LGPDCHECK: INSPEÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM ARTEFATOS DE SOFTWARE À LUZ DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD - 13.709/2018)

Diego André Cerqueira

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientadores: Guilherme Horta Travassos

Rafael Maiani de Mello

Rio de Janeiro

Fevereiro de 2024

LGPDCHECK: INSPEÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM ARTEFATOS DE SOFTWARE À LUZ DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD - 13.709/2018)

Diego André Cerqueira

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Orientadores: Guilherme Horta Travassos
Rafael Maiani de Mello

Aprovada por: Prof. Guilherme Horta Travassos.
Prof. Rafael Maiani de Mello.
Profª. Claudia Maria Lima Werner.
Profª. Juliana de Albuquerque Gonçalves Saraiva.

RIO DE JANEIRO, RJ - BRASIL
FEVEREIRO DE 2024

Cerqueira, Diego André

LGPDCHECK: Inspeção de Privacidade e Proteção de Dados Pessoais em Artefatos de Software à Luz dos Princípios da Lei Geral de Proteção de Dados Pessoais (LGPD - 13.709/2018) / Diego André Cerqueira. – Rio de Janeiro: UFRJ/COPPE, 2024.

XI, 118 p.: il.; 29,7 cm.

Orientadores: Guilherme Horta Travassos

Rafael Maiani de Mello

Dissertação (mestrado) – UFRJ/COPPE/Programa de Engenharia de Sistemas e Computação, 2024.

Referências Bibliográficas: p. 85 – 90.

1. Inspeção de Software. 2. Privacidade e Proteção de Dados. 3.Engenharia de Software Experimental. I. Travassos, Guilherme Horta *et al*. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia de Sistemas e Computação. III. Título.

Dedico este trabalho à minha querida mãe, Maria da Glória

Agradecimentos

Em primeiro lugar, gostaria de agradecer à minha família, em especial à minha querida mãe, dona Glória, que sempre foi minha fã número um, torcendo, colaborando e contribuindo, de maneira carinhosa e sincera, para que eu pudesse chegar a este momento de me tornar mestre. Agradeço à Mônica Santana, psicóloga, quem cuidou da minha saúde mental durante esse período de formação. Profissional que me ofereceu estratégias para enfrentar essa árdua, muitas vezes solitária, jornada acadêmica.

A todos os profissionais que colaboraram direta e indiretamente para que essa ideia, pouco convencional, pudesse vir a tornar-se ciência. Em especial, àqueles que ouviram minhas inquietações e ideias e, de alguma forma, foram capazes de oferecer sugestões ou caminhos.

Aos meus orientadores Guilherme Horta Travassos e Rafael Maiani de Mello por colocarem à minha disposição seus conhecimentos e anos de experiência acadêmica, essenciais para costurar um monte de ideias em trabalho robusto sobre privacidade e proteção de dados pessoais dentro da Engenharia de software.

Aos professores e membros do corpo docente da COPPE/UFRJ, com os quais tive a oportunidade de aprimorar meus conhecimentos e me tornar um melhor Engenheiro de Software, contribuindo para minha trajetória como pesquisador. À equipe administrativa, Mercedes, Gutierrez, Ricardo e outros, por auxiliarem em todas as etapas administrativas relacionadas à vida acadêmica no PESC/COPPE/UFRJ.

Às professoras Cláudia Maria Lima Werner e Juliana de Albuquerque Gonçalves Saraiva por aceitarem participar da banca de avaliação deste trabalho e contribuírem com valiosas considerações e observações sobre esta dissertação.

A todos os participantes do grupo Engenharia de Software Experimental (ESE), pelas trocas em reuniões, questionamentos e colaborações. Em especial ao Bruno Pedraça, Helvio Jerônimo e Vladimir Erthal, que compartilharam diversos conhecimentos não apenas sobre engenharia de software, mas foram sensíveis, colaborativos e companheiros nos momentos mais complexos e delicados deste período do mestrado, que inclusive, atravessou uma pandemia.

Por último, mas não menos importante, ao meu amor, Max, que me acompanhou nesta jornada pessoal-profissional-acadêmica, desde o dia em que recebi o e-mail de aprovação no programa até o dia em que submeti esta dissertação. São anos de trocas, parcerias e muito companheirismo.

Resumo da dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

LGPDCHECK: INSPEÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM ARTEFATOS DE SOFTWARE À LUZ DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD - 13.709/2018)

Diego André Cerqueira

Fevereiro/2024

Orientadores: Guilherme Horta Travassos
Rafael Maiani de Mello

Programa: Engenharia de Sistemas e Computação

Leis recentes para garantir a Privacidade e Proteção de Dados Pessoais (PPD) estabelecem novos requisitos de software. Consequentemente, novas tecnologias são necessárias para garantir a qualidade do software sob PPD. Contudo, a literatura destaca a existência de lacunas relacionadas à compreensão e implementação dessas regulações em sistemas de software. Portanto, com base nos princípios e conceitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD - 13.709/2018), esta dissertação propõe a *LGPDCheck*: uma técnica de inspeção baseada em checklist para apoiar a identificação de defeitos de PPD em artefatos de software. Por meio de instrumentos e processos bem definidos, a *LGPDCheck* tem como objetivo reduzir a lacuna entre profissionais envolvidos no desenvolvimento de sistemas de software e conceitos previstos na LGPD. Sua ênfase está na oferta de artefatos projetados para oferecer maior tangibilidade aos conceitos e definições presentes no primeiro capítulo da lei, com linguagem e exemplos adaptados aos contextos de sistemas de software. Os resultados alcançados durante o estudo de viabilidade indicam que a técnica demonstrou um desempenho excepcional na identificação de defeitos, sendo bem recebida em termos de aceitação e utilidade pelos participantes da pesquisa.

