo. A validade do construto se refere ao instrumento desenvolvido para avaliação do risco da *startup* em relação à LGPD. A sua construção foi baseada no extenso estudo do referencial teórico, nas leis e nas decisões administrativas e judiciais proferidas até o momento, o que minimiza a ameaça à validade de construto.

Ameaças à validade interna. A fim de mitigar essa ameaça buscaram-se tomadores de decisão de diferentes perfis de *startups* de diversos setores, com experiências, idade e área de formação variadas. Além disso, a ameaça de validade interna foi tratada garantindo que as identidades dos tomadores de decisão fiquem mantidas em sigilo e que todos os materiais utilizados permaneçam anonimizados. Assim, foi propiciado um contexto seguro, em que os tomadores de decisão pudessem se sentir livres para expressar opiniões sem quaisquer receios de inconvenientes futuros, permitindo que suas respostas fossem significativas para aprimorar o artefato avaliado neste estudo.

Ameaças à validade externa. Embora se tenha conseguido um número expressivo de tomadores de decisão - 24 no primeiro ciclo e 22 no segundo – não é possível generalizar os resultados aferidos, mas foi possível inferir que o instrumento desenvolvido pode auxiliar as *startups* a analisar o risco a que estão expostas. A fim de mitigar essa limitação, procurou-se aplicar o método com um grupo diverso de tomadores de decisão, que atuam em variados setores econômicos e que possuem graus variados de experiência.

Ameaças à validade de resposta. Como o pesquisador esteve presente durante as sessões de demonstração, tal fato pode influenciar as respostas dos tomadores de decisão, por conta do comportamento, linguagem utilizada, sugestões tácitas, entre outras possibilidades. Esta limitação foi mitigada por meio de um protocolo padrão de pesquisa em que, em sessões por videochamada, era apresentado apenas o passo a passo a ser seguido, comunicando com o tomador de decisão somente quando solicitado, e sempre mantendo uma postura de neutralidade sobre a avaliação.

Ameaças à validade de conclusão. A quantidade de tomadores de decisão é a principal ameaça. Porém, buscou-se mitigar essa ameaça ao realizar dois ciclos de avaliação. Considerando a natureza qualitativa da avaliação, embora um número maior de tomadores de decisão de *startups* pudesse ampliar a capacidade de generalização dos resultados, as contribuições existentes, em dois momentos diferentes, são valiosas para a qualidade da pesquisa.

Limitações de pesquisa. As principais limitações identificadas nesta pesquisa são:

- Avaliação qualitativa: a avaliação da proposta tem natureza qualitativa, o que pode ter efeito limitador em relação à precisão e exatidão do método proposto. Por essa razão, foram estabelecidas duas etapas de coleta na fase demonstração, a fim de reduzir limitações pelo uso de avaliação qualitativa. Além disso, pode também limitar a validade externa, referente à possibilidade de generalização de resultados. Porém, a segunda etapa contou com novos tomadores de decisão, o que permitiu buscar a generalização analítica e ter uma confiança dos resultados para esse modelo de empresa.
- Avaliação de contexto de risco: como a LGPD é recente, há poucas decisões sejam administrativas, da ANPD, sejam judiciais, que permitam aferir com mais precisão riscos financeiros de conformidade aos quais as *startups* estão expostas, o que traz dificuldade para calibrar a avaliação de risco proposta. Para mitigar essa limitação, realizou-se uma ampla análise de decisões administrativas de autoridades nacionais de proteção de dados europeias, dado que o GDPR tem forte influência na LGPD, e pode, ainda que parcialmente, suprir essa lacuna.

6.3 Contribuições de pesquisa

São contribuições desta pesquisa:

- **Método de tomada de decisão apoiado em um conjunto de recomendações para *startups*, na implementação da conformidade com a LGPD durante o processo de desenvolvimento de software:** A principal contribuição desta tese foi a proposta de um método para apoio de *startups* na avaliação de riscos de conformidade com a LGPD em suas atividades de engenharia de software, que fornece um conjunto de recomendações para os cenários de risco identificados. Preliminarmente, as escolhas feitas para a construção do artefato foram fundamentadas no contexto das *startups* e dos estudos sobre conformidade de proteção de dados na engenharia de software, conforme apresentado na revisão de literatura, nas normas técnicas existentes, e nas decisões administrativas de autoridades nacionais de países da união europeia. Após dois ciclos de validação com *startups*, foram realizadas modificações em prol da usabilidade e gerada versão final proposta.
- **Método proposto contribui para promover a qualidade de software:** Como o *legal accountability* é um aspecto de qualidade de software, o método proposto permite *startups* possam tomar decisões fundamentadas para desenvolver softwares em conformidade com a LGPD, reduzindo riscos de prejuízos financeiros, isso pode promover qualidade relativa à conformidade de proteção de dados, possibilitando às *startups* avançar em direção à sustentabilidade financeira e obter uma maior penetração de mercado. Essa é uma contribuição ao mesmo tempo prática (a ser utilizada pelas *startups*) e científica (contribui para o corpo de conhecimento de Engenharia de Software e, mais especificamente, Qualidade de Software).
- **Revisão sobre o contexto da pesquisa de métodos para implementação de conformidade de proteção de dados e do ambiente de *startups***: A revisão de literatura apresenta-se também como uma contribuição, uma vez que apresentou o contexto específico das *startups* e os desafios de implementação de normas de proteção de dados e pode ser útil para novos trabalhos de pesquisa. A pesquisa identificou lacunas substanciais no que tange a métodos adequados ao contexto das *startups*

para aplicar conformidade de proteção de dados no campo da engenharia de software.

- **Análise de decisões administrativas de autoridades nacionais de proteção de dados da União Europeia:** Uma contribuição significativa para a área foi a análise de 814 resumos de decisões administrativas de autoridades nacionais de proteção de dados de países pertencentes à União Europeia, cadastradas no site *CMS Law GDPR Enforcement Tracker*. Esse corpo de conhecimento permitiu compreender quais os principais artigos da legislação de proteção de dados foram violados na União Europeia, trazendo clareza sobre cenários mais demandados, possibilitando identificar os de maior risco. Isso permitiu aprimorar a aferição de probabilidade, com base em uma atribuição de pesos para os cenários de risco dos aspectos de conformidade avaliados no método proposto. Esta análise pode apoiar trabalhos futuros sobre o tema.
- **Descrição de cenários de risco com base nos dispositivos da LGPD, que possam ser impactados por atividades de engenharia de software:** Foram identificados cenários de risco de conformidade legal a partir do texto da LGPD relacionando-os a possibilidades de intervenção por meio de atividades de engenharia de software, a fim de mitigar riscos jurídicos.

6.4 Trabalhos futuros

Com base na pesquisa realizada são indicados os seguintes trabalhos futuros:

- Aprimorar a usabilidade do artefato, a fim de trazer melhoria de entendimento de questões técnicas. Realizar novo experimento com foco na Facilidade de Uso, com o objetivo de validar integralmente a proposta.
- Atualizar o estudo de análise de decisões administrativas de autoridades nacionais de proteção de dados da União Europeia, a fim de acompanhar a evolução dos cenários de risco na União Europeia e empreender novas investigações sobre o cenário de decisões administrativas e judiciais brasileiras. Isso permitirá avaliar se há necessidade de calibragem dos pesos referentes a cenários de risco, em especial relativos à conformidade de tratamento de dados e aos direitos dos titulares de dados.
- Aprimorar as informações trazidas no conjunto de recomendações. Há espaço para melhorias que podem trazer mais utilidade no uso do artefato.

Realizar novo experimento com foco no conjunto de recomendações, a fim de torná-lo mais robusto.

- Desenvolver um aplicativo web com o método, para torná-lo disponível para *startups*, a fim de contribuir com o ecossistema de inovação.
- Realizar estudo com as startups que participaram da pesquisa para verificar se as recomendações: foram pertinentes para as decisões de implementação; foram colocadas em práticas.
- Testar o método para organizações que não sejam *startups*, a fim de verificar se o uso do artefato pode ser generalizado para outros públicos.

Diante dos desafios que permeiam a interseção entre engenharia de software e conformidade com a LGPD, esta pesquisa propõe um método estruturado que auxilia startups na gestão de riscos e na implementação de medidas eficazes de proteção de dados. Ao integrar a conformidade desde o desenvolvimento, o estudo fortalece a sustentabilidade e competitividade dessas empresas, garantindo que inovação e regulamentação caminhem juntas. Mais que uma solução técnica, este trabalho reforça a importância de uma engenharia de software alinhada a princípios jurídicos, assegurando que a proteção de dados seja um pilar da inovação responsável.

REFERÊNCIAS BIBLIOGRÁFICAS

ABU-NIMEH, S.; MEAD, N. Combining Privacy and Security Risk Assessment in Security Quality Requirements Engineering. In: 2010 AAAI Spring Symposium, 2010, Stanford, California, USA. Intelligent Information Privacy Management. Stanford: AAAI, 2010. p. 1-5.

AHMADIAN, A. S.; STRÜBER, D.; RIEDIGER, V.; JÜRJENS, J. Supporting Privacy Impact Assessment by Model-Based Privacy Analysis. In: ACM Symposium on Applied Computing, Pau, France, 2018. Symposium on Applied Computing. New York: ACM. 2018, p. 1-8.

AKHIGBE, O.; AMYOT, D.; RICHARDS, G. A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requirements Engineering, v. 24, p. 459–481, 2019.

ALHAZMI, A.; ARACHCHILAGE, N. A. G. I'm all ears! Listening to software developers on putting GDPR principles into software development practice. In: Personal and Ubiquitous Computing, p. 1-14, 2021.

ALI-ELDIN, A.; ZUIDERWIJK, A.; JANSSEN, M. A Privacy Risk Assessment Model for Open Data. In: SHISHKOV B. (ed.) Business Modeling and Software Design. BMSD 2017. Lecture Notes in Business Information Processing, v. 309, p. 186-201. Cham: Springer, 2018.

ALJOHANI, M.; BLUSTEIN, J.; HAWKEY, K. Toward Applying Online Privacy Patterns Based on the Design Problem: A Systematic Review. In: MARCUS A., WANG W. (eds). Design, User Experience, and Usability: Theory and Practice. DUXU 2018. Lecture Notes in Computer Science, v. 10918. Cham: Springer, 2018.

ALKUBAISY, D.; COX, K.; MOURATIDIS, H. Towards Detecting and Mitigating Conflicts for Privacy and Security Requirements. In: 13th International Conference on Research Challenges in Information Science (RCIS), Brussels, Belgium, 2019. 2019 13th International Conference on Research Challenges in Information Science (RCIS). New York: IEEE, 2017. p. 1-6.

ALTORBAQ, A.; BLIX, F.; SÖRMAN, S. Data Subject Rights in the Cloud: A grounded study on data protection assurance in the light of GDPR. 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 2017. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), New York: IEEE, 2017. p. 305-310.

ALSHAMMARI, M.; SIMPSON, A. A model-based approach to support privacy compliance. In: Information and Computer Security, v. 26, n. 4, p. 437-453, 2018a.

ALSHAMMARI, M.; SIMPSON, A. Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Analysis. In: GARCIA-ALFARO J., HERRERA-JOANCOMARTÍ J., LIVRAGA G., RIOS R. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2018, CBT 2018. Lecture Notes in Computer Science, v. 11025, p. 209-224. Cham: Springer, 2018b.

ALVA, A.; YOUNG, L. L-SQUARE: Preliminary Extension of the SQUARE Methodology to Address Legal Compliance. In: 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), Karlskrona, Sweden. 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE). Karlskrona: IEEE, 2014. p. 25-30.

ANDRADE, V. C. Processo de Desenvolvimento de Software Baseado nos Princípios de Privacy by Design. 2024. p. 316. Tese de Doutorado - Pontifícia Universidade Católica do Paraná, Curitiba, 2024.

ANDRADE, V. C.; REINEHR, S.; FREITAS, C. O. A., MALUCELLI, A. Personal Data Privacy in Software Development Processes: A Practitioner's Point of View. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Exeter: IEEE, 2023. p. 2727-2734.

ANGERMEIR, F.; FISCHBACH, J.; MOYÓN, F.; MENDEZ, D. Towards Automated Continuous Security Compliance. In Proceedings of 18th ACM/IEEE International Symposium on Empirical Engineering and Measurement (ESEM '24). ACM, New York, NY, USA, 7 p., 2024.

ARTICLE 29 WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 22. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236>. Acesso em 30 ago. 2021.

ATAEI, M.; DEGBELO, A.; KRAY, C. Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. Journal of Location Based Services, v. 12, p. 141-178, 2018.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em:< https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf>. Acesso em: 30 ago. 2021.

AYALA-RIVERA, V.; PASQUALE, L. The grace period has ended: An approach to operationalize GDPR requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE), Banff, AB, Canadá, 2018. 2018 IEEE 26th International Requirements Engineering Conference (RE). Banff: IEEE, 2018. p. 136-146.

AYALA-RIVERA, V.; PORTILLO-DOMINGUEZ, A. O.; PASQUALE, L.. GDPR compliance via software evolution: Weaving security controls in software design. Journal of Systems and Software, p. 112144, 2024.

BACHLECHNER, D.; VAN LIESHOUT, M.; TIMAN, T. Privacy as Enabler of Innovation. In: FRIEDEWALD M., ÖNEN M., LIEVENS E., KRENN S., FRICKER S. (eds). Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, vol 576. Cham: Springer, 2020.

BALDASSARRE, M. T.; BARLETTA, V. S.; CAIVANO, D.; PICCINNO, A. A Visual Tool for Supporting Decision-Making in Privacy Oriented Software Development. In:

International Conference on Advanced Visual Interface (AVI'20), 2020, Salerno, Italy. International Conference on Advanced Visual Interfaces. New York: ACM, 2020a. p. 1-5.

BALDASSARRE, M. T.; BARLETTA, V.S.; CAIVANO, D.; SCALERA, M. Integrating security and privacy in software development. In: Software Quality Journal, v. 28, p. 987–1018 2020b.

BARBOSA, P.; BRITO, A.; ALMEIDA, H. Privacy by Evidence: A Methodology to develop privacy-friendly software applications. In: Information Sciences, v. 527, p. 294-310, 2020.

BERG, V.; BIRKELAND, J.; NGUYEN-DUC, A.; PAPPAS, I.; JACCHERI, L. Software Startup Engineering: A Systematic Mapping Study. In: Journal of Systems and Software, v. 144, October, p. 255-274, 2018.

BESKER, T.; MARTINI, A.; LOKUGE, R. E.; BLINCOE, K., BOSCH, J. Embracing technical debt, from a startup company perspective. In: International Conference on Software Maintenance and Evolution (ICSME), 2018, Madri, Spain. 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME). Madrid: IEEE, 2018. p. 415–425.

BREAUX, T D.; NORTON, T. Legal accountability as software quality: A us data processing perspective. In: 2022 IEEE 30th International Requirements Engineering Conference (RE). Melbourne: IEEE, 2022. p. 101-113.

BIONI, B. R. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2020. p. 298.

BIONI, B. R.; MENDES, L. S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In.: Tepedino, G.; Frazão, A.; Oliva, M. D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 799-820.

BLANK, S. Embrace failure to start up success. Nature, 477, n. 7363, 2011., p. 133.

BLANK, Steve; DORF, Bob. Startup: Manual do Empreendedor. Rio de Janeiro: Atlas Books Editora, 2014. p. 572.

