



UNIVERSIDADE FEDERAL DO MARANHÃO

Programa de Pós-Graduação em Ciência da Computação

João Pedro Marques Mendes

***LGPD-CHECK: Um Checklist para Avaliação da Aderência
de Sistemas Computacionais à Lei Geral de Proteção
de Dados Brasileira***

**São Luís - MA
2022**

João Pedro Marques Mendes

LGPD-CHECK: Um Checklist para Avaliação da Aderência de Sistemas Computacionais à Lei Geral de Proteção de Dados Brasileira

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciência da Computação, ao Programa de Pós-Graduação em Ciência da Computação, da Universidade Federal do Maranhão.

Programa de Pós-Graduação em Ciência da Computação

Universidade Federal do Maranhão

Orientador: Prof. Dr. Luis Jorge Enrique Rivero Cabrejos

Coorientador: Prof. Dr. Davi Viana dos Santos

São Luís - MA

2022

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Mendes, João Pedro Marques.

LGPD-CHECK: Um Checklist para Avaliação da Aderência de
Sistemas Computacionais à Lei Geral de Proteção de Dados
Brasileira / João Pedro Marques Mendes. - 2022.

112 p.

Coorientador(a): Davi Viana dos Santos.

Orientador(a): Luis Jorge Enrique Rivero Cabrejos.

Dissertação (Mestrado) - Programa de Pós-graduação em
Ciência da Computação/ccet, Universidade Federal do
Maranhão, São Luís - Maranhão, 2022.

1. Checklist de Inspeção. 2. Lei Geral de Proteção de
Dados. 3. Sistemas Computacionais. I. Cabrejos, Luis
Jorge Enrique Rivero. II. Santos, Davi Viana dos. III.
Título.

João Pedro Marques Mendes

LGPD-CHECK: Um Checklist para Avaliação da Aderência de Sistemas Computacionais à Lei Geral de Proteção de Dados Brasileira

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciência da Computação, ao Programa de Pós-Graduação em Ciência da Computação, da Universidade Federal do Maranhão.

Avaliação da dissertação em 13 de Setembro de 2022, em São Luís - MA:

**Prof. Dr. Luis Jorge Enrique Rivero
Cabrejos**
Orientador
Universidade Federal do Maranhão

Prof. Dr. Davi Viana dos Santos
Coorientador
Universidade Federal do Maranhão

Prof. Dr. Anselmo Cardoso de Paiva
Examinador Interno
Universidade Federal do Maranhão

Prof. Dr. Sergio Castelo Branco Soares
Examinador Externo
Universidade Federal de Pernambuco

São Luís - MA
2022

*Dedico aos meus avós Dedé Mendes e Dona Bequinha, guardarei com carinho as melhores
lembranças.*

Agradecimentos

A Deus, meu alicerce e apoio em momentos difíceis, um guia nessa minha jornada.

Agradecer à minha família pelo apoio incondicional que me deram, especialmente aos meus pais, Maria Ivoneide e José Pedro, meus avós, seu Juarez e dona Domingas, e meus irmãos, Júnior, Jean e Rayssa.

Não posso deixar de agradecer ao meu orientador, Prof. Dr. Luis Rivero, por toda a paciência, preocupação, empenho e sentido prático com que sempre me orientou na minha pesquisa e em todos os trabalhos que realizei durante as atividades do mestrado.

Ao meu coorientador Prof. Dr. Davi Viana, muito obrigado pela ajuda e pelas brilhantes considerações que me guiaram ao longo do mestrado.

Gostaria também de agradecer a banca examinadora desta pesquisa, o Prof. Dr. Anselmo Cardoso de Paiva e o Prof. Dr. Sérgio Castelo Branco Soares, por aceitarem ao convite para desempenhar este papel, dispondo de seu tempo e conhecimento para analisar este trabalho.

À Universidade Federal do Maranhão e ao Programa de Pós Graduação em Ciência da Computação, aos professores, a coordenação e funcionários pelo apoio durante o mestrado.

À CAPES pelo apoio financeiro ao longo do mestrado.

Ao Ivonildo, ao Professor Waldemar, e novamente o Professor Sérgio, da Universidade Federal de Pernambuco, pelas colaborações essenciais para conclusão deste trabalho.

Aos colegas do laboratório Dexter pela ajuda durante a minha pesquisa, especialmente ao Kastney e o Raimundo.

A todos os participantes dos estudos realizados na pesquisa, pela disposição e tempo despendido. Aos especialistas sobre LGPD e outros colaboradores que durante a pesquisa e publicações de trabalhos acadêmicos, forneceram informações importantes e apoio técnico.

"As verdadeiras recompensas são sempre proporcionais ao esforço e aos sacrifícios feitos."

(Nikola Tesla)

Resumo

A Lei Geral de Proteção de Dados (LGPD) foi criada para regulamentar a privacidade e tratamento de dados pessoais no Brasil. Embora tenha se tornado aplicável em 2020, várias equipes de desenvolvimento de software ainda não sabem quais atributos de qualidade são necessários para que um sistema cumpra essa lei e evite penalidades legais e monetárias. Além disso, ainda não há na literatura checklists específicos para verificação dos critérios de qualidade relacionados à LGPD. Nesta dissertação de mestrado é proposto um checklist de inspeção para avaliar os sistemas computacionais quanto à sua aderência à LGPD, chamado de LGPD-CHECK. A proposta é baseada na identificação dos atributos de qualidade da própria lei LGPD, e também de artigos que descrevem o impacto da lei no desenvolvimento de sistemas de software brasileiro e de sistemas de software às leis de outros países, como a GDPR. O checklist de inspeção contém um total de 56 atributos distribuídos em categorias, tais como: transparência, direitos legais, segurança, consentimento e responsabilidade, divididos em itens obrigatórios e itens recomendáveis. Em uma aplicação prática na indústria, o checklist de inspeção foi utilizado por profissionais que trabalham com desenvolvimento de software, para caracterizar e verificar a sua viabilidade de uso. Os participantes realizaram uma inspeção com o checklist, em um Instituto de Inovação Privado, em um sistema computacional real, que está implantado em pequenas e médias empresas de vários estados do Brasil, realizando o tratamento e coleta de dados de sensores instalados nos equipamentos industriais, onde era de suma importância a realização de uma avaliação da adequação à LGPD. Os profissionais que atuaram como inspetores, identificaram 42 defeitos que desrespeitam à LGPD, onde os inspetores obtiveram 54,16% de eficácia e uma eficiência média (defeitos por hora) de 14,79. Os resultados mostram evidências iniciais que o checklist proposto é viável para uso, útil, fácil de usar, e por fim, cumpre seu objetivo na identificação de defeitos e avaliação da aderência do sistema à LGPD. Além disso, os participantes da aplicação prática na indústria relataram que o checklist é completo, mas demanda um pouco de esforço mental, enquanto sugeriram que o mantenha sempre atualizado em detrimento da lei. Por fim, a pesquisa ainda apresenta uma versão adicional do checklist de inspeção, para que os titulares de dados possam avaliar a adequação do seu ponto de vista. Desse modo, pretende-se fornecer apoio as organizações e engenheiros de software, um mecanismo confiável, robusto e apropriado para detecção de defeitos e auxiliar na adequação dos sistemas computacionais à LGPD.

Palavras-chave: Checklist de Inspeção, Sistemas Computacionais, Lei Geral de Proteção de Dados.

Abstract

The General Data Protection Law (LGPD) was created to regulate the privacy and processing of personal data in Brazil. Although it became applicable in 2020, many software development teams still do not know what quality attributes are required for a system to comply with this law and avoid legal and monetary penalties. In addition, there are still no specific checklists in the literature to verify the quality criteria related to LGPD. In this master's thesis, an inspection checklist is proposed to evaluate computer systems regarding their adherence to LGPD, called LGPD-CHECK. The proposal is based on the identification of the quality attributes of the LGPD law itself, and also of articles that describe the impact of the law on the development of Brazilian software systems and software systems to the laws of other countries, such as the GDPR. The inspection checklist contains a total of 56 attributes distributed in categories such as: transparency, legal rights, security, consent and responsibility, divided into mandatory items and recommended items. In a practical application in the industry, the inspection checklist was used by professionals who work with software development, to characterize and verify its feasibility of use. The participants carried out an inspection with the checklist, in a Private Innovation Institute, in a real computer system, which is implemented in small and medium-sized companies in several states of Brazil, performing the treatment and collection of data from sensors installed in industrial equipment, where it was of paramount importance to carry out an assessment of compliance with the LGPD. The professionals who acted as inspectors identified 42 defects that disrespect the LGPD, where the inspectors obtained 54.16% of effectiveness and an average efficiency (defects per hour) of 14.79. The results show initial evidence that the proposed checklist is viable for use, useful, easy to use, and finally, it fulfills its objective in identifying defects and evaluating the system's adherence to the LGPD. In addition, the participants of the practical application in the industry reported that the checklist is complete, but requires a little mental effort, while they suggested to always keep it up to date at the expense of the law. Finally, the survey also presents an additional version of the inspection checklist, so that data subjects can assess the adequacy of their point of view. In this way, it is intended to provide support to organizations and software engineers, a reliable, robust and appropriate mechanism for detecting defects and assisting in the adequacy of computer systems to the LGPD.

Keywords: Inspection Checklist, Computer Systems, General Data Protection Law.

Lista de ilustrações

Figura 1.1 – Metodologia aplicada na pesquisa	20
Figura 2.1 – Revisão sistemática e revisão informal	30
Figura 3.1 – Atributos da Lei 13.709/2018	35
Figura 4.1 – Processo de Inspeção do <i>checklist</i>	58
Figura 4.2 – Gráfico dos Itens Obrigatórios do <i>checklist</i>	60
Figura 5.1 – Resultados sobre facilidade de uso percebida (FU)	69
Figura 5.2 – Resultados sobre utilidade percebida (U)	70
Figura 5.3 – Resultados sobre intenção de uso futuro percebida (IU)	70
Figura 6.1 – Itens Obrigatórios do Titular de Dados	80

Lista de tabelas

Tabela 2.1 – Formulário de extração	24
Tabela 2.2 – Relação da quantidade de artigos após aplicação dos respectivos filtros	25
Tabela 2.3 – Tabela com resultados da revisão.	26
Tabela 2.4 – Tabela com resultado da revisão informal.	30
Tabela 3.1 – Modelo da extração de atributos da Lei Federal 13.709/2018	36
Tabela 3.2 – Exemplos de artigos relacionados à LGPD na literatura	37
Tabela 3.3 – Exemplo da Análise e seleção de atributos	38
Tabela 3.4 – <i>Checklist</i> a partir da combinação de atributos identificados - Versão 1	39
Tabela 4.1 – Transformação dos itens antigos para segunda versão do <i>checklist</i>	48
Tabela 4.2 – Checklist de Inspeção Completo para LGPD - Versão 2	49
Tabela 4.3 – Defeitos Identificados Pelo Checklist durante uma inspeção	60
Tabela 5.1 – Objetivo do estudo da técnica de checklist	62
Tabela 5.2 – Caracterização dos participantes	63
Tabela 5.3 – Questionário de avaliação da técnica pós-inspeção	65
Tabela 5.4 – Resultados Quantitativos Individuais	68
Tabela 6.1 – Transformação do <i>checklist</i> para versão do Titular de Dados	77
Tabela 6.2 – Versão do <i>checklist</i> de inspeção aplicado ao Titular de Dados	78
Tabela A.1 – Formulário com o termo de consentimento e o questionário de caracterização	91
Tabela B.1 – Formulário de Pós Inspeção	92
Tabela C.1 – Formulário com as questões discursivas do grupo focal	94
Tabela D.1 – Listagem de Defeitos	95
Tabela E.1 – Checklist de Inspeção Completo para LGPD - Versão 2	103

Lista de abreviaturas e siglas

ACM	<i>Association for Computing Machinery</i>
FU	<i>Facilidade de Uso Percebida</i>
GDPR	<i>General Data Protection Regulation</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IU	<i>Intenção de Uso Futuro Percebida</i>
LGPD	<i>Lei Geral de Proteção de Dados Brasileira</i>
PDF	<i>Portable Document Format</i>
U	<i>Utilidade de Uso Percebida</i>

Sumário

1	INTRODUÇÃO	15
1.1	Problema e Justificativa	17
1.2	Objetivo Principal e Específicos	18
1.3	Metodologia	19
1.4	Organização do Documento	21
2	REVISÃO DA LITERATURA	22
2.1	Planejamento do Protocolo da Revisão	22
2.1.1	Questões de Pesquisa	22
2.1.2	Termos de Busca	23
2.1.3	Fontes de Busca	23
2.1.4	Critérios de Seleção	24
2.2	Execução da Revisão	25
2.3	Resultados e Discussão	26
2.3.1	Q1: Quais os atributos de qualidade da LGPD ou GDPR para aderência dos sistemas computacionais encontrados na Literatura?	31
2.3.2	Q2: Quais Técnicas de Avaliação para LGPD ou GDPR encontrados na Literatura?	32
2.4	Trabalhos Relacionados Posteriores	33
2.5	Considerações Finais	34
3	CRIAÇÃO DO <i>CHECKLIST</i> DE INSPEÇÃO LGPD	35
3.1	O Processo de Desenvolvimento do Checklist	35
3.1.1	Versão inicial do <i>Checklist</i> de Inspeção à LGPD	39
3.1.2	Prova de Conceito	45
3.2	Considerações Finais	46
4	REFINAMENTO E CRIAÇÃO DO ARTEFATO DO <i>CHECKLIST</i>	47
4.1	Segunda Versão do <i>Checklist</i>	48
4.2	O Processo de Inspeção Usando o <i>Checklist</i>	58
4.3	Considerações Finais	61
5	APLICAÇÃO DO CHECKLIST NA INDÚSTRIA	62
5.1	Descrição e Objetivo	62
5.1.1	Participantes do Estudo	63
5.1.2	Materiais Utilizados	64

5.1.3	Execução e Coleta da Inspeção do Sistema Computacional	66
5.2	Resultados da Avaliação do <i>Checklist</i> de Inspeção	67
5.2.1	Análise Quantitativa	67
5.2.2	Análise com o Modelo TAM	69
5.2.3	Análise Qualitativa	71
5.2.4	Limitações e Ameaças à Validade	74
5.3	Considerações Finais	75
6	REFINAMENTO DO <i>CHECKLIST</i> A PARTIR DOS RESULTADOS DO ESTUDO	76
6.1	Sugestões implementadas para o checklist LGPD-CHECK	76
6.2	Versão do <i>Checklist</i> para o Titular de Dados	77
6.3	Considerações Finais	80
7	CONCLUSÃO E TRABALHOS FUTUROS	82
7.1	Trabalhos Futuros	84
7.2	Contribuições	84
	REFERÊNCIAS	86
	APÊNDICES	90
	APÊNDICE A – QUESTIONÁRIO DE CARACTERIZAÇÃO E CONSENTIMENTO	91
	APÊNDICE B – QUESTIONÁRIO DE PÓS-INSPEÇÃO	92
	APÊNDICE C – QUESTIONÁRIO DO GRUPO FOCAL	94
	APÊNDICE D – LISTA COMPLETA DE DEFEITOS ENCONTRADOS NA INSPEÇÃO APLICADO NA INDÚSTRIA	95
	APÊNDICE E – CHECKLIST DE INSPEÇÃO LGPD-CHECK - VERSÃO FINAL	103

1 Introdução

A Lei Federal brasileira n.º 13.709/2018 denominada Lei Geral de Proteção de Dados Pessoais (LGPD) impõe novos requisitos de proteção de dados sobre empresas, que devem demonstrar que seus sistemas e negócios estão em conformidade, considerando a necessidade de atender aos requisitos de forma eficaz ([MUNCINELLI et al., 2020](#)). Em um mundo cada vez mais conectado e orientado por dados, o objetivo final da lei é promover o processamento responsável e justo de dados pessoais pelas empresas e proteger o direito dos usuários à privacidade ([DUARTE et al., 2020](#)).

Com o advento da LGPD, o Brasil integrou o grupo de países que possuem o seu próprio regulamento de proteção de dados pessoais, fundamentada nos princípios do respeito à privacidade, defesa do consumidor, não violação da intimidade e, principalmente, os direitos humanos ([BRASIL, 2018](#)). A lei estabelece regras mais seguras e confiáveis para o processamento e tratamento de dados, além de garantir maior transparência e privacidade aos usuários ([DUARTE et al., 2020](#)). Qualquer operação de tratamento realizada por pessoa natural ou pessoa jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, é regulamentado pela lei ([BRASIL, 2018](#)).

Outro grande marco na área de segurança e privacidade de dados, foi a criação do Regulamento Geral de Proteção de Dados Europeu GDPR em 2016, criando regras unificadas e consistentes em toda União Europeia ([RINGMANN; LANGWEG; WALDVOGEL, 2018](#)). A lei europeia, por ser pioneira no assunto, influenciou em diversas regulamentações de países, inclusive a brasileira, onde, vários princípios da GDPR são semelhantes ou se complementam à LGPD, com algumas diferenças sutis, que obedecem ao contexto em que cada uma se encontra, porém, ambas vieram para dar mais segurança na relação entre os usuários e as organizações ([LORENZON, 2021](#)).

Atender os critérios da lei se torna importante, pois sem a regulamentação, aumenta a possibilidade de abuso na coleta e no processamento de dados pessoais, assim também como a interferência de vários outros órgãos especializados para opinar sobre a utilização dos dados, o que pode ocasionar transtornos para os usuários finais desses tipos de sistemas ([SOUZA et al., 2020](#)). Os responsáveis pelo tratamento de dados pessoais dos usuários, deverão formular novas políticas para se adequarem à lei, estabelecendo condições para a organização em relação ao seu regimento de funcionamento, além de implementações de normas de segurança, padrões técnicos, obrigações específicas para os envolvidos no tratamento de dados, ações educativas para seus empregados e supervisão de riscos do negócio ([PIURCOSKY et al., 2019](#)).

Apesar da importância da lei para o desenvolvimento de sistemas de qualidade, (PIURCOSKY et al., 2019) identificaram que muitas organizações não estão preparadas para atender ao regulamento brasileiro, existindo um número baixo de engenheiros de software que demonstraram conhecimento da lei e um número elevado de engenheiros de software que não sabem da existência da mesma. As organizações precisam conseguir respeitar todas as diretrizes da lei de proteção de dados, e o não cumprimento coloca as empresas sujeitas a punições administrativas, podendo levar a penalidades financeiras (SOUZA et al., 2020). Além das punições, a inconformidade com o regulamento pode trazer vários problemas para a sociedade, como os vazamentos de dados de usuários, violação dos direitos do consumidor, proibição de coleta e tratamento de dados pessoais, entre outros (MACHADO et al., 2019).

Como é apresentado no trabalho de (FERRÃO et al., 2021), que realizaram uma pesquisa das organizações brasileiras, tanto públicas quanto privadas, em relação à sua adequação à LGPD, a partir da percepção de 105 profissionais de tecnologia da informação que atuam nessas organizações. Os resultados revelaram que 16,3% das organizações, não estabeleceram um procedimento para verificar se os princípios da LGPD estão sendo respeitados, 20% das organizações não estabeleceram um processo de comunicação aos titulares de dados pessoais, sobre as possíveis violações de dados, e apenas 27% das organizações processam dados pessoais de acesso público com base na boa-fé e nos princípios da LGPD. Por sua vez, (CANEDO et al., 2021) investigaram a percepção de membros de equipes de desenvolvimento ágil de software de diferentes organizações, quanto ao impacto que a LGPD terá nas atividades do processo de desenvolvimento de software. Os resultados revelam que as equipes ágeis conhecem os conceitos relacionados à legislação de privacidade de dados, mas não utilizam as técnicas propostas na literatura para realizar a elicitação de requisitos de privacidade. Além disso, as equipes ágeis enfrentam problemas com especificações de requisitos de software desatualizadas e falta de conhecimento das partes interessadas em relação à privacidade de dados.

Entretanto, avaliar e classificar um software como sendo de qualidade não é uma tarefa trivial (NETO; FREITAS, 2011). Segundo (BARTIÉ, 2002) define qualidade de software como um processo que tem como foco todas as etapas e artefatos produzidos visando garantir a conformidade de processos e produtos, prevenindo e eliminando defeitos. Para (PRESSMAN; MAXIM, 2016) define que a qualidade de software é uma conformidade com os requisitos funcionais e de desempenhos explicitamente declarados, padrões de desenvolvimento explicitamente documentados e características implícitas, esperadas em todo software desenvolvido profissionalmente.

A qualidade é normalmente tão influenciada pelas decisões administrativas quanto pelas decisões técnicas, até mesmo as melhores práticas de engenharia de software podem ser subvertidas por decisões de negócios inadequadas e ações questionáveis de gerenciamento

de projeto (PRESSMAN; MAXIM, 2016). A inspeção deve verificar a consistência e a completude dos artefatos de software em revisão e certificar-se de que os padrões de qualidade foram seguidos (NETO; FREITAS, 2011). O intuito de toda inspeção técnica é encontrar erros e revelar problemas que teriam um impacto negativo sobre o software a ser entregue (PRESSMAN; MAXIM, 2016). O checklist é uma técnica de inspeção, usada como uma ferramenta de qualidade que apresenta as diretrizes para a leitura de um determinado artefato visando encontrar defeitos, e segundo (LAITENBERGER; BEIL; SCHWINN, 2002), o checklist é a técnica de leitura mais empregada para a detecção de defeitos no contexto de inspeção de software.

Nesse contexto, as empresas necessitarão de significativas modificações nos seus processos de coleta e armazenamento de dados, além de muitas alterações na gestão em segurança da informação e na qualidade do software. Portanto, são necessárias novas investigações sobre como apoiar engenheiros de software na aplicação da lei e o impacto de tal aplicação nas empresas públicas e privadas.

1.1 Problema e Justificativa

A falta de antecedentes e estudos adequados da lei de proteção de dados apresenta um desafio para as equipes de desenvolvimento de softwares (BERNARDI et al., 2020), responsáveis por identificar os requisitos e atributos de qualidade relevantes, para assegurar a conformidade dos sistemas computacionais com as novas diretrizes definidas. Além disso, a interpretação de textos legais pode ser desafiador visto que a lei descreve direitos e obrigações em linguagem jurídica complexa e, às vezes, ambígua e com definições específicas de domínio (FERNANDES, 2018).

Essa pesquisa é motivada pela necessidade de tecnologias que possam ser empregadas por equipes de desenvolvimento de softwares que desejem avaliar adequação dos seus sistemas computacionais em relação à lei de proteção de dados. Nesse sentido, a questão de pesquisa desse trabalho é:

“Como apoiar equipes de desenvolvimento de software na avaliação da adequação à lei geral de proteção de dados brasileira?”

Por ser um regulamento novo, no contexto de avaliação, há uma escassez de trabalhos relacionados a LGPD. Portanto, são necessárias novas investigações sobre como apoiar engenheiros de software na aplicação da Lei e o impacto de tal aplicação nas empresas. Ainda sim, para esta pesquisa destacou-se o estudo (ROJAS, 2020) que avalia uma instituição de ensino através de entrevistas tendo como base um questionário. Porém, o questionário não cobre todos os aspectos da lei LGPD, possuindo apenas 13 questões,

sendo uma limitação para avaliar com cuidado todo um sistema de software para aderir à lei de proteção de dados.

Surge a necessidade de criação de uma técnica capaz de avaliar a aderência dos sistemas computacionais que englobe todos os requisitos que a LGPD determina. Diante desses fatos, a hipótese nesse trabalho é desenvolver um *checklist* de inspeção para detectar inconformidades nos sistemas computacionais. Pretende-se em particular, ajudar equipes de desenvolvimento de software que podem não ter acesso a recursos legais para avaliarem se os seus sistemas atendem os requisitos sugerido na LGPD.

No que concerne o processo de desenvolvimento e qualidade do software, a técnica de inspeção têm se mostrado uma abordagem de baixo custo (KALINOWSKI; SPÍNOLA; TRAVASSOS, 2004), onde possui um processo rigoroso e bem definido, que melhora a qualidade de software, sendo uma técnica eficiente na detecção de defeitos, reduzindo retrabalho. A técnica de *checklist* possui flexibilidade na sua elaboração, oferecendo um conjunto de questões, previamente formuladas, que os inspetores devem responder ao ler o documento, e que no final acabam adquirindo maior experiência e conhecimento melhor sobre as regras estabelecidas durante o próprio processo de inspeção (MELO, 2009).

Portanto, a avaliação da conformidade com a LGPD é uma necessidade, e o checklist de inspeção além de verificar as inconformidades com a lei, também impacta nos negócios da empresa, forçando a melhorar as práticas de segurança dos sistemas, evitando problemas legais, financeiros e de reputação, principalmente em empresas que operam em vários estados do Brasil e queiram expandir seus negócios nacionalmente e fora do país.

1.2 Objetivo Principal e Específicos

Este trabalho de mestrado tem como objetivo principal, apoiar o processo de desenvolvimento de software, identificando atributos de qualidade para propor um checklist de inspeção, para avaliação da aderência dos sistemas computacionais as diretrizes da lei geral de proteção de dados pessoais brasileira. Para atingir esse objetivo geral, os seguintes objetivos específicos foram definidos:

- Realizar uma revisão sistemática da literatura sobre as técnicas de avaliação e dos atributos de qualidade da lei geral de proteção de dados brasileira e da europeia;
- Criar um *checklist* de inspeção para a avaliação da aderência de sistemas computacionais à LGPD;
- Propor um artefato que facilite a aplicação da técnica, automatizando o processo de inspeção.

- Aplicar o checklist de inspeção na indústria de desenvolvimento de software, para verificar a sua viabilidade;
- Avaliar e ajustar os itens de verificação e do artefato do *checklist* proposto com base nos resultados da aplicação prática na indústria.

Em resumo, considerando esses objetivos, este trabalho propõe a criação de um novo checklist de inspeção para avaliar sistemas computacionais na esfera da LGPD brasileira, através: (a) da análise de atributos de qualidade extraídos da lei federal de proteção de dados 13.709/2018; (b) da análise de atributos identificados através de um mapeamento sistemático em veículos de publicação da área de computação; e (c) da análise de atributos identificados através de uma revisão informal no Google acadêmico visando identificar trabalhos em outras áreas. Além disso, apresenta uma aplicação no contexto real da indústria de software, em um instituto de inovação privado, com profissionais na área de tecnologia da informação que atuam nessa organização, com objetivo de verificar se os resultados do uso do *checklist* são viáveis, oferecendo informações sobre a eficiência e eficácia da técnica.