Abstract of dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

LGPDCHECK: INSPECTION OF PRIVACY AND DATA PROTECTION IN SOFTWARE ARTIFACTS IN LIGHT OF THE PRINCIPLES OF THE BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD - 13.709/2018)

Diego André Cerqueira

February/2024

Advisors: Guilherme Horta Travassos
Rafael Maiani de Mello

Department: Computer Science and Systems Engineering

Recent laws to guarantee the Privacy and Data Protection (PDP) set new requirements for software. Consequently, new technologies are needed to guarantee software quality under PDP. However, the literature highlights the existence of gaps related to the understanding and implementation of these regulations in software systems. Therefore, based on the principles and concepts established by the Brazilian General Data Protection Law (LGPD - 13.709/2018), this dissertation proposes *LGPDCheck*: a checklist-based inspection technique to support the identification of PDP defects in software artifacts. Using instruments and well-defined processes, *LGPDCheck* aims to reduce the gap between the professionals involved in the software development cycle and the PDP concepts established by the LGPD. Its emphasis is on providing auxiliary resources, tailored to offer more tangible concepts and definitions from the first chapter of the law, with language and examples adapted to the context of software systems. The results obtained during the validation phase indicate that *LGPDCheck* and its artifacts not only achieved excellent performance in identifying defects, but also excellent acceptance and perceived usefulness by the participants in the study.

SUMÁRIO

1 INTRODUÇÃO 1

1.1 - Motivação e contexto 1
1.2 - A Lei Geral de Proteção de Dados Pessoais (LGPD - 13.709/2018) 3
1.2.1 - Aplicabilidade e Abrangência da LGPD (Art. 3º) 3
1.2.2 - Definições da LGPD (Art. 5º) 3
1.2.3 - Princípios da LGPD (Art. 6º) 4
1.3 - Problema e Questão de Pesquisa 5
1.4 - Objetivo 6
1.5 - Metodologia 6
1.6 - Organização do Texto 8

2 FUNDAMENTAÇÃO TEÓRICA: PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM ENGENHARIA DE SOFTWARE 10

2.1 - Práticas de Privacidade e Proteção de Dados em Engenharia de Software 10
2.2 - Entrevistas sobre Privacidade e Proteção de Dados Aplicados ao Ciclo de Desenvolvimento de Software 12
2.2.1 - Critérios de Inclusão 13
2.2.2 - Perfil das especialistas 13
2.2.3 - Roteiro da Entrevista 14
2.2.4 - Descobertas nas Entrevistas 15
2.3 - Considerações finais 18

3 FUNDAMENTAÇÃO TEÓRICA: INSPEÇÃO DE SOFTWARE 19

3.1 - Inspeção de Software 19
3.1.1 - Processo de Inspeção de Software 19
3.1.2 - Técnicas para Inspeção de Software 21
3.2 - Trabalhos Relacionados 23
3.3 - Considerações finais 25

4 DESENVOLVENDO A *LGPDCHECK* 26

4.1 - Dos Princípios da LGPD à Tecnologia de Inspeção 26
4.1.1 - Abordagem Multinível de Inspeção 27
4.1.2 - Priorização dos princípios da LGPD por Nível de Inspeção 28
4.1.2.1 - Processo de priorização dos princípios ao nível de Inspeção 28
4.2 - Artefatos de Apoio à Verificação da *LGPDCheck* 32
4.2.1 - Material de Apoio 33
4.2.1.1 - O Glossário de Termos de Privacidade e Proteção de Dados para Sistemas de Software 33
4.2.1.2 - Quadros dos Princípios da LGPD para Sistemas de Software 33
4.2.2 - Formulário de Discrepâncias 35
4.3 - Instrumentalização da *LGPDCheck* 35
4.3.1 - Processo de Verificação da LGPDCheck 35
4.3 - Considerações finais 38

5 ESTUDO DE VIABILIDADE *LGPDCHECK* 39

5.1 - Planejamento 39
5.1.1 - Formação dos Grupos 40
5.2 - Execução 42
5.3 - Resultados Quantitativos 45
5.3.1 - Etapa de Discriminação de Defeitos 45
5.3.1.2 - Defeito (ND) 45
5.3.1.3 - Defeito LGPD (DEF_LGPD) 46
5.3.1.4 - Falso Positivo (FP) 47
5.3.2 - Resultados gerais 47
5.3.3 - Resultados por Inspetores 48
5.3.4 - Resultados por Módulo e Rodada 53

5.3.4.1 - Resultados dos Defeitos tipo LGPD por Rodada 53
5.3.5 - Defeitos únicos *55*
5.3.5.1 - Defeitos por técnica (rodada) 60
5.3.5.2 - Defeitos por técnica por tempo (segundos) 61
5.3.5.3 - Defeitos por técnica, tempo e módulo 62
5.3.5.4 - Defeitos LGPD por técnica 64
5.4 - Resultados Qualitativos 66
5.4.1 - Avaliação dos Participantes *67*
5.4.1.1 - Visualização dos resultados por questão 68
5.5 - Considerações Finais 78
6 CONCLUSÃO 80
6.1 - Conclusão 80
6.2 - Contribuições 81
6.3 - Ameaças à Validade 82
6.4 - Limitações da Pesquisa 82
6.5 - Publicações 83
6.6 - Perspectivas Futuras 84
REFERÊNCIAS 85
APÊNDICE A – COLETA DE INFORMAÇÕES COM ESPECIALISTAS AS ESPECIALISTAS 91
APÊNDICE B – MATERIAL DE APOIO 92
APÊNDICE C – FORMULÁRIO DE DISCREPÂNCIAS *LGPDCHECK* 104
APÊNDICE D – FORMULÁRIO DE DISCREPÂNCIAS AD-HOC 105
APÊNDICE E – CHECKLIST DE VERIFICAÇÃO *LGPDCHECK* 106
APÊNDICE F – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE) 108
APÊNDICE G – FORMULÁRIO DE CARACTERIZAÇÃO DOS PARTICIPANTES . 109
APÊNDICE H – QUESTIONÁRIO DE AVALIAÇÃO *LGPDCHECK* 111
APÊNDICE I – PROTOCOLO DO ESTUDO DE VIABILIDADE *LGPDCHECK* 113
ANEXO I – OUTRAS DEFINIÇÕES DA LGPD (ART. 5º) 118