BLEIER, A.; GOLDFARB, A.; TUCKER, C. Consumer privacy and the future of data-based innovation and marketing. In: International Journal of Research in Marketing, v.37, n.3, p. 466-480, 2020.

BRASIL. Lei Geral de Proteção de Dados. 2018. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 19 mar. 2021.

BRODIN, M. A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. In: European Journal for Security Research, v. 4, p. 243-264, 2019.

CAVALCANTE, B. H.; LEAL, L. C. G.; BALANCIERI, R.; FARIAS JUNIOR, I. Technical Aspects of Software Development in Startups: A Systematic Mapping. In.: XLIV Latin American Computer Conference (CLEI), São Paulo, Brazil. 2018 XLIV Latin American Computer Conference (CLEI). New York: IEEE, 2018. p. 100-109.

CAVOUKIAN, A.; SHAPIRO, S.; CRONK, R. J. Privacy engineering: Proactively embedding privacy, by design. Office of the Information and Privacy Commissioner, 2014.

CARMEL, E. Time-to-completion in software package startups. In: 27th Hawaii International Conference on System Sciences (HICSS). IEEE, p. 498–507, 1994. [Online]. http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=323468

COLEMAN, G.; O´CONNOR, R. V. An investigation into software development process formation in software start-ups. In: Journal of Enterprise Information Management, v. 21, n. 6, p. 633-648, 2008.

COLESKY, M.; CAIZA, J. C. A system of privacy patterns for informing users: Creating a pattern system. In: EuroPLoP '18: 23rd European Conference on Pattern Languages of Programs, n. 16, 2018, New York, NY, USA. EuroPLoP '18: 23rd European Conference on Pattern Languages of Programs New York: ACM, p. 1-11, 2018.

CORTINA, S.; VALOGGIA, P.; BARAFORT, B.; RENAULT, A. L. Designing a Data Protection Process Assessment Model Based on the GDPR. In.: In: WALKER, A.; O'CONNOR, R.; MESSNARZ, R. (eds.) Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science, v. 1060, p. 136-148. Cham: Springer, 2019.

CROWNE, M. Why software product startups fail and what to do about it. Evolution of software product development in startup companies. In: IEEE International Engineering Management Conference, v.1, 2002, Cambridge, UK. International Engineering Management Conference. New York: IEEE, 2002. p. 338-343.

DE, S. J.; MÉTAYER, D. L. PRIAM: A Privacy Risk Analysis Methodology. In: LIVRAGA G., TORRA V., ALDINI A., MARTINELLI F., SURI N. (eds.) Data Privacy Management and Security Assurance. DPM 2016, QASA 2016. Lecture Notes in Computer Science, v. 9963. Cham: Springer, 2016.

DEL-REAL, C.; DE BUSSER, El.; VAN DEN BERG, B. Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review. Computer Law & Security Review, v. 52, p. 105933, 2024.

DENG, M.; WUYTS, K.; SCANDARIATO, R.; PRENEL, B.; JOOSEN, W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. In: Requirements Engineering, v. 6, p. 3-32, 2011.

DIAMANTOPOULOU, V.; TSOHOU, A.; KARYDA, M. General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance. In: GRITZALIS S., WEIPPL E., KATSIKAS S., ANDERST-KOTSIS G., TJOA A., KHALIL I. (eds.). Trust, Privacy and Security in Digital Business. TrustBus. Lecture Notes in Computer Science, v. 11711. Cham: Springer, 2019.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In.: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, D.; SARLET, I. W.; RODRIGUES JR., O. L. (coord.). Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021. p. 22-39.

EASTON, C. Analysing the Role of Privacy Impact Assessments in Technological Development for Crisis Management. In: Journal of Contingencies and Crisis Management, v. 25, n. 1, p. 1-12, 2016.

EUROPEAN UNION AGENCY FOR CYBERSECURITY, Galan Manso, C., Górniak, S., Recommendations for a methodology of the assessment of severity of personal data breaches:, European Network and Information Security Agency, 2013, https://data.europa.eu/doi/10.2824/27590.

ESAYAS, S. Y. Structuring Compliance Risk Identification Using the CORAS Approach: Compliance as an Asset. In: IEEE International Symposium on Software Reliability Engineering Workshops, Naples, Italy, 2014, p. 281-286.

FÄHNRICH, N.; KUBACH, M. Enabling SMEs to comply with the complex new EU data protection regulation. In: ROßNAGEL, H., WAGNER, S. & HÜHNLEIN, D. (eds.), Open Identity Summit, p. 177-183, 2019.

FELTUS, C.; GRANDRY, E.; KUPPER, T.; COLIN, J. Model-driven approach for privacy management in business ecosystem. In: 5th MODELSWARD 2017: International Conference on Model-Driven Engineering and Software Development, [Online]. 5th MODELSWARD 2017: International Conference on Model-Driven Engineering and Software Development. Setubal: SCITEPRESS, 2017. p. 392-400.

FERREIRA, A. GDPR: What's in a year (and a half)? In: 22nd International Conference on Enterprise Information Systems, ICEIS, 2020. 22nd International Conference on Enterprise Information Systems – Volume 2. Setubal: SCITEPRESS, 2020. p. 209-216.

FUGGETTA, A. Software process: a roadmap, In: Proceedings of the Conference on The Future of Software Engineering (ICSE), ACM, p. 25–34, 2000.

GELLERT, R. Understanding the notion of risk in the General Data Protection Regulation. In: Computer Law & Security Review, v. 34 (2), p. 279–288, 2018.

GHARIB, M; GIORGINI, P.; MYLOPOULOS, J. An Ontology for Privacy Requirements via a Systematic Literature Review. In: Journal on Data Semantics, v. 9, p. 123-149, 2020.

GIARDINO, C.; UNTERKALMSTEINER, M.; PATERNOSTER, N.; GORSCHEK, T.; ABRAHAMSSON, P. What Do We Know about Software Development in Startups? In: IEEE Software, v. 31, n. 5, Set-Out p. 28-32, 2014.

GIARDINO, C.; WANG, X.; ABRAHAMSSON, P. Why early-stage software startups fail: A behavioral framework. In: LASSENIUS, C.; SMOLANDER, K. (Eds) Software Business. Towards Continuous Value Delivery, p. 27–41, 2014.

GIARDINO, C.; BAJWA, S.S.; WANG, X.; ABRAHAMSSON, P. Key Challenges in Early-Stage Software Startup. In.: Proceeding 16th International XP Conference (XP),

2015, Helsinki, Finland. Agile Processes in Software Engineering and Extreme Programming. Cham: Springer, 2015. p 52–63.

GLINZ, M.; WIERINGA, R. J. Guest Editors' Introduction: Stakeholders in Requirements Engineering. In: IEEE Software, v. 24, n. 2, p. 18-20, mar.-abr., 2007.

GOPAGONI, N. K.; SABELLA, S. R. R. Misalignment of Stakeholders in Software start-ups: A qualitative research based on Software start-ups in India. Dissertação (Software Engineering) – PAAPT Master of Science Programme in Software Engineering, Faculty of Comuting, Blekinge Institute of Technology. Karlskrona, Sweden, p. 80, 2020.

GRAEF, I.; HUSOVEC, M.; PURTOVA, N. Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. In: German Law Journal, v. 19, n. 6, 1359-1398, 2018.

GRUNDSTROM, C.; VÄYRYNEN, K.; IIVARI, N.; ISOMURSU, M. Making sense of the general data protection regulation — four categories of personal data access challenges. In: 52nd Hawaii International Conference on System Sciences, 2019, Hawaii, USA. Privacy and Economics. Hawaii: HICSS, 2019. p. 5039-5048.

GUMUSEL, E.; XIAO, Y.; QIN, Y.; LIAO, X. Understanding Legal Professionals' Practices and Expectations in Data Breach Incident Reporting. In: ACM Annual Conference on Computer and Communications Security. New York: ACM, 2024. 15 p.

HÄUSELMANN, A.; CUSTERS, B.. Substantive fairness in the GDPR: Fairness Elements for Article 5.1 a GDPR. Computer Law & Security Review, v. 52, p. 105942, 2024.

HERT, P. de.; PAPAKONSTATINOU, V.; MALGIERI, G.; BESLAY, L.; SANCHEZ, I. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. In: Computer Law & Security Review, v. 34, n. 2, p. 193-203, 2018.

HILMOLA, O. P.; HELO, P.; OJALA, L. The value of product development lead time in software startup. In: System Dynamics Review, v. 19, n. 1, p. 75-82, 2003.

HUTH, D.; MATTHES, F. Appropriate technical and organizational measures: Identifying privacy engineering approaches to meet GDPR requirements. In: Privacy Engineering Approaches for GDPR Requirements, p. 1-10, 2019.

ISO/IEC 27001. Information technology - Security techniques – Information security management systems - Requirements. International Organization for Standardization, 2022.

ISO/IEC 27002. Information technology - Security techniques – Code of practice for information security controls. International Organization for Standardization, 2022.

ISO/IEC 27005. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization, 2022.

ISO/IEC 27701. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. International Organization for Standardization, 2019.

JAMES, D. Data Protection Does it Apply to Start-Ups? In: ITNOW,v. 57, n. 4, p. 30-31, 2015.

JAVDANI GANDOMANI, T.; ZULZALIL, H.; BAHSOON, R.. Empowering software startups with agile methods and practices: A design science research. Software: Practice and Experience. Journal of Software: Practice and Experience, 2024.

JIMENE, C. do V. Capítulo VII: Da Segurança e das Boas Práticas. In: MALDONADO, V. N.; BLUM, R. O. (coord.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2020. p. 333-360.

JOHANSEN, J.; FISCHER-HÜBNER, S. Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. In: IFIP Advances in Information and Communication Technology, v. 576, p. 1-41. Cham: Springer 2020.

KLOTINS, E.; UNTERKALMSTEINER, M.; GORSCHEK, T. Software engineering practices in start-up companies: A mapping study. In: 6th International Conference on Software Business. Springer, p. 245–257, 2015.

KLOTINS, E. Using the case survey method to explore engineering practices in software start-ups. In.: 1st International Workshop on Software Engineering for Startups, 2017, Buenos Aires, Argentina. 2017 IEEE/ACM 1st International Workshop on Software Engineering for Startups (SoftStart). New York: IEEE, 2017. p. 24–26.

KLOTINS, E.; UNTERKALMSTEINER, M.; GORSCHEK, T. Software-intensive product engineering in start-ups: a taxonomy. In: IEEE Software, v. 35, n. 4, July/August, p. 44-52, 2018.

KLOTINS, E. Software start-ups through an empirical lens: Are start-ups snowflakes? In: Proceedings of the International Workshop on Software-Intensive Business: Start-Ups, Ecosystems and Platforms, p. 1-14, 2018.

KOOLEN, C.; WUYTS, K.; JOOSEN, W.; VALCKE, P. From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. Computer Law & Security Review, v. 52, p. 105914, 2024.

KNEUPER, R. Integrating Data Protection into the Software Life Cycle. In: FRANCH, X.; MÄNNISTÖ, T.; MARTÍNEZ-FERNÁNDEZ, S. (eds.) Product-Focused Software Process Improvement. PROFES 2019. Lecture Notes in Computer Science, v. 11915, p. 47-432. Cham: Springer, 2019.

KNEUPER, R. Translating data protection into software requirements. In: 6th International Conference on Information Systems Security and Privacy, pages 257–264, 2020.

KURTZ, C. F.; SNOWDEN, D. J. The new dynamics of strategy: Sensemaking in a complex and complicated world. In.: IBM Systems Journal, v. 42, n. 3, p. 462 –483, p. 2003.

LENHARD, J.; FRITSCH, L.; HEROLD, S. A. Literature Study on Privacy Patterns Research. In: 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA), 2018, Viena, Austria. 2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA). New York: IEEE, 2018. p. 194-201.

LGPD Brasil. 84% das Empresas brasileiras não estão preparadas para a LGPD. Disponível em: <https://www.lgpdbrasil.com.br/84-das-empresas-brasileiras-nao-estao-preparadas-para-a-lgpd/>. Acesso em: 18 mar. 2022.

LI, Z.; WERNER, C.; ERNST, N.; DAMIAN, D. GDPR Compliance in the Context of Continuous Integration. In: IEE Transactions on software engineering, p. 1-14, 2020.

LIU, J. Y.; CHEN, H.; CHEN, C.; SHEU, T. S. Relationships among interpersonal conflict, requirements uncertainty, and software project performance. In: International Journal of Project Management, v. 29, n. 5, p. 547-556, 2011.

LOPES, I. M.; OLIVEIRA, P. Evaluation of the implementation of the general data protection regulation in health clinics. In: Joural of Information Systems Engineering & Management, v. 3, n. 4, p. 1-28, 2018.

MACHIRIDZA, M. Misalignment challenges when integrating security requirements into mobile banking application development. In: CONF-IRM 2016 International Conference on Information Resources Management, 2016, Atlanta, Georgia, USA. International Conference on Information Resources Management: v. 33. Atlanta: AIS, 2016. p. 1-12.

MATULEVIČIUS, R.; TOM, J.; KALA, K.; SING, E. A Method for Managing GDPR Compliance in Business Processes. In: HERBAUT N., LA ROSA M. (eds). Advanced Information Systems Engineering. CAiSE 2020. Lecture Notes in Business Information Processing, v. 386, p. 100-112. Cham: Springer, 2020.

RIES, Eric. A Startup Enxuta. 1ª ed. São Paulo: Leya, 2012, p. 268.

MARANGUNIĆ, N.; GRANIĆ, A. Technology acceptance model: a literature review from 1986 to 2013. In: Universal Access in the Information Society, v. 14, n. 1, p. 81–95, 2015.

MARTIN, N.; MATT, C.; NIEBEL, C.; BLIND, K. How Data Protection Regulation Affects Startup Innovation. Information Systems Frontiers, 21, 2019, 1307-1324.

MASSEY, A.; OTTO, P. N.; HAYWARD, L. J.; ANTÓN, A. I. Evaluating existing security and privacy requirements for legal compliance, In: Requirement Engineering, v. 15, p. 119-137, 2010.

MEIS, R.; HEISEL, M. Systematic Identification of Information Flows from Requirements to Support Privacy Impact Assessments. In: 10th International Joint Conference on Software Technologies (ICSOFT), Colmar, France, 2015, p. 1-10.

MELEGATI, J.; CHANIN, R.; SALES, A.; PRIKLADNICKI, R. Towards Specific Software Engineering Practices for Early-Stage Startups. In.: PAASIVAARA, M.; KRUCHTEN, P. (Eds.) Agile Processes in Software Engineering and Extreme Programming - Workshops, LNBIP 396, 18-22, 2020.

MORALES-TRUJILLO, M. E.; GARCÍA-MIRELES, G. A.; MATLA-CRUZ, E. O.; PIATTINI, M. A Systematic Mapping Study of Privacy by Design in Software Engineering. Avances en Ingenieria de Software a Nivel Iberoamericano, v. 22, n. 1, p. 1-29, 2019.

NGUYEN-DUC, A.; KEMELL, K., ABRAHAMSSON, P. The entrepreneurial logic of startup software development: A study of 40 software startups. Disponível em: https://arxiv.org/abs/2103.07999. Acesso em 27 ago 2021.