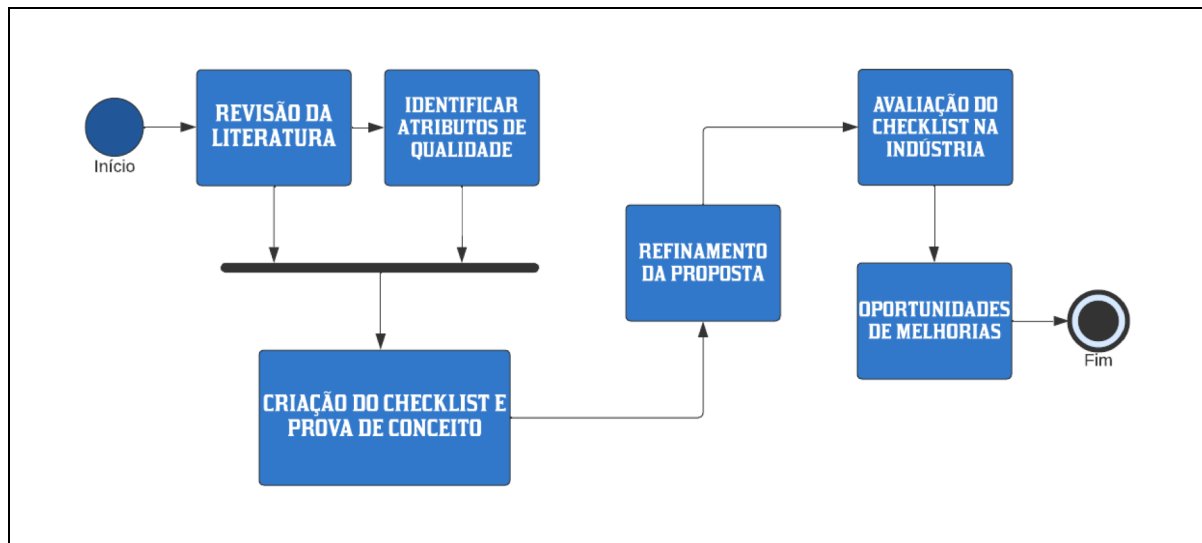
1.3 Metodologia

A principal contribuição que esta proposta de pesquisa de mestrado almeja alcançar é conceber um mecanismo capaz de avaliar os sistemas computacionais para aderência à lei geral de proteção de dados pessoais LGPD. Para tanto, foi projetada uma metodologia guiada por adaptações de trabalhos de (RINGMANN; LANGWEG; WALDVOGEL, 2018) sobre proteção de dados e (KALINOWSKI; SPÍNOLA; TRAVASSOS, 2004) na área de experimentação em engenharia de software, onde indicam a realização de uma revisão da literatura e estudos exploratórios, para desenvolver uma proposta inicial de uma tecnologia para a inspeção de software. A metodologia será descrita a seguir, e pode ser visualizada na Figura 1.1:

(A) Revisão da Literatura e Trabalhos Relacionados: A ideia inicial é levantar o estado da arte sobre a LGPD no Brasil, para identificar possíveis técnicas de avaliação, atributos que as empresas precisam incorporar para adequarem seus sistemas de software a esta lei. Por se tratar de uma lei recente e a escassez de trabalhos na área, por esse motivo estendeu-se a revisão para lei de proteção de dados similares a LGPD, nesse caso, a lei europeia GDPR, para complementar e usar como uma consulta a mais de dados para esta pesquisa.

(B) Identificação e Análise de Atributos: Nesta etapa, em resumo, foi realizado os seguintes passos: (i) análise de atributos de qualidade extraídos da lei federal de proteção de dados 13.709/2018; (ii) análise de atributos identificados através de um mapeamento

Figura 1.1 – Metodologia aplicada na pesquisa



sistemático em veículos de publicação da área de computação; e (iii) da análise de atributos identificados através de uma revisão informal no Google acadêmico visando complementar o mapeamento.

(C) Desenvolvimento do *Checklist* e Prova de Conceito: Para desenvolver o *checklist* de inspeção, foi realizado anteriormente a identificação dos atributos da análise (lei e de artigos da literatura), depois disso, foram agrupados os atributos semelhantes extraídos das análises, e por último transformação dos atributos em itens de um *checklist*, em formato de perguntas, selecionando as melhores descrições. Para validar do ponto de vista prático, é realizado uma prova de conceito, aplicando o *checklist* para encontrar defeitos em um sistema de software na web. Para comparação, buscou-se na literatura estudos que realizasse a mesma avaliação, de modo a comparar os resultados, analisando o seu desempenho.

(D) Refinamento da Proposta: O próximo passo é realizar o refinamento da proposta, aplicando as devidas recomendações, correções dos erros encontrados, onde novos atributos serão identificados ou atualizados, fornecendo maior confiabilidade. Além disso, a fim de automatizar o processo de inspeção dos sistemas e aplicação da proposta, será implementado um artefato em formato de planilha. Esse artefato dará o suporte para efetuar a detecção de defeitos pelo *checklist*, gerar relatórios e gráficos de conformidade, fornecer o grau de aderência do sistema avaliado, e planos para mitigação e avaliação de risco.

(E) Aplicação prática do *Checklist*: Estudo de uma aplicação na indústria para levantar mais informações e avaliar a viabilidade do *checklist*, com profissionais que atuam no desenvolvimento de software e estão começando a familiarizar com aplicação da lei de proteção de dados LGPD, para que assim, possa dar um feedback da proposta desta

pesquisa.

(F) Oportunidade de melhoria - Refinamento II: Conforme os resultados obtidos na avaliação do checklist na indústria, conceber um novo refinamento da técnica e realizar correções no checklist, adicionando características que melhoram a avaliação dos sistemas computacionais à LGPD.

1.4 Organização do Documento

Esta dissertação de mestrado apresenta um modo de apoiar equipes que desejem adequar seus projetos a LGPD. Durante a execução desta pesquisa são mostrados os resultados de cada etapa executada; o restante deste documento está organizado da seguinte forma:

Capítulo 2 - Revisão da literatura: O capítulo discute os resultados da revisão da literatura para identificar técnicas de inspeção existentes que podem ser aplicadas para a avaliação da adequação a lei de proteção de dados ou atributos de qualidade que a lei determina.

Capítulo 3 - Criação do *Checklist* de inspeção LGPD: O capítulo apresenta a criação do *checklist* de inspeção específico para LGPD, baseado na revisão da literatura. Além disso, é apresentada uma aplicação prática através de uma prova de conceito em um sistema web.

Capítulo 4 - Refinamento e Criação do Artefato do Checklist Com base nos resultados da prova de conceito, e de comentários de especialistas da área de engenharia de software, é realizado um refinamento do *checklist*, gerando uma segunda versão. Também é construído um artefato para automatizar o preenchimento e o processo de inspeção com o *checklist*.

Capítulo 5 - Aplicação do *Checklist* na Indústria: O capítulo apresenta o planejamento e execução de um estudo de aplicação na indústria para avaliar o desempenho e a aceitação dos mecanismos desenvolvidos nesta pesquisa, ou seja, a técnica e os artefatos gerados para o *checklist* LGPD. Além de apresentar uma discussão dos resultados obtidos no estudo.

Capítulo 6 - Refinamento do *Checklist* a partir dos Resultados do Estudo: No capítulo, são apresentadas algumas oportunidades de melhorias e alguns refinamentos para o *checklist* da LGPD. Além disso, é apresentada uma versão do checklist específico para o titular de dados.

Capítulo 7 - Conclusão e Trabalhos Futuros: O capítulo apresenta a conclusão desta pesquisa, e as principais contribuições. Além disso, é apresentada uma discussão sobre as perspectivas futuras que podem ser realizadas de modo a continuar esta pesquisa.

2 Revisão da Literatura

Entende-se a necessidade de estratégias claras, que incluem aspectos legais, tecnológicos e de gestão para auxiliar profissionais e empresas a pensarem sobre qual estratégia seguir para garantir adequação à LGPD (MUNCINELLI et al., 2020). Nesse contexto, decidimos realizar uma busca exploratória manual, para compreender o nível e quantidade de pesquisas sobre o tema.

Um dos trabalhos encontrados foi o de (CELIDONIO; NEVES; DONÁ, 2020) que apresenta o resultado de um mapeamento dos requisitos listados na LGPD, em uma instituição financeira no Brasil. Os autores do trabalho realizaram um diagnóstico e recomendações de ações necessárias para adequar uma empresa à LGPD. Porém, no documento não há uma descrição detalhada sobre os requisitos de software pertinentes à LGPD. Por sua vez, o trabalho de (MORTE et al., 2020) se propõe a analisar aspectos técnicos a respeito da utilização da tecnologia de registro distribuído DLT, para o tratamento de dados conforme a LGPD. Diversos aspectos foram analisados para trazer recomendações de como esta tecnologia DLT pode ser bem empregada no tratamento de dados pessoais segundo a legislação.

Os trabalhos citados acima apresentam resultados relacionados com o processo de desenvolvimento de software considerando a proteção de dados, encontrados através de uma busca inicial pelo tema. No entanto, poucos são os trabalhos específicos relacionados à LGPD brasileira, especificamente na definição detalhada de atributos de qualidade que a lei determina. A seguir, é apresentado o levantamento de trabalhos específicos para este fim, visando realizar uma pesquisa completa nas principais bases de dados nacionais e internacionais da computação e áreas relacionadas.

2.1 Planejamento do Protocolo da Revisão

Nessa seção, é descrito o planejamento do protocolo de estudo secundário sobre técnicas de avaliação e atributos de qualidade relacionados à adesão a LGPD. Isso inclui: as questões de pesquisa, as strings de busca, as bases de dados e os critérios de seleção de artigos. A seguir, são detalhadas as partes desse protocolo.

2.1.1 Questões de Pesquisa

O objetivo dessa revisão é levantar o estado da arte em relação às heurísticas de avaliação para adequação dos sistemas computacionais a LGPD e os seus atributos de qualidade. Tais metodologias consideram *checklists* de inspeções de software, heurísticas de

avaliações e diretrizes de avaliações, além de atributos, requisitos ou princípios da LGPD. A necessidade da realização do presente estudo secundário é justificada pela ausência de um estudo anterior que respondesse as seguintes questões (SQ):

- **Q1:** *Quais os atributos de qualidade da LGPD ou GDPR para aderência dos sistemas computacionais encontrados na Literatura?*
- **Q2:** *Quais Técnicas de Avaliação para LGPD ou GDPR encontrados na Literatura?*

2.1.2 Termos de Busca

Serão apresentados os termos utilizados para montar a *String* de busca. Logo após definir as questões de pesquisa, é preciso definir uma *String* de busca que englobe publicações científicas que tratem de heurísticas de avaliação para adequação dos sistemas computacionais a LGPD e de atributos de qualidade. Para obter mais publicações relevantes para essa revisão da literatura, foram realizadas buscas tanto com termos em inglês quanto português.

Com alguns sinônimos e palavras chaves derivados de trabalhos (CABREJOS; VIANA; SANTOS, 2018) e (MUNCINELLI et al., 2020) foi aplicada a seguinte string de busca em inglês: (((("Technique"OR "Approach"OR "Model"OR "Method"OR "Framework"OR "Instrument") AND ("Evaluation"OR "Assessment"OR "Testing"OR "Measurement"OR "Tracking"OR "Recognition"OR "Inspection")) OR ("Attribute"OR "Requirement"OR "Principle"OR "Feature"OR "Characteristic"OR "Restriction")) AND ("LGPD"OR "RGPD"OR "GDPR"OR "GDPL"OR "General data protection law"OR "General data protection regulation"))).

Já para os termos em português, a *String* de busca é apresentado a seguir: (((("Técnica"OR "Abordagem"OR "Modelo"OR "Método"OR "Framework"OR "Instrumento") AND ("Avaliação"OR "Teste"OR "Inspeção")) OR ("Atributo"OR "Requisito"OR "Princípio"OR "Característica"OR "Restrição")) AND ("LGPD"OR "RGPD"OR "GDPR"OR "GDPL"OR "Lei geral de proteção de dados"OR "Regulamento Geral de Proteção de dados"))).

Para todas as bases de dados digitais utilizadas, a string de busca padrão foi revisada conforme a particularidade ou limitação de sua máquina de busca, visando observar a importância dos termos usados e a pertinência das publicações retornadas.

2.1.3 Fontes de Busca

Essa revisão utilizou o Portal Capes¹ para realizar as buscas de artigos publicados na literatura nas principais bases de artigos. As publicações analisadas foram retiradas das

¹ <www.periodicos.capes.gov.br> O Portal Capes, mantido pelo Governo Federal Brasileiro, concede acesso a publicações científicas presentes em grandes bibliotecas digitais científicas privadas.

principais bibliotecas digitais relacionadas à computação: *Scopus Digital Library*, *IEEE Xplore Digital Library* e *ACM Digital Library* foram as bases de dados de computação.

2.1.4 Critérios de Seleção

Os trabalhos considerados nesse levantamento bibliográfico são publicações que passaram por uma revisão, publicados em eventos científicos e/ou periódicos. Para que fossem selecionadas as publicações com maior representatividade que respondam às questões de pesquisas desta revisão, foram definidos os seguintes critérios para incluir ou excluir uma publicação.

Critérios de inclusão (CI) (Todos precisam ser atendidos):

- **CI1:** Trabalhos que descrevem atributos de qualidade (na forma de heurísticas, regras, requisitos, sugestões) sugeridos pela lei LGPD ou GDPR;
- **CI2:** Trabalhos que descrevem técnicas de avaliação (na forma de heurísticas) sugeridos pela lei LGPD ou GDPR;.

Critérios de exclusão (CE):

- **CE1:** trabalhos indisponíveis para download ou leitura;
- **CE2:** trabalhos a partir de 2016, uma vez que a GDPR precursora foi criada neste ano.

Com o objetivo de facilitar a etapa de execução da revisão, foi criado um formulário de extração de dados, apresentado na Tabela 2.1, utilizado para conduzir a seleção dos artigos para a pesquisa. O formulário possui perguntas e suas respectivas descrições, conforme sugerido por [Cabrejos, Viana e Santos \(2018\)](#). O formulário de extração é utilizado para auxiliar a análise das informações vindas das publicações que serão consideradas no resultado final.

Tabela 2.1 – Formulário de extração

Campos	Descrições
Titulo	Escrever o nome do artigo pesquisado
Autor	Escrever o nome do autor do artigo
Nome e descrição da Técnica	Escrever o nome e a metodologia para realizar a avaliação.
Atributos Extraídos	Escrever os atributos de qualidade extraídos dos artigos
Descrição dos Atributos	Escrever a descrição dos atributos de qualidade extraídos
Categoria dos Atributos	Escrever a categoria e sua descrição dos atributos

LGPD ou GDPR	Escrever sobre qual lei se trata
Ano	Escrever o ano de publicação do artigo pesquisado

2.2 Execução da Revisão

A revisão foi realizada por 3 participantes, onde um participante foi responsável pela execução da string de busca e na coleta dos artigos encontrados nas bases digitais, e eram posteriormente discutidos e analisados os resultados da busca, com os outros dois participantes. A obtenção dos artigos dessa pesquisa se sucedeu executando a *String* de busca nos motores de busca das bibliotecas digitais da *Scopus*, *IEEE* e *ACM* no período de Janeiro a Abril de 2021, a *String* retornou ao todo 36 publicações. A relação completa da quantidade de artigos está contida na Tabela 2.2.

Tabela 2.2 – Relação da quantidade de artigos após aplicação dos respectivos filtros

Biblioteca	Qtd. Geral	Duplicados	Título e Resumo	Leitura Completa	Atributos e Técnicas com Atributos
Scopus	804	695	233	40	26
IEEE	123	123	30	11	8
ACM	34	33	15	7	2
Total:	961	851	278	58	36

Ao todo, foram retornados 961 artigos. Os critérios de inclusão (I) e exclusão (E) foram aplicados, realizada a leitura do título e resumo, da leitura completa, assim como a retirada de duplicação de artigos. Após isso, foi selecionado apenas artigos com atributos bem definidos ou artigos com técnicas de avaliação que continham atributos também bem definidos, para realizar a correlação dos artigos referentes a GDPR com a LGPD. No final da busca, foram selecionados um total de 36 artigos, sendo 35 artigos sobre atributos de qualidade e técnicas de avaliação para GDPR e 1 artigo que apresenta atributos para LGPD.

Conforme descrito acima, durante o mapeamento sistemático foram procurados trabalhos específicos para a avaliação da LGPD. Vale ressaltar, no entanto, que como apenas um único trabalho foi identificado para este fim, foram selecionados principalmente trabalhos que apresentassem atributos de qualidade relacionados com a LGPD ou GDPR. Considerando que a LGPD é recente e que outras áreas diferentes da computação estão investigando o impacto da lei no desenvolvimento de sistemas computacionais, optou-se por realizar uma pesquisa informal e manual na base do Google Acadêmico para considerar

estes trabalhos. Após aplicar uma string de busca similar à aplicada no mapeamento sistemático, retirando os termos da GDPR, foram encontrados 8 artigos que apresentam atributos de qualidade para LGPD.

2.3 Resultados e Discussão

Com os resultados do mapeamento sistemático e da busca informal no Google Acadêmico foram identificados 44 artigos reportando atributos de qualidade no contexto da LGPD ou da GDPR. De modo geral, observa-se que há um interesse na identificação de atributos de qualidade relacionados à LGPD e GDPR. Além disso, não foi identificado nenhum checklist de avaliação específico para a LGPD, tornando uma ideia promissora a proposta de um novo checklist agregando os atributos identificados. A seguir, será apresentado o processo de desenvolvimento do checklist específico para avaliação da aderência de sistemas computacionais à LGPD.

A Tabela 2.3 mostra a lista dos conjuntos de artigos, com o modelo de extração de dados executados durante a revisão da literatura, buscando encontrar atributos de qualidade sobre aderência a LGPD, assim como técnicas de avaliação, e também sobre outras leis de proteção de dados, no caso, a GDPR.

Tabela 2.3 – Tabela com resultados da revisão.

Titulo	Autor	Atributo e/ou Técnicas	Lei de Proteção	Ano
Designing Privacy Preserving Data Sharing Middleware for Internet of Things	Sameera	Atributo de Qualidade	GDPR	2020
Bringing Privacy Control Back to Citizens: DISPEL – a Distributed Privacy Management Platform for the Internet of Things	Christoph Stach et. al	Atributo de Qualidade	GDPR	2020
A Privacy Safeguard Framework for a WebRTC/WoT-Based Healthcare Architecture	Saad EL Jaouhari and Ahmed Bouabdallah	Atributo de Qualidade	GDPR	2018
Ethical and normative challenges of identification in the Internet of Things	Sandra Wachter	Atributo de Qualidade	GDPR	2018

An Architectural View for Data Protection by Design	Laurens Sion et. al	Atributo de Qualidade, Técnica de Avaliação	GDPR	2019
Blockchain for Identity Management: The Implications to Personal Data Protection	Wie Liang Sim et.al	Atributo de Qualidade	GDPR	2019
On Compliance of Cookie Purposes with the Purpose Specification Principle	Imane Fouad et al.	Atributo de Qualidade	GDPR	2020
Robots and Transparency: The Multiple Dimensions of Transparency in the Context of Robot Technologies	Heike Felzmann et. al	Atributo de Qualidade, Técnica de Avaliação	GDPR	2019
GDPR Compliance Verification in Internet of Things	Masoud Barati et. al	Atributo de Qualidade, Técnica de Avaliação	GDPR	2021
Data protection by design in systems development: From legal requirements to technical solutions	Fredrik Blix et.al	Atributo de Qualidade	GDPR	2017
Ethical, legal and privacy considerations for adaptive systems	Manon Knockaert and Nathan De Vos	Atributo de Qualidade	GDPR	2020
Requirements for legally compliant software based on the GDPR	Sandra Dominique Ringmann et.al	Atributo de Qualidade	GDPR	2018
EU General Data Protection Regulation: Changes and implications for personal data collecting companies	Christina Tikkinen-Piri et. al	Atributo de Qualidade	GDPR	2017
Identification of the relationships between the stages of the data lifecycle and the principles of the brazilian general data protection	Gislaine Parra Freund	Atributo de Qualidade	LGPD - Brasil	2020

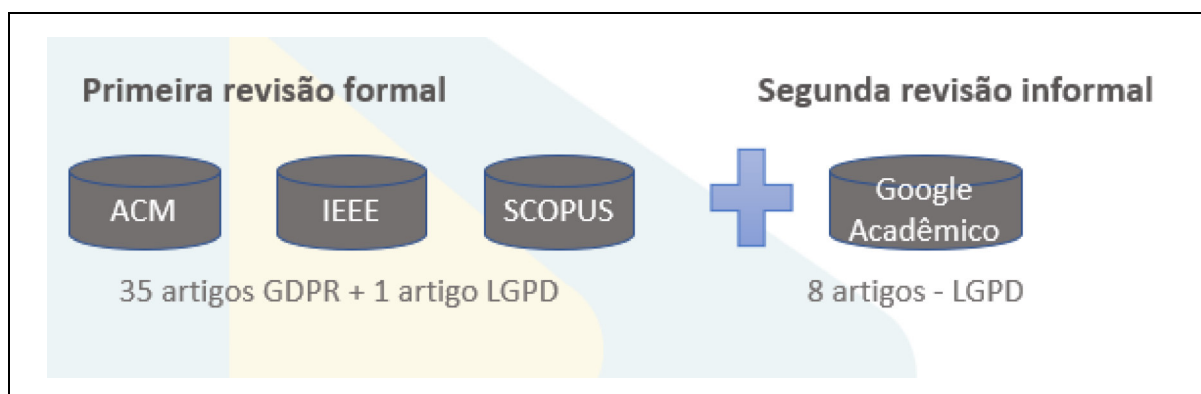
GDPR compliance: Proposed technical and organizational measures for cloud providers	Zafeiroula Georgiopoulou et.al	Atributo de Qualidade	GDPR	2020
Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers	Majid Hata-mian	Atributo de Qualidade	GDPR	2020
GDPR: What's in a year (and a Half)?	Ana Ferreira	Atributo de Qualidade	GDPR	2020
Making GDPR usable: A model to support usability evaluations of privacy	Johanna Johansen et.al	Atributo de Qualidade, Técnica de Avaliação	GDPR	2020
Developed Framework Based on Cognitive Computing to Support Personal Data Protection Under the GDPR	Soraya Sedkaoui e Dana Simian	Atributo de Qualidade	GDPR	2020
An Analysis of Blockchain and GDPR under the Data Lifecycle Perspective	Gislaine Parra Freund et. al	Atributo de Qualidade	GDPR	2020
From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance	Vasiliki Diamantopoulou et.al	Atributo de Qualidade	GDPR	2020
Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach	Jae Kyu Lee et.al	Atributo de Qualidade	GDPR	2020
Qualifying and measuring transparency: A medical data system case study	Dayana Spagnuolo et. al	Atributo de Qualidade	GDPR	2020
Security requirements identification and prioritization for smart toys	Luciano Gonçalves de Carvalho et.al	Atributo de Qualidade	GDPR	2020

An Edge Framework for the Application of Privacy Enhancing Technologies in IoT Communications	Immanuel Kunz et. al	Atributo de Qualidade	GDPR	2020
Development of GDPR - Compliant Software : Document Management System for HR Department	Emanuel Gonçalves et. al	Atributo de Qualidade	GDPR	2020
Compatibility of a security policy for a cloud-based healthcare system with the eu general data protection regulation (Gdpr)	Dimitra Georgiou * and Costas Lambrinoudakis	Atributo de Qualidade	GDPR	2020
Automatic assessment of privacy policies under the gdpr	David Sánchez et.al	Atributo de Qualidade, Técnica de Avaliação	GDPR	2021
An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance	Vasiliki Diamantopoulou et.al	Atributo de Qualidade	GDPR	2018
“Appropriate technical and organizational measures”: Identifying privacy engineering approaches to meet GDPR requirements	Dominik Huth et.al	Atributo de Qualidade	GDPR	2019
How Does GDPR (General Data Protection Regulation) Affect Persuasive System Design: Design Requirements and Cost Implication	Xiuyan Shao et. al	Atributo de Qualidade	GDPR	2019
GDPR Compliance in the Design of the INFORM e-Learning Platform: A Case Study	Evangelia Vanezi et. al	Atributo de Qualidade	GDPR	2019
GDPR Compliance: Implementation Use Cases for User Data Privacy in News Media Industry	Ahmedur Rahman Shovon et. al	Atributo de Qualidade	GDPR	2019

The privacy requirements for wearable IoT devices in healthcare domain	Rawan Alharbi et.al	Atributo de Qualidade	GDPR	2019
Blockchain and GDPR: Application scenarios and compliance requirements	florian zemler et.al	Atributo de Qualidade	GDPR	2019
The general data protection regulation: Requirements, architectures, and constraints	Kalle Hjerpe et.al	Atributo de Qualidade	GDPR	2019

Analisando o resultado, percebe-se apenas um artigo retornado sobre LGPD. Por se tratar de uma Lei brasileira, e ser recente, é compreensível o baixo número. Devido isso, motivamos a buscar uma alternativa para complementar o mapeamento, resolvemos realizar uma revisão informal no Google acadêmico para investigar trabalhos relacionados a LGPD.

Figura 2.1 – Revisão sistemática e revisão informal



Dessa forma, a string de busca foi adaptada para o contexto do Google, retirando os termos sobre a lei GDPR, aplicando os mesmos critérios de seleção anteriormente citados nas seções anteriores para revisão da literatura, e por fim, utilizando também o mesmo formulário de extração. Após realizada a busca da revisão informal, foram selecionados oito artigos relevantes, que reforçam o presente mapeamento, que descrevem atributos de qualidade, ou que descrevem atributos e técnica de avaliação, como é observado na Tabela 2.4 e na figura 2.1.

Tabela 2.4 – Tabela com resultado da revisão informal.