Lista de Tabelas

Tabela 1 - Vocabulário de conceitos da LGPD – Art.5 3
Tabela 2 - Princípios da LGPD (Art. 6º) 5
Tabela 3 - Perfil das especialistas entrevistadas 14
Tabela 4 - Roteiro de perguntas aos especialistas 15
Tabela 5 - Taxonomia de defeitos extraída de (TRAVASSOS, SHULL, et al., 1999) .. 21
Tabela 6 - Relação conhecimento do princípio da LGPD x uso pelas organizações (Extraído de (DIAS, ANGELICA, et al., 2022) adaptada) 25
Tabela 7 - Níveis de Inspeção 28
Tabela 8 - Grupo de princípios da LGPD 29
Tabela 9 - Princípios da LGPD VS Nível de Inspeção VS Priorização 32
Tabela 10 - Níveis de Inspeção, descrição, objetivos e princípios priorizados 38
Tabela 11 - Caracterização dos participantes do estudo de viabilidade *LGPDCheck* . 41
Tabela 12 - Grupos e participantes 41
Tabela 13 - Resumo do Experimento 43
Tabela 14 – Grupos, Rodadas, e Artefatos Inspecionados 43
Tabela 15 - Distribuição dos participantes 44
Tabela 16 - Números gerais das rodadas 47
Tabela 17 - Porcentagem de defeitos por rodada 47
Tabela 18 - Eficiência Ad-hoc x *LGPDCheck* 48
Tabela 19 - Resultados Ad-hoc por Inspetores 49
Tabela 20 - Resultados Ad-hoc por inspetores e tipos de defeito 50
Tabela 21 - Resultados *LGPDCheck* por inspetores e tipos de defeito 51
Tabela 22 - Resultados gerais x Tipo de Defeito 53
Tabela 23 - Resultados por Módulo e Defeitos LGPD 53
Tabela 24 - Defeitos por tipo LGPD por TIPO (O, FI, IN, A, IE) 54
Tabela 25 - Defeitos únicos Ad-hoc 57
Tabela 26 - Defeitos únicos *LGPDCheck* 58
Tabela 27 - Escala Likert do questionário de avaliação pontos e valores 67
Tabela 28 - Resultados gerais questionário de avaliação 68
Tabela 29 - Descrição das variáveis independentes 114
Tabela 30 - Descrição das variáveis dependentes 114
Tabela 31 - Grupos, Rodadas, e Artefatos Inspecionados 115

Lista de Figuras

Figura 1 - Etapas do processo de inspeção - Extraído de (KALINOWSKI, SPÍNOLA, et al., 2004) 20
Figura 2 - Visão geral construção da LGPDCheck 26
Figura 3 - Relação finalidade, necessidade e adequação 30
Figura 4 - Relação dos princípios Segurança, Prevenção, Não discriminação e Responsabilização e prestação de contas 31
Figura 5 - Relação dos princípios Livre acesso, Qualidade dos dados, Transparência 31
Figura 6 – Fluxo de Inspeção *LGPDCheck* 35
Figura 7 - Processo de Inspeção *LGPDCheck* expandido 37
Figura 8 - Defeitos Ad-hoc 51
Figura 9 - *LGPDCheck* defeitos 52
Figura 10 - Comparativo defeitos gerais Ad-hoc x *LGPDCheck* por tipo de defeito 52
Figura 11 - Ad-hoc defeitos tipo LGPD 54
Figura 12 - *LGPDCheck* defeitos tipo LGPD 54
Figura 13 - Comparativo defeitos associados à LGPD Ad-hoc x *LGPDCheck* por tipo de defeito 55
Figura 14 - Defeitos únicos MSL (Ad-hoc e LGPDCheck) 56
Figura 15 - Defeitos únicos MGU (Ad-hoc e LGPDCheck) 57
Figura 16 - Oneway Analysis of #Defects By Technique 60
Figura 17 – Teste de variância 60
Figura 18 - Oneway Analysis of Time (in seconds) By Technique 61
Figura 19 - Teste de variância 61
Figura 20 - Oneway Analysis of Time (in seconds) By Module 62
Figura 21 - Teste de variância 63
Figura 22 - Oneway Analysis of #Defects LGPD By Technique 64
Figura 23 - Teste de variância 64
Figura 24 - Oneway Analysis of #Defects *Ad-hoc* By Technique 65
Figura 25 - Teste de variância 65
Figura 26 - Percepção dos participantes sobre a facilidade de aplicação da *LGPDCheck* 68
Figura 27 - Percepção dos participantes sobre a facilidade de compreender as perguntas do Checklist da *LGPDCheck* 68
Figura 28 - Percepção dos participantes sobre a facilidade de compreender o material de apoio da *LGPDCheck* 69
Figura 29 - Percepção dos participantes sobre a facilidade de preencher o formulário de discrepâncias da *LGPDCheck* 69
Figura 30 - Percepção dos participantes sobre se a LGPDCheck os auxiliou a encontrar defeitos 70
Figura 31 - Percepção dos participantes se o checklist da LGPDCheck os auxiliou a encontrar defeitos 70
Figura 32 - Percepção dos participantes sobre se o Material de Apoio da *LGPDCheck* os auxiliou a encontrar defeitos 71
Figura 33 - Percepção dos participantes sobre usos futuros da *LGPDCheck* 71
Figura 34 - Percepção dos participantes sobre recomendação da *LGPDCheck* para outros profissionais 72
Figura 35 - Autoavaliação dos participantes sobre seus conhecimentos em Privacidade e proteção de dados pessoais em sistemas de software 75
Figura 36 - Autoavaliação dos participantes sobre o domínio do problema no Módulo de Gestão de Usuários (MGU) 75
Figura 37 - Autoavaliação dos participantes sobre o domínio do problema no Módulo de Solicitações (MSL) 76

1 Introdução

Neste capítulo são apresentados a motivação e contexto para a realização deste trabalho, além dos objetivos e metodologia utilizada. E por fim, a organização dessa dissertação.