NORVAL, C.; JANSSEN, H.; COBBE, J.; SINGH, J. Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny. In: Policy & Internet, 13, p. 278-299, 2021. Disponível em: <https://ssrn.com/abstract=3398204>. Acesso em: 25 ago 2021.

OETZEL, M. C.; SPIEKERMANN, S. Privacy-by-design through systematic privacy impact assessment: a design science approach. In.: European Conference on Information Systems, 2012, Atlanta, Georgia, USA. European Conference on Information Systems 2012. Atlanta: AIS, 2012. p. 1-13.

OLCA, E.; CAN, O. DICON: A Domain-independent consent management for personal data protection. IEEE Access, v. 10, p. 95479-95497, 2022.

PALHARES, F. O Dilema da Classificação de Controladores e Operadores. In: Palhares, F. (coord.). Estudos obre privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021, p. 11-37.

PALHARES, F. Cookies: contornos atuais. In.: Palhares, F. (coord.). Temas Atuais de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020, p. 9-60.

PALHARES, F; PRADO; L. F.; VIDIGAL, P. Compliance Digital e LGPD. São Paulo: Thomson Reuters Brasil, 2021, p. 399.

PATERNOSTER, N.; GIARDINO, C.; UNTERKALMSTEINER M. U.; GORSCHEK, T.; ABRAHAMSSON, P. Software development in startup companies: A systematic mapping study. In: Information and Software Technology, v. 56, n. 10, 2014, pp. 1200-1218, 2014.

PEFFERS, K.; TUUNANEN, T. TOTHENBERGER, M. A.; CHATTERJEE, S. A design science research methodology for information systems research. In: Journal of Management Information Systems, v. 24, n. 3, p. 45–77, 2007.

PEIXOTO, M. Privacy requirements engineering in agile software development: A specification method. In: M. SABETZADEH, A. VOGELSANG, S. ABUALHAIJA, M. BORG, F. DALPIAZ, M. DANEVA, N. FERN´ANDEZ, X. FRANCH, D. FUCCI, V. GERVASI, E. GROEN, R. GUIZZARDI, A. HERRMANN, J. HORKOFF, L. MICH, A. PERINI, A. SUSI (eds.). In: REFSQ-2020 Workshops, 2020, Pisa, Italy. Doctoral Symposium, Live Studies Track, and Poster Track. AAchen: CEUR, 2020. p. 1-7.

PEIXOTO, M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C.; VILELA, J.; ARAÚJO, J.; GORSCHEK, T. On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview. In: MADHAVJI, N.; PASQUALE, L.; FERRARI, A.; GNESI, S. (eds.) Requirements Engineering: Foundation for Software Quality. REFSQ 2020. Lecture Notes in Computer Science, v. 12045. Cham: Springer, 2020.

PEIXOTO, M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C; VILELA, J.; ARAÚJO, J; GORSCHEK, T. The perspective of Brazilian software developers on data privacy. Journal of Systems and Software, v. 195, p. 111523, 2023.

PIRAS, L.; GHAZI, M; PRAITANO, A.; TSOHOU, A.; MOURATIDIS, H.; CRESPO, B. G.; BERNARD, J. B.; FIORANI, M.; MAGKOS, E.; SANZ, A. C.; PAVLIDIS, M.; D´ADDARIO, R.; ZORZINO, G. G. DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. In: GRITZALIS S., WEIPPL E., KATSIKAS S., ANDERST-KOTSIS G., TJOA A., KHALIL I. (eds.) Trust, Privacy and Security in Digital Business, p. 78-93. Cham: Springer, 2019.

PIZZINI, A; VIEIRA, R. B.; GOMES, R. D., SANTOS, G; MALUCELLI, A.; REINEHR, S. Software Quality Practices in Growing Startups: A Qualitative Study. In.: XX Brazilian Symposium on Software Quality (SBQS ’21), 2021, online, Brazil. New York: ACM, 2021. p.1-10.

RINDELL, K.; HOLVITIE, J. Security Risk Assessment and Management as Technical Debt. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), p. 1-8, 2019.

RINGMANN, S.D.; LANGWEG, H.; WALDVOGEL, M. Requirements for Legally Compliant Software Based on the GDPR. In: PANETTO, H.; DEBRUYNE C.; PROPER, H.; ARDAGNA, C.; ROMAN; D.; MEERSMAN R. (eds) On the Move to Meaningful Internet Systems. Conferences. Lecture Notes in Computer Science, Cham: Springer, 2018. p. 258-276.

SAAD, A.; HIUNES, A. Ela, a LGPD, vista pelas empresas: uma proposta de visão prática – e otimista. In: CUEVA, R. V. B.; DONEDA, D.; MENDES, L. S.(coord.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018): A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 17-28.

SALDAÑA, J. The Coding Manual for Qualitative Researchers. Los Angeles: SAGE Publications, 2013, p. 329.

SALNITRI, M.; ANGELOPOULOS, K.; PAVLIDIS, M.; DIAMANTOPOULOU, V.; MORATIDIS, H.; GIORGINI, P. Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach. In: Software and Systems Modeling, v. 19, p. 467-491, 2020.

SARAIVA, J.; SOARES, S. Privacy and Security Documents for Agile Software Engineering: An Experiment of LGPD Inventory Adoption. In: 2023 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). IEEE, 2023. p. 1-9.

SATO, L; BRAGUIM, G. A Hora e a vez de aprovar o orçamento para adequação à lei geral de proteção de dados. Migalhas. Disponível em: <https://www.migalhas.com.br/depeso/313566/a-hora-e-a-vez-de-aprovar-o-orcamento-para-a-adequacao-a-lei-geral-de-protecao-de-dados>. Acesso em: 18 mar. 2022.

SHAKED, A.; REICH, YORAM. Model-based threat and risk assessment for systems design. In: 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), 2021, Vienna, Austria. 7th International Conference on Information Systems Security and Privacy. Setubal: SCITEPRESS, 2021. p. 331-338.

SILVA, M. P. da; BARROS, R. M. Maturity Model of Information Security for Software Developers. In: IEEE Latin America Transactions, v. 15, n. 10, p. 1994-1999, 2017.

SION, L.; VAN LANDUYT, D.; WUYTS, K.; JOOSEN, W. Privacy Risk Assessment for Data Subject-aware Threat Modeling. In: 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2019. 2019 IEEE Security and Privacy Workshops (SPW). New York: IEEE, 2019. p. 64-71.

SOUZA, C. F.; MAGRANI, E.; CARNEIRO, G. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. In: MULHOLLAND, C. (coord.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago Editorial Ltda, 2020, p. 45-69.

STANCIU, V.; RÎNDAȘU, S. The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania. In: Journal of Information Assurance & Cyber security, p. 1-9, 2018.

SUOMINEN, A.; HYRYNSALMI, S.; AARIKKA-STENROOS, L.; SEPPÄNEN, M. Are Software Start-Ups Different? An empirical study on performance of Finnish software companies. In: 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2017, Madeira, Portugal. 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC). New York: IEEE, 2017. p. 991-996.

SUTTON, S. M. The role of process in software start-up. In: IEEE Software, v. 17, n. 4, p. 33-39, 2000.

TIKKINEN-PIRI, C.; ROHUNEN, A.; MARKKULA, J. EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. Computer Law & Security Review, 34(1), p. 134–153, 2017.

TRIPATHI, N.; E. ANNANPERA; OIVO, M.; LIUKKUNEN, K. Exploring Processes in Small Software Companies: A Systematic Review. In: Communications in Computer and Information Science, vol. 609, pp. 150–165, 2016.

TRIPATHI, N.; KLOTINS, E; PRIKLADNICKI, R; OIVO, M.; POMPERMAIER, L. B.; KUDAKACHERIL, A. S.; UNTERKALMSTEINER, M.; LIUKKUNEN, K.; GORSCHEK, T. An anatomy of requirements engineering in software startups using multi-vocal literature and case survey. In: Journal of Systems and Software, v. 146, p. 130-151, 2018.

TSIODRA, M.; PANDA, S; CHRONOPOULOS, M.; PANAOUSIS, E. Cyber risk assessment and optimization: A small business case study. IEEE Access, v. 11, p. 44467-44481, 2023.

TSOHOU, A.; MAGKOS, E.; MOURATIDIS, H.; CHRYSOLARAS, G.; PIRAS, L.; PAVLIDIS, M.; DEBUSSCHE, J.; ROTOLONI, M.; CRESPO, B. G. Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. In: Information and Computer Security, v. 28, 2020.

UNIÃO EUROPEIA. Regulamento Geral sobre Proteção a Dados. 2016. Disponível em: < https://gdprinfo.eu/pt-pt >. Acesso em: 25 ago. 2021.

UNITED KINGDOM INFORMATION COMMISSIONER´S OFFICE. Conducting privacy impact assessments code of practice. Disponível em:<http:// https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf>. Acesso em 31 ago. 2021.

UNTERKALMSTEINER, M.; ABRAHAMSSON, P.; WANG, X.; NGUYEN-DUC, A.; SHAH, S.; BAJWA, S. S.; BALTES, G. H.; CONBOY, K.; CULLINA, E.; DENNEHY, D., EDISON, H.; FERNANDEZ-SANCHEZ, C.; GARBAJOSA, J.; GORSCHEK, T.; KLOTINS, E.; HOKKANEN, L.; KON, F.; LUNESU, I.; MARCHESI, M.; MORGAN, L.; OIVO, M.; SELIG, C.; SEPPÄNEN, P.; SWEETMAN, R.; TYRVÄINEN, P.; UNGERER, C.; YAGÜE, A. Software Startups – A Research Agenda. In: e-Informatica Software Engineering Journal 10 (1), 89–124, 2016.

URQUHART, L.; SAILAJA, N.; MCAULEY, D. Realising the right to data portability for the domestic Internet of things. Personal and Ubiquitious Computing, v. 22, p. 317–332, 2018.

VAINZOF, Roni. Capítulo I: Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2020. p. 19-177.

VANBERG, A. D.; ÜNVER, B. M. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo. In: European Journal of Law and Technology, v. 8, n. 1, p. 1-22, 2017.

VAN LE, H.; SUH, M.; Changing trends in internet startup value propositions, from the perspective of the customer. In: Technological Forecasting and Social Change, v. 146, p. 853-864, 2019.

VEMOU, K.; KARYDA, M. Evaluating privacy impact assessment methods: guidelines and best practice. Infarmation and Computer Security, v. 28, n. 1, 2019, p. 35-53.

VENKATESH, V.; BALA, H. Technology acceptance model 3 and a research agenda on interventions. In: Decision Sciences, v. 39, n. 2, p. 273–315, 2008.

VIDIGAL, P. Alternativas ao consentimento como base legal para o tratamento e dados pessoais de crianças e adolescentes. In: Palhares, F. (coord.). Estudos obre privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021, p. 247-269.

VIVIANI, L.; GUERRA, E.; MELEGATI, J.; WANG, X. An empirical study about the instability and uncertainty of non-functional requirements. In: International Conference on Agile Software Development. Cham: Springer Nature Switzerland, 2023. p. 77-93.

VOSS, C.; TSIKRIKTSIS, N.; FROHLICH, M. Case research in operations management. In: International Journal of Operations & Production Management, v.22, n.2, 2002, p.195-219.

WAGNER, I.; BOITEN, EERKE. Privacy Risk Assessment: From Art to Science, by Metrics. In: . In: GARCIA-ALFARO, J.; HERRERA-JOANCOMARTÍ, J.; LIVRAGA G.; RIOS, R. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2018, CBT 2018. Lecture Notes in Computer Science, v. 11025, p. 225-241. Cham: Springer, 2018.

WANG, Xiaofeng; EDISON, Henry; BAJWA, Sohaib S.; GIARDINO, Carmine; ABRAHAMSSON, Pekka. Key challenges in software startups across life cycle stages. In: International Conference on Agile Software Development, p. 169–182. Cham: Springer, 2016.

WANG, X.. Why the rise of software startup research: an insider's view. In: HYRYNSALMI, S; SUORANTA, M; NGUYEN-DUC, A; TYRVÄINEN, P; ABRAHAMSSON, P. (eds) ICSOB 2019: Software Business. Lecture Notes in Business Information Processing, v. 370, p. 11–18. Cham: Springer,2019.

WUYTS, K.; SION, L.; JOOSEN, W. LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020, Genoa, Italy. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). New York: IEEE, 2020. p. 302-309.

YRJÖNKOSKI, K.; SUOMINEN, A. Effectuation as a frame for networking decisions – the case of a Finnish information technology start-up. In: International Workshop on Software-intensive Business: Start-ups, Ecosystems and Platforms. Espoo, Finland. p. 230-243, 2018.

APÊNDICE A – ARTEFATO DE PESQUISA

A.1. Artefato do 1º Ciclo com *Startups*

Start of Block: Bloco de perguntas padrão

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado(a) como voluntário(a) a participar do estudo Conformidade Legal em Proteção de Dados no Desenvolvimento de Software de Startups: uma Abordagem Orientada à Tomada de Decisão, que tem como objetivo analisar a utilidade e a aplicabilidade do método de tomada de decisão e do conjunto de recomendações para a conformidade com a Lei Geral de Proteção de Dados (LGPD). Acreditamos que os resultados desta pesquisa possam contribuir para as práticas de conformidade com a LGPD para startups de tecnologia.

PARTICIPAÇÃO NO ESTUDO

A sua participação no referido estudo será participar em entrevista conduzida pelos pesquisadores e fornecer materiais, caso existam, que sejam relevantes no contexto da pesquisa e que tenham sido produzidos ao longo do uso do método de tomada de decisão e do conjunto de recomendações para a conformidade com a Lei Geral de Proteção de Dados (LGPD).

RISCOS E BENEFÍCIOS

Por meio deste Termo de Consentimento Livre e Esclarecido você está sendo alertado de que, da pesquisa a se realizar, não haverá a obtenção de benefícios diretos para o participante. No entanto, pode-se esperar benefícios relacionados ao conhecimento, tais como: conhecer um modelo de tomada de decisão aplicado à startups no que diz respeito à conformidade legal com a LGPD. Bem como, também que é possível que aconteçam os seguintes desconfortos ou riscos em sua participação, tais como sentir-se desconfortável com alguma questão que lhe seja feita. Para minimizar tais riscos, nós pesquisadores tomaremos as seguintes medidas: nenhuma informação será divulgada de forma individualizada ou atribuindo sua identidade ou da empresa à qual esteja vinculado. Você poderá pedir para se retirar do estudo a qualquer momento.

SIGILO E PRIVACIDADE

Nós pesquisadores garantiremos a você que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, lhe identificar, será mantido em sigilo. Nós pesquisadores nos responsabilizaremos pela guarda e confidencialidade dos dados, bem como a não exposição dos dados de pesquisa.

AUTONOMIA

Nós lhe asseguramos assistência durante toda pesquisa, bem como garantiremos seu livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo e suas consequências, enfim, tudo o que você queira saber antes, durante e depois de sua participação. Também informamos que você pode se recusar a participar do estudo, ou retirar seu consentimento a qualquer momento, sem precisar justificar, e de, por desejar sair da pesquisa, não sofrerá qualquer prejuízo à assistência que vem recebendo.