Titulo	Autor	Atributo e/ou Técnicas	Lei de Proteção	Ano
--------	-------	------------------------	-----------------	-----

Requisitos de Privacidade para Aplicações de Crowdsourcing no Contexto das Cidades Inteligentes	Mônica Silva et.al	Atributo de Qualidade	LGPD Brasileira	- 2019
Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)	Nairobi Spiecker de Oliveira	Atributo de Qualidade	LGPD Brasileira	- 2019
Uma Análise Sobre o Uso de DLTs no Tratamento de Dados Pessoais: Aderência aos Princípios e Direitos elencados na LGPD	Anderson Boa Morte	Atributo de Qualidade	LGPD Brasileira	- 2020
Perceptions of ICT Practitioners Regarding Software Privacy	Edna Dias et.al	Atributo de Qualidade	LGPD Brasileira	- 2020
Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais	Luiz Paulo Carvalho	Atributo de Qualidade	LGPD Brasileira	- 2019
The General Law Principles For Protection The Personal Data And Their Importance	Jonatas S. de Souza	Atributo de Qualidade	LGPD Brasileira	- 2020
Diagnostic of Data Processing by Brazilian Organizations - A Low Compliance Issue	Sâmmara Éllen Renner Ferrão	Atributo de Qualidade	LGPD Brasileira	- 2021
Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais	Marco Antonio Torrez Rojas	Atributo de Qualidade, Técnica de Avaliação	LGPD Brasileira	- 2021

2.3.1 Q1: Quais os atributos de qualidade da LGPD ou GDPR para aderência dos sistemas computacionais encontrados na Literatura?

Alguns trabalhos foram encontrados, sendo um deles, o trabalho de (OLIVEIRA et al., 2019), onde os autores abordam a segurança da informação sob os aspectos da lei brasileira que trata da proteção de dados dos usuários, aplicada a IoT. Nele é citado alguns atributos que a lei determina, como: confidencialidade, que visa garantir que somente quem deve acessar a informação de fato acesse; integridade, que garante que a informação

acessada realmente está correta; disponibilidade, visando garantir que a informação possa ser obtida sempre que for necessário. Já o trabalho de (SILVA et al., 2019), identificaram a partir de uma revisão, os principais requisitos de privacidade abrangendo o uso de crowdsourcing no contexto de cidades inteligentes e as novas legislações de privacidade. Alguns atributos, devem ser adaptados para um contexto geral de sistemas computacionais, sendo eles: o aplicativo deve informar o objetivo envolvido na coleta de dados, ou seja, transparente; o armazenamento não deve permitir a restauração dos dados após a aplicação de uma solução de privacidade.

A pesquisa de (CARVALHO et al., 2019), tem o objetivo de elencar futuros desafios para área de Transparência em Tecnologia de Informação e Comunicação (TIC) relacionados a LGPD. Alguns atributos encontrados são: usabilidade e informativo, que deve fornecer as informações de maneira simples, clara e acessível; acessibilidade, os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado. Para o processo de desenvolvimento de software que satisfaça os princípios da GDPR, (RINGMANN; LANGWEG; WALDVOGEL, 2018) apresenta uma proposta de requisitos técnicos reutilizáveis. Nesse trabalho é sugerido também a inclusão de especialistas jurídicos no processo de engenharia de requisitos, a fim de verificar quais requisitos se aplicam. É outro desafio principalmente para as pequenas organizações que no dia a dia não podem contar com um especialista na área. Os principais atributos identificados são: minimização de dados, que exige que o período pelo qual os dados pessoais são armazenados é limitado a um mínimo; transparência, que envolverá principalmente documentação para provar a legalidade ou fornecer informações ao titular dos dados, ou autoridade supervisora.

2.3.2 Q2: Quais Técnicas de Avaliação para LGPD ou GDPR encontrados na Literatura?

No contexto da avaliação, o trabalho de Rojas (ROJAS, 2020) buscou identificar a aplicação da lei em instituições de ensino, realizando um estudo de caso para avaliar o grau de adesão de um instituto federal aos requisitos da LGPD. Esta avaliação foi efetuada por meio de entrevistas com questões pertinentes a necessidades apresentadas na lei. Na avaliação efetuada, identificou-se que o instituto federal encontra-se no estágio inicial de atendimento à lei, crítico devido ao volume de trabalho em que consiste a adequação dos processos e sistemas da instituição. Em seguida, é proposto por (MORTE et al., 2020) uma análise de características técnicas a respeito da utilização da tecnologia de registro distribuído DLT, para o tratamento de dados pessoais. Como resultado da análise, verificou-se que a tecnologia DLT pode ser bem utilizada, trazendo recomendações para o tratamento de dados pessoais conforme a lei determina.

No contexto da lei de proteção de dados estrangeira GDPR, (BECKER et al., 2019) desenvolveram uma ferramenta de software chamada Daisy, para permitir que instituições

de pesquisa no contexto da biomedicina, possam cumprir o requisito de responsabilidade. Ao analisarem o armazenamento e a documentação, observaram que a ferramenta Daisy atende ao requisito de responsabilidade de forma eficaz. A documentação nesse caso é um grande desafio que a GDPR e outras leis trazem para as empresas cumprirem, necessitando de ferramentas específicas e dedicadas para esse contexto. O trabalho de (PAUL et al., 2018) utiliza uma abordagem chamada RegTech para a avaliação da conformidade com a GDPR, utilizando questões criadas por regulamentações com as próprias autoridades para poderem servir como uma forte plataforma de avaliação de conformidade. A ferramenta de avaliação atende ao requisito de ser abrangente enquanto cobre a amplitude da GDPR.

2.4 Trabalhos Relacionados Posteriores

O tema sobre proteção de dados pessoais está em expansão, onde a cada ano surgem novas pesquisas relacionadas a lei e tecnologias implementadas para adequação. Posteriormente a publicação do artigo base dessa dissertação, surgiram outros trabalhos relacionados a área da LGPD e GDPR, a serem apresentados a seguir.

No que lhe concerne, o trabalho (SANCHEZ; VIEJO; BATET, 2021) apresentam um sistema que avalia automaticamente as políticas de privacidade em relação aos requisitos de proteção de dados. A proposta quantifica o grau de conformidade da política com relação aos atributos de proteção de dados declaradas pela GDPR; e apresenta pontuações de privacidade claras e intuitivas para o usuário. Desta forma, os usuários se tornarão imediatamente cientes dos riscos associados aos serviços e sua gravidade. Com isso, eles estarão capacitados a tomar decisões informadas ao aceitar (ou não) os termos de um serviço.

Em outra pesquisa, (ARAUJO et al., 2021) propõe o método LGPD4BP para processos de negócio. O método foi aplicado em um estudo de caso na Universidade Federal de Pernambuco e validado por uma turma de pós-graduação que aplicou o método e respondeu a um questionário sobre facilidade e completude da proposta. Os resultados das avaliações dos alunos mostraram que a etapa mais difícil é a modelagem do processo de negócio e não os componentes do método proposto.

Por sua vez, no artigo de (COSTA et al., 2021) apresenta uma análise da conformidade do WooCommerce com a lei de proteção de dados brasileira, verificando se o plugin do WordPress está aderente com a LGPD. A análise de conformidade foi realizada através de um estudo de caso em que quatro clientes fictícios realizam compras em uma loja virtual, e que para verificar a segurança do WordPress, foi utilizado uma ferramenta, chamada WPScan. Através do estudo, foi observado que o WordPress está consoante a lei brasileira, mas apenas para usuários com a versão 4.9.6 ou superior, onde 92,05% dos domínios analisados que usam o plugin WooCommerce para comércio eletrônico estão

aderente à LGPD.

No estudo de (BARATI et al., 2021) propõe uma nova técnica de auditoria e verificação das operações realizadas nos dados de usuário de computação em nuvem. A pesquisa aproveita tecnologias de rede blockchain para verificar de forma transparente operações realizadas nos dados do usuário. Para validar a viabilidade da técnica proposta, usaram um serviço de saúde real. Embora os pesquisadores tenham usados apenas um único cenário, a arquitetura proposta pode ser generalizada para outros cenários. Por fim, (KUBICEK et al., 2022) criaram um procedimento para verificar a conformidade do consentimento GDPR dos sites para e-mails de marketing. Foi avaliado 1.000 sites e 5.000 e-mails resultantes de registros em sites. Os resultados do estudo indicam que vários sites podem estar violando a privacidade europeia que diz respeito a e-mails de marketing. O descumprimento de tais regras é recorrente, dado que é complicado detectar essas violações em relação ao consentimento do titular, principalmente para o marketing para empresas comerciais.

2.5 Considerações Finais

Neste capítulo foi realizado um levantamento teórico em relação à avaliação de adequação a LGPD e de atributos de qualidade. Foram descritos, o planejamento e os resultados de um mapeamento sistemático sobre atributos de qualidade e técnicas de avaliação sobre a lei geral de proteção de dados brasileira, incluindo a lei geral europeia GDPR. Durante a sua condução, foram obtidos 961 registros no total do estudo. Foram excluídos os trabalhos duplicados pelas máquinas de busca, trabalhos com referências sem disponibilidade de acesso pela Web, trabalhos que não descrevem atributos de qualidade (na forma de heurísticas, regras, requisitos, sugestões) sugeridos pela lei LGPD ou GDPR, ou técnicas de avaliação de conformidade, com auxílio da leitura dos títulos, resumos, e leitura completa dos artigos.

No final, selecionamos 36 artigos relevantes para esta pesquisa. Porém, 35 artigos são relacionados a GDPR, e apenas um artigo sobre LGPD. Isso ressalta a importância e necessidade de mais estudos para esta área. Por isso, realizamos uma revisão informal no Google Acadêmico para complementar o mapeamento, retornando oito artigos relevantes. Ao todo, foram selecionados 44 artigos relevantes para esta pesquisa. No próximo capítulo, será apresentado o processo de criação do checklist de inspeção.

3 Criação do *Checklist* de Inspeção LGPD

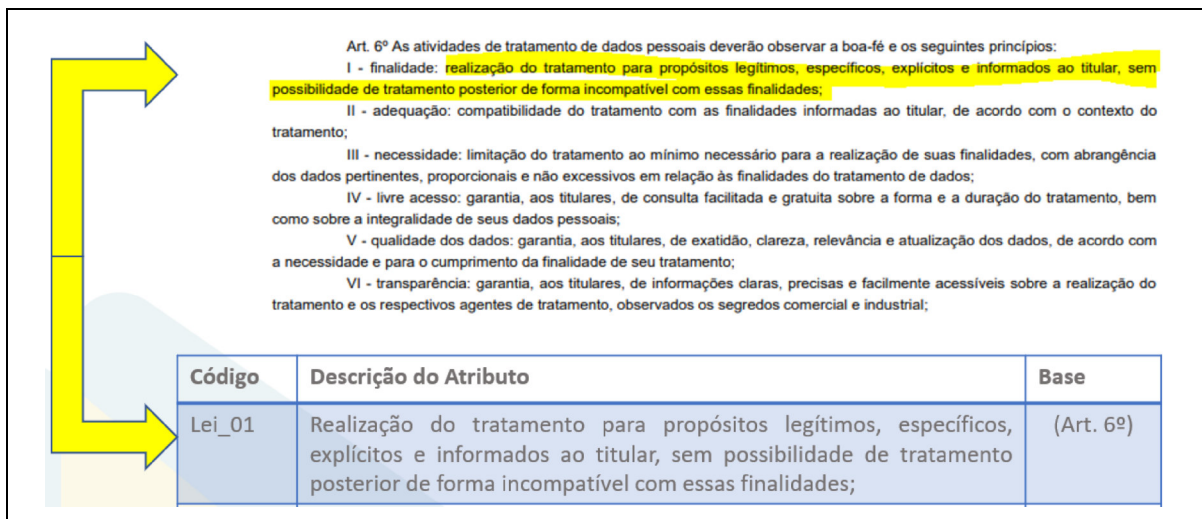
O processo de desenvolvimento do checklist seguiu as recomendações de (RINGMANN; LANGWEG; WALDVOGEL, 2018). Nesse trabalho, os autores rastrearam requisitos de artigos correspondentes a textos jurídicos, derivando requisitos técnicos de requisitos legais. Na metodologia aplicada pelos autores, a primeira etapa era a definição de requisitos legais através da seleção de: artigos relevantes de leis aplicáveis, características não funcionais de um sistema de TI, e por fim elaboração de propostas de desenho técnico com base nos requisitos técnicos.

Considerando a metodologia citada acima, os autores deste trabalho aplicaram o processo a seguir para criar o checklist: (1) extrair requisitos e atributos de qualidade da Lei Federal 13.708/2018 - LGPD; (2) extrair atributos dos artigos identificados na revisão da literatura da Seção 2.2; (3) correlacionar atributos semelhantes e agrupá-los em categorias sugeridas pelos autores de trabalhos anteriores; e (4) seleção das melhores descrições entre os atributos da lei federal, dos artigos do mapeamento sistemático e da revisão informal, transformando-os em itens do checklist.

3.1 O Processo de Desenvolvimento do Checklist

Com relação à primeira etapa, após a leitura do texto jurídico, foram identificados prováveis atributos que possam ajudar no desenvolvimento dos sistemas aderentes a lei. Na Figura 3.1 é mostrado a extração do primeiro atributo sobre finalidades encontrado na lei 13.709/2018, atribuímos um código, além da sua descrição e de onde foi retirado.

Figura 3.1 – Atributos da Lei 13.709/2018



Código	Descrição do Atributo	Base
Lei_01	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;	(Art. 6º)

A Tabela 3.1 apresenta um exemplo de como foi organizado os atributos extraídos da LGPD que podem descrever o que um sistema computacional precisa atender para que o mesmo permita a proteção de dados. Esses atributos foram considerados importantes e obrigatórios, já que estão explícitos na lei, e as empresas devem estabelecer planos para implementarem quanto antes tais atributos. Nesta tabela, o atributo LEI_01, por exemplo, sugere que deve haver um tratamento dos dados internamente, e deve obedecer aos princípios legais, específicos e explícitos à lei, e deve ser informado para o titular. Para permitir a rastreabilidade dos trechos identificados, também foi coletado em que local da Lei, esta informação pode ser obtida.

Tabela 3.1 – Modelo da extração de atributos da Lei Federal 13.709/2018

Código	Atributo	Base
LEI_01	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;	(Art. 6º)
LEI_02	Necessidade de 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;	(Art. 6º)
LEI_03	O tratamento de dados pessoais somente poderá ser realizado: I - mediante o fornecimento de consentimento pelo titular.	(Art. 7º)
LEI_04	O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado.	(Art. 8º)
LEI_05	O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.	(Art.10)

No que lhe concerne, a segunda etapa consistiu na extração dos atributos para cada artigo identificado na revisão da literatura. Desta forma, foram agrupados os atributos semelhantes, e selecionada a melhor das descrições do atributo, conforme exemplificado na Tabela 3.2. Nesta tabela, é apresentado um exemplo de como dois artigos distintos apresentaram atributos similares.

Por exemplo, dois artigos (Artigo01 e Artigo02) reportaram o atributo LGPD_01. Nesse exemplo, este atributo correspondia ao primeiro atributo identificado no Artigo01 e o primeiro atributo identificado no Artigo02. É possível que mais de um atributo tenha sido identificado no mesmo artigo. Por exemplo, o atributo LGPD_02 foi encontrado também no artigo 02. No caso de haver dois ou mais artigos relatando o mesmo atributo, foi escolhida aquela que tivesse mais detalhes sobre o atributo e/ou fosse mais fácil de entender. Vale ressaltar que este processo foi feito para todos os artigos que continham

atributos da LGPD e depois para todos os artigos que continham atributos da GDPR, gerando duas listas como a apresentada na Tabela 3.2.

Tabela 3.2 – Exemplos de artigos relacionados à LGPD na literatura

Código	Melhor_Descrição	Atributo
LGPD_01	(LGPD_01) Especificar para o usuário qual a finalidade da coleta de seus dados, além de ser transparente em relação ao tratamento dessas informações e adotar medidas que garantam sua segurança;	(Artigo01_01) O aplicativo deve informar o objetivo/razão envolvida na coleta de dados, sendo transparente. (Artigo02_01) Especificar para o usuário qual a finalidade da coleta de seus dados, além de ser transparente em relação ao tratamento dessas informações e adotar medidas que garantam sua segurança;
LGPD_02	(Artigo05-08) “O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.”	(Artigo02-06) Qualquer vazamento ou falha de segurança que comprometa os dados de algum usuário devem ser relatados imediatamente às autoridades competentes, para que o problema seja resolvido. (Artigo05-08) “O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.”

Para desenvolver a primeira versão do checklist proposto, foi feita a junção dos atributos identificados, considerando inicialmente os atributos advindos dos artigos relacionados com a LGPD e os atributos advindos da análise da própria Lei. O processo de análise foi o mesmo utilizado na Etapa 2. Contudo, nesta reaplicação, foram utilizados apenas as principais descrições identificadas nas análises anteriores.

Vale ressaltar que nesta nova análise também foram considerados os atributos da GDPR. No entanto, estes atributos não substituíram nenhuma das descrições advindas de artigos da LGPD ou da própria Lei. Isto foi feito para evitar que especificidades do contexto europeu fossem incluídos no checklist. O resultado da análise completa é apresentado na Tabela 3.3. Nesta tabela é possível observar que quando há uma relação entre atributos da LGPD e da GDPR, as propriedades da GDPR são acrescentadas como complemento e caso contradigam algum dos atributos da LGPD, estas são desconsideradas.

Após o agrupamento dos atributos, foi feita a definição das categorias às quais os mesmos iriam pertencer. Essas categorias foram extraídas dos artigos relatando atributos da LGPD ou GDPR, identificando um total de cinco categorias: transparência, segurança, consentimento, responsabilidade, direitos dos titulares. A Transparência(TR) é um princípio que diz respeito à informação aos titulares dos dados sobre as finalidades do processamento,

Tabela 3.3 – Exemplo da Análise e seleção de atributos

Melhor_Descrição	Atributo	Categoria
(Lei_01) Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular;	(Lei_01) Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular; (Lgpd_01) Especificar para o usuário qual a finalidade da coleta de seus dados; (Gdpr_01) os dados pessoais devem ser coletados para fins específicos, explícitos e legítimos;	Transparência (KNOCKAERT; VOS, 2020)
(Lei_06) garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; EXTRA: (Gdpr_18) Os titulares dos dados devem ser notificados com informação sobre o seu âmbito.	(Lei_06) garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; (Lgpd_20) “As informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível. (Gdpr_18) Os titulares dos dados devem estar cientes das informações de processamento e deve ser fornecido com notificação adequada e informação sobre o seu âmbito;	Transparência (KNOCKAERT; VOS, 2020)
(Lei_08) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados;	(Lei08) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados; (Gdpr_03) É exigida apropriada segurança dos dados pessoais, incluindo proteção contra processamento ilegal ou perda, destruição ou dano acidental.	Segurança da Informação (KNOCKAERT; VOS, 2020)

informações e recomendações sobre o tratamento ([KNOCKAERT; VOS, 2020](#)). A Segurança (SE) é um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento ([GEORGIPOULOU; MAKRI; LAMBRINOUDAKIS, 2020](#)). O Consentimento(CO), em certos casos, é a base jurídica das empresas, trata-se principalmente da obtenção de um consentimento dos titulares dos dados ([BLIX; ELSHEKEIL; LAOYOOKHONG, 2017](#)). A Responsabilidade (RE) refere-se aos controladores de dados que devem ser responsáveis e capazes de demonstrar conformidade com as disposições dos regulamentos ([BLIX; ELSHEKEIL; LAOYOOKHONG, 2017](#)). Por último, a categoria Direitos dos Titulares (DI) se refere aos

direitos dos titulares dos dados com relação à confirmação sobre se os seus dados pessoais estão sendo processados, além das informações complementares quanto à retificação, portabilidade, acesso, entre outros (FERREIRA, 2020).

3.1.1 Versão inicial do Checklist de Inspeção à LGPD

Após a identificação das categorias, as descrições dos atributos identificados relacionados à LGPD e complementados com atributos relacionados à GDPR foram reescritas, transformando-as em perguntas. Estas descrições se tornariam os itens de verificação do checklist proposto. Além disso, os itens definidos foram validados por um engenheiro de software com mais de dez anos de experiência na produção de itens de verificação para checklists, analisando a sua clareza e semântica. Após a escrita dos itens, os mesmos foram analisados para encaixá-los em uma das cinco categorias identificadas. Vale ressaltar que caso um autor tenha indicado uma categoria para algum dos atributos que originaram os itens, esta mesma categoria foi aplicada ao item de verificação. Caso contrário, os autores deste trabalho definiram as categorias do item. A Tabela 3.4 apresenta os 52 itens do checklist resultantes da análise da Lei 13.709, artigos relatando atributos sobre a LGPD e artigos relatando atributos sobre a GDPR. A seguir é apresentada uma prova de conceito, visando obter indícios da viabilidade de uso do checklist para avaliar a aderência de um sistema computacional à LGPD.

Tabela 3.4 – Checklist a partir da combinação de atributos identificados - Versão 1

Cat.	Itens	LEI	LGPD	GDPR
TR01	Os dados pessoais foram tratados apenas para fins específicos, explícitos, legítimos para qual foi originalmente coletado e informado ao titular de dados?	X	X	X
TR02	O tratamento de dados foi adequado e compatível com a finalidade para qual foi originalmente coletado?	X	X	
TR03	Os titulares de dados têm acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e a duração do tratamento, sempre que requisitar?	X	X	X
TR04	Os dados pessoais são mantidos precisos, atualizados, corrigidos ou apagados se incorretos, sem demora, para cumprimento das suas finalidades?	X		X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
TR05	Os titulares de dados estão cientes da política de privacidade, das finalidades, de processamento, fornecendo notificação adequada e informação clara e precisa sobre seu âmbito?	X	X	X
TR06	O controlador de dados adota medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse?	X		X
TR07	O controlador de dados mantém registro das operações de tratamento de dados pessoais que realizam especialmente quando baseado em seu legítimo interesse?	X	X	
TR08	Para atender as finalidades, o processamento de dados pessoais ou dados sensíveis são realizados de forma que não possam ser conectados a um titular de dados aplicando anonimização e pseudonimização?	X		X
TR09	Os titulares de dados são informados da existência de tratamento dos seus dados?	X		
TR10	São fornecidos aos titulares de dados, nos termos e compromisso ou mediante solicitação do titular, informações sobre a identidade e contato do controlador, os dados envolvidos e finalidades do processamento, a base legal, detalhes de transferências de dados fora do Brasil, período de retenção de dados e os direitos dos titulares?		X	X
CO01	Para o tratamento de dados pessoais, o titular tem acesso aos termos e condições, políticas de privacidade, e podem dar o seu consentimento de forma livre e clara?	X	X	X
CO02	O controlador de dados exige o consentimento específico para comunicar ou compartilhar os dados pessoais com outros controladores?	X		
CO03	O controlador de dados possui meios para provar que o consentimento foi obtido em conformidade com o disposto nesta lei, atendendo as condições de consentimento livre, específico, informado e presumido?	X	X	X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
CO04	Os titulares de dados possuem meios para recusar ou retirar o consentimento sem prejuízo a qualquer momento?	X		X
CO05	O tratamento de dados pessoais de crianças e adolescentes é realizado com consentimento específico, de fácil compreensão e em destaque dado pelos pais ou responsável legal, possuindo um meio para certificar que é o responsável legítimo que está dando o consentimento e que somente ele pode atualizá-lo?	X	X	X
CO06	O controlador de dados informa ou notifica previamente os titulares de dados sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	X		X
CO07	A declaração de consentimento foi proposta de forma inteligível e facilmente acessível, não contendo linguagem e termos abusivos?		X	X
CO08	Os requisitos de consentimento para cada uso de dados pessoais, dados sensíveis e suas finalidades, foram atendidas?		X	
DI01	Os titulares de dados têm acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e duração do tratamento, sempre que requisitar?	X		X
DI02	Os dados pessoais são armazenados em formato que facilite o titular de dados acessá-los?	X	X	
DI03	São fornecidos aos titulares de dados, informações e dados pessoais por meio eletrônico ou sob forma impressa?	X		
DI04	Em caso de consentimento ou contrato, o controlador de dados fornece a cópia eletrônica integral dos dados pessoais do titular em formato que permita sua utilização subsequente em outras operações de tratamento?	X		X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
DI05	O controlador de dados, fornece caso requisitado, a inserção de dados pessoais atualizados ou retificados para armazenamento?	X		X
DI06	O controlador de dados usa apenas dados úteis, relevantes e adequados a finalidades, garantindo que não há nenhum dado extra, fora do escopo, realizando anonimização, bloqueio ou eliminação de dados desnecessários?	X	X	X
DI07	O controlador de dados garante a portabilidade de dados a outro fornecedor de serviço ou produto mediante requisição expressa?	X	X	X
DI08	O controlador de dados exclui os dados pessoais do titular nos prazos estabelecidos, mediante seu consentimento?	X	X	X
DI09	O controlador de dados revisa periodicamente os dados pessoais que mantém e removem após o término de seu tratamento, quando cumprimento legal, transferência a terceiro, respeitando as obrigações da lei, por órgão de pesquisa ou uso exclusivo do controlador, desde que anonimizados?	X	X	X
DI10	O controlador de dados fornece informações por meio de sua política de privacidade e/ou requisição dos titulares dos dados sobre entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados?	X	X	X
DI11	O controlador de dados fornece informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa?	X		
DI12	Os titulares de dados são informados com destaque sobre quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou para o exercício de direito?	X		X
DI13	O controlador de dados fornece aos titulares de dados o direito de se opor a um processamento de dados de forma fácil e segura, onde o tratamento é interrompido e os dados associados não podem mais ser processados, modificados ou excluídos?	X		X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
DI14	O controlador de dados notifica os titulares de dados ou representante legal em caso de impossibilidade de adoção imediata dos direitos dos titulares?	X		
DI15	Os titulares de dados são informados quando uma decisão foi tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a criação do seu perfil pessoal, possuindo o direito de contestar ou solicitar revisão da decisão?	X	X	X
SE01	Os dados pessoais são processados de uma forma que garanta a segurança adequada, incluindo proteção contra acesso não autorizado ou ilegal, contra perda acidental, destruição ou dano, usando medidas técnicas ou administrativas apropriadas?	X		X
SE02	Os riscos de segurança de informações e proteção de dados são mapeados, bem como possui um plano de mitigação?	X	X	X
SE03	Existe adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?	X	X	X
SE04	A proteção de privacidade desde o design (privacy by design) é adotada por padrão e desde o início do projeto que será implementado?		X	X
SE05	São fornecidos meios para demonstrar as medidas organizacionais e técnicas de segurança que foram aplicadas aos dados pessoais, garantindo anonimato?		X	
SE06	O controlador de dados tem mapeado os dados pessoais utilizados, bem como tem o registro onde e como eles estão armazenados e utilizados? Além disso, o controlador tem mapeado os dados pessoais sensíveis e aplica as medidas de proteção adequadas?		X	X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
SE07	Foram adotados meios para demonstrar as medidas organizacionais e técnicas de segurança eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais?	X	X	X
SE08	O controlador de dados garante a disponibilidade de dados em formato comumente usados, legível por máquina, interoperável e informa ao titular de dados por quanto tempo os dados pessoais serão armazenados e disponíveis?			X
SE09	O controlador de dados garante a confidencialidade que nenhuma pessoa tenha permissão para acessar os dados pessoais sem autorização?			X
SE10	O controlador de dados garante a integridade dos dados pessoais a serem processados e que permaneçam intactos, completos e atualizados?			X
SE11	Os titulares de dados têm o controle sobre seus próprios dados pessoais e são informadas sobre todos os seus direitos?		X	X
SE12	Há realização de auditorias de conformidade periódicas e fornecidos aos titulares de dados?	X	X	X
RE01	O controlador de dados indicou um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais e divulgou publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador, a identidade e as informações de contato do encarregado?	X	X	X
RE02	O controlador de dados de dados comunica à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos prazos, conforme definido pela autoridade nacional?	X	X	X
RE03	O controlador de dados fornece sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada?	X		X

Tabela 3.4 – Continuação da página anterior

Cat.	Itens	LEI	LGPD	GDPR
RE04	Existe avaliação de impacto à proteção de dados pessoais, quando o processamento provavelmente resultará em um alto risco para os direitos e liberdades dos titulares dos dados e se esse processo é registrado e documentado para envio e publicação de relatórios de impacto à proteção de dados pessoais quando solicitado pela autoridade nacional a agentes do Poder Público?	X		X
RE05	O controlador de dados possui meios para transferir dados pessoais para países internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta lei, para a cooperação jurídica internacional ou quando o titular tiver fornecido o seu consentimento e em destaque para a transferência?	X	X	X
RE06	São mantidos os registros de acesso e de todas as atividades pelo oficial de proteção de dados (DPO) e que seja possível enviar relatórios para autoridades competentes?			X
RE07	São fornecidos aos titulares de dados, meios para registrar reclamações em relação a proteção de dados aplicável e no processamento de seus dados pessoais?	X		X
	Total	41	29	42

3.1.2 Prova de Conceito

Para avaliar se o *checklist* proposto poderia permitir a identificação de problemas em sistemas computacionais com relação à aderência à LGPD, aplicou-se o checklist considerando os dados disponíveis de uma avaliação por questionário apresentada no trabalho de (ROJAS, 2020). Como indicado na Seção 2.2., os autores do trabalho avaliaram o grau de adesão do site institucional de um Instituto Federal aos requisitos da LGPD, esta avaliação foi efetuada por entrevistas tendo como base um questionário elaborado pela empresa ICTS Protiviti com questões pertinentes às necessidades apresentadas na lei. Os autores identificaram sete aspectos que não foram atendidos pelo sistema. Cabe ressaltar, que o questionário avaliado (ROJAS, 2020) foi considerado na definição deste

checklist proposto.