1.1 - Motivação e contexto

Nas últimas décadas, com a produção massiva de dados causada pela popularização de dispositivos móveis, aparelhos inteligentes e o uso generalizado de redes sociais, a privacidade e a proteção de dados pessoais tornaram-se preocupações e necessidades globais. Nesse contexto, o direito à privacidade, reconhecido pela ONU desde 1948 como um direito humano universal (ONU, 1948), e à proteção de dados, são constantemente desafiados na era digital (UN, 2017). Em meio a esse cenário, é crucial reconhecer que, ao serem colocados em segundo plano por soluções e novas tecnologias, esses direitos propiciam o surgimento de violações difíceis de serem observadas pelos cidadãos, mas que podem ter impactos significativos em diversas esferas de suas vidas (UN, 2022).

Na tentativa de acompanhar tais inovações tecnológicas, em 2016, a União Europeia aprovou o Regulamento Geral sobre a Proteção de Dados - 2016/679 ou *General Data Protection Regulation* (GDPR), ordenamento jurídico sobre a temática de privacidade e proteção de dados e as principais atividades relacionadas ao tratamento de dados pessoais para o continente Europeu (PARLAMENTO EUROPEU E DO CONSELHO, 2016). Em efeito cascata, a criação da *GDPR* na Europa impulsiona países como o Brasil na regulamentação da matéria de forma estratégica (LEMOS, DOUDEK, et al., 2018), dando origem a Lei Geral de Proteção de Dados Pessoais (LGPD) - 13.709/2018, arcabouço legal com importantes definições à privacidade e à proteção de dados para a sociedade brasileira.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) e, na Europa, o Regulamento Geral de Proteção de Dados (GDPR), introduzem uma série de novos direitos aos cidadãos, reconhecidos como titulares dos dados. E para aqueles que processam, armazenam ou utilizam dados caracterizados como pessoal, ou seja, realizam algum tipo de tratamento de dados pessoais, foram atribuídos deveres e responsabilidades sobre suas atividades (BRASIL, 2018).

Embora o efeito positivo provocado pela aprovação, a criação de instrumentos regulatórios como a LGPD ou GDPR por si só não podem ser encarados como bala de prata aos múltiplos desafios relacionados à coleta e tratamento de dados de dados

pessoais na sociedade da informação. Em especial nos contextos de sistemas de software, onde são necessários além de instrumentos legais, ferramentas e processos de software que deem suporte à cultura de Privacidade e Proteção de Dados (PPD) ainda em formação.

Apesar da LGPD não tratar diretamente de produtos de software, os regulamentos de proteção de dados pessoais ao redor do mundo vêm impactando diversas atividades e processos relacionados ao desenvolvimento de sistemas de software (DIAS, ANGELICA, *et al.*, 2022). E mesmo assim, boa parte das organizações e profissionais possuem pouco conhecimento sobre os possíveis impactos que novas leis como a LGPD podem ter sobre suas atividades ou negócios (HADAR, HASSON, *et al.*, 2018). Agora com a lei em vigor, organizações e profissionais necessitam que seus produtos e práticas organizacionais atendam aos requisitos legais da LGPD, porém ainda há pouco ou nenhum suporte para que isso aconteça na prática.

Estabelecer uma mudança cultural em direção à PPD exige passos coletivos em direção à efetivação de novos direitos, deveres, e à consciência sobre os possíveis danos em decorrência de acessos indevidos, práticas abusivas ou coletas excessivas de dados pessoais. Esta mudança cultural se faz necessária não apenas para evitar possíveis sanções por não cumprimento à LGPD, mas também por ser crítica à qualidade de produtos e sistemas de software.

Em uma sociedade na qual o digital se faz cada vez mais presente, é imperativo que não só os cidadãos compreendam e façam uso de seus novos direitos adquiridos com a LGPD, mas que existam organizações e indivíduos comprometidos a construir sistemas de software aderentes às preocupações globais de privacidade e proteção de dados pessoais. São necessários esforços para que práticas cotidianas, como a coleta, manipulação e armazenamento dados pessoais, em serviços digitais ou analógicos, sejam constantemente repensadas e adaptadas.

Para além de engajados e comprometidos, estes profissionais precisam ser permitidos a contribuir ativamente para a Cultura de Privacidade e Proteção de Dados (CPP) em construção. E para isso, se faz necessário a elaboração de tecnologias, no amplo sentido, que auxiliem estas organizações e indivíduos a construir e refletir sobre seus requisitos, funcionalidades, produtos e práticas organizacionais à luz de arcabouços como a LGPD e necessidades globais de privacidade e proteção de dados pessoais.

1.2 - A Lei Geral de Proteção de Dados Pessoais (LGPD - 13.709/2018)

Este trabalho recorre, majoritariamente, ao primeiro capítulo da LGPD. Durante o desenvolvimento desta dissertação são utilizadas disposições gerais da lei, que se dedica aos fundamentos, ao propósito da legislação, aos termos e aos princípios aplicáveis a LGPD (GUIMARÃES, 2021).

1.2.1 - Aplicabilidade e Abrangência da LGPD (Art. 3º)

No Art. 3º é possível encontrar uma definição sobre a abrangência e escopo de aplicação da lei, ao verificar sua redação é possível verificar que a

> "(...) Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei." (BRASIL, 2018)

1.2.2 - Definições da LGPD (Art. 5º)

Ao recorrer à lei, é possível extrair diversos conceitos e definições importantes sobre privacidade e proteção de dados, que auxiliam não só na definição de conceitos, mas também na normatização de um vocabulário comum de termos associados à cultura de proteção de dados pessoais. Ainda no Capítulo I, no Art. 5º da LGPD são definidos os 19 principais conceitos em relação ao universo da proteção de dados, numerados do inciso I ao XIX, e que foram adotados por convenção na construção deste trabalho. Neste trabalho são utilizados 12 dos 19 conceitos na lei, que podem ser vistos na Tabela 1.