RESSARCIMENTO E INDENIZAÇÃO

No entanto, caso tenha qualquer despesa decorrente da participação nesta pesquisa, tais como transporte, alimentação entre outros, bem como de seu acompanhante, haverá ressarcimento dos valores gastos na forma seguinte: depósito em conta corrente. De igual maneira, caso ocorra algum dano decorrente de sua participação no estudo, você será devidamente indenizado, conforme determina a lei.

CONTATO

Os pesquisadores envolvidos com o referido projeto são Sheila Reinehr, Andreia Malucelli e Rhodrigo Deda Gomes, todos da Pontifícia Universidade Católica do Paraná (PUCPR) e com eles você poderá manter contato pelos telefones (041) 99997-4083, (41) 99994-2492 e (41) 99166-5611.

O Comitê de Ética em Pesquisa em Seres Humanos (CEP) é composto por um grupo de pessoas que estão trabalhando para garantir que seus direitos como participante de pesquisa sejam respeitados. Ele tem a obrigação de avaliar se a pesquisa foi planejada e se está sendo executada de forma ética. Se você achar que a pesquisa não está sendo realizada da forma como você imaginou ou que está sendo prejudicado de alguma forma, você pode entrar em contato com o Comitê de Ética em Pesquisa da PUCPR (CEP) pelo telefone (41) 3271-2103 entre segunda e sexta-feira das 08h00 às 17h30 ou pelo e-mail nep@pucpr.br.

DECLARAÇÃO

Declaro que li e entendi todas as informações presentes neste Termo de Consentimento Livre e Esclarecido e tive a oportunidade de discutir as informações deste termo. Todas as minhas perguntas foram respondidas e eu estou satisfeito com as respostas. Entendo que receberei uma via assinada e datada deste documento e que outra via assinada e datada será arquivada nos pelo pesquisador responsável do estudo.

Enfim, tendo sido orientado quanto ao teor de todo o aqui mencionado e compreendido a natureza e o objetivo do já referido estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

1.1 Você concorda em participar?

- ○ Sim
- ○ Não

Skip To: End of Survey If Você concorda em participar? = Não

End of Block: Bloco de perguntas padrão

Start of Block: Bloco 1

Conformidade Legal em Proteção de Dados no Desenvolvimento de Software de Startups: uma Abordagem Orientada à Tomada de Decisão

Olá, você está participando de uma pesquisa de doutorado cujo tema é "Método de tomada de decisão de conformidade com a LGPD para engenharia software em startups".

A pesquisa apresenta um método que apoia tomadores de decisão de startups em relação a aspectos de conformidade com a Lei Geral de Proteção de Dados (LGPD) no que se refere às atividades de engenharia de software.

Ao aplicar o método, você irá avaliar a exposição de sua startup a riscos relativos à LGPD e lhe será proposto um conjunto de recomendações para mitigá-los. Isso irá lhe ajudar na tomada de decisão sobre suas escolhas de engenharia. Pois, ao avaliar o risco e ter à disposição recomendações, você pode ponderar sobre quais as atividades devem ser priorizadas, sejam aquelas relativas ao negócio, sejam as relativas à conformidade com a LGPD.

Para entender como aplicar o método, siga as instruções abaixo.

Para cada conjunto de perguntas você terá um texto explicativo do contexto a fim de ajudá-lo a compreender do que se trata o tópico e auxiliá-lo nas respostas.

Ao terminar de aplicar o método, você receberá o resultado do teste até 60 minutos. O resultado trará sua exposição ao risco para cada aspecto analisado, bem como um link para que responda um formulário de avaliação. É muito importante que você responda o formulário, pois, servirá de subsídio para que possamos aprimorar o método.

Desde já agradecemos sua participação!

Seus dados Para começar, insira seus dados. Eles serão imprescindíveis para que possamos encaminhar a você o resultado, bem como para enviarmos o formulário de avaliação.

2.1. Nome completo:

_____

2.2. Nome da Startup:

_____

2.3 E-mail:

_____

2.4 Telefone:

_____

End of Block: Bloco 1

Start of Block: Iniciando

Esta é uma abordagem que tem como base uma avaliação de risco.

Para usar o método, o primeiro passo é:

Definir o conjunto de dados que você vai usar nesta avaliação.

IMPORTANTE: É muito provável que você utilize vários conjuntos de dados, de diferentes categorias, para diversas finalidades em suas aplicações ou seus softwares. Isso torna geralmente a tarefa de avaliar riscos complexa. Por essa razão, simplificamos a forma de avaliação. **Você deve identificar quais dados podem atrair os riscos mais severos e utilizar somente eles nesta avaliação.** Assim, o método vai ajudar você a compreender quais são os maiores riscos que precisa lidar.

Você deve, portanto, escolher apenas o conjunto de dados que pode lhe trazer as consequências mais severas caso haja algum tipo de violação (acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito).

Para descobrir qual é o conjunto de dados que você deve utilizar, acesse o link. Ali presentamos quatro categorias de dados para você:

Dados Simples: por exemplo, dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.

Dados de Comportamento: por exemplo, dados de localização, trânsito, preferências e hábitos pessoais, etc.

Dados Financeiros: por exemplo, dados de renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.

Dados Sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Cada categoria traz quatro descrições de dados e uma pontuação correspondente, com base nas consequências em caso de violação. São atribuídos valores de 1 a 4 para cada descrição de dados (1 = pouco impacto, 2 = médio impacto, 3 = alto impacto, 4 = muito alto impacto). O link explica a gradação desses valores.

Leia atentamente as descrições em cada tabela e verifique a pontuação correspondente. Escolha o conjunto de dados que possui a pontuação mais alta.

Será o conjunto de dados com a pontuação mais alta que você deve incluir como resposta na questão a seguir.

COMENTÁRIO: É claro que sua startup utiliza diversas categorias de dados. Mas como você quer saber qual é o seu maior nível de risco, selecione aquela que tiver o valor mais alto.

Q1.1 **Categoria de Dados Pessoais**

Para responder as questões sobre Categorias de Dados, defina o conjunto de dados pessoais mais relevante de sua aplicação. A seguir escolha a categoria abaixo a que ele se refere e selecione a assertiva mais adequada sobre os dados:

- ○ Dados Simples? (p. e., dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.). (1)
- ○ Dados de Comportamento? (p. e., dados de localização, de trânsito, sobre preferências e hábitos pessoais, etc). (2)
- ○ Dados Financeiros? (p. e., renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.. Inclui dados de bem-estar social relacionados a informações financeiras.). (3)
- ○ Dados Sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político,

dado referente à saúde ou à vida sexual, dado genético ou biométrico [reconhecimento facial, de digital, ou outra captura de dado corporal para análise automatizada]). (4)

Q63 **Categoria de Dados Pessoais**
Para responder as questões sobre Categorias de Dados, defina o conjunto de dados pessoais mais relevante de sua aplicação. A seguir escolha a categoria abaixo a que ele se refere e selecione a assertiva mais adequada sobre os dados:

○ Dados Simples? (p. e., dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.). (1)

○ Dados de Comportamento? (p. e., dados de localização, de trânsito, sobre preferências e hábitos pessoais, etc). (2)

○ Dados Financeiros? (p. e., renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.. Inclui dados de bem-estar social relacionados a informações financeiras.). (3)

○ Dados Sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico [reconhecimento facial, de digital, ou outra captura de dado corporal para análise automatizada]). (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Simples? (p. e., dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.).

Q1.2 **Dados Simples**
Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados simples e a empresa não tem conhecimento de quaisquer circunstâncias consideradas agravantes. (Impacto 1) (1)
- O volume de dados e/ou características extraídas deles permite estabelecer perfis ou podem ser feitas suposições sobre o status social/financeiro do indivíduo. (Impacto 2) (2)
- Os dados e/ou as características extraídas deles podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas. (Impacto 3) (3)
- Características do indivíduo (por exemplo, grupos vulneráveis, crianças, adolescentes, idosos) fazem com que as informações possam ser críticas para sua segurança pessoal ou condições físicas/psicológicas. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados de Comportamento? (p. e., dados de localização, de trânsito, sobre preferências e hábitos pessoais, etc).

Q1.2 **Dados de Comportamento**
Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados de comportamento e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 2) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre dados comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web). (Impacto 1) (2)
- O volume de dados e/ou as características extraídas deles são tais que pode ser criado um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos. (Impacto 3) (3)
- Um perfil baseado em dados confidenciais ou de acesso restrito do indivíduo pode ser criado. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Financeiros? (p. e., renda, transações financeiras, extratos bancários,

investimentos, cartões de crédito, faturas, etc.. Inclui dados de bem-estar social relacionados a informações financeiras.).

Q1.2 **Dados Financeiros**
Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados financeiros e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 3) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre as informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem maiores detalhes). (Impacto 1) (2)
- O conjunto de dados inclui algumas informações financeiras, mas ainda não fornece informações significativas sobre a situação/status financeiro do indivíduo (por exemplo, números simples de contas bancárias sem mais detalhes). (Impacto 2) (3)
- A natureza e/ou volume do conjunto de dados tratam de informações financeiras completas (por exemplo, cartão de crédito) que, se divulgadas, poderiam permitir fraudes ou criar um perfil social/financeiro detalhado. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico [reconhecimento facial, de digital, ou outra captura de dado corporal para análise automatizada]).

Q1.2 **Dados Sensíveis**
Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados sensíveis (sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 4) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre os dados sensíveis do indivíduo ou os dados podem ser coletados facilmente

(independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web). (Impacto 1) (2)

○ A natureza dos dados sensíveis pode levar apenas a suposições gerais. (Impacto 2) (3)

○ A natureza dos dados sensíveis pode levar a suposições sobre informações confidenciais (Impacto 3) (4)

Q1.3 **Quantidade de Pessoas**
Defina a quantidade de pessoas que estão tendo seus dados coletados e utilizados.

○ Até 99 pessoas (1)

○ Maior ou igual a 100 pessoas (2)

End of Block: Iniciando

Start of Block: Bloco 3

Ciclo de Vida dos Dados
As questões desta seção tratam da segurança de informação ao longo do seu ciclo de vida dos dados, contemplando: (i) **Coleta e Acesso**; (ii) **Armazenamento**; (iii) **Compartilhamento**; (iv) **Retenção e Eliminação**. São questões que essencialmente tratam de práticas de segurança da informação que devem ter especial atenção desde o momento de coleta até a eliminação.

Responda as questões a seguir tendo em mente o conjunto de dados escolhido anteriormente, que utiliza em sua aplicação.

Em relação às atividades de **Coleta e Acesso**:

Q2.1 Os usuários são autenticados de forma segura (**apenas a título de exemplo**: certificação digital, autenticação multifator)?

○ Sim. (1)

○ Não. (2)

○ Não sei informar. (3)

Q2.2 Os usuários são autenticados com uso de protocolos de segurança contra acessos indevidos (**apenas a título de exemplo**: https, tls)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.3 Usuários autenticados acessam somente dados para os quais são autorizados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.4 Eventos de segurança (como login/logout, ou criação, alteração, exclusão de usuários) são monitorados em um sistema, de modo a permitir a visualização de tentativas de login com falhas combinadas com tentativas de login bem sucedidas?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.5 São realizados testes de vulnerabilidades e analisados os resultados ou testes para identificar possíveis falhas de sistema e código a fim de evitar vazamento de dados (**apenas a título de exemplo:** PENTEST, análise DAST e SAST, SQL INJECTION)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Armazenamento**:

Q2.6 O sistema tem controle de acesso que permite somente usuários autorizados acessarem ou alterarem os dados pessoais armazenados (como firewall, API gateway, ou outros recursos, que permitam protocolos seguros de entrada e saída)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.7 O sistema registra o rastreamento de usuários que fizeram alterações nos dados relevantes da aplicação?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.8 Os dados pessoais armazenados estão protegidos com criptografia, ou outras técnicas de segurança (como ofuscação, por exemplo)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.9 Há uma política e procedimento para cópias de segurança e/ou rotinas de backup criptografados que permitam a recuperação dos dados pessoais?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Compartilhamento**:

Q2.10 O sistema possui mecanismos de segurança que protegem o compartilhamento de dados (**por exemplo**, compartilhamento por usuários ou entre sistemas)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.11 O sistema possui criptografia dos dados para compartilhamento de dados ou o conteúdo foi anonimizado, criptografado, desidentificado ou ofuscado?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.12 O sistema possibilita que somente usuários autorizados possam compartilhar dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q.2.13 O sistema possui controle de acesso baseado em função (RBAC - técnica de atribuição de direitos de acesso para usuários com base em funções e tarefas que desempenham)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Retenção e Eliminação**:

Q2.14 O sistema tem controle de acesso que permite somente usuários autorizados realizarem a eliminação de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.15 O sistema possui política e procedimento de descarte de dados com base no cumprimento das finalidades de tratamento e que leve em conta a legislação específica do contexto do negócio?

(**Importante**: A LGPD determina que os dados devem ser retidos apenas pelo tempo necessário para atingir a finalidade pretendida, precisando ser eliminados após o cumprimento de seu propósito. Portanto, uma vez cumprida a finalidade, deve haver mecanismos que garantam a eliminação dos dados. A política/procedimento/prática de de descarte deve incluir no mínimo: definição de

responsáveis pelo descarte, procedimento para eliminar os dados em todos os backups realizados, relação de finalidades de tratamento e tempo de retenção de dados para cada finalidade.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.16 O sistema tem procedimentos para que os dados de backup também possam ser eliminados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.17 Dados não estruturados, como vídeos e imagens relativos ao titular da informação, são correlacionados para também poderem ser eliminados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Bloco 3

Start of Block: Block 4

Desenvolvimento

Quando são realizadas atividades de desenvolvimento de software é preciso tomar precauções específicas para evitar violações de dados pessoais. As questões dessa seção tratam de atividades de desenvolvimento de software. Responda as questões a seguir tendo em mente o conjunto de dados utilizados em sua aplicação.

Em relação às atividades de **Desenvolvimento**:

Q3.1 Em ambiente de testes e desenvolvimento todos os dados utilizados são fictícios ou anonimizados?

- ○ Sim, são fictícios ou anonimizados. (1)
- ○ Não, não são fictícios ou anonimizados. (2)
- ○ Não sei informar. (3)

Q3.2 A empresa possui política de acesso para os envolvidos nas atividades de desenvolvimento do sistema?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q3.3 São realizados (ou estão previstos como obrigatórios) testes de vulnerabilidade e segurança?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q3.4 Há uma política de desenvolvimento seguro, com regras explícitas que devem ser aplicadas no desenvolvimento de sistemas?

(**Por exemplo**: o ambiente de teste é segregado do ambiente de produção; as estações de trabalho dos integrantes das equipes envolvidas no processo de implantação possuem softwares e sistemas operacionais atualizados e seguro; entre outras prescrições.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Block 4

Start of Block: Block 5

Conformidade de Tratamento

Não basta cuidar da segurança de informação, o tratamento de dados precisa ser realizado em conformidade com a LGPD. Tratar dados, para a LGPD significa qualquer coisa que você faça com os dados. Se o mero acesso é considerado um tratamento de dados, o que dirá atividades como coleta, armazenamento, compartilhamento ou outras operações mais complexas, como criação de perfis para classificar pessoas, uso de IA e dados pessoais, etc. Alguns tipos de tratamentos de dados podem inerentemente trazer mais risco que outros, sendo classificados como de alto risco, requerendo cuidados maiores. Esta seção traz questões relativas ao risco da aplicação por conta da forma como os dados são tratados.