Ao aplicar o *checklist* proposto no mesmo portal da instituição federal¹, foi identificado que 23 atributos foram feridos ou não foram atendidos, 16 dos 23 atributos são provenientes somente dos atributos da nova técnica do *checklist* proposto (TR10, CO01, CO02, CO03, CO04, CO05, CO06, CO07, DI10, DI11, DI12, DI13, SE03, SE05, SE11, RE04). Os sete problemas identificados por (ROJAS, 2020) também foram identificados pelo *checklist* proposto, são eles (CO08, SE01, SE04, SE06, SE07, SE09, RE05). Vale ressaltar que não foi possível avaliar 13 itens (TR01, TR02, TR06, TR07, TR09, DI02, DI07, DI14, DI15, SE12, RE02, RE03, RE06), pois requeria um alto nível de acesso ao sistema da instituição. O restante dos itens do *checklist* não foram violados. Após a análise, foi identificado que os maiores problemas que precisam se adequar são os atributos relacionados a segurança dos dados, direitos e consentimentos do titular. Portanto, a inspeção com essa nova proposta de *checklist* se mostrou promissora para atualizar abordagens existentes, como o questionário utilizado por (ROJAS, 2020); e fornecer uma primeira versão de um *checklist* para avaliação da aderência de sistemas computacionais à LGPD.

3.2 Considerações Finais

Para apoiar equipes de desenvolvimento de software, esse capítulo apresentou uma versão inicial de um *checklist* de inspeção para a avaliação de aderência de sistemas computacionais à LGPD. O novo *checklist* foi gerado a partir da análise de atributos da Lei LGPD, de um mapeamento sistemático, e de uma revisão informal de artigos de áreas complementares à computação. Como resultado preliminar, foi gerado um *checklist* com 52 itens em formato de perguntas, relacionados ao sistema de software e à empresa, agrupados em cinco categorias.

Quando comparado com o trabalho de Rojas (ROJAS, 2020), obteve-se um resultado superior, encontrando 16 defeitos adicionais. Tais resultados servem como apoio para direcionar recursos para áreas de não conformidade, possibilitando assim, a redução do risco de penalidades da LGPD. Com relação à completude do *checklist*, todos os aspectos e tipos de tratamentos identificados pelos autores foram considerados. Para diminuir possíveis ambiguidades nos itens, as descrições mais detalhadas e completas dos atributos foram consideradas, para construir itens mais completos e claros. O próximo capítulo, descreve o processo de criação da segunda versão do *checklist*, após o refinamento.

¹ Portal do IFSC - <<https://www.ifsc.edu.br/>>

4 Refinamento e Criação do Artefato do *Checklist*

Em nossos trabalhos anteriores (MENDES; VIANA; RIVERO, 2021), apresentamos uma versão preliminar de um *checklist* de inspeção para a avaliação da aderência de sistemas de software à LGPD. O *checklist* inicial era composto por 52 itens, gerado a partir da análise de atributos extraídos da lei LGPD, de um mapeamento sistemático da literatura, e de uma revisão informal complementar. Para o processo de refinamento, a pesquisa baseou em dois feedbacks importantes: 1-Avaliadores do simpósio de engenharia de software Sbes; 2-Uma profissional da área de desenvolvimento de software e LGPD.

- 1 — Avaliadores do simpósio de engenharia de software Sbes: Nesta etapa, principalmente no processo de rebuttal do artigo publicado sobre a proposta inicial do checklist, no simpósio brasileiro de engenharia de software, foi analisado os comentários fornecidos pelos avaliadores do congresso. Por exemplo, um avaliador comenta: *"Faz sentido classificar itens em mais, médios e menos críticos, ajudando a estratégia de atar os mesmos numa construção ou adaptação incremental de um sistema"*. Nesse caso, adicionamos no checklist o grau de severidade. Em resumo as principais contribuições são: a classificação do grau do defeito encontrado; o nível de resposta que o checklist propõe, se está total com defeito ou não se aplica; correção na escrita.
- 2 — Profissional da área de desenvolvimento de software e LGPD: Nesta outra etapa, a fim de explorar mais sobre o tema da LGPD, buscamos o contato de uma profissional que trabalha na área de adequação dos sistemas computacionais à LGPD. Foi realizado uma reunião por videoconferência, com a profissional e os autores da técnica proposta, para validar e discutir melhorias. Dessa forma, como resultado, a profissional relatou que a técnica apresentada tinha alguns pontos que precisavam ser modificados, sendo eles: eliminar ambiguidades e itens repetitivos; ter mais objetividade e clareza nas descrições dos itens; separar o que era obrigatoriedade de recomendações, foram as principais contribuições sugeridas.

A seguir, serão apresentadas: a) a segunda versão do *checklist* LGPD, após a realização de ajustes e melhorias; b) a construção do artefato, para automatizar a inspeção; c) um exemplo de uso do *checklist*, na detecção de defeitos.

4.1 Segunda Versão do Checklist

A segunda versão do *checklist* é fruto de um refinamento, realizado de um processo de revisão por pares, composto por dois alunos de pós-graduação em ciência da computação, realizado através da análise de cada item, com a supervisão de um doutor em engenharia de software, com objetivo de fornecer um mecanismo mais confiável, robusto e apropriado para utilização pela indústria de software. O primeiro ajuste foi realizado para diminuir ambiguidades, onde itens considerados grandes, genéricos e muitas vezes com muita informação, eram adaptados. A Tabela 4.1 descreve a transformação dos itens antigos para nova versão refinada. Como exemplo, o item T-01 possui mais de um atributo na sua descrição: se os dados foram tratados para fins *específicos*, *explícitos*, *legítimos*, e, além disso, se o tratamento é informado ao titular de dados. A partir dessa análise, o item é dividido em itens mais simples e com maior clareza.

Tabela 4.1 – Transformação dos itens antigos para segunda versão do *checklist*

Cod.	Itens Antigos	Itens da Segunda Versão
T-01	Os dados pessoais foram tratados apenas para fins específicos, explícitos, legítimos para qual foi originalmente coletado e informado ao titular de dados?	(T-01) As finalidades de tratamento de dados foram definidas na organização? (T-02) O tratamento de dados pessoais é realizado de acordo com uma base legal? (T-03) O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?
T-02	O tratamento de dados foi adequado e compatível com a finalidade para qual foi originalmente coletado?	(T-04) O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?
T-03	Os titulares de dados têm acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e a duração do tratamento, sempre que requisitar?	(T-05) O sistema informa para o titular a forma e duração do tratamento dos seus dados pessoais de maneira gratuita e acessível? (T-06) O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?

Após realizado o estudo de refinamento, foi gerada a segunda versão do *checklist* de inspeção, chegando ao total de **56 itens**. Os itens do *checklist* foram classificados em itens obrigatórios e itens não obrigatórios. **Os itens obrigatórios** são itens que estão explicitamente descritos na lei 13.709/2018 da LGPD, e são itens que obrigatoriamente as

organizações deverão cumprir, pois, são exigidos pela lei. **Os itens não-obrigatórios** são itens que não estão explícitos na lei da LGPD, porem são recomendáveis ou opcionais para as empresas terem uma oportunidade de melhoria para adequação dos seus sistemas, e são oriundos e descritos também de outros regulamentos como a GDPR. Desse modo, dos 56 itens totais do *checklist*, 47 são itens obrigatórios, e nove itens considerados itens não-obrigatórios.

Os itens do *checklist* também estão classificados por sua categoria, definidos anteriormente por (MENDES; VIANA; RIVERO, 2021), possuindo cinco categorias no total, sendo elas: transparência de dados, consentimento, direitos dos titulares, segurança de dados e responsabilidade do controlador.

Por fim, o *checklist* possui um campo com **Recomendações** para os itens. Essas recomendações são sugestões opcionais para correção ou implementação dos requisitos da lei LGPD, e baseadas por algumas regras determinadas pela ANPD, agência nacional de proteção de dados, além também do mapeamento sistemático da literatura, realizado pelos autores (MENDES; VIANA; RIVERO, 2021) que buscaram identificar os atributos que a lei determina. O objetivo é auxiliar os desenvolvedores de software a entender o problema e buscar soluções.

Na tabela E.1 é apresentado o *checklist* na segunda versão completo para avaliar a aderência dos sistemas computacionais à LGPD. Nessa tabela, são apresentados os 56 itens de verificação do *checklist*, além do seu código, conforme a categoria, e classificados em obrigatórios e não obrigatórios, e recomendações.

Tabela 4.2 – Checklist de Inspeção Completo para LGPD - Versão 2

Cat.	Itens	Recomendações
	ITENS OBRIGATÓRIOS	
T	Sobre Transparência de Dados	
T-01	As finalidades de tratamento de dados foram definidas na organização?	Crie um documento definindo uma Política de Privacidade e os Termos de Consentimento, descrevendo quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.
T-02	O tratamento de dados pessoais é realizado de acordo com uma base legal?	Na documentação da Política de Privacidade e dos Termos de Consentimento, explique a base legal em que fundamenta o tratamento de dados pessoais.

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	O sistema deve disponibilizar a Política de Privacidade e/ou Termos de Consentimento para o titular dos dados, sobre as finalidades de tratamento.
T-04	O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?	Revisar o consentimento e implementar as alterações que não estão de acordo com o que foi informado ao titular.
T-05	O sistema informa para o titular a forma e duração do tratamento dos seus dados pessoais de maneira gratuita e acessível?	Descreva no documento da Política de Privacidade e no Termo de Consentimento, sobre a forma que se realizará o tratamento de dados e qual a sua duração, disponibilizando essas informações sempre para o titular.
T-06	O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?	Crie um canal de comunicação entre o titular e a empresa para facilitar que o titular possa requisitar a integralidade dos seus dados pessoais, sempre de forma gratuita e sem lentidão da operação.
T-07	O sistema armazena com exatidão e clareza os dados pessoais coletados dos titulares?	Durante a coleta, garanta que os dados pessoais estão sendo informados corretamente.
T-08	O sistema mantém atualizados os dados pessoais, conforme necessário e para o cumprimento da finalidade de seu tratamento?	Crie um processo para mapear e revisar os dados pessoais no banco de dados, e se descobrir que os dados pessoais estão incorretos, é necessário corrigir ou apagar o mais rápido possível.

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
T-09	O sistema disponibiliza para o titular as informações sobre a realização do tratamento de dados e a identidade do controlador?	Disponibilizar para o titular sobre: a) Finalidades de Processamento; b) A identidade e contato do controlador; c) Os dados envolvidos; d) A base legal; e) Detalhes de transferências de dados fora do Brasil; f) Período de retenção de dados; g) Os direitos do titular.
T-10	A organização realiza o tratamento de dados quando baseado no seu legítimo interesse, de forma adequada com a lei?	A empresa deve realizar uma análise do legítimo interesse para verificar se a hipótese de tratamento pode se enquadrar na base legal.
T-11	O sistema mantém registros das operações de tratamento de dados, especialmente quando baseado em seu legítimo interesse?	Armazenar no banco de dados informações sobre as operações de tratamento dos dados, para possíveis comprovações legais.
T-12	O sistema informa para o titular e autoridades competentes sobre informações de tratamento de dados, principalmente quando baseado em seu legítimo interesse?	Elaborar relatórios das operações de tratamento de dados, principalmente quando baseado no seu legítimo interesse, e disponibilizar quando requisitado para o titular e para as autoridades competentes, como a ANPD.
T-13	O sistema realiza o tratamento de dados pessoais ou dados sensíveis, de forma que não possam ser conectados a um titular de dados, quando for requisitado?	Analisar quais dados pessoais deverão ser anonimizados, ou em outros casos, realizar uma pseudonimização.
T-14	O sistema informa ao titular de dados sobre a existência de tratamento dos seus dados, antes da coleta?	Disponibilizar ao titular, sempre em destaque e com avisos, sobre os dados pessoais que serão coletados e solicitar o consentimento do titular.
C	Sobre Consentimento do Titular	

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
C-01	O sistema permite que o titular forneça o seu consentimento de forma autônoma e clara, para realizar o tratamento de seus dados?	Recomenda-se usar uma linguagem clara e objetiva, sem propaganda enganosa, evitando caixas pré-marcadas, e também possuir uma opção para que o titular possa negar ou retirar o seu consentimento sem ter nenhum prejuízo.
C-02	O sistema solicita o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?	É obrigatório ser transparente para o titular sobre a finalidade de tratamento dos seus dados.
C-03	O sistema armazena o consentimento dado pelo titular para comprovações legais?	Armazenar no banco de dados os registros de consentimento do titular para comprovação.
C-04	O sistema permite ao titular de dados meios para recusar ou retirar o consentimento sem prejuízo ao titular?	O titular deve ter acesso ao seu termo de consentimento ou contrato com a opção de negar a realização do tratamento de dados.
C-05	O sistema realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico pelos pais ou responsável legal, de uma forma acessível e fácil de entender?	Deve certificar que apenas o responsável legítimo poderá dar o consentimento, e somente ele poderá atualizá-lo.
C-06	O sistema informa o titular sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	Sempre que for alterar a finalidade de tratamento, deverá informar o titular da mudança e solicitar o novo consentimento para realizar o tratamento de dados, com a opção de negar o tratamento caso o titular discorde da alteração.
C-07	O sistema fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo termos abusivos?	O Termo de Consentimento deve ser bem escrito, com linguagem de fácil compreensão, respeitando os direitos do titular.

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
C-08	O sistema informa o titular de dados sobre todos os seus direitos no consentimento?	Informar no Termo de Consentimento e na Política de Privacidade, os direitos que os titulares de dados possuem.
D	Sobre os Direitos do Titular	
D-01	O sistema armazena os dados pessoais em formato que facilite o titular de dados acessá-los?	Os dados pessoais devem ser armazenados em formato comumente usados por computador, em arquivos estruturados, para que os aplicativos de software possam facilmente identificar, reconhecer e extrair os dados pessoais.
D-02	O sistema fornece ao titular de dados, meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?	Disponibilizar o contato de DPO ou responsável pelo tratamento de dados, na política de privacidade ou uma página exclusiva para reclamações.
D-03	O sistema fornece a cópia eletrônica integral dos dados pessoais para o titular?	Transmitir diretamente os dados solicitados ao titular; ou fornecer acesso a uma ferramenta que permite que o próprio titular extraia os dados solicitados.
D-04	O sistema permite que o titular atualize seus dados pessoais?	É recomendado criar um mecanismo para que o próprio titular possa atualizar seus dados pessoais.
D-05	O sistema utiliza apenas dados relevantes e adequados à finalidade?	É recomendado realizar a anonimização de dados desnecessários, realizar bloqueio ou eliminação dos dados pessoais irrelevantes.
D-06	O sistema permite a portabilidade de dados a outro controlador mediante requisição do titular?	Os dados pessoais devem ser armazenados em formato acessível e legível por máquina, para poder exportar os dados do titular quando ele requisitar.
D-07	O sistema permite excluir os dados pessoais do titular, mediante a sua requisição?	Criar um mecanismo para que o titular possa solicitar a remoção dos seus dados pessoais.

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
D-08	O sistema remove os dados pessoais do titular após o término de seu tratamento?	É necessário excluir os dados pessoais do titular após o cumprimento da finalidade, no prazo estabelecido.
D-09	O sistema fornece informações sobre entidades públicas e privadas, caso tenha realizado compartilhamento de dados pessoais?	Armazenar as informações das entidades e das operações de tratamento realizadas, como o compartilhamento de dados, para comprovações legais e disponibilizar quando requisitado.
D-10	O sistema informa o titular sobre a possibilidade de não fornecer consentimento e sobre as consequências caso seja negada?	Deve fornecer no Termo de Consentimento a possibilidade de recusar o tratamento, e as consequências caso não queira consentir.
D-11	O sistema informa o titular quando o tratamento de dados for uma condição para fornecimento de produto, serviço ou para o exercício de direito?	Deve ficar claro no momento do consentimento do titular os objetivos e pré-requisitos do tratamento de dados.
D-12	O sistema permite aos titulares, o direito de se opor a um tratamento de dados de forma fácil?	É necessário fornecer um mecanismo para que o titular consiga retirar seu consentimento. Caso o consentimento seja retirado, os dados do titular não poderão ser mais processados.
D-13	O sistema informa ao titular, as razões do não exercício imediato dos direitos do titular?	Comunicar que a empresa não é agente de tratamento dos dados e indicar, sempre que possível, o agente responsável; ou indicar as razões de fato, ou de direito que impedem a adoção imediata da operação.
D-14	O sistema informa ao titular quando uma decisão foi tomada com base no tratamento automatizado, incluídas as decisões destinadas à criação do seu perfil pessoal?	Disponibilizar para o titular as informações das decisões automatizadas realizadas.

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
D-15	O sistema fornece a opção do titular contestar ou solicitar revisão da decisão automatizada?	Caso seja requisitado, deverá revisar a decisão automatizada contestada, podendo interromper o tratamento de dados e realizar um novo consentimento para essa finalidade.
S	Sobre a Segurança de Dados	
S-01	O sistema realiza o tratamento de dados de uma forma segura, incluindo proteção contra acesso não autorizado?	Garantir a segurança no tratamento dos dados pessoais, possibilitando apenas indivíduos autorizados possam ler, modificar ou excluir dados do sistema.
S-02	O sistema respeita as normas de transferência de dados pessoais para países internacionais, com grau de proteção de dados pessoais adequado às normas da LGPD?	Verifique se o país destino da transferência tenha um nível de proteção igual ou superior aos previstos na LGPD, e/ou que a empresa destinatária comprove possuir as mesmas garantias de proteção através de normas ou certificados.
S-03	O sistema informa para o titular sobre as informações das transferências dos dados pessoais realizadas para países internacionais?	Informar no documento da Política de Privacidade e no Termo de Consentimento, informações sobre a realização de transferências de dados para países internacionais.
S-04	O sistema utiliza mecanismos para prevenir a ocorrência de danos, destruição ou perda de dados?	Como boas práticas, deve-se implementar um backup de dados, armazenamento em nuvem, e quaisquer outras ações que protegerão as informações originais em caso de danos, destruição ou perda de dados.
S-05	O sistema utiliza medidas de proteção adequadas para dados pessoais sensíveis?	É necessário implementar uma camada adicional à segurança e armazenamento, especialmente aos dados pessoais sensíveis.
R	Sobre a Responsabilidade do Controlador	

Tabela 4.2 – Continuação da página anterior

Cat.	Itens	Recomendações
R-01	A organização indica um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais?	A organização deverá indicar um encarregado pelo tratamento de dados pessoais (DPO), podendo ser pessoa física ou pessoa jurídica, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional (ANPD).
R-02	A organização divulga publicamente de forma clara e objetiva a identidade e as informações de contato do encarregado DPO?	A informação deve estar de forma clara, na Política de Privacidade e no Termo de Consentimento, para que os titulares e a autoridade nacional possa ter acesso facilitado.
R-03	A organização comunica à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos titulares, nos prazos estabelecidos pelas autoridades?	Na ocorrência de incidente de segurança, é necessário comunicar ao titular e autoridade nacional ANPD.
R-04	A organização realiza avaliação de impacto à proteção de dados pessoais, quando o tratamento resulta em um alto risco para os direitos e liberdades dos titulares dos dados?	A organização deve realizar uma avaliação de impacto de proteção de dados, quando existir um elevado risco no tratamento de dados.
R-05	A organização realiza relatório de impactos à proteção de dados pessoais e disponibiliza a autoridade nacional, quando solicitado?	É necessário realizar um relatório de impactos à proteção de dados e disponibilizar-lo quando requisitado. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações.
	ITENS NÃO OBRIGATÓRIOS	
No-S	Sobre a Segurança de Dados	

Tabela 4.2 – Continuação da página anterior

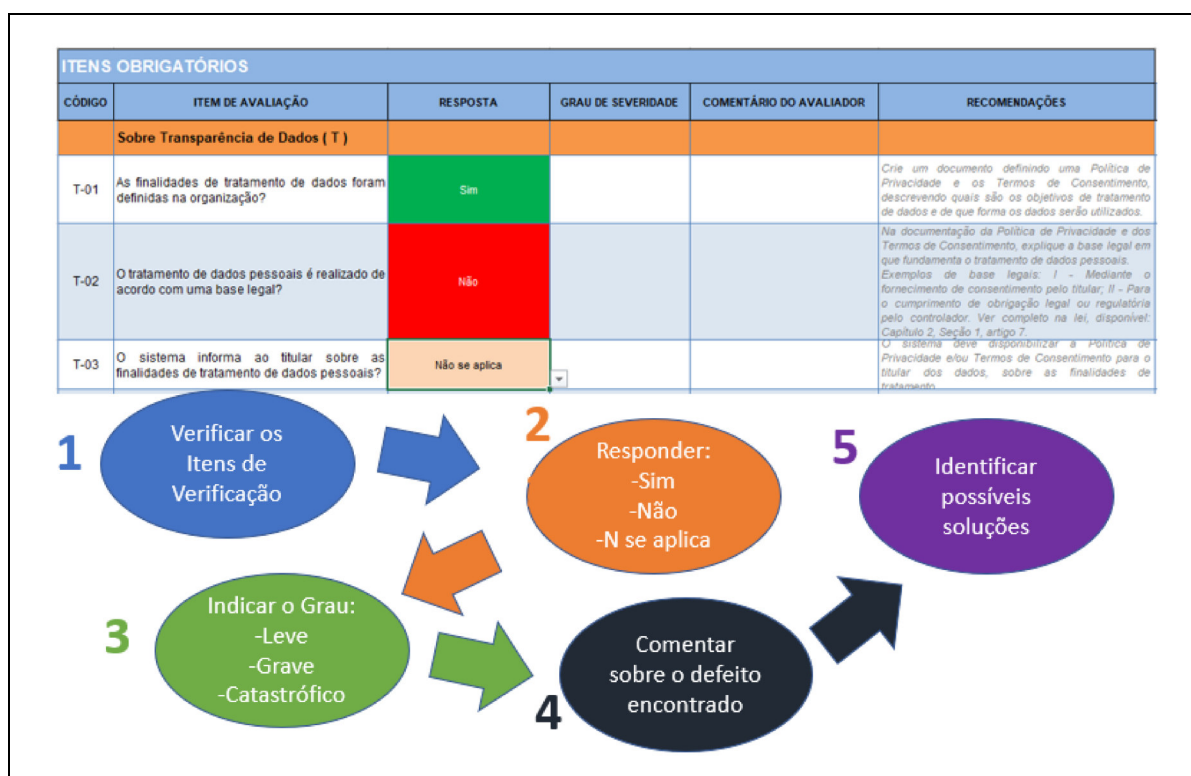
Cat.	Itens	Recomendações
No-S01	O sistema utiliza boas práticas de proteção de privacidade, como privacy by design?	Como boa prática para o desenvolvimento e adequação do sistema, implementar a metodologia privacy by design.
No-S02	O sistema realiza o mapeamento dos dados pessoais e mantém em segurança?	Organizar os locais onde os dados são coletados e armazenados.
No-S03	O sistema possui certificação ou selos, para comprovar a observância e o cumprimento das normas de proteção de dados pessoais?	Realizar a proteção contra acesso não autorizado, no uso de dados pessoais armazenados ou em transição, como exemplos realizar a autenticação e controle de acesso.
No-S04	O sistema fornece a confidencialidade, usando medidas técnicas apropriadas?	Verificar a integridade dos dados durante a coleta e no tratamento dos dados pessoais.
No-S05	O sistema fornece a integridade dos dados pessoais, impedindo modificações?	Uma solução seria documentar os dados das auditorias realizadas para fornecer ao titular.
No-S06	O sistema mantém registros de auditorias de conformidades e disponibiliza informação ao titular de dados, caso requisitado?	A organização deve documentar um plano para correção de falhas ou incidentes de segurança.
No-S07	A organização possui um plano de correção a incidentes de privacidade e segurança?	É recomendável que os sistemas tenham uma certificação, que comprovem que seguem um código de conduta ou política de segurança confiável para aderência da lei de proteção de dados.
No-R	Sobre a Responsabilidade do Controlador	
No-R01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?	Armazene e documente o histórico de atividades do encarregado DPO.
No-R02	A organização realiza capacitação para seus funcionários sobre a aderência à LGPD?	Capacite os funcionários e colaboradores sobre as informações que a LGPD determina.