Tabela 1 - Vocabulário de conceitos da LGPD – Art.5

Conceito	Definição
I - Dado Pessoal	informação relacionada a pessoa natural identificada ou identificável;
II - Dado Pessoal Sensível	dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - Dado Anonimizado	dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
IV - Banco de Dados	conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
V - Titular	pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - Controlador	pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
VII - Operador	pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlado
VIII - Encarregado	pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
IX - Agentes de Tratamento	o controlador e o operador;
X - Tratamento	toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XI - Anonimização	utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - Consentimento	manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

1.2.3 - Princípios da LGPD (Art. 6º)

No Capítulo I, o Art. 6, em 10 incisos, são definidos os princípios da LGPD. Os princípios previstos em lei são a base para qualquer atividade de tratamento, que, ao serem realizadas, devem ser observados, além da boa-fé. Princípios que auxiliam não apenas na compreensão de fundamentos da lei, mas para guiar todo tipo tratamento previstos no Art. 5, inciso X que define tratamento como

> "(...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018).

Os dez princípios da LGPD e suas definições podem ser vistos na Tabela 2.

Tabela 2 - Princípios da LGPD (Art. 6º)

Princípio	Descrição
I - Finalidade	realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - Adequação	compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - Necessidade	limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - Livre Acesso	garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - Qualidade Dos Dados	garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - Transparência	garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - Segurança	utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - Prevenção	adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - Não Discriminação	impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - Responsabilização e Prestação de Contas	demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1.3 - Problema e Questão de Pesquisa

Com o estabelecimento de novas leis como a LGPD e GDPR, novos requisitos relacionados à privacidade e à proteção de dados pessoais surgem no território nacional. Seu impacto pode ser percebido em diversas atividades, incluindo aquelas relacionadas ao desenvolvimento de sistemas de software (DIAS, ANGELICA, *et al.*, 2022), criando desafios aos profissionais envolvidos. Esses desafios surgem devido à falta de treinamento, compreensão das leis ou dificuldades em incorporar os requisitos legais nos projetos e fluxos de trabalho de software (SERASA EXPERIAN, 2020).

Ao recorrer a literatura, é possível evidenciar lacunas de conhecimento entre os profissionais técnicos e em relação aos requisitos jurídicos sobre como atuar na implementação dos direitos, deveres e responsabilidades previstas em leis. Uma possível explicação pode estar relacionada ao tipo de conhecimento específico sobre linguagem jurídica, necessário para compreender os arcabouços jurídicos (GÜRSES,

TRONCOSO, et al., 2011), não exclusivo à LGPD. Regulações ou textos jurídicos são repletos de referências a outros arcabouços, ainda fazendo uso de vocabulários de domínio específico e ambiguidades. Características da escrita jurídica que dificultam a extração de requisitos e conceitos que podem ser aplicados ao ciclo de desenvolvimento de software (OTTO, ANTON, 2007). Problemas atenuados pela falta de tecnologias e metodologias capazes de suportar o trabalho de profissionais envolvidos no ciclo de desenvolvimento de produtos de software (SHAPIRO, 2010).

Estreitar a lacuna entre as áreas jurídicas e técnicas exige que a privacidade e a proteção de dados façam parte integral da cultura dos profissionais envolvidos no desenvolvimento de software de software (GÜRSES, TRONCOSO, DIAZ et al., 2011, 2015). Mas para isso, são necessários que princípios e requisitos de PPD presentes em arcabouços como a LGPD sejam compreendidos e instrumentalizados durante o desenvolvimento de soluções e sistemas. A realização dessa tarefa será possível apenas quando houver artefatos, ferramentas e metodologias que organizem o conhecimento e auxiliem os profissionais a extrair, compreender e instrumentalizar requisitos presentes em arcabouços jurídicos, como a LGPD (SHAPIRO, 2010).

Com objetivo de contribuir para a redução desta lacuna entre áreas de conhecimento e fomentar o desenvolvimento de uma cultura de PPD na disciplina de engenharia de software, este trabalho busca responder à pergunta de pesquisa: *"Pode uma técnica de inspeção baseada em checklist melhorar a eficácia e a eficiência das inspeções para verificar a conformidade dos sistemas de software com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD)?"*

1.4 - Objetivo

O objetivo deste trabalho é desenvolver uma tecnologia de inspeção de software, baseada em evidência, para apoiar a verificação de artefatos de software conforme os princípios da LGPD. Especificamente, este trabalho se propõe a construir uma técnica de inspeção, baseada em *checklist,* para a apoiar a identificação de defeitos (falta de conformidade com os princípios da LGPD) nos artefatos produzidos em diferentes etapas do ciclo de desenvolvimento de software.

1.5 - Metodologia

O desenvolvimento deste trabalho segue uma metodologia de pesquisa inspirada em *Design Science* (DS) de March e Smith (1995), uma abordagem muito utilizada em Sistemas de informação e Engenharias. Seu objetivo é resolver problemas do mundo real através da instrumentalização de conhecimentos específicos de um

campo ou área, e auxiliar profissionais a criar soluções para problemas a partir das experiências ou vivências na área (ENGSTRÖM, STOREY, et al., 2020).