Assim, em relação ao **tratamento** dos dados pessoais:

Q4.1 O tratamento é realizado em larga escala.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.2 O tratamento afeta significativamente interesses e direitos fundamentais das pessoas. (Por exemplo: põe em risco a vida do titular; há tratamento de dados sensíveis, de crianças, de adolescentes ou de idosos; pode causar impacto irreversível ou de difícil reversão sobre os titulares afetados, seja de ordem material ou moral; apresenta risco para a ocorrência de situações de discriminação, de violação à integridade física, ao direito à imagem e à reputação; traz risco de fraudes financeiras ou uso indevido de identidade)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.3 O tratamento é feito com uso de tecnologias emergentes ou inovadoras (IA, IoT, blockchain, realidade virtual, metaverso etc.).

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.4 O tratamento de dados é de vigilância, monitoramento por vídeo ou controle de zonas de acesso ao público.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.5 As decisões são tomadas unicamente com base em tratamento automatizado de dados pessoais, como, por exemplo, aquelas destinadas a criar perfil pessoal, profissional, de saúde, de consumo e de crédito ou de aspectos da personalidade do titular.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.6 São usados dados pessoais sensíveis ou dados pessoais de crianças, de adolescentes e de idosos.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.7 O sistema possui controles que garantam que os dados coletados e armazenados em servidor são usados apenas para atingir propósitos pré-estabelecidos, legítimos (não ilegais e não abusivos, ou seja, de forma a não prejudicar indevidamente), específicos e informados para o titular dos dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.8 Há procedimento que garanta que o sistema armazena e trata somente o mínimo necessário de dados para os propósitos previamente definidos?

(**Exemplo**: Informações em tempo real podem não ser estritamente necessárias, agregação de conjuntos de dados que não são usados para atingir a finalidade pretendida, dados que são coletados para uma finalidade diferente do propósito original, dados que são armazenamos por um tempo de período maior que o necessário para atingir o propósito pretendido.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.9 Há mecanismos que garantam que os dados usados, ao longo do ciclo de vida (da coleta até sua eliminação), são exatos, atualizados, relevantes e necessários, para o cumprimento do propósito do tratamento?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.10 O sistema possui controles que garantem que o tratamento não causa prejuízos nem discriminação dos titulares de dados?

(**Exemplos de situações que podem trazer prejuízos ou discriminações:** criações de perfis pessoais, profissionais, de consumo, de crédito ou de aspectos da

personalidade; tomada de decisões sobre questões referentes a seguro-saúde, recrutamento, promoção em emprego, ingresso ou seleção em escolas.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Block 5

Start of Block: Block 6

Direitos dos Titulares de Dados

Os titulares de dados, ou seja, as pessoas a quem os dados se referem, possuem direitos assegurados pela LGPD e que devem ser respeitados. Isso envolve uma série de questões que precisam ser levadas em consideração, desde o fornecimento de informação aos titulares sobre como os dados são tratados, até ter um canal de comunicação para que os titulares possam solicitar medidas a respeito de seus direitos, ou estabelecer medidas que permitam apagar dados, entre outras ações.

Em relação à capacidade de atendimento dos **direitos dos titulares**:

Q5.1 Há procedimento estabelecido previamente para ser seguido em casos de solicitações dos titulares de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.2 Há pessoa designada como responsável para responder solicitações realizadas por titulares de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.3 Há conhecimento na organização sobre os deveres impostos pela LGPD a respeito dos direitos dos titulares, para responder de forma segura as solicitações de titulares?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.4 O sistema foi projetado de modo a garantir aos titulares mecanismos de informação sobre como seus dados são tratados: (a) aviso/política de privacidade; e (b) canal de comunicação que permita o titular, mediante requisição, exercer seus direitos em relação a seus dados pessoais (Por exemplo: formulário, sistema próprio, sistema de terceiros, e-mail, etc)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.5 O sistema permite facilmente: (a) extrair dados do titular para entregá-los a ele, em caso de requisição, inclusive cópia integral dos dados ou em formato lido por computador; (b) responder pedido do titular, informando como os dados são tratados, para quais finalidades, duração do tratamento e com quem são compartilhados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.6 O sistema permite a correção de dados incompletos, inexatos ou desatualizados, diretamente pelo titular ou mediante requisição ao responsável, com

possibilidade de verificação do histórico de alterações realizadas e de quem as realizou?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.7 O sistema possui um procedimento que garanta a eliminação, ou a anonimização, ou bloqueio de dados, (com possibilidade de verificação de histórico de realização do procedimento) quando eles: (a) não forem mais necessários; (b) tenham alcançado a sua finalidade de tratamento; (c) quando o titular retirar o consentimento (em casos que os dados sejam tratados mediante consentimento prévio, como no caso de uso de cookies para marketing ou rastreamento de comportamento); ou (d) quando o titular solicitar que cesse o envio de correspondência de marketing?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.8 O responsável pelo sistema tem um procedimento para informar outros agentes de tratamento com quem tenha compartilhado dados, para que repitam procedimento de correção, eliminação, anonimização ou bloqueio de dados, quando tenha sido requerido pelo titular?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Block 6

A.2. Artefato do 2º Ciclo com *Startups*

Start of Block: Bloco de perguntas padrão

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado(a) como voluntário(a) a participar do estudo Conformidade Legal em Proteção de Dados no Desenvolvimento de Software de Startups: uma Abordagem Orientada à Tomada de Decisão, que tem como objetivo analisar a utilidade e a aplicabilidade do método de tomada de decisão e do conjunto de recomendações para a conformidade com a Lei Geral de Proteção de Dados (LGPD). Acreditamos que os resultados desta pesquisa possam contribuir para as práticas de conformidade com a LGPD para startups de tecnologia.

PARTICIPAÇÃO NO ESTUDO
A sua participação no referido estudo será participar em entrevista conduzida pelos pesquisadores e fornecer materiais, caso existam, que sejam relevantes no contexto da pesquisa e que tenham sido produzidos ao longo do uso do método de tomada de decisão e do conjunto de recomendações para a conformidade com a Lei Geral de Proteção de Dados (LGPD).

RISCOS E BENEFÍCIOS
Por meio deste Termo de Consentimento Livre e Esclarecido você está sendo alertado de que, da pesquisa a se realizar, não haverá a obtenção de benefícios diretos para o participante. No entanto, pode-se esperar benefícios relacionados ao conhecimento, tais como: conhecer um modelo de tomada de decisão aplicado à startups no que diz respeito à conformidade legal com a LGPD. Bem como, também que é possível que aconteçam os seguintes desconfortos ou riscos em sua participação, tais como sentir-se desconfortável com alguma questão que lhe seja feita. Para minimizar tais riscos, nós pesquisadores tomaremos as seguintes medidas: nenhuma informação será divulgada de forma individualizada ou atribuindo sua identidade ou da empresa à qual esteja vinculado. Você poderá pedir para se retirar do estudo a qualquer momento.

SIGILO E PRIVACIDADE
Nós pesquisadores garantiremos a você que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, lhe identificar, será mantido em sigilo. Nós pesquisadores nos responsabilizaremos pela guarda e confidencialidade dos dados, bem como a não exposição dos dados de pesquisa.

AUTONOMIA
Nós lhe asseguramos assistência durante toda pesquisa, bem como garantiremos seu livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo e suas consequências, enfim, tudo o que você queira saber antes, durante e depois de sua participação. Também informamos que você pode se recusar a participar do

estudo, ou retirar seu consentimento a qualquer momento, sem precisar justificar, e de, por desejar sair da pesquisa, não sofrerá qualquer prejuízo à assistência que vem recebendo.

RESSARCIMENTO E INDENIZAÇÃO
No entanto, caso tenha qualquer despesa decorrente da participação nesta pesquisa, tais como transporte, alimentação entre outros, bem como de seu acompanhante, haverá ressarcimento dos valores gastos na forma seguinte: depósito em conta corrente. De igual maneira, caso ocorra algum dano decorrente de sua participação no estudo, você será devidamente indenizado, conforme determina a lei.

CONTATO
Os pesquisadores envolvidos com o referido projeto são Sheila Reinehr, Andreia Malucelli e Rhodrigo Deda Gomes, todos da Pontifícia Universidade Católica do Paraná (PUCPR) e com eles você poderá manter contato pelos telefones (041) 99997-4083, (41) 99994-2492 e (41) 99166-5611.
O Comitê de Ética em Pesquisa em Seres Humanos (CEP) é composto por um grupo de pessoas que estão trabalhando para garantir que seus direitos como participante de pesquisa sejam respeitados. Ele tem a obrigação de avaliar se a pesquisa foi planejada e se está sendo executada de forma ética. Se você achar que a pesquisa não está sendo realizada da forma como você imaginou ou que está sendo prejudicado de alguma forma, você pode entrar em contato com o Comitê de Ética em Pesquisa da PUCPR (CEP) pelo telefone (41) 3271-2103 entre segunda e sexta-feira das 08h00 às 17h30 ou pelo e-mail nep@pucpr.br.

DECLARAÇÃO
Declaro que li e entendi todas as informações presentes neste Termo de Consentimento Livre e Esclarecido e tive a oportunidade de discutir as informações deste termo. Todas as minhas perguntas foram respondidas e eu estou satisfeito com as respostas. Entendo que receberei uma via assinada e datada deste documento e que outra via assinada e datada será arquivada nos pelo pesquisador responsável do estudo.
Enfim, tendo sido orientado quanto ao teor de todo o aqui mencionado e compreendido a natureza e o objetivo do já referido estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

1.1 Você concorda em participar?

- ○ Sim (1)
- ○ Não (2)

Skip To: End of Survey If Você concorda em participar? = Não

End of Block: Bloco de perguntas padrão

Start of Block: Bloco 1

Conformidade Legal em Proteção de Dados no Desenvolvimento de Software de Startups: uma Abordagem Orientada à Tomada de Decisão

Olá, você está participando de uma pesquisa de doutorado cujo tema é "Método de tomada de decisão de conformidade com a LGPD para engenharia software em startups".

A pesquisa apresenta um método que apoia tomadores de decisão de startups em relação a aspectos de conformidade com a Lei Geral de Proteção de Dados (LGPD) no que se refere às atividades de engenharia de software.

Ao aplicar o método, você irá avaliar a exposição de sua startup a riscos relativos à LGPD e lhe será proposto um conjunto de recomendações para mitigá-los. Isso irá lhe ajudar na tomada de decisão sobre suas escolhas de engenharia. Pois, ao avaliar o risco e ter à disposição recomendações, você pode ponderar sobre quais as atividades devem ser priorizadas, sejam aquelas relativas ao negócio, sejam as relativas à conformidade com a LGPD.

Para entender como aplicar o método, siga as instruções abaixo. Você pode consultar também o link, que traz algumas explicações para conceitos (dados pessoais, dados sensíveis, tratamento de dados), situações de empresas B2B, e sobre categorias de dados.

Para cada conjunto de perguntas você terá um texto explicativo do contexto a fim de ajudá-lo a compreender do que se trata o tópico e auxiliá-lo nas respostas.

Ao terminar de aplicar o método, você receberá o resultado do teste até 60 minutos. O resultado trará sua exposição ao risco para cada aspecto analisado, bem como um link para que responda um formulário de avaliação. É muito importante que você responda o formulário, pois, servirá de subsídio para que possamos aprimorar o método.

Desde já agradecemos sua participação!

Seus dados Para começar, insira seus dados. Eles serão imprescindíveis para que possamos encaminhar a você o resultado, bem como para enviarmos o formulário de avaliação.

2.1. Nome completo:

_____

2.2. Nome da Startup:

_____

2.3 E-mail:

_____

2.4 Telefone:

_____

End of Block: Bloco 1

Start of Block: Iniciando

Esta é uma abordagem que tem como base uma avaliação de risco.

Para usar o método, o primeiro passo é:

Definir o conjunto de dados que você vai usar nesta avaliação.

IMPORTANTE: É muito provável que você utilize vários conjuntos de dados, de diferentes categorias, para diversas finalidades em suas aplicações ou seus softwares. Isso torna geralmente a tarefa de avaliar riscos complexa. Por essa razão, simplificamos a forma de avaliação. **Você deve identificar quais dados podem atrair os riscos mais severos e utilizar somente eles nesta avaliação.** Assim, o método vai ajudar você a compreender quais são os maiores riscos que precisa lidar.

Você deve, portanto, escolher apenas o conjunto de dados que pode lhe trazer as consequências mais severas caso haja algum tipo de violação (acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito).

Para descobrir qual é o conjunto de dados que você deve utilizar, acesse o link. **A partir do slide 5 do Tutorial** apresentamos quatro categorias de dados para você:

Dados Simples: por exemplo, dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.

Dados de Comportamento: por exemplo, dados de localização, trânsito, preferências e hábitos pessoais, etc.

Dados Financeiros: por exemplo, dados de renda, transações financeiras, extratos

bancários, investimentos, cartões de crédito, faturas, etc.

Dados Sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Cada categoria traz quatro descrições de dados e uma pontuação correspondente, com base nas consequências em caso de violação. São atribuídos valores de 1 a 4 para cada descrição de dados (1 = pouco impacto, 2 = médio impacto, 3 = alto impacto, 4 = muito alto impacto). O link explica a gradação desses valores.

Leia atentamente as descrições em cada tabela e verifique a pontuação correspondente. Escolha o conjunto de dados que possui a pontuação mais alta.

Será o conjunto de dados com a pontuação mais alta que você deve incluir como resposta na questão a seguir.

COMENTÁRIO: É claro que sua startup utiliza diversas categorias de dados. Mas como você quer saber qual é o seu maior nível de risco, selecione aquela que tiver o valor mais alto.

Q1.1 **Categoria de Dados Pessoais**

Para responder as questões sobre Categorias de Dados, defina o conjunto de dados pessoais mais relevante de sua aplicação. A seguir escolha a categoria abaixo a que ele se refere e selecione a assertiva mais adequada sobre os dados:

- ○ Dados Simples? (p. e., dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.). (1)

- ○ Dados de Comportamento? (p. e., dados de localização, de trânsito, sobre preferências e hábitos pessoais, etc). (2)

- ○ Dados Financeiros? (p. e., renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.. Inclui dados de bem-estar social relacionados a informações financeiras.). (3)

- ○ Dados Sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico [reconhecimento facial, de digital, ou outra captura de dado corporal para análise automatizada]). (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Simples? (p. e., dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.).

Q1.2 **Dados Simples**

Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados simples e a empresa não tem conhecimento de quaisquer circunstâncias consideradas agravantes. (Impacto 1) (1)
- O volume de dados e/ou características extraídas deles permite estabelecer perfis ou podem ser feitas suposições sobre o status social/financeiro do indivíduo. (Impacto 2) (2)
- Os dados e/ou as características extraídas deles podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas. (Impacto 3) (3)
- Características do indivíduo (por exemplo, grupos vulneráveis, crianças, adolescentes, idosos) fazem com que as informações possam ser críticas para sua segurança pessoal ou condições físicas/psicológicas. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados de Comportamento? (p. e., dados de localização, de trânsito, sobre preferências e hábitos pessoais, etc).

Q1.2 **Dados de Comportamento**

Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados de comportamento e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 2) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre dados comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web). (Impacto 1) (2)
- O volume de dados e/ou as características extraídas deles são tais que pode ser criado um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos. (Impacto 3) (3)
- Um perfil baseado em dados confidenciais ou de acesso restrito do indivíduo pode ser criado. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Financeiros? (p. e., renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.. Inclui dados de bem-estar social relacionados a informações financeiras.).