4.2 O Processo de Inspeção Usando o *Checklist*

O *checklist* é uma técnica de inspeção relativamente de baixo custo, podendo ser adaptado às diversas fases de avaliações (LAITENBERGER; EMAM; HARBICH, 2001). No entanto, o uso pode ser considerado trabalhoso devido à atividade necessária para identificação de defeitos. Assim, a utilização de um apoio ferramental pode ajudar no processo de inspeção dos softwares.

Por essa razão, foi implementado um artefato em formato de planilha para incluir o *checklist* de inspeção para LGPD. Esse artefato dará o suporte para efetuar a detecção de defeitos pelo *checklist*, realizar o acompanhamento de preenchimento, fornecer gráficos com o grau de inconformidade e aderência do sistema, são alguns dos exemplos de funcionalidades. O artefato completo, pode ser acessado a partir do link¹.

Figura 4.1 – Processo de Inspeção do *checklist*



Na Figura 4.1 é apresentado o processo de inspeção utilizando o *checklist* de inspeção. Como visto na seção anterior e demonstrado na figura, o *checklist* apresenta a classificação dos itens obrigatórios e não obrigatórios, o código para cada item de acordo com sua categoria, e a descrição do item de avaliação em formato de pergunta.

Para o preenchimento, o avaliador ao iniciar a inspeção de software, deve indicar na coluna **Resposta** três opções para responder o item: *Sim*, *Não*, e *Não se aplica*. Se

¹ Checklist Completo: <<https://shre.ink/Rl7>>

o avaliador informar que *Sim*, significa que o item está adequado ou conforme a LGPD. Caso informe *Não*, quer dizer que o item está com defeito, que não está adequado. E se informar que *Não se aplica*, nesse caso o item não faz parte do contexto da empresa, ou não realiza determinado tratamento de dados, como exemplo: nem toda organização compartilha dados com países estrangeiros, ou que realiza o tratamento de dados pessoais de crianças e adolescente, são alguns casos que podem não se aplicarem.

Segundo (BASTOS et al., 2007), indicar a severidade do defeito é a melhor maneira de priorizar a ação corretiva e sua implementação. Por isso, o grau de severidade serve como um guia para ajudar os inspetores a avaliar o impacto dos defeitos e vulnerabilidades encontrados nos sistemas. Para cada item com defeito, o avaliador deve assinalar o **Grau de Severidade**. O *checklist* proposto possui três graus de severidade adaptada pela escala (NIELSEN, 1994): *Leve*, *Grave*, e *Catastrófico*. O grau Leve têm baixa prioridade para consertá-lo, impacta nos dados menos importantes e nas funções menores. O grau Grave, têm alta prioridade para consertá-lo, o defeito afeta as principais funcionalidades e dados, e requer ações corretivas a curto prazo. Já o grau maior Catastrófico é obrigatório consertá-lo, afeta severamente o sistema, e deve ser corrigido de imediato, para minimizar os efeitos significativos sobre a organização.

A coluna **Comentário do Avaliador** é um campo opcional e livre para ser preenchido com qualquer informação sobre o item que está sendo avaliado. Como sugestão, o avaliador poderá indicar informações como a localização do defeito no sistema para correção, quais são os responsáveis pela funcionalidade defeituosa, quem irá corrigir e quando será implementado, entre outros comentários.

Outra funcionalidade do apoio ferramental do *checklist*, são os gráficos automatizados para acompanhamento e indicam: progresso de preenchimento do *checklist* pelo avaliador, o índice de aderência, os itens adequados, o percentual de defeitos encontrados, a quantidade de itens não aplicáveis para a empresa, e o número de itens que ainda não foram preenchidos. O gráfico apresenta os índices tanto para os itens obrigatórios quanto para os itens não obrigatórios. A Figura 4.2 apresenta um exemplo do gráfico dos itens obrigatórios do *checklist* de inspeção LGPD.

Para facilitar o preenchimento e diminuir possíveis dúvidas, foi produzido um vídeo tutorial apresentando o funcionamento do *checklist* proposto, que poderá ser acessado através do seguinte link ². A Tabela 4.3 mostra alguns itens de verificação da técnica de *checklist*, e respectivos defeitos, identificados em uma inspeção de software, avaliando aderência à LGPD.

² Vídeo Tutorial do Checklist: <<https://shre.ink/RIS>>

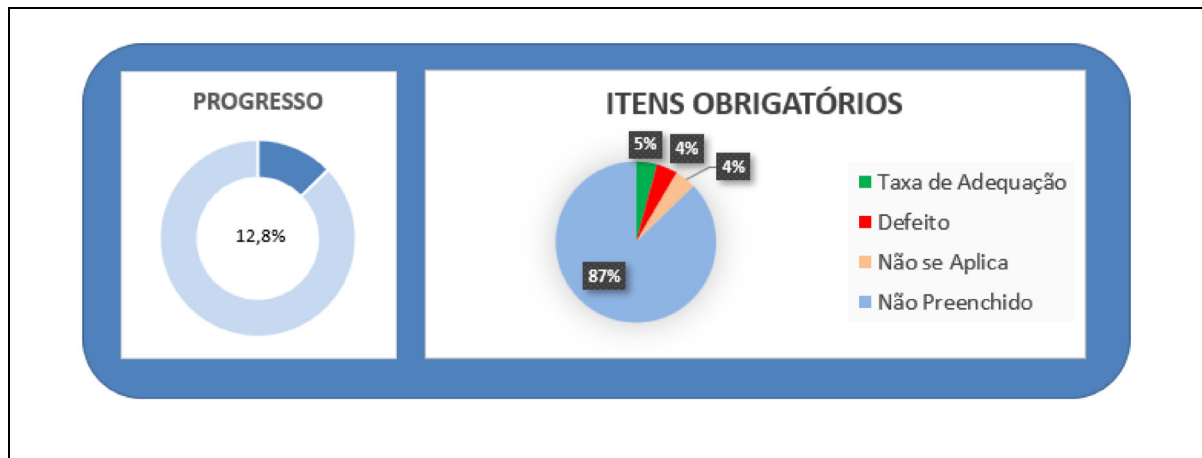
Figura 4.2 – Gráfico dos Itens Obrigatórios do *checklist*

Tabela 4.3 – Defeitos Identificados Pelo Checklist durante uma inspeção

Cod.	Item	Resp.	Grau	Comentário do Avaliador
T-04	O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?	Não	Grave	<i>A finalidade não é apresentada ao titular, não tem como fazer conformidade.</i>
D-03	O sistema fornece a cópia eletrônica integral dos dados pessoais para o titular?	Não	Grave	<i>Depende do nível de acesso que o usuário possui, tem usuário que não tem acesso nenhum.</i>
D-04	O sistema permite que o titular atualize seus dados pessoais?	Não	Grave	<i>O usuário não tem acesso às suas próprias informações, ele fica impossibilitado de atualizar.</i>
D-08	O sistema remove os dados pessoais do titular após o término de seu tratamento?	Não	Grave	<i>A empresa teria que mapear o dado, até o backup, e a estrutura do banco precisaria está igual, é um defeito para gente.</i>
R-01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?	Não	Leve	<i>Nós ainda não definimos um responsável específico para essa função.</i>

4.3 Considerações Finais

Este capítulo apresentou a segunda versão refinada do *checklist* de inspeção para LGPD e seus artefatos para realizar uma inspeção de software para a avaliação de aderência de sistemas computacionais. O refinamento foi baseado nos resultados obtidos de uma prova de conceito, de comentários de especialistas da área de direito e tecnologia da informação que trabalham na implementação das diretrizes da LGPD nos sistemas de software. Um artefato em formato de planilha foi gerado para automatizar a inspeção. No artefato, além dos itens de verificação, foram adicionados o grau de severidade para os defeitos encontrados, e também uma lista de recomendações para correção ou implementação de cada item do *checklist*. No próximo capítulo, será apresentada a aplicação prática na indústria do checklist.

5 Aplicação do Checklist na Indústria

Na engenharia de software, alguns estudos devem ser realizados ao avaliar uma nova proposta, como o estudo de viabilidade, para melhorar a credibilidade da pesquisa, tornando público a outros pesquisadores os seus resultados (SHULL; CARVER; TRAVASSOS, 2001).

Em função disso, esse capítulo apresenta a execução de um estudo através de uma aplicação na indústria, envolvendo pessoas em seu próprio ambiente de trabalho em condições realistas, para caracterizar a técnica proposta do *checklist* e verificar sua viabilidade de uso. Serão descritos o planejamento e a execução do estudo aplicado na indústria, realizado para avaliar o desempenho e a viabilidade do checklist e seus artefatos.

5.1 Descrição e Objetivo

A Tabela 5.1 apresenta o objetivo desta aplicação usando o paradigma GQM (Goal Question Metric) (BASILI; ROMBACH, 1988). A viabilidade da técnica de *checklist* foi caracterizada com base nos seus indicadores de Eficácia e Eficiência. Para estes indicadores, foram utilizadas as mesmas definições usadas por (FERNANDEZ; ABRAHÃO; INSFRAN, 2013): a eficácia é a razão entre o número de problemas detectado pelo inspetor e o número de problemas existentes. A eficiência é a razão entre o número de problemas detectado pelo inspetor e o tempo gasto por ele/ela para encontrá-los.

Além disso, a avaliação foi caracterizada utilizando o modelo de aceitação de tecnologias TAM (*Technology Acceptance Model*) (DAVIS; BAGOZZI; WARSHAW, 1989). Três características serão utilizadas nessa avaliação: a facilidade de uso percebida, utilidade de uso percebida, e a intenção de uso futuro percebida.

Tabela 5.1 – Objetivo do estudo da técnica de checklist

Analisar	A técnica de checklist de inspeção LGPD
Com o propósito de	Caracterizá-la
Com respeito a	Sua viabilidade em termos dos indicadores de eficácia, eficiência, facilidade, utilidade e intenção de uso.
Do ponto de vista de	Profissionais que atuam na indústria
No contexto de	Uma avaliação de um sistema real.

5.1.1 Participantes do Estudo

O estudo foi realizado remotamente entre janeiro a março de 2022 em uma parceria de pesquisadores da Universidade Federal do Maranhão e da Universidade Federal de Pernambuco, aplicado em um Instituto de Inovação Privado no estado de Pernambuco, com a participação de profissionais que atuam nessa organização em um sistema computacional real. Além da praticidade, nesse período alguns estados do Brasil permanecia em situação de pandemia em decorrência da Covid-19, e a maioria dos profissionais trabalhava remotamente, desse modo, optou-se por executar o estudo remotamente.

No total, quatro profissionais participaram desse estudo. Os participantes assinaram um Termo de Consentimento Livre e Esclarecido e preencheram um formulário de caracterização. O termo serviu para informar os participantes que estariam fazendo parte de um estudo relacionado com inspeções para adesão à LGPD.

O formulário de caracterização continha perguntas sobre: (1) escolaridade e formação acadêmica; (2) experiência no cargo atual que trabalha (3) conhecimento em inspeção de software e experiência na LGPD. Para classificar a experiência dos participantes no que diz respeito à LGPD, foi considerado: (a) Baixa, se o participante não estudou ou tido experiência prática na Lei; (b) Intermediária, se o participante estudou LGPD, mas tinha pouca experiência prática na avaliação; e (c) Alta, se o participante estudou LGPD, e tinha muita experiência prática em projetos envolvendo adequação para LGPD.

Outros envolvidos também participaram deste estudo, além dos participantes mencionados até o momento: (a) dois moderadores da inspeção, responsáveis por planejar e coletar os dados durante o estudo; (b) quatro engenheiros de software com experiência em inspeção de software, responsáveis por validar todos os materiais e instrumentações. Além disso, os moderadores com um engenheiro de software, e os profissionais da indústria, foram responsáveis por decidirem quais dos defeitos apontados eram realmente problemas de inconformidade. A Tabela 5.2 apresenta o questionário de caracterização e os principais aspectos dos profissionais da indústria, que atuaram como inspetores no estudo.

Tabela 5.2 – Caracterização dos participantes

Inspetor	I-01	I-02	I-03	I-04
Qual seu nível atual de escolaridade?	Mestrado Incompleto	Pós Graduação	Pós Graduação	Doutorado Incompleto
Qual sua formação acadêmica?	Ciência da Computação	Engenharia Elétrica	Analista e desenvolvimento de sistemas	Sistema de Informação

Tabela 5.2 – Continuação da página anterior

Inspetor	I-01	I-02	I-03	I-04
Qual cargo atual na empresa?	Analista de Informática I	Consultor de Vendas	DevOps - Tecnologia e Inovação	Pesquisador
Quanto tempo de experiência no cargo?	2 anos e 7 meses	3 anos	3 anos	5 anos
Você possui conhecimento sobre inspeção?	Sim	Não	Sim	Sim
Você possui conhecimento sobre a LGPD?	Sim	Sim	Sim	Sim
Qual o nível de conhecimento sobre a LGPD?	Baixo	Intermediário	Intermediário	Intermediário

5.1.2 Materiais Utilizados

Em relação ao material utilizado na inspeção, foram elaborados os seguintes materiais para apoio aos inspetores: a) apresentação e instruções gerais da técnica do *checklist*; b) especificação do roteiro descrevendo as atividades executadas durante a inspeção; c) um vídeo tutorial com uma demonstração de utilização do *checklist*; d) o arquivo do *checklist* de inspeção para LGPD; e por último e) os questionários para avaliação da técnica aplicada. Em resumo, o roteiro com as atividades do estudo é apresentado a seguir:

1. Cada participante recebeu por e-mail um arquivo compactado contendo todos os materiais utilizados, como baixar e descompactar o arquivo, as primeiras instruções e o cronograma.
2. A segunda etapa é o preenchimento do termo de consentimento e questionário de caracterização, na qual o participante deve acessar o link disponível nas instruções, fornecendo o consentimento para pesquisa e respondendo algumas questões sobre o seu perfil;
3. Recomenda-se a visualização das instruções para preenchimento do *checklist*, e do

vídeo tutorial da técnica, que poderá ser acessado através do seguinte link ¹.

4. Realizar o preenchimento do formulário de avaliação da técnica pós-inspeção, conforme a tabela 5.3, e enviar o checklist preenchido pelo próprio formulário.
5. Participar da reunião de um Grupo Focal, com os participantes do estudo, para discriminação dos defeitos encontrados nas inspeções, além de discutir sobre a técnica, e responder questões subjetivas para identificar: (a) as maiores facilidades e dificuldades no uso do checklist; (b) avaliar possíveis mudanças e/ou melhorias da técnica.

A Tabela 5.3 contém as questões objetivas para avaliação do *checklist* de inspeção, por meio do modelo de aceitação de tecnologias TAM. O modelo TAM é um dos modelos mais influentes de aceitação de tecnologia, que propõe que a facilidade de uso percebida, intenção e a utilidade de uma ferramenta tecnológica determinam a extensão da aceitação do usuário (DAVIS; BAGOZZI; WARSHAW, 1989). Essa tabela está organizada em três colunas: a primeira coluna refere-se ao código da questão, sobre a facilidade de uso percebida (FU), utilidade percebida (U); e as 3 últimas questões são sobre a intenção de uso percebida (IU). Depois é apresentado o aspecto geral da questão e um detalhamento do aspecto que está sendo avaliado.

As respostas das questões objetivas dos formulários de avaliações da técnica pós-inspeção, foram dadas sobre a escala *Likert* (MCIVER; CARMINES, 1981) com quatro opções de respostas: (1) Concordo Totalmente; (2) Concordo Parcialmente; (3) Discordo Parcialmente; e (4) Discordo Totalmente.

Tabela 5.3 – Questionário de avaliação da técnica pós-inspeção

Cód.	Aspecto	Descrição
Facilidade de uso percebida		
FU-1	Compreensível	O checklist utilizado foi claro e fácil de entender.
FU-2	Fácil de usar	De maneira geral, eu acho fácil encontrar defeitos / problemas no sistema com o checklist utilizado.
FU-3	Pouco Esforço mental	O checklist utilizado demandou pouco esforço mental.
Utilidade percebida		
U-1	Trabalho mais rápido	O checklist utilizado me permite realizar a inspeção do sistema mais rapidamente.

Continua na próxima página

¹ Vídeo Tutorial do Checklist: <<https://shre.ink/RIS>>

Tabela 5.3 – *Prévia na página anterior*

U-2	Aumento de produtividade	O checklist utilizado melhora a minha produtividade ao identificar defeitos / problemas no sistema.
U-3	É útil	Eu acho que o checklist utilizado é útil para encontrar defeitos / problemas no sistema.
Intenção de uso futuro percebida		
IU-1	Prever usar	Eu prevejo usar o checklist para encontrar defeitos / problemas no sistema futuramente.
IU-2	Pretende usar	Assumindo que eu tenha acesso ao checklist, pretendo usá-lo para encontrar defeitos / problemas em outros sistemas.
IU-3	Recomendável	Eu recomendaria o checklist utilizado para outras empresas.

5.1.3 Execução e Coleta da Inspeção do Sistema Computacional

O processo de inspeção utilizado baseou-se no processo sugerido por (SAUER et al., 2000), dividido em quatro etapas: planejamento, detecção, coleção e discriminação. Os participantes do estudo utilizaram o *checklist* para inspecionar um sistema computacional de um Instituto de Inovação Privado, que monitora a produção industrial. O sistema é uma plataforma que atende pequenas e médias empresas de todo o Brasil com objetivo de promover um acompanhamento da produção em tempo real, avaliando a eficiência de processos e instrumentos.

A atividade de detecção de defeitos foi realizada individualmente pelos inspetores, que tiveram um prazo inicialmente de quatro dias, porém, como os participantes são profissionais da indústria e cumprem horário de trabalho, tiveram um prazo de seis dias para sua realização. Isso inclui baixar o material indicado, responder o formulário de consentimento e caracterização, preencher o *checklist*, o enviar respondido, e por último, responder o questionário de avaliação da técnica pós-inspeção.

Cada inspetor seguiu o roteiro, e teve a liberdade de realizar a detecção de defeitos quando mais lhe fosse conveniente, respeitando e seguindo claro as atividades e os prazos determinados. Os moderadores na inspeção foram responsáveis por coletar todas as planilhas e questionários preenchidos. No prazo de seis dias, os quatro inspetores enviaram as suas planilhas preenchidas e finalizaram o questionário de consentimento, de caracterização, e da avaliação da técnica pós-inspeção.

As listas com as discrepâncias individuais foram coletadas e integradas a uma

única lista, retirando-se a referência do inspetor, para que os integrantes da reunião de discriminação de defeitos não soubessem qual inspetor havia apontado a discrepância. A reunião de discriminação, que visa verificar se as discrepâncias são defeitos reais foi realizada em um Grupo Focal, contou com a participação dos dois moderadores, de um engenheiro de software, três dos quatro participantes do estudo e um coordenador da empresa que atuou como ouvinte. Após a discussão, a equipe classificava a discrepância em defeito ou falso-positivo. Além disso, na reunião do grupo focal, os profissionais da indústria foram questionados sobre as suas maiores dificuldades e facilidades no uso do *checklist*, sobre quais eram os pontos fortes e fracos da técnica, e quais mudanças fariam.

Todos os dados do formulário de avaliação da técnica de pós-inspeção foram compilados em gráficos e serão discutidos na seção seguinte. Além disso, na próxima seção, serão apresentados os resultados obtidos na avaliação quantitativa, com o modelo Tam e na avaliação qualitativa, analisando o desempenho do uso do *checklist* de inspeção.

5.2 Resultados da Avaliação do Checklist de Inspeção

Nessa seção são discutidos os resultados da avaliação do *checklist* de inspeção para LGPD, utilizando três perspectivas: (1) Análise Quantitativa, voltada para os dados quantitativos coletados na inspeção; (2) Análise com o Modelo TAM, voltada para os dados objetivos coletados do formulário de avaliação pós-inspeção; e (3) Análise Qualitativa, uma análise das opiniões dos inspetores, com os dados coletados na reunião do grupo focal sobre o *checklist*.

5.2.1 Análise Quantitativa

Para análise quantitativa foi utilizado os resultados da reunião de discriminação, onde foi contabilizado o número de discrepâncias, falsos positivos e defeitos reais, além das variáveis que mediram o desempenho dos inspetores: eficiência e eficácia. Foi considerado também o tempo gasto que cada inspetor levou para executar o processo de inspeção por meio da técnica do checklist.

A análise realizada para calcular as métricas de eficácia e eficiência, são as mesmas utilizadas pelos autores (FERNANDEZ; ABRAHÃO; INSFRAN, 2013). As Equações 5.1 e 5.2 apresentam as relações de eficácia e eficiência, respectivamente. Nas equações, a variável 'd' é o total de defeitos que um inspetor identificou na sua inspeção; 'D' é o total de defeitos identificados após a reunião de discriminação; e 't' é o tempo gasto pelo inspetor para realizar a sua inspeção.

$$Eficácia = (d / D) * 100 \quad (5.1)$$

$$Eficiência = d / (t / 60) \quad (5.2)$$

Ao todo, com a participação de quatro profissionais da indústria, que atuaram como inspetores, foram identificados **42 defeitos** de fato. A Tabela D.1 localizada no apêndice deste trabalho, apresenta a listagem completa com os defeitos e seu respectivos graus de severidade, assinaladas pelos inspetores. Devido ao pouco tempo para discriminação dos defeitos, o grau de severidade não foi levado para reunião de discriminação. Porém, pela lei ser recente, são poucos os trabalhos que avaliam o grau de severidade dos atributos da lei. Portanto, as respostas assinaladas pelos participantes, e analisadas pelos autores, são uma importante contribuição.

A Tabela 5.4 apresenta os resultados individuais de cada inspetor, em relação: experiência na LGPD; o tempo gasto em minutos; o número de discrepâncias; o número de falsos positivos; número de defeitos reais.

Tabela 5.4 – Resultados Quantitativos Individuais

Inspetor	I-01	I-02	I-03	I-04
Experiência na LGPD	Baixo	Intermediário	Intermediário	Intermediário
Tempo Gasto(min)	150	Não coletado	53	60
Total de Discrepâncias	33	33	21	11
Falsos Positivos	4	1	0	2
Total de Defeitos	29	32	21	9
Eficácia (%)	69,04	76,19	50,00	21,42
Eficiência(Defeitos por Hora)	11,60	Sem Cálculo	23,78	9,00
Eficácia Média (%)				54,16
Eficiência Média (Defeitos por Hora)				14,79

Para exemplificar, calculamos a eficácia e a eficiência do inspetor I-01 da Tabela 5.4. O número de defeitos 'd' que este inspetor identificou foi 29, e o número total de defeito 'D' é 42; dessa forma, após aplicar a equação, o resultado é *69,04% de eficácia*. O tempo gasto 't' do inspetor I-01 é de 150 minutos, após aplicar a Equação 5.2, este inspetor possui *11,6 de eficiência*. Para o caso do inspetor I-02 não conseguimos coletar o tempo gasto na inspeção, e dessa forma não foi possível calcular a sua eficiência.

Com o olhar inicial desses resultados, pode-se verificar que o *checklist* ajudou os inspetores a detectarem defeitos na inspeção. O *checklist* da LGPD obteve uma eficácia média 54,16% e uma eficiência média (defeitos por hora) de 14,79. Não houve comparação

do resultado do *checklist* com outra técnica, justamente por ser pioneira, porém o resultado obtido do *checklist* aplicado na indústria é um indício de que a técnica proposta para LGPD cumpre com o seu propósito.

5.2.2 Análise com o Modelo TAM

Na avaliação com o modelo TAM foram consideradas as respostas objetivas do formulário de avaliação pós-inspeção. A Figura 5.1 apresenta os dados sobre a facilidade de uso percebida, dos inspetores que utilizaram o *checklist*.

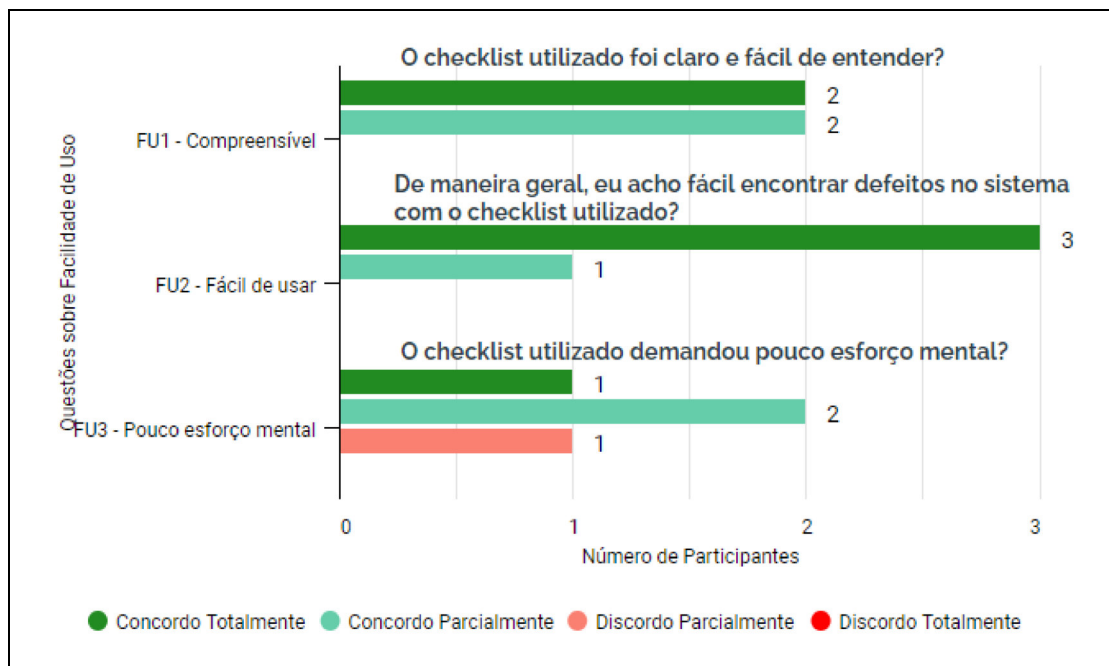


Figura 5.1 – Resultados sobre facilidade de uso percebida (FU)

Percebe-se que metade dos inspetores concordam totalmente sobre a clareza e entendimento do *checklist* e a outra metade concordam parcialmente. A maioria dos inspetores concorda totalmente sobre a facilidade em encontrar defeitos. No entanto, metade dos inspetores concordam parcialmente que a técnica demanda pouco esforço mental, e um inspetor discorda parcialmente. A Figura 5.2 apresenta os dados sobre a utilidade percebida.