Ao invés de propor teorias, a DS busca criar modelos, métodos e implementações que sejam inovadoras e gerem valor. Esta dissertação busca conectar-se com esta prática através da:

1) Realização de Entrevistas com Especialistas em Direito: foram conduzidas entrevistas com profissionais com formação em Direito, especializados em Direito Digital, com atuação na interseção entre a área jurídica e o desenvolvimento de produtos de software. Nesta etapa, o objetivo foi investigar a aplicação prática da LGPD a partir da experiência de profissionais que atuam na aplicação da LGPD nos contextos de desenvolvimento de sistemas de software. O objetivo foi reunir informações relevantes sobre o *modus operandi* das profissionais em relação à implementação da LGPD em produtos de software. Como resultado, foram coletadas diversas práticas utilizadas por estas especialistas durante a aplicação da LGPD.
2) Levantamento Bibliográfico em PPD na Engenharia de Software: foi realizado um levantamento bibliográfico sobre as práticas de Proteção de Dados (PPD) na Engenharia de Software. O levantamento foi realizado com o propósito de compreender os principais arcabouços, práticas, dificuldades e desafios relacionados à implementação de Privacidade e Proteção de dados no desenvolvimento de sistemas de software.
3) Levantamento Bibliográfico em Inspeção de Software: etapa em que foi realizado um levantamento bibliográfico sobre inspeção de software e técnicas de inspeção. Esta etapa, concentrou-se na identificação dos tipos de técnicas de inspeção disponíveis na literatura, processo de inspeção e seus principais artefatos. Também foram identificados diversos trabalhos e abordagens que buscam aproximar a Privacidade e Proteção de Dados com a Engenharia de Software.
4) Desenvolvimento da Técnica de Inspeção *LGPDCheck*: nessa etapa foram exploradas abordagens para conectar o arcabouço jurídico da lei ao desenvolvimento de sistemas. Os esforços focaram na integração do conteúdo teórico da LGPD, especialmente do Capítulo I, com linguagem acessível aos profissionais, visando reduzir o jargão jurídico. Durante esta etapa, foram construídos os artefatos que compõem a técnica de inspeção,

cujo arcabouço é constituído por: **(I)** Níveis de Inspeção: em que os princípios da LGPD foram priorizados em dois níveis de inspeção; **(II)** Material de Apoio: composto do **(a)** Glossário de termos de Privacidade e Proteção de Dados para Sistemas de Software; **(b)** Quadros dos princípios da LGPD para Sistemas de Software; e **(c)** checklist de treinamento do inspetor. Além disso, são apresentados o **(IV)** checklist de inspeção, conjunto de perguntas da verificação orientada aos princípios da LGPD, **(V)** Fluxo de Inspeção da Técnica e **(VI**) Formulários de Discrepância.

5) Avaliação de viabilidade da Técnica da *LGPDCheck*: foi realizada a avaliação de viabilidade da técnica de inspeção e seus instrumentos através de um estudo de viabilidade. O estudo de viabilidade proposto para avaliar a eficiência e eficácia da técnica na identificação de defeitos. Por fim, neste estudo foram comparados diversos aspectos de inspeções tipo *Ad-hoc* e inspeções *LGPDCheck*, em análises quantitativas e qualitativas.

1.6 - Organização do Texto

Além do Capítulo 1 Introdução, que descreve o contexto geral em que este trabalho está inserido, apresenta os principais conceitos e termos presentes na Lei Geral de Proteção de Dados Pessoais (LGPD) incorporados no trabalho, o problema de pesquisa, objetivo e metodologia, esta dissertação está organizada da seguinte forma:

Capítulo 2 Fundamentação Teórica: Privacidade e Proteção de dados Pessoais em Engenharia de Software. Este capítulo apresenta a revisão bibliográfica sobre práticas de privacidade e proteção de dados (PPD) na disciplina de Engenharia de Software e seus desafios à implementação em sistemas de software. Detalha-se, ainda, a fase de entrevistas com profissionais especialistas em LGPD. Por fim, são apresentando diversos achados durante a etapa de entrevistas.

Capítulo 3 Fundamentação Teórica: Inspeção de Software: este capítulo apresenta os principais conceitos relacionados à Inspeção de Software, processo de inspeção de software e diversas técnicas de inspeção encontradas na literatura. Também inclui uma seção dedicada aos trabalhos relacionados e suas investigações sobre a LGPD em várias abordagens, com o objetivo de compreender e integrar a LGPD ao desenvolvimento de sistemas de software.

Capítulo 4 Desenvolvendo a *LGPDCheck*: este capítulo apresenta em detalhes o processo de construção da versão atual da *LGPDCheck*. Ademais, o capítulo conta com a descrição dos artefatos de apoio à verificação desenvolvidos e seus objetivos, e por fim, apresenta detalhes sobre o fluxo de aplicação da *LGPDCheck*.

Capítulo 5 Estudo de Viabilidade *LGPDCheck*: neste capítulo, são descritos o protocolo e estudo de viabilidade. Por fim, são apresentados os resultados quantitativos obtidos durante a execução do estudo, e por fim, são detalhados e discutidos os resultados qualitativos.

Capítulo 6 Conclusão: neste capítulo, são apresentadas as conclusões do estudo, destacando as principais colaborações do trabalho para a área, suas limitações, e por fim, as perspectivas futuras da pesquisa.

2 Fundamentação Teórica: Privacidade e Proteção de dados Pessoais em Engenharia de Software

Neste capítulo, são abordados os achados na bibliografia e desafios em relação à implementação da cultura de privacidade e proteção de dados na engenharia de Software.

2.1 - Práticas de Privacidade e Proteção de Dados em Engenharia de Software

Ao investigar a literatura sobre privacidade e proteção de dados, um conceito bastante difundido é o da Privacidade por Concepção ou *Privacy by Design* (PbD), conceito relevante e investigado globalmente, em especial no meio jurídico.

Proposto por Anne Cavoukian (2012), PbD tem sua origem na década de 1990, e busca de maneira conceitual ilustrar princípios para que a privacidade possa ser embarcada nos estágios iniciais de concepção até a sua implementação (CAVOUKIAN, 2009). Seus 7 princípios são: (I) proativo e não reativo, que foca na prevenção, (II) privacidade como configuração padrão, (III) privacidade incorporada ao design, (IV) funcionalidade completa, (V) segurança de ponta a ponta, (VI) visibilidade e transparência, e por fim, (VII) respeito à privacidade do usuário. Com a possibilidade de ser aplicado em tecnologias à negócios, e à diversas estruturas, sejam elas físicas ou digitais (CAVOUKIAN, 2009).

Na perspectiva de PbD, a preocupação com a privacidade, antes secundária no *modus-operandi* atual, passa a ser objetivo, onde não se espera por movimentos externos, como instrumentos legais, por exemplo, para agir sobre as questões de proteção de dados e privacidade (CAVOUKIAN, 2009).