Q1.2 **Dados** **Financeiros**

Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados financeiros e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 3) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre as informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem maiores detalhes). (Impacto 1) (2)
- O conjunto de dados inclui algumas informações financeiras, mas ainda não fornece informações significativas sobre a situação/status financeiro do indivíduo (por exemplo, números simples de contas bancárias sem mais detalhes). (Impacto 2) (3)
- A natureza e/ou volume do conjunto de dados tratam de informações financeiras completas (por exemplo, cartão de crédito) que, se divulgadas, poderiam permitir fraudes ou criar um perfil social/financeiro detalhado. (Impacto 4) (4)

Display This Question:

If Categoria de Dados Pessoais Para responder as questões sobre Categorias de Dados, defina o conjun... = Dados Sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico [reconhecimento facial, de digital, ou outra captura de dado corporal para análise automatizada]).

Q1.2 **Dados** **Sensíveis**

Qual assertiva é mais adequada ao contexto de uso dos dados:

- São dados sensíveis (sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes que uma violação de dados possa causar. (Impacto 4) (1)
- A natureza do conjunto de dados não fornece informações substanciais sobre os dados sensíveis do indivíduo ou os dados podem ser coletados facilmente

(independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web). (Impacto 1) (2)

○ A natureza dos dados sensíveis pode levar apenas a suposições gerais. (Impacto 2) (3)

○ A natureza dos dados sensíveis pode levar a suposições sobre informações confidenciais (Impacto 3) (4)

Q1.3 **Quantidade de Pessoas**
Defina a quantidade de pessoas que estão tendo seus dados coletados e utilizados.

○ Até 99 pessoas (1)

○ Maior ou igual a 100 pessoas (2)

End of Block: Iniciando

Start of Block: Bloco 3

Ciclo de Vida dos Dados
As questões desta seção tratam da segurança de informação ao longo do seu ciclo de vida dos dados, contemplando: (i) **Coleta e Acesso**; (ii) **Armazenamento**; (iii) **Compartilhamento**; (iv) **Retenção e Eliminação**. São questões que essencialmente tratam de práticas de segurança da informação que devem ter especial atenção desde o momento de coleta até a eliminação.

Responda as questões a seguir tendo em mente o conjunto de dados escolhido anteriormente, que utiliza em sua aplicação.

Em relação às atividades de **Coleta e Acesso**:

Q2.1 Os usuários são autenticados de forma segura (**apenas a título de exemplo**: certificação digital, autenticação multifator)?

○ Sim. (1)

○ Não. (2)

○ Não sei informar. (3)

Q2.2 Os usuários são autenticados com uso de protocolos de segurança contra acessos indevidos (**apenas a título de exemplo**: https, tls)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.3 Usuários autenticados acessam somente dados para os quais são autorizados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.4 Eventos de segurança (como login/logout, ou criação, alteração, exclusão de usuários) são monitorados em um sistema, de modo a permitir a visualização de tentativas de login com falhas combinadas com tentativas de login bem sucedidas?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.5 São realizados testes de vulnerabilidades e analisados os resultados ou testes para identificar possíveis falhas de sistema e código a fim de evitar vazamento de dados (**apenas a título de exemplo:** PENTEST, análise DAST e SAST, SQL INJECTION)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Armazenamento**:

Q2.6 O sistema tem controle de acesso que permite somente usuários autorizados acessarem ou alterarem os dados pessoais armazenados (como firewall, API gateway, ou outros recursos, que permitam protocolos seguros de entrada e saída)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.7 O sistema registra o rastreamento de usuários que fizeram alterações nos dados relevantes da aplicação?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.8 Os dados pessoais armazenados estão protegidos com criptografia, ou outras técnicas de segurança (como ofuscação, por exemplo)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.9 Há uma política e procedimento para cópias de segurança e/ou rotinas de backup criptografados que permitam a recuperação dos dados pessoais?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Compartilhamento**:

Q2.10 O sistema possui mecanismos de segurança que protegem o compartilhamento de dados (**por exemplo**, compartilhamento por usuários ou entre sistemas)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.11 O sistema possui criptografia dos dados para compartilhamento de dados ou o conteúdo foi anonimizado, criptografado, desidentificado ou ofuscado?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.12 O sistema possibilita que somente usuários autorizados possam compartilhar dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q.2.13 O sistema possui controle de acesso baseado em função (RBAC - técnica de atribuição de direitos de acesso para usuários com base em funções e tarefas que desempenham)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Em relação às atividades de **Retenção e Eliminação**:

Q2.14 O sistema tem controle de acesso que permite somente usuários autorizados realizarem a eliminação de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.15 O sistema possui política e procedimento de descarte de dados com base no cumprimento das finalidades de tratamento e que leve em conta a legislação específica do contexto do negócio?

(**Importante**: A LGPD determina que os dados devem ser retidos apenas pelo tempo necessário para atingir a finalidade pretendida, precisando ser eliminados após o cumprimento de seu propósito. Portanto, uma vez cumprida a finalidade, deve haver mecanismos que garantam a eliminação dos dados. A política/procedimento/prática de de descarte deve incluir no mínimo: definição de responsáveis pelo descarte, procedimento para eliminar os dados em todos os backups realizados, relação de finalidades de tratamento e tempo de retenção de dados para cada finalidade.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.16 O sistema tem procedimentos para que os dados de backup também possam ser eliminados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q2.17 Dados não estruturados, como vídeos e imagens relativos ao titular da informação, são correlacionados para também poderem ser eliminados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Bloco 3

Start of Block: Block 4

Desenvolvimento

Quando são realizadas atividades de desenvolvimento de software é preciso tomar precauções específicas para evitar violações de dados pessoais. As questões dessa seção tratam de atividades de desenvolvimento de software. Responda as questões a seguir tendo em mente o conjunto de dados utilizados em sua aplicação.

Em relação às atividades de **Desenvolvimento**:

Q3.1 Em ambiente de testes e desenvolvimento todos os dados utilizados são fictícios ou anonimizados?

- ○ Sim, são fictícios ou anonimizados. (1)
- ○ Não, não são fictícios ou anonimizados. (2)
- ○ Não sei informar. (3)

Q3.2 A empresa possui política de acesso para os envolvidos nas atividades de desenvolvimento do sistema?

- Sim. (1)
- Não. (2)
- Não sei informar. (3)

Q3.3 São realizados (ou estão previstos como obrigatórios) testes de vulnerabilidade e segurança?

- Sim. (1)
- Não. (2)
- Não sei informar. (3)

Q3.4 Há uma política de desenvolvimento seguro, com regras explícitas que devem ser aplicadas no desenvolvimento de sistemas?

(**Por exemplo**: o ambiente de teste é segregado do ambiente de produção; as estações de trabalho dos integrantes das equipes envolvidas no processo de implantação possuem softwares e sistemas operacionais atualizados e seguro; entre outras prescrições.)

- Sim. (1)
- Não. (2)
- Não sei informar. (3)

End of Block: Block 4

Start of Block: Block 5

Conformidade de Tratamento

Não basta cuidar da segurança de informação, o tratamento de dados precisa ser realizado em conformidade com a LGPD.

Tratar dados, para a LGPD significa qualquer coisa que você faça com os dados. Se o mero acesso é considerado um tratamento de dados, o que dirá atividades como coleta, armazenamento, compartilhamento ou outras operações mais complexas,

como criação de perfis para classificar pessoas, uso de IA e dados pessoais, etc. Alguns tipos de tratamentos de dados podem inerentemente trazer mais risco que outros, sendo classificados como de alto risco, requerendo cuidados maiores.

Se o seu sistema é uma plataforma ou você oferece serviços a empresas que, por sua vez, irão oferecer serviços ao clientes delas, pode ser útil ler as considerações **do slide 4 do link**
.

Esta seção traz questões relativas ao risco da aplicação por conta da forma como os dados são tratados. Assim, em relação ao **tratamento** dos dados pessoais:

Q4.1 O tratamento é realizado em larga escala.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.2 O tratamento afeta significativamente interesses e direitos fundamentais das pessoas. (Por exemplo: põe em risco a vida do titular; há tratamento de dados sensíveis, de crianças, de adolescentes ou de idosos; pode causar impacto irreversível ou de difícil reversão sobre os titulares afetados, seja de ordem material ou moral; apresenta risco para a ocorrência de situações de discriminação, de violação à integridade física, ao direito à imagem e à reputação; traz risco de fraudes financeiras ou uso indevido de identidade)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.3 O tratamento é feito com uso de tecnologias emergentes ou inovadoras (IA, IoT, blockchain, realidade virtual, metaverso etc.).

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.4 O tratamento de dados é de vigilância, monitoramento por vídeo ou controle de zonas de acesso ao público.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.5 As decisões são tomadas unicamente com base em tratamento automatizado de dados pessoais, como, por exemplo, aquelas destinadas a criar perfil pessoal, profissional, de saúde, de consumo e de crédito ou de aspectos da personalidade do titular.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.6 São usados dados pessoais sensíveis ou dados pessoais de crianças, de adolescentes e de idosos.

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.7 O sistema possui controles que garantam que os dados coletados e armazenados em servidor são usados apenas para atingir propósitos pré-estabelecidos, legítimos (não ilegais e não abusivos, ou seja, de forma a não prejudicar indevidamente), específicos e informados para o titular dos dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.8 Há procedimento que garanta que o sistema armazena e trata somente o mínimo necessário de dados para os propósitos previamente definidos?

(**Exemplo**: Informações em tempo real podem não ser estritamente necessárias, agregação de conjuntos de dados que não são usados para atingir a finalidade pretendida, dados que são coletados para uma finalidade diferente do propósito original, dados que são armazenamos por um tempo de período maior que o necessário para atingir o propósito pretendido.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.9 Há mecanismos que garantam que os dados usados, ao longo do ciclo de vida (da coleta até sua eliminação), são exatos, atualizados, relevantes e necessários, para o cumprimento do propósito do tratamento?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q4.10 O sistema possui controles que garantem que o tratamento não causa prejuízos nem discriminação dos titulares de dados?

(**Exemplos de situações que podem trazer prejuízos ou discriminações:** criações de perfis pessoais, profissionais, de consumo, de crédito ou de aspectos da

personalidade; tomada de decisões sobre questões referentes a seguro-saúde, recrutamento, promoção em emprego, ingresso ou seleção em escolas.)

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Block 5

Start of Block: Block 6

Direitos dos Titulares de Dados

Os titulares de dados, ou seja, as pessoas a quem os dados se referem, possuem direitos assegurados pela LGPD e que devem ser respeitados. Isso envolve uma série de questões que precisam ser levadas em consideração, desde o fornecimento de informação aos titulares sobre como os dados são tratados, até ter um canal de comunicação para que os titulares possam solicitar medidas a respeito de seus direitos, ou estabelecer medidas que permitam apagar dados, entre outras ações.

Se o seu sistema é uma plataforma ou você oferece serviços a empresas que, por sua vez, irão oferecer serviços ao clientes delas, importante alertar que mesmo nesses casos, é importante que o seu sistema seja capaz de atender solicitações de titulares. Pode ser útil ler as considerações **do slide 4 do link**
.

Em relação à capacidade de atendimento dos **direitos dos titulares**:

Q5.1 Há procedimento estabelecido previamente para ser seguido em casos de solicitações dos titulares de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.2 Há pessoa designada como responsável para responder solicitações realizadas por titulares de dados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.3 Há conhecimento na organização sobre os deveres impostos pela LGPD a respeito dos direitos dos titulares, para responder de forma segura as solicitações de titulares?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.4 O sistema foi projetado de modo a garantir aos titulares mecanismos de informação sobre como seus dados são tratados: (a) aviso/política de privacidade; e (b) canal de comunicação que permita o titular, mediante requisição, exercer seus direitos em relação a seus dados pessoais (Por exemplo: formulário, sistema próprio, sistema de terceiros, e-mail, etc)?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.5 O sistema permite facilmente: (a) extrair dados do titular para entregá-los a ele, em caso de requisição, inclusive cópia integral dos dados ou em formato lido por

computador; (b) responder pedido do titular, informando como os dados são tratados, para quais finalidades, duração do tratamento e com quem são compartilhados?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.6 O sistema permite a correção de dados incompletos, inexatos ou desatualizados, diretamente pelo titular ou mediante requisição ao responsável, com possibilidade de verificação do histórico de alterações realizadas e de quem as realizou?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.7 O sistema possui um procedimento que garanta a eliminação, ou a anonimização, ou bloqueio de dados, (com possibilidade de verificação de histórico de realização do procedimento) quando eles: (a) não forem mais necessários; (b) tenham alcançado a sua finalidade de tratamento; (c) quando o titular retirar o consentimento (em casos que os dados sejam tratados mediante consentimento prévio, como no caso de uso de cookies para marketing ou rastreamento de comportamento); ou (d) quando o titular solicitar que cesse o envio de correspondência de marketing?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

Q5.8 O responsável pelo sistema tem um procedimento para informar outros agentes de tratamento com quem tenha compartilhado dados, para que repitam procedimento

de correção, eliminação, anonimização ou bloqueio de dados, quando tenha sido requerido pelo titular?

- ○ Sim. (1)
- ○ Não. (2)
- ○ Não sei informar. (3)

End of Block: Block 6

APÊNDICE B – QUESTÕES E RECOMENDAÇÕES PARA TRATAMENTO DE RISCOS

B.1 - Questões do Ciclo de Vida dos Dados - Probabilidade

I. Em relação às atividades de Coleta e Acesso:	**Referência**	**Tratamento**
Os usuários são autenticados de forma segura (apenas a título de exemplo: certificação digital, autenticação multifator)?	ISO/IEC 27001, 8.5	Usar procedimentos de autenticação seguros (por exemplo: certificação digital, autenticação multifator)
Os usuários são autenticados com uso de protocolos de segurança contra acessos indevidos (apenas a título de exemplo: https, tls)?	ISO/IEC 27001,5.15, 8.24	Usar protocolos de segurança (por exemplo: https, tls).
Usuários autenticados acessam somente dados para os quais são autorizados?	ISO/IEC 27001, 8.2, 8.5	Implantar processo de controle de acesso para que usuários acessem somente dados para os quais são autorizados.
Eventos de segurança (como login/logout, ou criação, alteração, exclusão de usuários) são monitorados em um sistema, de modo a permitir a visualização de tentativas de login com falhas combinadas com tentativas de login bem sucedidas?	Open Worldwide Application Security Project, 2022; ISO/IEC 27001, 8.16	Monitorar eventos de segurança, de forma que permita a correlação e visualização de tentativas de login com falhas, combinadas com tentativas de login bem sucedidas.
São realizados testes de vulnerabilidades e analisados os resultados ou testes para identificar possíveis falhas de sistema e código a fim de evitar vazamento de dados (apenas a título de exemplo: PENTEST, análise DAST e SAST, SQL INJECTION)?	Open Worldwide Application Security Project, 2022; ISO/IEC 27001, 8.34	Realizar testes de vulnerabilidade e para identificar possíveis falhas que possam permitir vazamento de dados.
II. Em relação às atividades de Armazenamento:		
O sistema tem controle de acesso que permite somente usuários autorizados acessarem ou alterarem os dados pessoais armazenados (como firewall, API gateway, ou outros recursos, que permitam protocolos seguros de entrada e saída)?	ISO/IEC 27001, 8.2, Li et al., 2020	Implantar processo de controle de acesso para que somente usuários autorizados possam acessar dados pessoais armazenados.