Sobre a utilidade percebida, todos concordaram que o *checklist* de maneira geral, realiza a inspeção do sistema mais rapidamente. Mais da metade dos inspetores concordam que melhora a sua produtividade ao identificar defeitos utilizando o *checklist*. Por fim, todos concordam totalmente que o *checklist* utilizado é útil para identificar os defeitos no sistema. A Figura 5.3 apresenta os dados sobre a intenção de uso futuro percebida, dos inspetores que utilizaram o *checklist*.

É visto sobre a intenção de uso futuro percebida, todos os inspetores pretendem

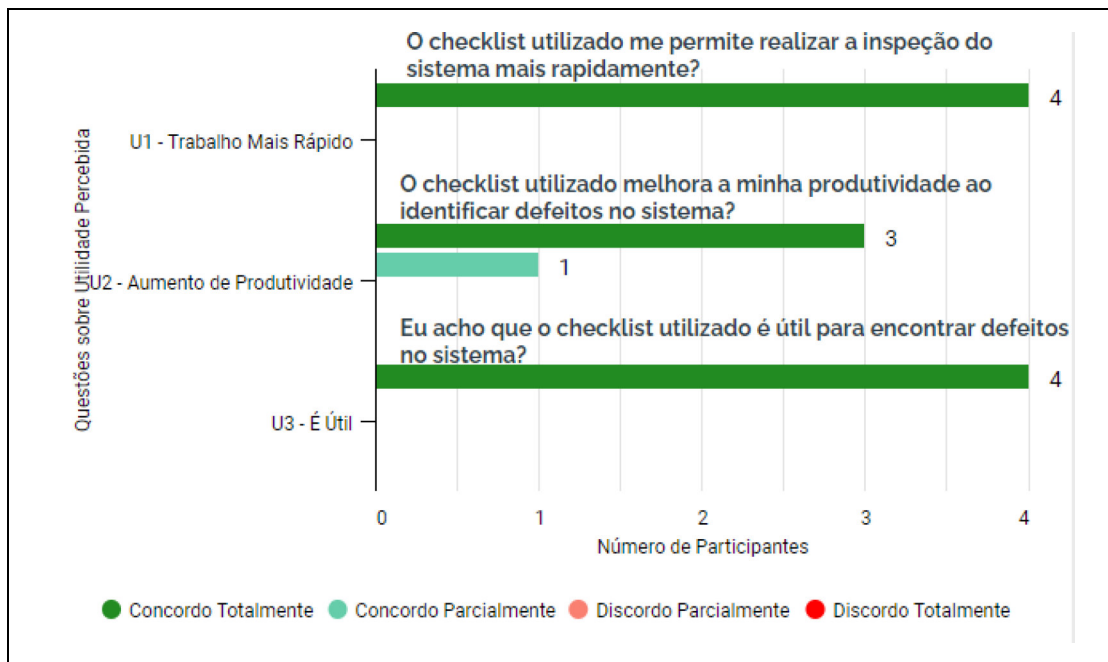


Figura 5.2 – Resultados sobre utilidade percebida (U)

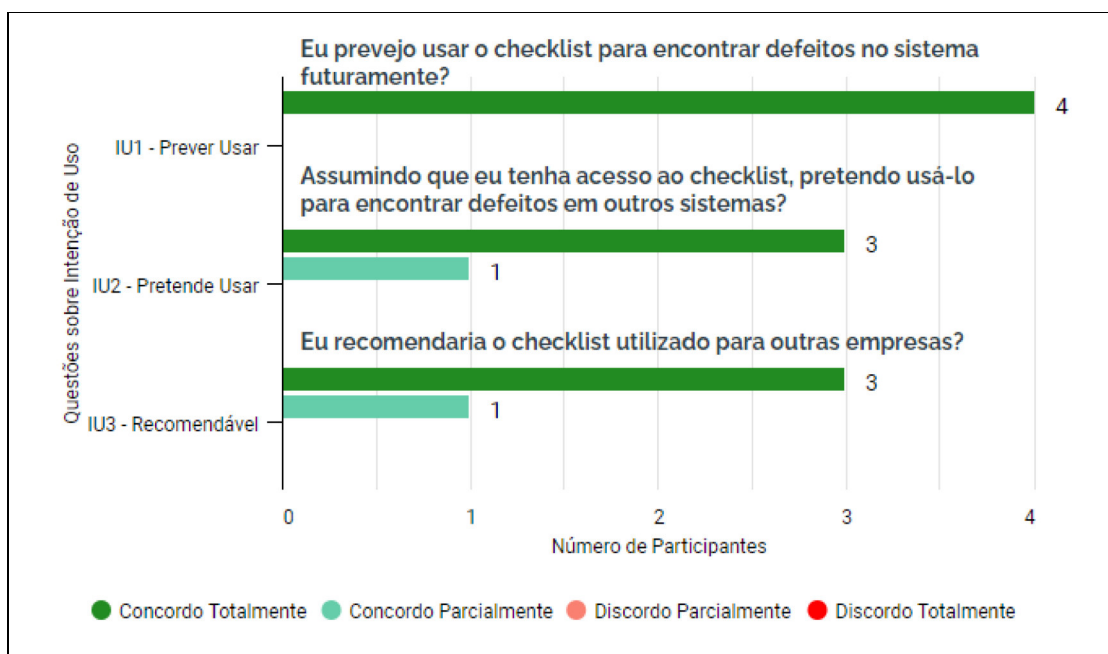


Figura 5.3 – Resultados sobre intenção de uso futuro percebida (IU)

usar o *checklist* no futuro. Mais da metade dos inspetores pretendem utilizar o *checklist* em outros sistemas computacionais para avaliar a sua aderência a LGPD. E por fim, mais da metade dos inspetores recomendariam o *checklist* para outras empresas que realizam o tratamento de dados e queiram avaliar seu sistema quanto a aderência a LGPD.

Conforme os resultados das três perspectivas sobre a facilidade, utilidade e intenção de uso, pode-se concluir que a maioria dos inspetores concordou totalmente que o *checklist*

é fácil de utilizar, que é bastante útil para identificação de defeitos, e pretendem usar futuramente. Porém, alguns inspetores acreditam que o *checklist* demanda um pouco de esforço mental para o preenchimento de itens de verificação para adequação do sistema a LGPD.

5.2.3 Análise Qualitativa

A análise qualitativa considerou os dados coletados durante a reunião do grupo focal com três participantes do estudo, o inspetor I-04 não compareceu na reunião. Algumas questões foram levadas e discutidas visando entender melhor as maiores dificuldades e benefícios ao usar o *checklist* avaliado e seus artefatos, além de possíveis mudanças ou melhorias sugeridas pelos participantes. A primeira questão levada para a reunião foi a seguinte: ***Quais são os principais benefícios que o checklist traz para sua empresa?***

- *Inspetor I-01: “ver os pontos cegos, aqueles pontos que ou não sabe, ou tem dúvida... esses pontos vão ajudar a gente a definir novas sprints com base nas orientações que contam no checklist (...) isso é muito massa porque a gente não só pode aplicar nesse projeto que a gente avaliou, mas estender para outros projetos”.*
- *Inspetor I-02: “provoca indagações, porque se a gente tem dúvida ou não sabe, então tem algo que precisa evoluir, melhorar, ficar mais claros (...) Será uma coisa que a gente pode está multiplicando não só para um mais para vários outros projetos”.*
- *Inspetor I-03: “ajuda a localizar os pontos não muito claros do projeto em relação às leis da LGPD (...) um dos benefícios é verificar aonde é que a gente não consegue enxergar o que o projeto consegue entregar da LGPD”.*

Nota-se na opinião dos três inspetores que o *checklist* consegue explorar lacunas no sistema para identificar possíveis defeitos, esclarecer as dúvidas do projeto em relação à lei, auxiliar na criação de novas sprints para evolução do sistema, além de adquirir experiência e conhecimento sobre os novos requisitos que a lei determina, que poderá se aplicar não só no sistema inspecionado, quanto para os vários outros projetos no futuro. A segunda questão diz sobre alguns problemas encontrados no uso do *checklist*: ***Quais mudanças você faria no checklist para melhorar a identificação de defeitos/problemas no sistema?***

- *Inspetor I-01: “Eu não. Estou bem tranquilo, eu gostei”. Inspetor I-02: “Eu não. Referente a isso, eu não tenho nenhuma mudança”.*
- *Inspetor I-03: “Gostei muito a respeito das recomendações, porém sobre o comentário do avaliador, acredito que ficou muito aberto, pode ficar perdido (...) Para pontos*

importantes, seria uma sugestão colocar um comentário mínimo (...) trancar ou obrigar a pessoa”.

A primeira sugestão de melhoria é sobre a ferramenta criada para automatizar o preenchimento do *checklist*, na coluna comentários do avaliador. Analisando a planilha com o *checklist*, é descrito possíveis comentários que os avaliadores deveriam realizar, porém, realmente não tem nenhuma informação quando deveria ser realizado, e nem mesmo a ferramenta obriga a fazê-lo. Nesse caso, uma melhoria seria tentar criar uma forma de informar automaticamente o avaliador a comentar nos casos importantes, e descrever da melhor maneira. Já a próxima questão diz sobre: ***Vocês acharam as recomendações úteis no entendimento da pergunta em si, e podem ajudar a resolver os possíveis defeitos?***

- *Inspetor I-01: “No meu entendimento ajudou, e até inclusive me forçou a pesquisar informações que pensava que fazia e não fazia, e coisas que eu fazia que não sabia que fazia (...) Então no meu caso ajudou bastante”.*
- *Inspetor I-03: “As recomendações para mim, foram uma surpresa boa, que eu consegui entender o contexto daquilo em relação à pergunta, ficou muito mais claro (...) Para mim, foi positivo”.*

Segundo os inspetores, as recomendações listadas na planilha de preenchimento do *checklist* foram úteis e surpreendeu positivamente, onde ajuda e motiva a se especializar ainda mais no assunto. Sobre os materiais de apoio, foi questionado na reunião: ***Para vocês as instruções e o vídeo de treinamento para preenchimento do checklist foram úteis?***

- *Inspetor I-01: “Achei as orientações do PDF, do Excel tá bem didático e que os materiais são necessários (...) A planilha realmente ficou bem feita e também o tutorial, ficou muito bem elaborado, e acredito que o caminho é manter isso mesmo.”.*
- *Inspetor I-03: “No meu ponto de vista o próprio Excel ele já me orienta muito bem aonde que devo colocar as informações (...) na questão do comentário e sobre o grau de severidade, eu não sei se limitasse ou obrigasse a pessoa a colocar, ela já entenderia que precisa colocar, meio que só essa única coisa que ficou solta”.*

De fato, houve uma preocupação de facilitar o processo de inspeção do *checklist*, desde o vídeo tutorial explicando o objetivo, as funcionalidades existentes, até o próprio artefato do *checklist*, deixando-o bem intuitivo para que os inspetores possam preencher corretamente e com rapidez. Com a ressalva no campo de comentário do avaliador, que no

primeiro momento, foi planejado para ser opcional, no entanto, para alguns inspetores, o melhor seria obrigar em certos casos. Em relação à completude do *checklist*, foi debatido com os participantes: ***Você considera o checklist completo em relação à aderência a LGPD? Se não, que aspectos você acha que devem ser incluídos para que todos os possíveis defeitos sejam identificados?***

- *Inspetor I-01: “Acredito que assim (...) a 2 semanas atrás a LGPD se tornou causa pétrea, participando do artigo quinto do inciso, e agora faz parte do direito fundamental (...) Acho interessante criar só uma rotina de atualização do checklist, em decorrente dessa atualização que teve”.*
- *Inspetor I-02: “Para mim, compreendeu bastante coisa (...) me provocou até para pesquisar algumas coisas que a gente pensa que sabe e não sabe (...) me proporcionou até um conhecimento a mais”.*
- *Inspetor I-03: “Na minha cabeça englobou bastante (...) eu não sei se tem informações extras a mais em contextos específicos, para mim, está bem, eu não consigo afirmar se ainda falta coisa ou não, para mim, está completo”.*

Para alguns inspetores, por terem um conhecimento intermediário sobre LGPD, não conseguiam avaliar se precisaria incluir algum requisito a mais. Porém, forneceram uma sugestão que vale destacar, sobre manter uma rotina de atualização para acompanhar decretos, leis, incisos e entre outras regulamentações. É algo que deve ser analisado, uma forma de viabilizar esse procedimento de atualização da técnica em casos de mudanças no regulamento. Outro questionamento realizado foi a respeito do processo interno da empresa: ***Haveria algum aspecto muito específico da empresa em que você acrescentaria ao checklist para melhor tratar o problema?***

- *Inspetor I-01: “Tem perguntas que fogem do meu entendimento porque fica com uma parte terceirizada do processo (...) Como sugestão, seria prever cenários aos quais a equipe de desenvolvimento seja terceirizada, para que a pesquisa se estenda para todos os membros tanto da empresa legada quanto da terceirizada”.*
- *Inspetor I-03: “Eu tava lendo a LGPD, pensando no cenário que fosse exclusivamente do nosso sistema, até um que não se encaixava, era questão de criança e adolescente não é o foco da empresa (...) Por mim tá ótimo, eu não tenho nada a acrescentar, por mim, está bom já”.*

Avaliar aderência de um sistema complexo é uma tarefa difícil, visto que a LGPD engloba áreas com equipes de setores diferentes. As empresas devem criar canais para que as informações possam ser compartilhadas entre os setores. O *checklist* proposto avalia

os requisitos que a lei determina de maneira geral. No futuro, pretende-se incorporar questões específicas envolvendo outros contextos, designando um papel responsável para quem avalia. Por fim, foi discutido a respeito das facilidades e dificuldades enfrentadas durante a inspeção, temos: ***Quais aspectos foram fáceis e difíceis ao utilizar o checklist na inspeção?***

- *Inspetor I-01: “Para mim, foi bem tranquilo, a dificuldade que teve foi natural (...) em relação somente com aquelas perguntinhas assim de coisas que eu realmente desconhecia (...) fui provocado a pesquisar, isso aí é massa, é bom, a ideia é essa mesma”.*
- *Inspetor I-02: “A meu ver, as coisas que achei difícil, ficou assim um entendimento na identificação de algumas coisas relacionadas às pessoas (...) se elas estão disponibilizando ou não (...) aí é onde a gente cai em campo, pesquisando tudinho”.*
- *Inspetor I-03: “Em relação ao checklist achei bem prático, bem direto ao ponto (...) só uma revisão de como o texto está escrita (...) em relação ao Excel, para mim, está ótimo, eu consigo entender onde começa onde termina”.*

Por ser baseado de um texto jurídico, o *checklist* abrange questões complexas sobre a legislação, porém, a intenção é apoiar o entendimento dos inspetores buscarem lacunas nos seus sistemas a fim de detectar inconformidades e corrigir o mais rápido possível. A maioria dos inspetores tinha conhecimento intermediário sobre a LGPD, instigados a se aprofundarem mais no assunto, e para alguns participantes, tiveram o *checklist* como um guia, para melhor adequação à LGPD.

5.2.4 Limitações e Ameaças à Validade

Em todos os estudos existem ameaças que podem afetar a validade dos resultados. Este trabalho é uma aplicação prática na indústria, e não foi fundamentado em um estudo experimental, por isso não possui uma análise estatística, ou variáveis dependentes e independentes. Portanto, algumas validades, como a validade interna, que está mais voltada a força do método estatístico, não se aplica a este trabalho. As limitações encontradas e ameaças relacionadas a este estudo, que precisam ser consideradas, serão apresentadas a seguir.

Uma primeira limitação é que o estudo foi aplicado apenas em uma empresa, e com um número baixo de participantes. Devido a este fato, não é possível generalizar os resultados encontrados, sendo estes considerados não conclusivos, e evidências iniciais, sendo necessário realizar outras avaliações para concluir se esses resultados se aplicam em outras empresas.

Os profissionais da indústria nesse estudo, possuem conhecimento razoável a intermediário sobre a LGPD. Portanto, não podemos avaliar a completude total dos itens do checklist de inspeção em relação a sua experiência. Para facilitar a compreensão dos inspetores, acrescentamos ao *checklist* uma lista de recomendações de implementação do item, que facilita o entendimento do regulamento, na prática, além também de um vídeo tutorial, explicando o funcionamento da técnica proposta.

Outra limitação foi em relação à discriminação de defeitos, devido ao pouco tempo de disponibilidade dos participantes, alguns itens do *checklist* não foram levados para reunião de discriminação. Uma solução para amenizar a ameaça à validade, foi levar para reunião todos os itens que havia alguma discordância entre os inspetores. Aqueles itens que eram unânimes, ou seja, que todos concordaram serem defeitos, foram discutidos entre os moderadores do estudo.

Em relação aos indicadores para caracterizar a técnica proposta, considerou-se a definição dos indicadores eficiência, eficácia, e o modelo TAM, os quais são comumente utilizados em estudos que investigam técnicas de detecção de defeitos. No entanto, houve uma limitação na medição do tempo de uso total do checklist pelos inspetores, na qual, foi solicitado que os participantes informassem o tempo gasto para uso do checklist, isso acaba afetando o cálculo da eficiência dos inspetores, por não ter sido coletado de forma mais precisa.

5.3 Considerações Finais

Este capítulo apresentou a aplicação prática do checklist de inspeção da LGPD, com profissionais que atuam na indústria de software. Na aplicação foram realizadas análises quantitativas, qualitativas e uma análise com o modelo Tam.

No geral, os resultados mostram indícios que a técnica de *checklist* de inspeção para LGPD pode ser aplicada em um contexto real na indústria, para avaliar os sistemas de software quanto a sua aderência à lei, e também que cumpre seu objetivo na detecção de defeitos. Contudo, os resultados qualitativos indicam que ainda existem possibilidades de melhoria que será discutido no próximo capítulo, sobre os refinamentos da técnica proposta.

6 Refinamento do *Checklist* a partir dos Resultados do Estudo

Após aplicação prática do *checklist* de inspeção na indústria, os profissionais que participaram do estudo, deram feedback sobre a técnica de inspeção utilizada, por um formulário de pós-inspeção, e também da realização de um grupo focal entre os participantes, para discutir as vantagens e desvantagens do uso do *checklist*.

O resultado do estudo apresentou evidências da viabilidade de uso, porém, devido à baixa quantidade de participantes, e também pela técnica já ter passado por alguns processos de refinamentos, foram poucas sugestões e oportunidades de melhorias apontadas pelos participantes, mas foram atendidas, implementadas, e algumas colocadas para um estudo mais aprofundado no futuro.

6.1 Sugestões implementadas para o checklist LGPD-CHECK

A primeira melhoria foi sobre Comentário do Avaliador. Alguns inspetores tiveram dificuldade em entender o campo de comentário no artefato do *checklist*, como é informado: “*sobre o comentário, penso que ficou muito aberto, não ficou objetivo*”; essa dificuldade aconteceu por não ter sido bem definido em quais casos é necessário o preenchimento. Dessa forma, implementamos um campo com aviso para o avaliador: Não se esqueça de inserir o grau de severidade e um comentário sobre o defeito! nos casos em que for preenchido que o item é um defeito, informando também sobre o grau de severidade.

Na reunião do grupo focal e no formulário de pós-inspeção, analisamos as principais dúvidas dos participantes. Por exemplo, no item: (D-08) O sistema remove os dados pessoais do titular após o término de seu tratamento; “*que tratamento é esse?*” relata um inspetor. Nesse caso, no campo de recomendação que pode ser consultado pelo inspetor, adicionamos a descrição: De acordo com a LGPD, alguns tipos de tratamentos de dados: coleta, armazenamento, classificação, modificação, extração, entre outros.

Outro inspetor diz sobre a questão que deve excluir os dados do usuário, no item (D-07) “*se resulta em excluir os dados do sistema atual e excluir os dados de vários backups que a gente armazena*”. Como sugestão, incluímos a descrição em recomendação: Recomenda-se um mapeamento dos dados pessoais, para que o sistema entenda quais lugares estaria armazenado, e que a estrutura do banco precisa está igual para remover os dados pessoais, inclusive dos vários backups, caso seja necessário.

No item (D-01) O sistema armazena os dados pessoais em formato que facilite o

titular de dados acessá-los, pergunta um inspetor: “qual o nível de acesso que o usuário possui para ele ter acesso, é user normal, um super admin”. Para melhor compreensão, inserimos nas descrições em recomendação: Recomenda-se que a empresa gerencie o nível de acesso aos dados que o usuário possui, para poder atender ao critério de consulta, cópia, portabilidade, edição, exclusão, entre outros direitos que a LGPD determina.

Sobre o artefato do checklist LGPD, a planilha em formato Excel restringe a realização de inspeção somente para aquele tipo de formato. Além disso, o avaliador não consegue visualizar o tempo que lhe custou preencher o checklist, para acompanhar seu desempenho. Desse modo uma alternativa é exportar o checklist de inspeção para planilha Google, para que assim, poderá além da facilidade de preencher online, em qualquer computador sem ter a necessidade de instalação de uma executador de planilha, ganha a segurança de backup dos dados, de salvar a inspeção de forma automática, podendo exportar para outros tipos de formatos, além de contabilizar o tempo gasto para preenchimento. O checklist LGPD-CHECK pode ser utilizado por engenheiros de software, controladores e oficiais de proteção de dados DPO. A seguir será apresentada uma versão do checklist para uso do titular de dados, conforme a sua perspectiva sobre o sistema e seus dados pessoais.

6.2 Versão do *Checklist* para o Titular de Dados

Conforme a lei LGPD ([BRASIL, 2018](#)), o titular de dados é toda pessoa a quem se referem os dados que são objeto de tratamento, detentores do direito de obter informações sobre o tratamento de seus dados, a forma em que ocorrerá, duração, entre outros. Por isso, o titular é uma peça fundamental para avaliar a aderência dos sistemas computacionais que realizam o tratamento de dados pessoais.

Desse modo, foi implementada uma versão do *checklist* de inspeção através de uma revisão por pares, analisando os itens de verificação do checklist proposto anteriormente, e transformando para que os titulares de dados, ou usuários do sistema, possam avaliar a adequação do sistema, conforme a sua perspectiva. Desta forma, os itens do *checklist* foram analisados para o perfil do titular, e reescritos para atender a avaliação do ponto de vista do titular. Alguns itens específicos para empresa não se encaixam nessa nova versão do *checklist*, pois o titular não tem o acesso por de trás do sistema que está sendo utilizado, e também questões relacionados a organização, especificamente as responsabilidades do controlador de dados. A Tabela 6.1 apresenta como aconteceu a transformação dos itens do *checklist* para versão do titular.

Tabela 6.1 – Transformação do *checklist* para versão do Titular de Dados

Cod.	Itens Empresa	Itens Titular
------	---------------	---------------

T-01	As finalidades de tratamento de dados foram definidas na organização?	Você foi informado sobre as finalidades do tratamento de seus dados pessoais, de uma forma acessível e fácil de entender?
C-06	O sistema informa o titular sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	Você foi informado ou notificado previamente sobre as mudanças de finalidade e atualização de consentimentos, podendo revogar o consentimento caso discorde das alterações?
D-02	O sistema fornece ao titular de dados, meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?	Você possui meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?
C-07	O sistema fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo termos abusivos?	A declaração de consentimento foi facilmente compreendida, não contendo termos abusivos?
T-06	O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?	Você tem acesso para consultar todos os seus dados de forma fácil e gratuita?

Com essa versão, os titulares dos dados recebem a ferramenta necessária para avaliar seus direitos à privacidade, o direito de estar no controle de como seus dados pessoais são processados. E a empresa recebe um diagnóstico importante do ponto de vista do usuário, a sua percepção para adequação dos sistemas de software em relação a LGPD. A tabela 6.2 apresenta os 28 itens do checklist para o titular de dados, classificados em 3 categorias: transparência, consentimento e os direitos do titulares. Para acessar o checklist completo, poderá ter acesso pelo link: ¹

Tabela 6.2 – Versão do *checklist* de inspeção aplicado ao Titular de Dados

Cat.	Itens
T	Sobre Transparência de Dados
T-01	Você foi informado sobre as finalidades do tratamento de seus dados pessoais, de uma forma acessível e fácil de entender?