Pesquisadores têm se debruçado sobre a temática de PPD a fim de compreender as principais questões relacionadas à sua implementação, seja o arcabouço de PbD proposto por Cavoukian, regulações ou leis de proteção de dados em geral. Gürses *et al*. (2011) evidenciam dificuldades causadas por vaguidade ou imprecisão de tais documentos em relação às definições de conceitos, e o que significa estar adequado tecnicamente à lei. Ao revelar tal distanciamento, na percepção dos engenheiros existem poucos recursos práticos *("How's to")* sobre como se dá a implementação de aparatos legais de PPD nos sistemas de forma prática. Uma saída possível parece ser a necessidade de trabalhos cada vez mais interdisciplinares, no

intercâmbio e compreensão entre essas duas grandes áreas (GÜRSES, TRONCOSO, *et al.*, 2011).

Com novas regulações sendo criadas ao redor do mundo, Gürses *et al.* (2015) argumentam sobre necessidades de mudanças na forma de pensar de parte de quem desenha e implementa sistemas. Os pesquisadores chamam atenção sobre as atividades de coleta e processamento de dados, relativamente comuns aos sistemas de software, em que profissionais envolvidos estão acostumados a coletar a maior quantidade de dados possíveis, sem que haja uma reflexão entre *"dados que eu posso coletar*" e *"dados que eu preciso coletar"* para uma determinada funcionalidade ou sistema (GÜRSES, TRONCOSO, *et al.*, 2015).

Dentre outros desafios, Hadar, Hasson *at al.* (2018) revelam, através de entrevistas com desenvolvedores de software, uma confusão conceitual em relação ao vocabulário por parte destes profissionais, em que conceitos de PPD são confundidos com os de segurança da informação. Através de um mapeamento sistemático, Morales-Morales-Trujillo *et. al* (2018) se debruçam sobre a implementação prática de Privacidade por Concepção (PbD) em Engenharia de Software. No mapeamento, os pesquisadores buscam organizar definições e compreensões sobre o que significa PbD nos contextos do ciclo de desenvolvimento de software (MORALES-TRUJILLO, MATLA-CRUZ, *et al.*, 2018). E, apesar da confusão conceitual identificada por Hadar, Hasson *at al.* (2018), há compreensão por parte dos profissionais que a inclusão do PbD pode ocorrer nos estágios mais iniciais da construção de produtos de software, ainda que faltem metodologias que suportem sua implementação nos diferentes estágios do ciclo de vida (MORALES-TRUJILLO, MATLA-CRUZ, *et al.*, 2018).

Shapiro (2010) argumenta que na implementação de um arcabouço como PbD na prática é necessária uma abordagem multinível, e que leve em consideração:

(1) Tradução efetiva de princípios abstratos de privacidade, modelos de risco de privacidade e mecanismos de privacidade em requisitos implementáveis;

(2) Integração dessas atividades em um processo de desenvolvimento de software apropriado;

(3) Incorporar esse processo ao ciclo de vida de desenvolvimento do software.

Ao observar a abordagem proposta pôr Shapiro (2010) em conjunto com as descobertas de Morales-Trujillo, Matla-Cruz, *et al.* (2018), compreende-se que para

instrumentalização de PbD na disciplina de Engenharia de Software é necessário a construção de artefatos e tecnologias que auxiliem os profissionais na materialização de conceitos “abstratos”, como sugerido por Gürses *et al*. (2011). Para que os benefícios da inclusão de PbD nos produtos de software possa de fato existir, se faz necessária a existência de metodologias capazes de traduzir tais princípios às práticas de Engenharia de Software (ALSHAMMARI, SIMPSON, 2017).

A necessidade por metodologias e artefatos que ofereçam apoio à inclusão de PbD no ciclo de desenvolvimento de software pode ser encarada como uma oportunidade para equipar os profissionais com capacidades de projetar, desenvolver produtos e práticas organizacionais alinhadas com PPD e PbD. Incluir requisitos e necessidades de arcabouços de PPD e PbD, desde as etapas mais iniciais do desenvolvimento, é investir na construção de produtos e sistemas de software mais confiáveis e com maior qualidade, cada vez mais alinhados às regulações como a LGPD.

2.2 - Entrevistas sobre Privacidade e Proteção de Dados Aplicados ao Ciclo de Desenvolvimento de Software

Para elucidar questões relacionadas às práticas de PPD, duas especialistas em direito digital, com ênfase na aplicação da LGPD, foram convidadas a compartilhar com seus repertórios e experiência na aplicação da LGPD durante o desenvolvimento de sistemas de software.

Para isso, foram realizadas entrevistas individuais e estruturadas, via videoconferência, cada uma com duração média de 60 minutos, realizadas em maio de 2022. As entrevistas foram gravadas e armazenadas, e posteriormente transcritas com auxílio de ferramentas de transcrição. Ambas as participantes consentiram com a gravação e utilização do conteúdo, desde que as informações utilizadas, mesmo para fins acadêmicos, não as identificassem individualmente ou as organizações as quais fazem parte. O processo de recrutamento foi realizado por meio de conexões pessoais dos pesquisadores envolvidos no desenvolvimento deste trabalho.

A etapa de entrevistas teve como objetivo a coleta de evidências, mesmo que anedóticas, e trazer à superfície detalhes sobre suas práticas de aplicação da LGPD. Nas seções seguintes é possível verificar em detalhes cada uma das etapas, desde a seleção das participantes, seus perfis, detalhes das perguntas e roteiro. Por fim, são apresentados os achados, evidências baseadas no conhecimento prático e aplicado das rotinas e conhecimento tácito que as especialistas possuem. Esperamos que os

achados encontrados durante a etapa promovam reflexões essenciais para o desenvolvimento das próximas etapas deste trabalho.