O sistema registra o rastreamento de usuários que fizeram alterações nos dados relevantes da aplicação?	ISO/IEC 27001, 8.15	Implantar rastreamento de usuários que fizeram alterações em dados armazenados.
Os dados pessoais armazenados estão protegidos com criptografia, ou outras técnicas de segurança (como ofuscação, por exemplo)?	Li et al., 2020, ISO/IEC 27001, 8.24	Implantar mecanismos para que os dados sejam protegidos por criptografia ou outras técnicas (como ofuscamento, por exemplo), de modo a não identificá-los.
Há uma política e procedimento para cópias de segurança e/ou rotinas de backup criptografados que permitam a recuperação dos dados pessoais?	ISO/IEC 27001, 8.13	Implantar política e procedimento de backup e cópias de segurança.
III. Em relação às atividades de Compartilhamento:		
O sistema possui mecanismos de segurança que protegem o compartilhamento de dados (por exemplo, compartilhamento por usuários ou entre sistemas)?	ISO/IEC 27001, 8.3, 8.9	Implantar mecanismos de controle de acesso para que somente usuários autorizados possam compartilhar dados pessoais. Implantar mecanismos de segurança que limitem/restrinjam a comunicação entre sistemas.
O sistema possui criptografia dos dados para compartilhamento de dados ou o conteúdo foi anonimizado, criptografado, desidentificado ou ofuscado?	Wuyts, Sion e Joosen, 2020; ISO/IEC 27001, 8.24	Implantar criptografia para compartilhamento de dados, ou anonimizar, criptografar ou desidentificar dados que serão compartilhados.
O sistema possibilita que somente usuários autorizados possam compartilhar dados?	ISO/IEC 27001, 8.2, 8.3	Implantar controle de acesso para que somente usuários autorizados possam compartilhar dados.
O sistema possui controle de acesso baseado em função (RBAC - técnica de atribuição de direitos de acesso para usuários com base em funções e tarefas que desempenham)?	ISO/IEC 27001, 8.2, 8.4	Implantar controle de acesso baseado em função (RBAC) para que o recebimento de dados ocora somente para usuários autorizados a receber dados.
IV. Em relação às atividades de Retenção e Eliminação: (4Q)		
O sistema tem controle de acesso que permite somente usuários autorizados realizarem a eliminação de dados?	ISO/IEC 27001, 8.2, 8.3	Implantar processo de controle de acesso para que somente usuários autorizados possam eliminar dados pessoais.

O sistema possui política e procedimento de descarte de dados com base no cumprimento das finalidades de tratamento e que leve em conta a legislação específica do contexto do negócio? (Importante: A LGPD determina que os dados devem ser retidos apenas pelo tempo necessário para atingir a finalidade pretendida, precisando ser eliminados após o cumprimento de seu propósito. Portanto, uma vez cumprida a finalidade, deve haver mecanismos que garantam a eliminação dos dados. A política/procedimento/prática de de descarte deve incluir no mínimo: definição de responsáveis pelo descarte, procedimento para eliminar os dados em todos os backups realizados, relação de finalidades de tratamento e tempo de retenção de dados para cada finalidade.)	Brasil, 2018 (art. 6º, I, art; 15, I, II, 16, LGPD); ISO/IEC 27001 (8.10)	Implantar uma política e procedimento de regras de descarte de dados com base no cumprimento de finalidades de tratamento, que contenha, no mínimo: definação de responsáveis pelo descarte, procedimento para eliminar os dados em todos os backups realizados, relação de finalidades de tratamento e tempo de retenção de dados para cada finalidade. Implantar um procedimento para eliminar dados nos backups pré-existentes, quando o caso.
O sistema tem procedimentos para que os dados de backup também possam ser eliminados?	Brasil, 2018 (art. 6º, I, art; 15, I, II, 16, LGPD)	Implantar procedimentos para que, quando necessário, seja possível eliminar dados também dos backups existentes.
Dados não estruturados, como vídeos e imagens relativos ao titular da informação, são correlacionados para também poderem ser eliminados?	Brasil, 2018 (art. 6º, I, art; 15, I, II, 16, LGPD)	Implantar mecanismos para que, quando necessário, dados sejam correlacionados e também possam ser eliminados.

B.2 - Questões de Desenvolvimento - Probabilidade

Questões de Desenvolvimento:	**Referência**	**Tratamento**
Em ambiente de testes e desenvolvimento todos os dados utilizados são fictícios ou anonimizados?	ISO/IEC 27001, 8.33	Usar bancos de dados que não contenham dados de pessoas identificadas ou passíveis de identificação, ou anonimizar os dados. Caso isso não seja possível, reduzir ao mínimo necessário o uso de dados pessoais, implementar mecanismos de segurança, política de eliminação de dados imediatamente após o uso, controle rígido de acesso, e proteção contra remoção ou modificação das informações.
A empresa possui política de acesso para os envolvidos nas atividades de desenvolvimento do sistema?	ISO/IEC 27001, 8.3, 8.4	Implantar controle de acesso, com uma política de privilégios mínimos (possibilidade de acesso a recursos

		estritamente necessários para realizar a execução das atividades programadas).
São realizados (ou estão previstos como obrigatórios) testes de vulnerabilidade e segurança?	ISO/IEC 27002, 8.29	Realizar testes de vulnerabilidade e segurança antes de implementar o sistema, bem como nova versão do sistema.
Há uma política de desenvolvimento seguro, com regras explícitas que devem ser aplicadas no desenvolvimento de sistemas? (Por exemplo: o ambiente de teste é segregado do ambiente de produção; as estações de trabalho dos integrantes das equipes envolvidas no processo de implantação possuem softwares e sistemas operacionais atualizados e seguro; entre outras prescrições.)	ISO/IEC 27001, 8.27, 8.28	Implantar política de desenvolvimento seguro, com regras explícitas a serem aplicadas no desenvolvimento de sistemas, entre elas: segregar o ambiente de teste do ambiente de produção; implementar softwares e sistemas operacionais atualizados e seguros nas estações de trabalho dos integrantes das equipes envolvidas no processo de implantação.

B.3 - Questões de Conformidade de Tratamento - Impacto

Assertivas de Conformidade de Tratamento - Impacto	**Referência**	**Tratamento**
O tratamento é realizado em larga escala.	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),	Quando está presente uma das duas primeiras assertivas e uma das quatro últimas assertivas, o tratamento é considerado de alto risco e apresenta-se como recomendação: Realizar relatório de impacto, treinar equipe de desenvolvimento em conformidade com a LGPD, realizar avaliação de risco, implantar medidas que reduzam o risco do impacto em caso de violação de direitos.
O tratamento afeta significativamente interesses e direitos fundamentais das pessoas. (Por exemplo: põe em risco a vida do titular; há tratamento de dados sensíveis, de crianças, de adolescentes ou de idosos; pode causar impacto irreversível ou de difícil reversão sobre os titulares afetados, seja de ordem material ou moral; apresenta risco para a ocorrência de situações de discriminação, de violação à integridade física, ao direito à imagem e à reputação; traz risco de fraudes financeiras ou uso indevido de identidade)	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),	
O tratamento é feito com uso de tecnologias emergentes ou inovadoras (IA, IoT, blockchain, realidade virtual, metaverso etc.)	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),	
O tratamento de dados é de vigilância, monitoramento por vídeo ou controle de zonas de acesso ao público.	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),	
As decisões são tomadas unicamente com base em tratamento automatizado de dados pessoais, como, por exemplo, aquelas destinadas a criar perfil pessoal, profissional, de saúde, de consumo	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),	

e de crédito ou de aspectos da personalidade do titular.	
São usados dados pessoais sensíveis ou dados pessoais de crianças, de adolescentes e de idosos.	Brasil, 2022 (Resolução CD/ANPD nº 2, Artigo 4º),

B.4 - Questões de Desenvolvimento - Probabilidade

Questões de Conformidade de Tratamento - Probabilidade	Referência	Peso	Tratamento
O sistema possui controles que garantam que os dados coletados e armazenados em servidor são usados apenas para atingir propósitos pré-estabelecidos, legítimos (não ilegais e não abusivos, ou seja, de forma a não prejudicar indevidamente), específicos e informados para o titular dos dados?	Brasil, 2018 (art. 6º, I, LGPD), Li et al., 2020	1	Estabelecer uma correlação clara entre dados coletados e finalidade e para qual são utilizados, e informá-la ao titular do dado (por meio, por exemplo, de aviso de privacidade).
Há procedimento que garanta que o sistema armazena e trata somente o mínimo necessário de dados para os propósitos previamente definidos?	Brasil, 2018 (art. 6º, II, III, LGPD), Li et al., 2020	5	A LGPD determina que o tratamento precisa ser adequado com as finalidades informadas. Portanto, há a necessidade de corrigir casos de incompatibilidade. Eliminar dados que não são utilizados para finalidades previamente informadas.
Há mecanismos que garantam que os dados usados, ao longo do ciclo de vida (da coleta até sua eliminação), são exatos, atualizados, relevantes e necessários, para o cumprimento do propósito do tratamento?	Brasil, 2018 (art. 6º, V, LGPD)	1	Criar mecanismos que facilitem a atualização dos dados ao longo de todo o fluxo de informação.
O sistema possui controles que garantem que o tratamento não causa prejuízos nem discriminação dos titulares de dados?	Brasil, 2018 (art. 6º, IX, LGPD). Wuyts, Sion e Joosen, 2020	3	Realizar relatório de impacto para avaliar potencial discriminação ou prejuízo para o titular do dado.

B.5 - Questões de Direitos dos Titulares - Impacto

Questões de Direitos dos Titulares - Impacto:	Referência	Tratamento
Há procedimento estabelecido previamente para ser seguido em casos de solicitações dos titulares de dados?	Brasil, 2018 (LGPD, art. 18, caput, art. 19)	Criar um procedimento para atender as solicitações dos titulares de dados pessoais, referentes ao exercício de seus direitos.

Há pessoa designada como responsável para responder solicitações realizadas por titulares de dados?	Brasil, 2018 (LGPD, art. 18, caput, art. 19)	Designar um responsável pelo atendimento das solicitações dos titulares de dados, referentes ao exercício de seus direitos.
Há conhecimento na organização sobre os deveres impostos pela LGPD a respeito dos direitos dos titulares, para responder de forma segura as solicitações de titulares?	Brasil, 2018 (LGPD, art. 18, caput, art. 19)	Buscar conhecimento sobre os direitos dos titulares de dados que precisam ser atendidos pela startup.

B.6 - Questões de Direitos dos Titulares- Probabilidade

Questões de Direitos dos Titulares - Probabilidade	**Referência**	**Peso**	**Tratamento**
O sistema foi projetado de modo a garantir aos titulares mecanismos de informação sobre como seus dados são tratados: (a) aviso/política de privacidade; e (b) canal de comunicação que permita o titular, mediante requisição, exercer seus direitos em relação a seus dados pessoais (Por exemplo: formulário, sistema próprio, sistema de terceiros, e-mail, etc)?	Brasil, 2018 (LGPD, art. 18, caput, art. 19). Brasil, 2018 (LGPD, art. 9 º, art. 18, VII)	5	Disponibilizar aviso/política de privacidade para informar ao titular como os dados dele estão sendo tratados. E/ou disponibilizar canal de comunicação para que o titular possa exercer seus direitos.
O sistema permite facilmente: (a) extrair dados do titular para entregá-los a ele, em caso de requisição, inclusive cópia integral dos dados ou em formato lido por computador; (b) responder pedido do titular, informando como os dados são tratados, para quais finalidades, duração do tratamento e com quem são compartilhados?	Brasil, 2018 (LGPD, art. 9º, art. 18, II, V, art. 19, §1º, §3º).	5	Criar mecanismos para extração de dados do sistema, de forma a facilitar a entrega de dados para o titular, em formatos lidos por computador.
O sistema permite a correção de dados incompletos, inexatos ou desatualizados, diretamente pelo titular ou mediante requisição ao responsável, com possibilidade de verificação do histórico de alterações realizadas e de quem as realizou?	Brasil, 2018 (LGPD, art. 18, III, LGPD)	1	Criar mecanismos para a correção de dados no sistema.
O sistema possui um procedimento que garanta a eliminação, ou a anonimização, ou bloqueio de dados, (com possibilidade de verificação de histórico de realização do procedimento) quando eles: (a) não forem mais necessários; (b) tenham alcançado a sua finalidade de tratamento; (c) quando o titular retirar o consentimento (em casos que os dados sejam tratados mediante consentimento prévio, como no caso de uso de cookies para marketing ou	Brasil, 2018 (LGPD, art. 8º, §1º, §2º, §4º, §5º, §6º, art. 15, art. 18, IV; art. 8º, §5º, art. 18, VIII, IX, LGPD)	3	Criar mecanismos que permitam a eliminação, anonimização ou bloqueio de dados.

rastreamento de comportamento); ou (d) quando o titular solicitar que cesse o envio de correspondência de marketing?			
O responsável pelo sistema tem um procedimento para informar outros agentes de tratamento com quem tenha compartilhado dados, para que repitam procedimento de correção, eliminação, anonimização ou bloqueio de dados, quando tenha sido requerido pelo titular?	Brasil, 2018 (art. 6º, IX, LGPD). Brasil, 2018 (LGPD, art. 18, §6º)	1	Criar procedimento para informar outros agentes de tratamento, quando for necesário que também corrijam, eliminem, anonimizem ou bloqueiem dados, conforme requerido pelo titular de dados.

APÊNDICE C – TECHNOLOGY ACCEPTANCE MODEL

Start of Block: Default Question Block

Por favor, responda às seguintes questões sobre à sua experiência durante a análise do método e das recomendações propostos.