¹ Checklist Titular de Dados: <<https://shre.ink/mQGr>>

Tabela 6.2 – Continuação da página anterior

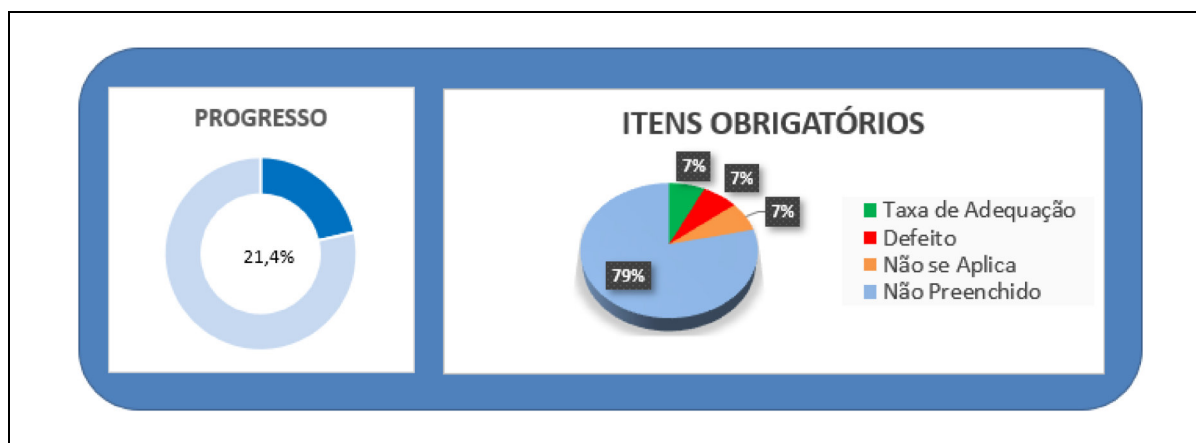
Cat.	Itens
T-02	Você foi informado sobre a forma e duração do tratamento dos dados pessoais, de forma gratuita e acessível?
T-03	Você tem acesso para consultar todos os seus dados de forma fácil e gratuita?
T-04	Você tem acesso às informações da identidade do controlador dos seus dados?
T-05	Você tem acesso às informações sobre o tratamento dos seus dados pessoais?
T-06	Você foi informado da existência do tratamento dos seus dados, antes da coleta?
C	Sobre Consentimento do Titular
C-01	O sistema apresentou o consentimento claramente?
C-02	Você deu o seu consentimento de livre e espontânea vontade?
C-03	No caso de compartilhamento de dados com outros controladores, você autorizou em um consentimento específico?
C-04	O sistema permitiu meios para recusar ou retirar o seu consentimento sem nenhum prejuízo?
C-05	Quando há tratamento de dados de crianças e adolescentes, o sistema solicita o consentimento específico dos pais ou responsável legal, de uma forma acessível e fácil de entender?
C-06	Você foi informado ou notificado previamente sobre as mudanças de finalidade e atualização de consentimentos, podendo revogar o consentimento caso discorde das alterações?
C-07	A declaração de consentimento foi facilmente compreendida, não contendo termos abusivos?
C-08	O sistema informa sobre todos os seus direitos no consentimento?
C-09	Para compartilhamento de dados para países estrangeiros, o sistema solicita sua autorização especificamente?
D	Sobre os Direitos do Titular
D-01	Você possui meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?
D-02	O sistema fornece a cópia eletrônica integral dos seus dados pessoais?
D-03	O sistema permite você atualizar seus dados pessoais?
D-04	O sistema permite solicitar a portabilidade ou transferir os seus dados pessoais?
D-05	O sistema permite solicitar a remoção dos seus dados pessoais?
D-06	O sistema fornece informações das entidades e das operações de tratamento, caso tenha compartilhado seus dados pessoais?
D-07	O sistema informa sobre a possibilidade de não fornecer consentimento e sobre as consequências caso recuse?

Tabela 6.2 – Continuação da página anterior

Cat.	Itens
D-08	O sistema informa quando o tratamento de dados é condição para o fornecimento de produto, serviço ou para o exercício de direito?
D-09	O sistema permite o direito de se opor ao tratamento de dados de forma fácil?
D-10	O sistema informa em caso de impossibilidade de adoção imediata dos seus direitos?
D-11	O sistema informa quando uma decisão foi tomada com base em tratamento automatizado que afetem seus interesses, incluídas as decisões destinadas à criação do seu perfil pessoal?
D-12	O sistema fornece a opção de contestar ou solicitar revisão da decisão automatizada?
D-13	O sistema permite solicitar a transferência internacional dos seus dados de forma segura?

A Figura 6.1 apresenta o gráfico dos itens referentes ao *checklist* de inspeção para avaliar a perspectiva do titular de dados. Nesse gráfico temos o percentual de preenchimento do *checklist*, chamado de progresso, temos o percentual de aderência dos itens a LGPD, e também o percentual de defeitos encontrados ou inconformidades. e por fim temos o percentual de itens não aplicáveis e itens que não foram preenchidos.

Figura 6.1 – Itens Obrigatórios do Titular de Dados



6.3 Considerações Finais

Este capítulo apresentou oportunidades de melhorias para técnica desenvolvida do checklist de inspeção LGPD. O refinamento e correções foi baseado no resultado da avaliação do checklist aplicado com profissionais em um contexto real na indústria. Os

principais aspectos corrigidos foram em relação à lista de recomendações, nos itens D-01, D-07, D-08. Sobre o campo de comentário do avaliador, foi adicionado um campo de lembrete para melhor descrição pelos inspetores na detecção dos defeitos.

Além disso, foi gerado uma nova versão do *checklist*, para avaliação na perspectiva do titular de dados, que poderá avaliar o sistema do seu ponto de vista, e analisar como os seus dados estão sendo tratados, se estão protegidos, e na verificação dos seus direitos como titular dos dados pessoais. O último capítulo a seguir, mostrará as conclusões referentes a esta pesquisa, e as perspectivas futuras sobre o tema.

7 Conclusão e Trabalhos Futuros

Esta dissertação de mestrado apresentou uma pesquisa sobre avaliação da adequação dos sistemas computacionais à lei brasileira de proteção de dados pessoais. Visando apoiar equipes de desenvolvimento de software, esse trabalho desenvolveu um *checklist* de inspeção para a avaliação de aderência de sistemas computacionais à LGPD.

A etapa inicial apresentou uma revisão da literatura, de modo a identificar as principais técnicas utilizadas para avaliar os sistemas de softwares relacionados aos regulamentos sobre tratamento de dados. Além disso, identificou atributos de qualidade que o regulamento da LGPD determina para adequação dos sistemas. A proposta inicial do *checklist* surgiu a partir da análise de atributos extraídos da Lei LGPD, de um mapeamento sistemático da literatura, e de uma revisão informal de artigos de áreas complementares à computação. Como resultado preliminar, foi gerado uma primeira versão do *checklist*, com 52 itens em formato de perguntas, relacionados ao sistema de software e à empresa ou controlador de dados, agrupados em cinco categorias, sendo elas: transparência de dados, consentimento, direitos do titular, segurança dos dados e responsabilidade do controlador.

A prova de conceito indicou resultados promissores com relação ao uso do checklist para identificar defeitos que revelariam futuras inconsistências com relação à lei. Quando comparado com o trabalho de (ROJAS, 2020), obteve-se um resultado superior, encontrando 16 defeitos adicionais. Tais resultados servem como apoio para direcionar recursos para áreas de não conformidade, possibilitando assim, a redução do risco de penalidades da LGPD.

No segundo momento, foi realizado um refinamento do *checklist* de inspeção, por feedback fornecido por uma especialista que atua na indústria e na implementação da LGPD, além de revisores de conferências sobre engenharia de software. O primeiro refinamento do *checklist* dividiu os itens de verificação em duas partes: itens obrigatórios e não obrigatórios. Depois, para diminuir ambiguidades e facilitar a leitura do item, foi analisado se haveria oportunidades de dividir cada item em itens mais específicos e objetivos, como por exemplo: itens que antes possuíam mais de um atributo no mesmo item (clareza, facilidade, integridade).

Além disso, foi desenvolvido um artefato para automatizar a aplicação do *checklist* na realização de inspeções de software. Foi gerado uma segunda versão do *checklist*, agora com 56 itens totais, seguindo a divisão de itens obrigatórios e não obrigatórios, além da adição de campos onde os inspetores poderiam indicar o grau de severidade do defeito encontrado, comentários sobre cada item, e visualizar recomendações para soluções da aderência dos itens de checagem. Por fim, o artefato apresenta gráficos com os percentuais

de conformidade, defeito, e itens não aplicáveis.

Em seguida, buscou-se avaliar a viabilidade da técnica proposta e dos artefatos gerados. Para isso, o *checklist* foi aplicado diretamente por profissionais da indústria em um sistema real, para avaliar o seu desempenho. Os inspetores efetuaram o preenchimento do *checklist*, para encontrar possíveis defeitos no sistema que realiza tratamento de dados. O *checklist* foi avaliado em relação a sua facilidade de uso, utilidade e intenção de uso, eficácia e eficiência. Além disso, foi realizado uma reunião com os inspetores para discriminação de defeitos, além de debater os pontos fortes e fracos da técnica apresentada em um grupo focal.

Os profissionais que atuaram como inspetores, diagnosticaram 42 defeitos reais na inspeção, obtendo uma eficácia média de 54,16% e uma eficiência média (defeitos por hora) de 14,79. O resultado da análise quantitativa indica uma evidência de que a técnica de *checklist* para LGPD cumpre com o seu propósito. Seguindo a análise com o modelo TAM dos dados coletados nos formulários de pós-inspeção, para maioria dos inspetores, a técnica foi fácil e útil para identificar defeitos e possibilitar uma melhor adequação dos requisitos que a lei obriga. Outros concordam, mais ressaltam que *checklist* demanda um pouco de esforço mental. Sobretudo, a maioria dos inspetores utilizará no futuro o *checklist* e o recomendaria para outras empresas.

Para análise qualitativa que coletou os dados da reunião do grupo focal com os participantes, apresentou resultados positivos no uso do *checklist*, considerado apropriado para inspeções, além de esclarecer as dúvidas do projeto em relação à lei, auxiliará na evolução do sistema para melhor adequação à lei. No entanto, foram apontadas algumas oportunidades de melhorias, implementadas: definir a funcionalidade do campo de comentário para o avaliador, alertar quando é obrigatório utilizar; ajustar o campo de recomendações, adicionando melhores descrições.

Por fim, o trabalho apresenta uma versão adicional do *checklist* de inspeção, para que os titulares de dados, ou usuários do sistema, possam avaliar a adequação do seu ponto de vista, avaliando o quanto seus dados pessoais estão sendo protegidos. Desse modo, os itens do *checklist* foram reescritos para atender a avaliação do ponto de vista do titular de dados.

Espera-se que os resultados obtidos neste trabalho de mestrado sejam utilizados para melhoria do estado atual das pesquisas sobre adequação à LGPD e na qualidade de software. Espera-se também apoiar as equipes de desenvolvimento de software, fornecendo um *checklist* mais confiável, robusto e apropriado para utilização pela indústria de software, viabilizando a manutenção segura dos dados dos usuários.

7.1 Trabalhos Futuros

O desenvolvimento dessa pesquisa de mestrado nos permitiu criar um *checklist* de inspeção para avaliar sistemas computacionais à LGPD. Os resultados dessa pesquisa fornecem novas perspectivas que podem ser exploradas no futuro. A seguir, são apresentados alguns trabalhos futuros:

- Desenvolver um mecanismo para atualizar os itens de verificação do *checklist* conforme a lei for alterada, para deixar os itens de checagem sempre atualizados.
- Desenvolver uma ferramenta completa de compliance, com a opção de carregar o *checklists* geral para LGPD, adicionar outros mais específicos para inspeção, como o checklist do titular, checklist específico para IOT.
- Adicionar campos dinâmicos, usando validação para habilitar ou desabilitar campos opcionais e obrigatórios.
- Automatizar a geração de relatório da inspeção, com filtros para selecionar listagem de defeitos encontrados, itens aderentes, percentual do grau de adequação, sem os itens não aplicáveis.
- Realizar uma prova de conceito e um estudo experimental para avaliar o checklist específico para o titular de dados, avaliando a aplicabilidade no processo de desenvolvimento de sistemas computacionais que lidem com o processamento de dados.
- Desenvolver Padrões de Projeto ou soluções catalogadas para situações comuns que a LGPD determina, definindo como os sistemas computacionais devem ser modelados e implementados a fim de adequar-se a LGPD.
- Utilizar o checklist de inspeção LGPD como base para avaliar sistemas específicos e de outras áreas da computação, podendo ser estendido em um novo contexto. Como, por exemplo, o trabalho de Neto, que utilizou como base o checklist de inspeção, estendendo novos itens específicos para avaliar sistemas IoT.

7.2 Contribuições

As principais contribuições dessa dissertação de mestrado são:

- Uma revisão sobre técnicas de avaliação e dos atributos de qualidade obrigatórios e recomendáveis da qual a lei geral de proteção de dados pessoais determina para os sistemas computacionais.

- A criação de um *checklist* de inspeção específico para lei geral de proteção de dados LGPD. Esse *checklist*, contém itens baseados no texto jurídico da lei 13.709/2018, além de artigos encontrados na literatura sobre LGPD e outros regulamentos, como a europeia GDPR.
- Desenvolvimento de um artefato que automatiza o preenchimento do *checklist*, facilitando a inspeção dos sistemas computacionais em relação aos atributos que a LGPD impõe.
- Colaboração com a Universidade Federal de Pernambuco com a Universidade Federal do Maranhão, na realização da aplicação prática do *checklist* na Indústria; Realização de refinamentos e geração de outras versões do *checklist* para LGPD.
- Criação de um *Checklist* específico para o Titular de Dados, baseado no *checklist* proposto, para avaliar os sistemas computacionais em relação à LGPD do ponto de vista do usuário.
- Divulgação dos resultados iniciais dessa pesquisa por meio de artigos científicos. Durante o desenvolvimento dessa pesquisa, foi publicado um artigo com os resultados iniciais encontrados. A seguir, é apresentado o artigo publicado referente a essa pesquisa, e a submissão de outros artigos sobre os resultados da aplicação do *checklist*:

Artigos relacionados com essa pesquisa

- Publicado: MENDES, J. P.; VIANA, D; RIVERO, L. Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal In: SBES '21: 35th Brazilian Symposium on Software Engineering, 2021, Joinville Brazil. Proceedings of the 35th Brazilian Symposium on Software Engineering. New York, NY, USA: Association for Computing Machinery, 2021.
- Publicado: Neto, I.; Mendes, J; VIANA, D; RIVERO, L.; Waldemar; Soares, S. Extending a LGPD Compliance Inspection Checklist to Assess IoT Solutions: A Initial Proposal In: SBES '22: 36th Brazilian Symposium on Software Engineering, 2022.
- Em processo de Submissão: MENDES, J. P.; Neto, I.; Waldemar; Soares, S.; VIANA, D; RIVERO, L. Evaluating an Inspection Checklist for the Adequacy of Software System of LGPD In: ISys '22.

Referências

- ARAUJO, E. et al. Are my business process models compliant with lgpd? the lgpd4bp method to evaluate and to model lgpd aware business processes. In: *XVII Brazilian Symposium on Information Systems*. New York, NY, USA: Association for Computing Machinery, 2021. (SBSI 2021). ISBN 9781450384919. Disponível em: <<https://doi.org/10.1145/3466933.3466982>>. Citado na página 33.
- BARATI, M. et al. Privacy-aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, IEEE, 2021. Citado na página 34.
- BARTIÉ, A. *Garantia da qualidade de software*. [S.l.]: Gulf Professional Publishing, 2002. Citado na página 16.
- BASIL, V. R.; ROMBACH, H. D. The tame project: Towards improvement-oriented software environments. *IEEE Transactions on software engineering*, IEEE, v. 14, n. 6, p. 758–773, 1988. Citado na página 62.
- BASTOS, A. et al. Base de conhecimento em teste de software. *São Paulo*, v. 30, p. 32, 2007. Citado na página 59.
- BECKER, R. et al. Daisy: A data information system for accountability under the general data protection regulation. *GigaScience*, Oxford University Press, v. 8, n. 12, p. giz140, 2019. Citado na página 32.
- BERNARDI, E. et al. Brazilian scenarios for smart cities deployment from public policies perspectives. In: *2020 IEEE International Smart Cities Conference (ISC2)*. [S.l.: s.n.], 2020. p. 1–8. Citado na página 17.
- BLIX, F.; ELSHEKEIL, S. A.; LAOYOOKHONG, S. Data protection by design in systems development: From legal requirements to technical solutions. In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*. [S.l.: s.n.], 2017. p. 98–103. Citado na página 38.
- BRASIL, A. L. Lei 13.709/2018. *Regulamenta a proteção de dados*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>, v. 13709, 2018. Citado 2 vezes nas páginas 15 e 77.
- CABREJOS, L. J. E. R.; VIANA, D.; SANTOS, R. P. dos. Planejamento e execução de estudos secundários em informática na educação: Um guia prático baseado em experiências. *Jornada de Atualização em Informática na Educação*, v. 7, n. 1, p. 21–52, 2018. Citado 2 vezes nas páginas 23 e 24.
- CANEDO, E. D. et al. Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In: IEEE. *2021 IEEE 29th International Requirements Engineering Conference (RE)*. [S.l.], 2021. p. 58–69. Citado na página 16.
- CARVALHO, L. et al. Desafios de transparência pela lei geral de proteção de dados pessoais. In: SBC. *Anais do VII Workshop de Transparência em Sistemas*. [S.l.], 2019. p. 21–30. Citado na página 32.

- CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na lgpd (lei geral de proteção de dados do brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira-um estudo de caso/methodology for mapping and adequacy of the requirements listed in lgpd (brazil data protection general law number 13 709/18) in a financial institution-a case study. *Brazilian Journal of Business*, v. 2, n. 4, p. 3626–3648, 2020. Citado na página 22.
- COSTA, C. P. A. et al. Woocommerce e lgpd: Uma análise de uso e conformidade. In: SBC. *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro*. [S.l.], 2021. p. 100–103. Citado na página 33.
- DAVIS, F. D.; BAGOZZI, R. P.; WARSHAW, P. R. User acceptance of computer technology: A comparison of two theoretical models. *Management science*, INFORMS, v. 35, n. 8, p. 982–1003, 1989. [GS Search](#). Citado 2 vezes nas páginas 62 e 65.
- DUARTE, T. X. D. et al. Tecnologia, uso, coleta e tratamento de dados: o futuro do poder econômico? Universidade Nove de Julho, 2020. Citado na página 15.
- FERNANDES, M. A. Catalog of security requirements aligned with the general data protection regulation (gdpr)(eu) 2016/679. 2018. Citado na página 17.
- FERNANDEZ, A.; ABRAHÃO, S.; INSFRAN, E. Empirical validation of a usability inspection method for model-driven web development. *Journal of Systems and Software*, Elsevier, v. 86, n. 1, p. 161–186, 2013. [GS Search](#). Citado 2 vezes nas páginas 62 e 67.
- FERRÃO, S. É. R. et al. Diagnostic of data processing by brazilian organizations—a low compliance issue. *Information*, Multidisciplinary Digital Publishing Institute, v. 12, n. 4, p. 168, 2021. Citado na página 16.
- FERREIRA, A. Gdpr: What’s in a year (and a half)? In: *ICEIS (2)*. [S.l.: s.n.], 2020. p. 209–216. Citado na página 39.
- GEORGIOPOULOU, Z.; MAKRI, E.-L.; LAMBRINOUDAKIS, C. Gdpr compliance: Proposed technical and organizational measures for cloud providers. In: *Computer Security*. Cham: Springer International Publishing, 2020. p. 181–194. ISBN 978-3-030-42048-2. Citado na página 38.
- KALINOWSKI, M.; SPÍNOLA, R. O.; TRAVASSOS, G. H. Infra-estrutura computacional para apoio ao processo de inspeção de software. *III Simpósio Brasileiro de Qualidade de Software, Brasília, Brasil*, p. 62–77, 2004. Citado 2 vezes nas páginas 18 e 19.
- KNOCKAERT, M.; VOS, N. D. Ethical, legal and privacy considerations for adaptive systems. In: _____. *Engineering Data-Driven Adaptive Trust-based e-Assessment Systems: Challenges and Infrastructure Solutions*. Cham: Springer International Publishing, 2020. p. 267–296. ISBN 978-3-030-29326-0. Disponível em: https://doi.org/10.1007/978-3-030-29326-0_12. Citado na página 38.
- KUBICEK, K. et al. Checking websites’ gdpr consent compliance for marketing emails. *Proceedings on Privacy Enhancing Technologies*, Proceedings on Privacy Enhancing Technologies, 2022. Citado na página 34.
- LAITENBERGER, O.; BEIL, T.; SCHWINN, T. An industrial case study to examine a non-traditional inspection implementation for requirements specifications. *Empirical Software Engineering*, Springer, v. 7, n. 4, p. 345–374, 2002. Citado na página 17.

- LAITENBERGER, O.; EMAM, K. E.; HARBICH, T. An internally replicated quasi-experimental comparison of checklist and perspective based reading of code documents. *IEEE Transactions on Software Engineering*, v. 27, n. 5, p. 387–421, 2001. Citado na página 58.
- LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, v. 1, p. 39–52, 2021. Citado na página 15.
- MACHADO, R. et al. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. In: SBC. *Anais da XVII Escola Regional de Redes de Computadores*. [S.l.], 2019. p. 154–159. Citado na página 16.
- MCIVER, J.; CARMINES, E. G. *Unidimensional scaling*. [S.l.]: Sage, 1981. v. 24. [GS Search](#). Citado na página 65.
- MELO, S. M. Inspeção de software. *University of São Paulo: São Carlos, SP*, 2009. Citado na página 18.
- MENDES, J.; VIANA, D.; RIVERO, L. Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In: *Brazilian Symposium on Software Engineering*. [S.l.: s.n.], 2021. p. 263–268. Citado 2 vezes nas páginas 47 e 49.
- MORTE, A. B. et al. Uma análise sobre o uso de dlts no tratamento de dados pessoais: Aderência aos princípios e direitos elencados na lgpd. In: *Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações*. Porto Alegre, RS, Brasil: SBC, 2020. p. 74–87. ISSN 0000-0000. Disponível em: <<https://sol.sbc.org.br/index.php/wblockchain/article/view/12435>>. Citado 2 vezes nas páginas 22 e 32.
- MUNCINELLI, G. et al. Components of the preliminary conceptual model for process capability in lgpd (brazilian data protection regulation) context. In: . [S.l.: s.n.], 2020. Citado 3 vezes nas páginas 15, 22 e 23.
- NETO, M. M. F.; FREITAS, A. L. P. Metodologia para avaliação da qualidade de software sob a perspectiva da qualidade em serviços. 2011. Citado 2 vezes nas páginas 16 e 17.
- NIELSEN, J. Usability inspection methods. In: *Conference companion on Human factors in computing systems*. [S.l.: s.n.], 1994. p. 413–414. Citado na página 59.
- OLIVEIRA, N. de et al. Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019. Citado na página 31.
- PAUL, N. et al. Assessing privacy policies of internet of things services. In: JANCZEWSKI, L. J.; KUTYŁOWSKI, M. (Ed.). *ICT Systems Security and Privacy Protection*. Cham: Springer International Publishing, 2018. p. 156–169. ISBN 978-3-319-99828-2. Citado na página 33.
- PIURCOSKY, F. P. et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de Negócios*, v. 10, n. 23, p. 89–99, 2019. Citado 2 vezes nas páginas 15 e 16.

- PRESSMAN, R.; MAXIM, B. *Engenharia de Software-8ª Edição*. [S.l.]: McGraw Hill Brasil, 2016. Citado 2 vezes nas páginas 16 e 17.
- RINGMANN, S. D.; LANGWEG, H.; WALDVOGEL, M. Requirements for legally compliant software based on the gdpr. In: SPRINGER. *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*. [S.l.], 2018. p. 258–276. Citado 4 vezes nas páginas 15, 19, 32 e 35.
- ROJAS, M. A. T. Avaliação da adequação do instituto federal de santa catarina à lei geral de proteção de dados pessoais. 2020. Citado 5 vezes nas páginas 17, 32, 45, 46 e 82.
- SANCHEZ, D.; VIEJO, A.; BATET, M. Automatic assessment of privacy policies under the gdpr. *Applied Sciences*, v. 11, n. 4, 2021. ISSN 2076-3417. Disponível em: <<https://www.mdpi.com/2076-3417/11/4/1762>>. Citado na página 33.
- SAUER, C. et al. The effectiveness of software development technical reviews: A behaviorally motivated program of research. *IEEE Transactions on Software Engineering*, IEEE, v. 26, n. 1, p. 1–14, 2000. Citado na página 66.
- SHULL, F.; CARVER, J.; TRAVASSOS, G. H. An empirical methodology for introducing software processes. *ACM SIGSOFT Software Engineering Notes*, ACM New York, NY, USA, v. 26, n. 5, p. 288–296, 2001. Citado na página 62.
- SILVA, M. et al. Requisitos de privacidade para aplicações de crowdsourcing no contexto das cidades inteligentes. In: SBC. *Anais Estendidos do XVIII Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais*. [S.l.], 2019. p. 186–187. Citado na página 32.
- SOUZA, J. S. et al. The general law principles for protection the personal data and their importance. *arXiv preprint arXiv:2009.14313*, 2020. Citado 2 vezes nas páginas 15 e 16.

Apêndices

APÊNDICE A – Questionário de Caracterização e Consentimento

Tabela A.1 – Formulário com o termo de consentimento e o questionário de caracterização

	Formulário I
1)	Você concorda em participar desta pesquisa e disponibilizar os seus dados para análise? () Sim () Não
2)	E-mail *:
3)	Nome Completo do participante *:
4)	Idade *:
5)	Gênero *:
6)	Qual seu nível atual de escolaridade? *:
7)	Qual o nome do curso? *
8)	Qual cargo atual na empresa *
9)	Quanto tempo de experiência no cargo: *
10)	Já possui conhecimento sobre inspeção de software? * () Sim () Não
11)	Já possui conhecimento sobre a Lei LGPD? * () Sim () Não
12)	Descreva que tipo(s) de experiência(s) possui:

APÊNDICE B – Questionário de Pós-Inspeção

Tabela B.1 – Formulário de Pós Inspeção

	Formulário II
1)	Nome *:
2)	E-mail *
	Como base no uso deste checklist, selecione o seu grau de concordância com as afirmativas a seguir com relação a sua percepção de FACILIDADE DE USO do mesmo. *
3)	O checklist utilizado foi claro e fácil de entender. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
4)	De maneira geral, eu acho fácil encontrar defeitos problemas no sistema com o checklist utilizado. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
5)	O checklist utilizado demandou pouco esforço mental. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
	Como base no uso desta técnica, selecione o seu grau de concordância com as afirmativas a seguir com relação a sua percepção de UTILIDADE do mesmo. *
6)	O checklist utilizando me permite realizar a inspeção do sistema mais rapidamente. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
7)	O checklist utilizado melhora a minha produtividade ao identificar defeitos problemas no sistema. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
8)	Eu acho que o checklist utilizado é útil para encontrar defeitos problemas no sistema. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()

Tabela B.1 – Continuação da página anterior

	Formulário II
	Como base no uso desta técnica, selecione o seu grau de concordância com as afirmativas a seguir com relação a sua INTENÇÃO DE USO do mesmo. *
9)	Eu prevejo usar o checklist para encontrar defeitos problemas no sistema futuramente. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
10)	Assumindo que eu tenha acesso ao checklist, pretendo usá-lo para encontrar defeitos problemas em outros sistemas. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()
11)	Eu recomendaria o checklist utilizado para outras empresas. Concordo Totalmente () Concordo Parcialmente () Discordo Parcialmente () Discordo Totalmente ()

APÊNDICE C – Questionário do Grupo Focal

Tabela C.1 – Formulário com as questões discursivas do grupo focal

	Formulário III
1)	Quais são os principais benefícios que o checklist traz para sua empresa?
2)	Quais mudanças você faria no checklist para melhorar a identificação de defeitos/problemas no sistema?
3)	Vocês acharam as recomendações úteis no entendimento da pergunta em si, e podem ajudar a resolver os possíveis defeitos? *
4)	Para vocês as instruções e o vídeo de treinamento para preenchimento do checklist foram úteis?
5)	Você considera o <i>checklist</i> completo em relação à aderência a LGPD? Se não, que aspectos você julga que devem ser incluídos para que todos os possíveis defeitos sejam identificados?
6)	Haveria algum aspecto muito específico da empresa em que você acrescentaria ao checklist para melhor tratar o problema?
7)	Quais aspectos foram fáceis e difíceis ao utilizar o checklist na inspeção?

APÊNDICE D – Lista Completa de Defeitos Encontrados na Inspeção aplicado na Indústria

Tabela D.1 – Listagem de Defeitos

Cat.	Itens	Grau	Recomendações
	ITENS OBRIGATÓRIOS		
T	Sobre Transparência de Dados		
T-01	As finalidades de tratamento de dados foram definidas na organização?	Grave	Crie um documento definindo uma Política de Privacidade e os Termos de Consentimento, descrevendo quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	Grave	O sistema deve disponibilizar a Política de Privacidade e/ou Termos de Consentimento para o titular dos dados, sobre as finalidades de tratamento.
T-04	O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?	Grave	Revisar o consentimento e implementar as alterações que não estão de acordo com o que foi informado ao titular.
T-05	O sistema informa para o titular a forma e duração do tratamento dos seus dados pessoais de maneira gratuita e acessível?	Grave	Descreva no documento da Política de Privacidade e no Termo de Consentimento, sobre a forma que se realizará o tratamento de dados e qual a sua duração, disponibilizando essas informações sempre para o titular.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
T-06	O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?	Leve	Crie um canal de comunicação entre o titular e a empresa para facilitar que o titular possa requisitar a integralidade dos seus dados pessoais, sempre de forma gratuita e sem lentidão da operação.
T-07	O sistema armazena com exatidão e clareza os dados pessoais coletados dos titulares?	Grave	Durante a coleta, garanta que os dados pessoais estão sendo informados corretamente.
T-08	O sistema mantém atualizados os dados pessoais, conforme necessário e para o cumprimento da finalidade de seu tratamento?	Leve	Crie um processo para mapear e revisar os dados pessoais no banco de dados, e se descobrir que os dados pessoais estão incorretos, é necessário corrigir ou apagar o mais rápido possível.
T-09	O sistema disponibiliza para o titular as informações sobre a realização do tratamento de dados e a identidade do controlador?	Grave	Disponibilizar para o titular sobre: a) Finalidades de Processamento; b) A identidade e contato do controlador; c) Os dados envolvidos; d) A base legal; e) Detalhes de transferências de dados fora do Brasil; f) Período de retenção de dados; g) Os direitos do titular.
T-11	O sistema mantém registros das operações de tratamento de dados, especialmente quando baseado em seu legítimo interesse?	Grave	Armazenar no banco de dados informações sobre as operações de tratamento dos dados, para possíveis comprovações legais.
T-12	O sistema informa para o titular e autoridades competentes sobre informações de tratamento de dados, principalmente quando baseado em seu legítimo interesse?	Grave	Elaborar relatórios das operações de tratamento de dados, principalmente quando baseado no seu legítimo interesse, e disponibilizar quando requisitado para o titular e para as autoridades competentes, como a ANPD.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
T-13	O sistema realiza o tratamento de dados pessoais ou dados sensíveis, de forma que não possam ser conectados a um titular de dados, quando for requisitado?	Grave	Analisar quais dados pessoais deverão ser anonimizados, ou em outros casos, realizar uma pseudonimização.
T-14	O sistema informa ao titular de dados sobre a existência de tratamento dos seus dados, antes da coleta?	Grave	Disponibilizar ao titular, sempre em destaque e com avisos, sobre os dados pessoais que serão coletados e solicitar o consentimento do titular.
C	Sobre Consentimento do Titular		
C-01	O sistema permite que o titular forneça o seu consentimento de forma autônoma e clara, para realizar o tratamento de seus dados?	Grave	Recomenda-se usar uma linguagem clara e objetiva, sem propaganda enganosa, evitando caixas pré-marcadas, e também possuir uma opção para que o titular possa negar ou retirar o seu consentimento sem ter nenhum prejuízo.
C-02	O sistema solicita o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?	Grave	É obrigatório ser transparente para o titular sobre a finalidade de tratamento dos seus dados.
C-03	O sistema armazena o consentimento dado pelo titular para comprovações legais?	Grave	Armazenar no banco de dados os registros de consentimento do titular para comprovação.
C-04	O sistema permite ao titular de dados meios para recusar ou retirar o consentimento sem prejuízo ao titular?	Grave	O titular deve ter acesso ao seu termo de consentimento ou contrato com a opção de negar a realização do tratamento de dados.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
C-05	O sistema realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico pelos pais ou responsável legal, de uma forma acessível e fácil de entender?	Não se Aplica	Deve certificar que apenas o responsável legítimo poderá dar o consentimento, e somente ele poderá atualizá-lo.
C-06	O sistema informa o titular sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	Grave	Sempre que for alterar a finalidade de tratamento, deverá informar o titular da mudança e solicitar o novo consentimento para realizar o tratamento de dados, com a opção de negar o tratamento caso o titular discorde da alteração.
C-07	O sistema fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo termos abusivos?	Grave	O Termo de Consentimento deve ser bem escrito, com linguagem de fácil compreensão, respeitando os direitos do titular.
C-08	O sistema informa o titular de dados sobre todos os seus direitos no consentimento?	Grave	Informar no Termo de Consentimento e na Política de Privacidade, os direitos que os titulares de dados possuem.
D	Sobre os Direitos do Titular		
D-01	O sistema armazena os dados pessoais em formato que facilite o titular de dados acessá-los?	Grave	Os dados pessoais devem ser armazenados em formato comumente usados por computador, em arquivos estruturados, para que os aplicativos de software possam facilmente identificar, reconhecer e extrair os dados pessoais.
D-02	O sistema fornece ao titular de dados, meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?	Grave	Disponibilizar o contato de DPO ou responsável pelo tratamento de dados, na política de privacidade ou uma página exclusiva para reclamações.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
D-03	O sistema fornece a cópia eletrônica integral dos dados pessoais para o titular?	Grave	Transmitir diretamente os dados solicitados ao titular; ou fornecer acesso a uma ferramenta que permite que o próprio titular extraia os dados solicitados.
D-04	O sistema permite que o titular atualize seus dados pessoais?	Leve	É recomendado criar um mecanismo para que o próprio titular possa atualizar seus dados pessoais.
D-06	O sistema permite a portabilidade de dados a outro controlador mediante requisição do titular?	Leve	Os dados pessoais devem ser armazenados em formato acessível e legível por máquina, para poder exportar os dados do titular quando ele requisitar.
D-07	O sistema permite excluir os dados pessoais do titular, mediante a sua requisição?	Grave	Criar um mecanismo para que o titular possa solicitar a remoção dos seus dados pessoais.
D-08	O sistema remove os dados pessoais do titular após o término de seu tratamento?	Grave	É necessário excluir os dados pessoais do titular após o cumprimento da finalidade, no prazo estabelecido.
D-09	O sistema fornece informações sobre entidades públicas e privadas, caso tenha realizado compartilhamento de dados pessoais?	Leve	Armazenar as informações das entidades e das operações de tratamento realizadas, como o compartilhamento de dados, para comprovações legais e disponibilizar quando requisitado.
D-10	O sistema informa o titular sobre a possibilidade de não fornecer consentimento e sobre as consequências caso seja negada?	Grave	Deve fornecer no Termo de Consentimento a possibilidade de recusar o tratamento, e as consequências caso não queira consentir.
D-11	O sistema informa o titular quando o tratamento de dados for uma condição para fornecimento de produto, serviço ou para o exercício de direito?	Grave	Deve ficar claro no momento do consentimento do titular os objetivos e pré-requisitos do tratamento de dados.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
D-12	O sistema permite aos titulares, o direito de se opor a um tratamento de dados de forma fácil?	Grave	É necessário fornecer um mecanismo para que o titular consiga retirar seu consentimento. Caso o consentimento seja retirado, os dados do titular não poderão ser mais processados.
D-13	O sistema informa ao titular, as razões do não exercício imediato dos direitos do titular?	Grave	Comunicar que a empresa não é agente de tratamento dos dados e indicar, sempre que possível, o agente responsável; ou indicar as razões de fato, ou de direito que impedem a adoção imediata da operação.
D-14	O sistema informa ao titular quando uma decisão foi tomada com base no tratamento automatizado, incluídas as decisões destinadas à criação do seu perfil pessoal?	Grave	Disponibilizar para o titular as informações das decisões automatizadas realizadas.
D-15	O sistema fornece a opção do titular contestar ou solicitar revisão da decisão automatizada?	Grave	Caso seja requisitado, deverá revisar a decisão automatizada contestada, podendo interromper o tratamento de dados e realizar um novo consentimento para essa finalidade.
S	Sobre a Segurança de Dados		
S-02	O sistema respeita as normas de transferência de dados pessoais para países internacionais, com grau de proteção de dados pessoais adequado às normas da LGPD?	Catastrofófico	Verifique se o país destino da transferência tenha um nível de proteção igual ou superior aos previstos na LGPD, e/ou que a empresa destinatária comprove possuir as mesmas garantias de proteção através de normas ou certificados.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
S-03	O sistema informa para o titular sobre as informações das transferências dos dados pessoais realizadas para países internacionais?	Grave	Informar no documento da Política de Privacidade e no Termo de Consentimento, informações sobre a realização de transferências de dados para países internacionais.
R	Sobre a Responsabilidade do Controlador		
R-01	A organização indica um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais?	Grave	A organização deverá indicar um encarregado pelo tratamento de dados pessoais (DPO), podendo ser pessoa física ou pessoa jurídica, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional (ANPD).
R-02	A organização divulga publicamente de forma clara e objetiva a identidade e as informações de contato do encarregado DPO?	Leve	A informação deve estar de forma clara, na Política de Privacidade e no Termo de Consentimento, para que os titulares e a autoridade nacional possa ter acesso facilitado.
	ITENS NÃO OBRIGATÓRIOS		
No-S	Sobre a Segurança de Dados		
No-S01	O sistema utiliza boas práticas de proteção de privacidade, como privacy by design?	Leve	Como boa prática para o desenvolvimento e adequação do sistema, implementar a metodologia privacy by design.
No-S05	O sistema fornece a integridade dos dados pessoais, impedindo modificações?	Leve	Uma solução seria documentar os dados das auditorias realizadas para fornecer ao titular.
No-S06	O sistema mantém registros de auditorias de conformidades e disponibiliza informação ao titular de dados, caso requisitado?	Leve	A organização deve documentar um plano para correção de falhas ou incidentes de segurança.

Tabela D.1 – Continuação da página anterior

Cat.	Itens	Grau	Recomendações
No-S07	A organização possui um plano de correção a incidentes de privacidade e segurança?	Leve	É recomendável que os sistemas tenha uma certificação, que comprovem que seguem um código de conduta ou política de segurança confiável para aderência da lei de proteção de dados. Alguns exemplos: ISO 27001, ISO 27701.
No-R	Sobre a Responsabilidade do Controlador		
No-R01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?	Leve	Armazene e documente o histórico de atividades do encarregado DPO.

APÊNDICE E – Checklist de Inspeção

LGPD-CHECK - Versão Final

Segue abaixo a versão final do checklist de inspeção proposto, chamado de LGPD-CHECK, e pode ser operacionalizado através do link a seguir: ¹

Tabela E.1 – Checklist de Inspeção Completo para LGPD - Versão 2

Cat.	Itens	Recomendações
	ITENS OBRIGATÓRIOS	
T	Sobre Transparência de Dados	
T-01	As finalidades de tratamento de dados foram definidas na organização?	Crie um documento definindo uma Política de Privacidade e os Termos de Consentimento, descrevendo quais são os objetivos de tratamento de dados e de que forma os dados serão utilizados.
T-02	O tratamento de dados pessoais é realizado de acordo com uma base legal?	Na documentação da Política de Privacidade e dos Termos de Consentimento, explique a base legal em que fundamenta o tratamento de dados pessoais.
T-03	O sistema informa ao titular sobre as finalidades de tratamento de dados pessoais?	O sistema deve disponibilizar a Política de Privacidade e/ou Termos de Consentimento para o titular dos dados, sobre as finalidades de tratamento.
T-04	O sistema realiza o tratamento de dados em conformidade com a finalidade apresentada ao titular?	Revisar o consentimento e implementar as alterações que não estão de acordo com o que foi informado ao titular.

¹ Checklist Final: <<https://shre.ink/mQVf>>

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
T-05	O sistema informa para o titular a forma e duração do tratamento dos seus dados pessoais de maneira gratuita e acessível?	Descreva no documento da Política de Privacidade e no Termo de Consentimento, sobre a forma que se realizará o tratamento de dados e qual a sua duração, disponibilizando essas informações sempre para o titular.
T-06	O sistema permite o titular consultar sobre a integralidade dos seus dados pessoais de maneira gratuita e acessível?	Crie um canal de comunicação entre o titular e a empresa para facilitar que o titular possa requisitar a integralidade dos seus dados pessoais, sempre de forma gratuita e sem lentidão da operação.
T-07	O sistema armazena com exatidão e clareza os dados pessoais coletados dos titulares?	Durante a coleta, garanta que os dados pessoais estão sendo informados corretamente.
T-08	O sistema mantém atualizados os dados pessoais, conforme necessário e para o cumprimento da finalidade de seu tratamento?	Crie um processo para mapear e revisar os dados pessoais no banco de dados, e se descobrir que os dados pessoais estão incorretos, é necessário corrigir ou apagar o mais rápido possível.
T-09	O sistema disponibiliza para o titular as informações sobre a realização do tratamento de dados e a identidade do controlador?	Disponibilizar para o titular sobre: a) Finalidades de Processamento; b) A identidade e contato do controlador; c) Os dados envolvidos; d) A base legal; e) Detalhes de transferências de dados fora do Brasil; f) Período de retenção de dados; g) Os direitos do titular.
T-10	A organização realiza o tratamento de dados quando baseado no seu legítimo interesse, de forma adequada com a lei?	A empresa deve realizar uma análise do legítimo interesse para verificar se a hipótese de tratamento pode se enquadrar na base legal.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
T-11	O sistema mantém registros das operações de tratamento de dados, especialmente quando baseado em seu legítimo interesse?	Armazenar no banco de dados informações sobre as operações de tratamento dos dados, para possíveis comprovações legais.
T-12	O sistema informa para o titular e autoridades competentes sobre informações de tratamento de dados, principalmente quando baseado em seu legítimo interesse?	Elaborar relatórios das operações de tratamento de dados, principalmente quando baseado no seu legítimo interesse, e disponibilizar quando requisitado para o titular e para as autoridades competentes, como a ANPD.
T-13	O sistema realiza o tratamento de dados pessoais ou dados sensíveis, de forma que não possam ser conectados a um titular de dados, quando for requisitado?	Analisar quais dados pessoais deverão ser anonimizados, ou em outros casos, realizar uma pseudonimização.
T-14	O sistema informa ao titular de dados sobre a existência de tratamento dos seus dados, antes da coleta?	Disponibilizar ao titular, sempre em destaque e com avisos, sobre os dados pessoais que serão coletados e solicitar o consentimento do titular.
C	Sobre Consentimento do Titular	
C-01	O sistema permite que o titular forneça o seu consentimento de forma autônoma e clara, para realizar o tratamento de seus dados?	Recomenda-se usar uma linguagem clara e objetiva, sem propaganda enganosa, evitando caixas pré-marcadas, e também possuir uma opção para que o titular possa negar ou retirar o seu consentimento sem ter nenhum prejuízo.
C-02	O sistema solicita o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?	É obrigatório ser transparente para o titular sobre a finalidade de tratamento dos seus dados.
C-03	O sistema armazena o consentimento dado pelo titular para comprovações legais?	Armazenar no banco de dados os registros de consentimento do titular para comprovação.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
C-04	O sistema permite ao titular de dados meios para recusar ou retirar o consentimento sem prejuízo ao titular?	O titular deve ter acesso ao seu termo de consentimento ou contrato com a opção de negar a realização do tratamento de dados.
C-05	O sistema realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico pelos pais ou responsável legal, de uma forma acessível e fácil de entender?	Deve certificar que apenas o responsável legítimo poderá dar o consentimento, e somente ele poderá atualizá-lo.
C-06	O sistema informa o titular sobre as mudanças de finalidade e atualização de consentimentos, podendo o titular revogar o consentimento caso discorde das alterações?	Sempre que for alterar a finalidade de tratamento, deverá informar o titular da mudança e solicitar o novo consentimento para realizar o tratamento de dados, com a opção de negar o tratamento caso o titular discorde da alteração.
C-07	O sistema fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo termos abusivos?	O Termo de Consentimento deve ser bem escrito, com linguagem de fácil compreensão, respeitando os direitos do titular.
C-08	O sistema informa o titular de dados sobre todos os seus direitos no consentimento?	Informar no Termo de Consentimento e na Política de Privacidade, os direitos que os titulares de dados possuem.
D	Sobre os Direitos do Titular	
D-01	O sistema armazena os dados pessoais em formato que facilite o titular de dados acessá-los?	Os dados pessoais devem ser armazenados em formato comumente usados por computador, em arquivos estruturados, para que os aplicativos de software possam facilmente identificar, reconhecer e extrair os dados pessoais. Recomenda-se que a empresa gerencie o nível de acesso aos dados que o usuário possui, para poder atender ao critério de consulta, cópia, entre outros.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
D-02	O sistema fornece ao titular de dados, meios para registrar reclamações em relação à proteção e ao tratamento de seus dados pessoais?	Disponibilizar o contato de DPO ou responsável pelo tratamento de dados, na política de privacidade ou uma página exclusiva para reclamações.
D-03	O sistema fornece a cópia eletrônica integral dos dados pessoais para o titular?	Transmitir diretamente os dados solicitados ao titular; ou fornecer acesso a uma ferramenta que permite que o próprio titular extraia os dados solicitados.
D-04	O sistema permite que o titular atualize seus dados pessoais?	É recomendado criar um mecanismo para que o próprio titular possa atualizar seus dados pessoais.
D-05	O sistema utiliza apenas dados relevantes e adequados à finalidade?	É recomendado realizar a anonimização de dados desnecessários, realizar bloqueio ou eliminação dos dados pessoais irrelevantes.
D-06	O sistema permite a portabilidade de dados a outro controlador mediante requisição do titular?	Os dados pessoais devem ser armazenados em formato acessível e legível por máquina, para poder exportar os dados do titular quando ele requisitar.
D-07	O sistema permite excluir os dados pessoais do titular, mediante a sua requisição?	Criar um mecanismo para que o titular possa solicitar a remoção dos seus dados pessoais. Recomenda-se um mapeamento dos dados pessoais, para que o sistema entenda quais lugares estaria armazenado, e que a estrutura do banco precisa está igual para remover os dados pessoais, inclusive dos vários backups, caso seja necessário.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
D-08	O sistema remove os dados pessoais do titular após o término de seu tratamento?	É necessário excluir os dados pessoais do titular após o cumprimento da finalidade, no prazo estabelecido. De acordo com a LGPD, alguns tipos de tratamentos de dados: coleta, armazenamento, classificação, modificação, extração, entre outros.
D-09	O sistema fornece informações sobre entidades públicas e privadas, caso tenha realizado compartilhamento de dados pessoais?	Armazenar as informações das entidades e das operações de tratamento realizadas, como o compartilhamento de dados, para comprovações legais e disponibilizar quando requisitado.
D-10	O sistema informa o titular sobre a possibilidade de não fornecer consentimento e sobre as consequências caso seja negada?	Deve fornecer no Termo de Consentimento a possibilidade de recusar o tratamento, e as consequências caso não queira consentir.
D-11	O sistema informa o titular quando o tratamento de dados for uma condição para fornecimento de produto, serviço ou para o exercício de direito?	Deve ficar claro no momento do consentimento do titular os objetivos e pré-requisitos do tratamento de dados.
D-12	O sistema permite aos titulares, o direito de se opor a um tratamento de dados de forma fácil?	É necessário fornecer um mecanismo para que o titular consiga retirar seu consentimento. Caso o consentimento seja retirado, os dados do titular não poderão ser mais processados.
D-13	O sistema informa ao titular, as razões do não exercício imediato dos direitos do titular?	Comunicar que a empresa não é agente de tratamento dos dados e indicar, sempre que possível, o agente responsável; ou indicar as razões de fato, ou de direito que impedem a adoção imediata da operação.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
D-14	O sistema informa ao titular quando uma decisão foi tomada com base no tratamento automatizado, incluídas as decisões destinadas à criação do seu perfil pessoal?	Disponibilizar para o titular as informações das decisões automatizadas realizadas.
D-15	O sistema fornece a opção do titular contestar ou solicitar revisão da decisão automatizada?	Caso seja requisitado, deverá revisar a decisão automatizada contestada, podendo interromper o tratamento de dados e realizar um novo consentimento para essa finalidade.
S	Sobre a Segurança de Dados	
S-01	O sistema realiza o tratamento de dados de uma forma segura, incluindo proteção contra acesso não autorizado?	Garantir a segurança no tratamento dos dados pessoais, possibilitando apenas indivíduos autorizados possam ler, modificar ou excluir dados do sistema.
S-02	O sistema respeita as normas de transferência de dados pessoais para países internacionais, com grau de proteção de dados pessoais adequado às normas da LGPD?	Verifique se o país destino da transferência tenha um nível de proteção igual ou superior aos previstos na LGPD, e/ou que a empresa destinatária comprove possuir as mesmas garantias de proteção através de normas ou certificados.
S-03	O sistema informa para o titular sobre as informações das transferências dos dados pessoais realizadas para países internacionais?	Informar no documento da Política de Privacidade e no Termo de Consentimento, informações sobre a realização de transferências de dados para países internacionais.
S-04	O sistema utiliza mecanismos para prevenir a ocorrência de danos, destruição ou perda de dados?	Como boas práticas, deve-se implementar um backup de dados, armazenamento em nuvem, e quaisquer outras ações que protegerão as informações originais em caso de danos, destruição ou perda de dados.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
S-05	O sistema utiliza medidas de proteção adequadas para dados pessoais sensíveis?	É necessário implementar uma camada adicional à segurança e armazenamento, especialmente aos dados pessoais sensíveis.
R	Sobre a Responsabilidade do Controlador	
R-01	A organização indica um oficial de proteção de dados (DPO) encarregado pelo tratamento de dados pessoais?	A organização deverá indicar um encarregado pelo tratamento de dados pessoais (DPO), podendo ser pessoa física ou pessoa jurídica, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional (ANPD).
R-02	A organização divulga publicamente de forma clara e objetiva a identidade e as informações de contato do encarregado DPO?	A informação deve estar de forma clara, na Política de Privacidade e no Termo de Consentimento, para que os titulares e a autoridade nacional possa ter acesso facilitado.
R-03	A organização comunica à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos titulares, nos prazos estabelecidos pelas autoridades?	Na ocorrência de incidente de segurança, é necessário comunicar ao titular e autoridade nacional ANPD.
R-04	A organização realiza avaliação de impacto à proteção de dados pessoais, quando o tratamento resulta em um alto risco para os direitos e liberdades dos titulares dos dados?	A organização deve realizar uma avaliação de impacto de proteção de dados, quando existir um elevado risco no tratamento de dados.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
R-05	A organização realiza relatório de impactos à proteção de dados pessoais e disponibiliza a autoridade nacional, quando solicitado?	É necessário realizar um relatório de impactos à proteção de dados e disponibilizar-lo quando requisitado. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações.
	ITENS NÃO OBRIGATÓRIOS	
No-S	Sobre a Segurança de Dados	
No-S01	O sistema utiliza boas práticas de proteção de privacidade, como privacy by design?	Como boa prática para o desenvolvimento e adequação do sistema, implementar a metodologia privacy by design.
No-S02	O sistema realiza o mapeamento dos dados pessoais e mantém em segurança?	Organizar os locais onde os dados são coletados e armazenados.
No-S03	O sistema possui certificação ou selos, para comprovar a observância e o cumprimento das normas de proteção de dados pessoais?	Realizar a proteção contra acesso não autorizado, no uso de dados pessoais armazenados ou em transição, como exemplos realizar a autenticação e controle de acesso.
No-S04	O sistema fornece a confidencialidade, usando medidas técnicas apropriadas?	Verificar a integridade dos dados durante a coleta e no tratamento dos dados pessoais.
No-S05	O sistema fornece a integridade dos dados pessoais, impedindo modificações?	Uma solução seria documentar os dados das auditorias realizadas para fornecer ao titular.
No-S06	O sistema mantém registros de auditorias de conformidades e disponibiliza informação ao titular de dados, caso requisitado?	A organização deve documentar um plano para correção de falhas ou incidentes de segurança.

Tabela E.1 – Continuação da página anterior

Cat.	Itens	Recomendações
No-S07	A organização possui um plano de correção a incidentes de privacidade e segurança?	É recomendável que os sistemas tenham uma certificação, que comprovem que seguem um código de conduta ou política de segurança confiável para aderência da lei de proteção de dados.
No-R	Sobre a Responsabilidade do Controlador	
No-R01	A organização registra as atividades realizadas pelo DPO, para possíveis comprovações legais?	Armazene e documente o histórico de atividades do encarregado DPO.
No-R02	A organização realiza capacitação para seus funcionários sobre a aderência à LGPD?	Capacite os funcionários e colaboradores sobre as informações que a LGPD determina.