Dados da Startup

Q1 Nome da Startup

_____

Q2 Grau de maturidade

- ○ Inicial (apenas testando ideias) (1)
- ○ Testando protótipo (com ao menos um cliente) (2)
- ○ Em crescimento (com mais de um cliente recorrente) (3)

Q3 Número de clientes

_____

Q4 Número de funcionários

_____

Q5 Setor de atuação

- ○ Saúde (1)
- ○ Educação (2)
- ○ Financeiro (3)
- ○ Agropecuário (4)
- ○ Comunicação (5)
- ○ Comércio (6)
- ○ Outro (7) _____

Q6 Modelo de negócio

_____

Q7 Descrição do produto

_____

Q8 Tempo de atuação

_____

End of Block: Default Question Block

Start of Block: Block 1

Dados do Respondente

Q9 Nome do Respondente

_____

Q10 Função na Startup

_____

Q11 Formação Escolar

- Ensino fundamental (1)
- Ensino Médio (2)
- Ensino Superior (3)
- Especialização (4)
- Mestrado (5)
- Doutorado (6)

Q12 Área de Formação

_____

Q13 Idade

_____

Q14 Tempo de dedicação por semana para a startup (em horas)

_____

Q15 Descreva brevemente sua trajetória

_____

End of Block: Block 1

Start of Block: Block 2

Q16 1. De acordo com sua percepção de Facilidade de Uso do método e conjunto de recomendações proposto, o quanto você concorda com as seguintes afirmações:

	Discordo totalmente (1)	Discordo parcialmente (2)	Não discordo, nem concordo (3)	Concordo parcialmente (4)	Concordo integralmente (5)
O método e as recomendações são claros e compreensíveis para mim (1)	○	○	○	○	○
Interagir com o método e as recomendações e interpretá-los não requer muito esforço cognitivo (mental) para mim (2)	○	○	○	○	○
Acho fácil aprender como usar o método e as recomendações (3)	○	○	○	○	○
Acho fácil o uso do método e das recomendações para fazer o que eu quero (4)	○	○	○	○	○

Q17 Comentários sobre Facilidade de Uso:

_____

Q18 De acordo com sua percepção de Utilidade do método e conjunto de recomendações proposto, o quanto você concorda com as seguintes afirmações:

	Discordo totalmente (1)	Discordo parcialmente (2)	Não discordo, nem concordo (3)	Concordo parcialmente (4)	Concordo integralmente (5)
O uso do método e das recomendações melhorou meu desempenho para cumprir com a LGPD (1)	○	○	○	○	○
O uso do método e das recomendações pode aumentar minha eficácia para cumprir com a LGPD (3)	○	○	○	○	○
Eu considero que o método e as recomendações são úteis para cumprir com a LGPD (4)	○	○	○	○	○

Q19 Comentários sobre Utilidade do método:

_____

Q20 De acordo com sua possível intenção de Uso Futuro do método e conjunto de recomendações proposto, o quanto você concorda com as seguintes afirmações

	Discordo totalmente (1)	Discordo parcialmente (2)	Não discordo, nem concordo (3)	Concordo parcialmente (4)	Concordo integralmente (5)
Levando em consideração que eu tenha domínio para escolher uma abordagem para conformidade de LGPD, eu prevejo que irei usar o método e as recomendações propostas (1)	○	○	○	○	○

Q21 Comentários sobre Uso Futuro do método:

End of Block: Block 2

APÊNDICE D – ALTERAÇÕES ENTRE CICLOS

D1. Alterações dos formulários

Seção	Primeiro ciclo	Segundo ciclo
Bloco 1 - Introdução	Para entender como aplicar o método, siga as instruções abaixo.	Para entender como aplicar o método, siga as instruções abaixo. Você pode consultar também o Tutorial, que traz algumas explicações para conceitos (dados pessoais, dados sensíveis, tratamento de dados), situações de empresas B2B, e sobre categorias de dados.
Bloco 2 – Definir o conjunto de dados	Para descobrir qual é o conjunto de dados que você deve utilizar, acesse o Tutorial - Categorias de Dados. Ali presentamos quatro categorias de dados para você:	Para descobrir qual é o conjunto de dados que você deve utilizar, acesse o **Tutorial**. **A partir do slide 5 do Tutorial** apresentamos quatro categorias de dados para você:
Bloco 5 – Conformidade de Tratamento	**Conformidade de Tratamento** Não basta cuidar da segurança de informação, o tratamento de dados precisa ser realizado em conformidade com a LGPD. Tratar dados, para a LGPD significa qualquer coisa que você faça com os dados. Se o mero acesso é considerado um tratamento de dados, o que dirá atividades como coleta, armazenamento, compartilhamento ou outras operações mais complexas, como criação de perfis para classificar pessoas, uso de IA e dados pessoais, etc. Alguns tipos de tratamentos de dados podem inerentemente trazer mais risco que outros, sendo classificados	**Conformidade de Tratamento** Não basta cuidar da segurança de informação, o tratamento de dados precisa ser realizado em conformidade com a LGPD. Tratar dados, para a LGPD significa qualquer coisa que você faça com os dados. Se o mero acesso é considerado um tratamento de dados, o que dirá atividades como coleta, armazenamento, compartilhamento ou outras operações mais complexas, como criação de perfis para classificar pessoas, uso de IA e dados pessoais, etc. Alguns tipos de tratamentos de dados podem inerentemente trazer mais risco que outros, sendo classificados como de alto risco, requerendo cuidados maiores. Se o seu sistema é uma plataforma ou você

	como de alto risco, requerendo cuidados maiores. Esta seção traz questões relativas ao risco da aplicação por conta da forma como os dados são tratados. Assim, em relação ao **tratamento** dos dados pessoais:	oferece serviços a empresas que, por sua vez, irão oferecer serviços ao clientes delas, pode ser útil ler as considerações **do slide 4 do Tutorial**. Esta seção traz questões relativas ao risco da aplicação por conta da forma como os dados são tratados. Assim, em relação ao **tratamento** dos dados pessoais:
Bloco 6 – Direitos dos Titulares	**Direitos dos Titulares de Dados** Os titulares de dados, ou seja, as pessoas a quem os dados se referem, possuem direitos assegurados pela LGPD e que devem ser respeitados. Isso envolve uma série de questões que precisam ser levadas em consideração, desde o fornecimento de informação aos titulares sobre como os dados são tratados, até ter um canal de comunicação para que os titulares possam solicitar medidas a respeito de seus direitos, ou estabelecer medidas que permitam apagar dados, entre outras ações. Em relação à capacidade de atendimento dos **direitos dos titulares**:	**Direitos dos Titulares de Dados** Os titulares de dados, ou seja, as pessoas a quem os dados se referem, possuem direitos assegurados pela LGPD e que devem ser respeitados. Isso envolve uma série de questões que precisam ser levadas em consideração, desde o fornecimento de informação aos titulares sobre como os dados são tratados, até ter um canal de comunicação para que os titulares possam solicitar medidas a respeito de seus direitos, ou estabelecer medidas que permitam apagar dados, entre outras ações. Se o seu sistema é uma plataforma ou você oferece serviços a empresas que, por sua vez, irão oferecer serviços ao clientes delas, importante alertar que mesmo nesses casos, é importante que o seu sistema seja capaz de atender solicitações de titulares. Pode ser útil ler as considerações **do slide 4 do Tutorial**. Em relação à capacidade de atendimento dos **direitos dos titulares**:

D2. Tutorial – Primeiro Ciclo

Tutorial – Categoria de Dados

Como escolher o conjunto de dados para uso no método

Categorias de Dados

- Em uma aplicação você utiliza dados de diversas categorias.
- Isso torna geralmente a tarefa de avaliar riscos complexa.
- Por essa razão, optamos por utilizar nesta avaliação **apenas os dados que podem atrair os riscos mais severos (ou seja, de maior impacto).**
- Assim, para definir quais dados você irá usar na avaliação, trazemos **quatro categorias** de dados a seguir:
  - Dados Simples
  - Dados de Comportamento
  - Dados Financeiros
  - Dados Sensíveis
- **Antes de escolher o conjunto de dados avalie nos próximos slides as quatro categorias e escolha o conjunto de dados que tenha maior impacto.**

Categorias de Dados: Simples

Dados Simples	**Por exemplo: dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados simples" e a empresa não tem conhecimento de quaisquer circunstâncias consideradas agravantes.	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de "dados simples" e/ou as características deles são tais que certos perfis do indivíduo podem ser habilitados ou podem ser feitas suposições sobre o status social/financeiro do indivíduo.	**2**
	A pontuação pode ser de 2, por exemplo, quando os "dados simples" e/ou as características deles podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas.	**3**
	A pontuação pode ser aumentada em 3, por exemplo, quando devido a certas características do indivíduo (por exemplo, grupos vulneráveis, crianças, adolescentes, idosos), as informações podem ser críticas para sua segurança pessoal ou condições físicas/psicológicas.	**4**

Categorias de Dados: de Comportamento

Dados de Comportamento	**Por exemplo: localização, dados de trânsito, dados sobre preferências e hábitos pessoais, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados comportamentais" e o controlador não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes.	**2**
	A pontuação pode ser diminuída em 1, e. quando a natureza do conjunto de dados não fornece informações substanciais sobre dados comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de "dados comportamentais" e/ou as características deles são tais que pode ser criado um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos.	**3**
	A pontuação pode ser aumentada em 2, por exemplo, se um perfil baseado em dados confidenciais ou de acesso restrito do indivíduo puder ser criado.	**4**

Categorias de Dados: Financeiros

Dados financeiros	**Dado de renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados financeiros" e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes.	3
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobre as informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem maiores detalhes).	1
	A pontuação pode ser diminuída em 1, por exemplo, quando o conjunto de dados específico inclui algumas informações financeiras, mas ainda não fornece informações significativas sobre a situação/status financeiro do indivíduo (por exemplo, números simples de contas bancárias sem mais detalhes).	2
	A pontuação pode ser aumentada em 1, por exemplo, quando devido à natureza e/ou volume do conjunto de dados específico, informações financeiras completas (por exemplo, cartão de crédito) são divulgadas, que poderiam permitir fraudes ou um perfil social/financeiro detalhado ser criado	4

Categorias de Dados: Sensíveis

Dados Sensíveis	**Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural**	
	Pontuação básica preliminar: quando a violação envolve "dados sensíveis" e a empresa não está ciente de nenhum fator de redução.	4
	A pontuação pode ser diminuída em 3, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobreos dados sensíveis do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	1
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza dos dados pode levar apenas a suposições gerais.	2
	A pontuação pode ser diminuída em 1, por exemplo, quando a natureza dos dados pode levar a suposições sobre informações confidenciais.	3

D3. Tutorial – Segundo Ciclo

Tutorial

Método de tomada de decisão de conformidade com a LGPD para engenharia software em startups

Sobre o método e a LGPD

- O uso do método apoia as decisões de engenharia para que a produção de software atenda aos aspectos de conformidade da LGPD.
- A LGPD é uma norma complexa, e há aspectos que não são de engenharia e que deverão ser tratados diretamente no âmbito jurídico. **O método não trata dos aspectos estritamente jurídicos**.
- A LGPD trata **somente** de dados de pessoas naturais (físicas).
- Entretanto, importante destacar que mesmo em relações entre empresas **há uso de dados pessoais**, seja para a realização do próprio contrato entre elas, seja para casos de avaliação de crédito ou para outras finalidades contratuais.
- Com o objetivo de ser ágil e simples, o método vai tratar **apenas de seu maior risco, com base nos dados de mais alto impacto (com consequências mais severas) que você utilizar**.

Termos mais usados

- **Dados pessoais:** informação relacionada a pessoa natural (física) identificada ou identificável
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
- **Tratamento de dados:** toda operação realizada com dados pessoais, desde à coleta, acesso, armazenamento, até o processamento, avaliação, extração e eliminação.

Se você for uma plataforma ou oferece serviços para que seus clientes prestem serviços aos clientes deles... Atenção!

- Se você for uma plataforma B2B (ou seja, ofereça serviços para empresas que, por sua vez, irão prestar serviços para outros clientes), é necessário alguns cuidados adicionais.
- Nas seções em que você for responder sobre Conformidade de Tratamento de Dados e sobre Direitos dos Titulares fique atento:
  - Embora o **responsável direto** pelos dados dos titulares armazenados em seu sistema sejam **as empresas** que contratam seus serviços, você também é **responsável indireto** por assegurar que direitos dos titulares sejam resguardados.
  - Por essa razão:
    - Em relação à seção **Conformidade de Tratamento**, tenha em mente, dentro de suas obrigações contratuais, **quais são as formas de tratamento de dados que você realiza** .
    - Em relação à seção **Direitos dos Titulares**: o método questiona sobre se você, caso necessário (por pedido da empresa que te contrata ou decisão judicial, por exemplo **), é capaz de atender a solicitações dos titulares** , entre elas: extração de dados; correção de dados; eliminação de dados, etc.

Tutorial – Categoria de Dados

Como escolher o conjunto de dados para uso no método

Categorias de Dados

- Em uma aplicação você utiliza dados de diversas categorias.
- Isso torna geralmente a tarefa de avaliar riscos complexa.
- Por essa razão, optamos por utilizar nesta avaliação **apenas os dados que podem atrair os riscos mais severos (ou seja, de maior impacto).**
- Assim, para definir quais dados você irá usar na avaliação, trazemos **quatro categorias** de dados a seguir:
  - Dados Simples
  - Dados de Comportamento
  - Dados Financeiros
  - Dados Sensíveis
- **Antes de escolher o conjunto de dados avalie nos próximos slides as quatro categorias e escolha o conjunto de dados que tenha maior impacto.**

Categorias de Dados: Simples

Dados Simples	**Por exemplo: dados biográficos, contatos, nome completo, dados sobre formação, vida familiar, experiência profissional, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados simples" e a empresa não tem conhecimento de quaisquer circunstâncias consideradas agravantes.	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de "dados simples" e/ou as características deles são tais que certos perfis do indivíduo podem ser habilitados ou podem ser feitas suposições sobre o status social/financeiro do indivíduo.	**2**
	A pontuação pode ser de 2, por exemplo, quando os "dados simples" e/ou as características deles podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas.	**3**
	A pontuação pode ser aumentada em 3, por exemplo, quando devido a certas características do indivíduo (por exemplo, grupos vulneráveis, crianças, adolescentes, idosos), as informações podem ser críticas para sua segurança pessoal ou condições físicas/psicológicas.	**4**

Categorias de Dados: de Comportamento

Dados de Comportamento	**Por exemplo: localização, dados de trânsito, dados sobre preferências e hábitos pessoais, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados comportamentais" e o controlador não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes.	**2**
	A pontuação pode ser diminuída em 1, e. quando a natureza do conjunto de dados não fornece informações substanciais sobre dados comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	**1**
	A pontuação pode ser aumentada em 1, por exemplo, quando o volume de "dados comportamentais" e/ou as características deles são tais que pode ser criado um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos.	**3**
	A pontuação pode ser aumentada em 2, por exemplo, se um perfil baseado em dados confidenciais ou de acesso restrito do indivíduo puder ser criado.	**4**

Categorias de Dados: Financeiros

Dados financeiros	**Dado de renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas, etc.**	
	Pontuação básica preliminar: quando a violação envolve "dados financeiros" e a empresa não tem conhecimento de quaisquer circunstâncias agravantes ou atenuantes.	3
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobre as informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem maiores detalhes).	1
	A pontuação pode ser diminuída em 1, por exemplo, quando o conjunto de dados específico inclui algumas informações financeiras, mas ainda não fornece informações significativas sobre a situação/status financeiro do indivíduo (por exemplo, números simples de contas bancárias sem mais detalhes).	2
	A pontuação pode ser aumentada em 1, por exemplo, quando devido à natureza e/ou volume do conjunto de dados específico, informações financeiras completas (por exemplo, cartão de crédito) são divulgadas, que poderiam permitir fraudes ou um perfil social/financeiro detalhado ser criado	4

Categorias de Dados: Sensíveis

Dados Sensíveis	**Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural**	
	Pontuação básica preliminar: quando a violação envolve "dados sensíveis" e a empresa não está ciente de nenhum fator de redução.	4
	A pontuação pode ser diminuída em 3, por exemplo, quando a natureza do conjunto de dados não fornece informações substanciais sobreos dados sensíveis do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes publicamente disponíveis (por exemplo, combinação de informações de pesquisas na web).	1
	A pontuação pode ser diminuída em 2, por exemplo, quando a natureza dos dados pode levar apenas a suposições gerais.	2
	A pontuação pode ser diminuída em 1, por exemplo, quando a natureza dos dados pode levar a suposições sobre informações confidenciais.	3