2.2.1 - Critérios de Inclusão

O perfil das profissionais consideradas aptas a participar da etapa de entrevistas seguiu os seguintes critérios:

1. **Experiência prática:** o primeiro requisito para inclusão das profissionais foi sua experiência prática com a aplicação da LGPD. Para ser considerada apta, era necessário ter participado de forma ativa no desenvolvimento de um sistema de software. Não foram feitos recortes em relação ao tempo de carreira da profissional, esta decisão é apoiada pelo fato de a regulação sobre o tema ser recente às realidades brasileiras.
2. **Atuação guarda-chuva temático do "Direito Digital" ou "Direito e Novas Tecnologias":** O direito digital nasceu da necessidade do direito a acompanhar evoluções tecnológicas e com a expansão da internet, responsáveis por introduzir novas complicações à sociedade da Informação (EDUARDO, PIMENTEL, 2018). A especialização na temática foi um critério relevante durante a consideração do perfil das profissionais no processo de entrevistas.
3. **Nível de Instrução:** Por conta da área de atuação, as profissionais além de possuir o título de Bacharel em Direito, precisavam também ter a carteira da Ordem dos Advogados do Brasil (OAB).

2.2.2 - Perfil das especialistas

As especialistas foram convidadas a compartilhar detalhes sobre suas áreas de atuação em formato de minibiografias, maiores detalhes como suas áreas de atuação, especialidades e temas de interesse (podem ser encontrados na Tabela 3). Após a caracterização, os dados das participantes foram anonimizados, ação de remover informações pessoais que possam auxiliar na identificação das participantes de forma individual ou instituições as quais pertencem. Esta estratégia adotada para proteger não apenas a privacidade das participantes entrevistadas, mas também para proteger possíveis segredos industriais e propriedade intelectual das organizações em que as especialistas representam durante as próximas etapas deste trabalho.

Para reportar as descobertas, um identificador foi atribuído a cada uma das especialistas, Especialista A e Especialista B. A convenção será utilizada para o desenvolvimento deste e futuros trabalhos.

Tabela 3 - Perfil das especialistas entrevistadas

ID	Formação Superior	Cargo	Observação	Temas de atuação
Especialista A	- Bacharel em Direito; - Pós-graduada em Direito Digital.	*Product Owner* (PO) em uma equipe de desenvolvimento de software	Atua há mais de 6 anos com Direito Digital; Possui publicações sobre LGPD; Tem experiência com aplicação da LGPD em um produto de software.	Atuação focada nos temas de proteção de dados pessoais, inteligência artificial e cibersegurança.
Especialista B	- Bacharel em Direito; - Mestre em direito; - Pós-graduanda em Direito Digital.	Pesquisadora Sênior em Direito em Tecnologia	Atua há mais de 3 anos com Direito Digital; Possui publicações sobre LGPD; Tem experiência com aplicação da LGPD em mais de 4 produtos de software.	Atuação focada nos temas de proteção de dados pessoais, governança de Inteligência artificial e identidades digitais.

2.2.3 - Roteiro da Entrevista

O roteiro foi dividido conceitualmente para abordar três eixos: **Eixo I - Histórico com a LGPD**, com uma pergunta aberta, o **Eixo II: LGPD no Desenvolvimento de Software,** composto de duas perguntas, e por fim, o **Eixo III - Perguntas de sequência,** composto de cinco perguntas.

No **Eixo I – Histórico com a LGPD**, as especialistas foram convidadas ao relato através da instrução ***"Solicitar ao especialista que conte sobre a sua experiência e relação com a LGPD"***. A pergunta foi elaborada para ser genérica e abrangente. Seu objetivo foi convidar a especialista entrevistada a navegar por suas próprias práticas, experiências, processos e projetos, oportunidade para capturar detalhes específicos sobre suas rotinas com PPD e explorá-las nas próximas etapas da investigação.

Ao avançar para a segunda etapa, no **Eixo II – LGPD no Desenvolvimento de Software**, a especialista foi convidada a compartilhar detalhes específicos sobre o objeto de interesse: a aplicação da lei na prática, em seus contextos através da

pergunta: "***Como você aplica a LGPD no seu contexto? Pode contar como é o processo?***". Nesta etapa surgiram maiores detalhes sobre a sua experiência com a aplicação da lei.

Por último, no **Eixo III - Perguntas de sequência,** utilizadas para extrair informações específicas sobre os relatos e complementar pontos relevantes à investigação que, porventura, necessitavam de aprofundamento. As perguntas foram introduzidas ao longo do relato das especialistas, caso a especialista abordasse o tema de interesse. Em outras situações, as perguntas foram introduzidas como argumento direto durante o relato para aprofundamento do tema. A lista com todas as perguntas utilizadas na etapa de entrevista com as especialistas pode visualizada na Tabela 4.

Tabela 4 - Roteiro de perguntas aos especialistas

Eixo I: Histórico com a LGPD	1) Solicitar ao especialista que conte sobre a sua experiência e relação com a LGPD;
Eixo II: LGPD no Desenvolvimento de Software	2) Como você aplica a LGPD no seu contexto? Pode contar como é o processo?
Eixo III - Perguntas de continuidade e sequência	3) Do ponto de vista do ciclo de desenvolvimento, como isso chega até você?
	4) É o mesmo processo para produtos existentes ("no mercado") e produtos novos (em desenvolvimento)?
	5) É correto pensar, aos olhos da LGPD que: para produtos existentes existe um processo de Adequação e para novos produtos e para funcionalidades existe um processo de conformidade?
	6) A LGPD se aplica para todos os casos? Todos os sistemas/produtos?
	7) Como garantir que o produto está em conformidade e/ou adequado à lei?
	8) Quais as ações para lidar com o problema de não-conformidade uma vez identificado?

2.2.4 - Descobertas nas Entrevistas

Nesta seção, são apresentadas as principais descobertas obtidas na etapa de entrevistas com as especialistas. As informações estão organizadas da seguinte forma: inicialmente, são apresentadas as contribuições da Especialista A, seguidas pelas da Especialista B.

Especialista A:

(1) Criação de sistemas orientados à privacidade: A especialista destaca seu esforço na tentativa de criar produtos "*Privacy by Design*": em tentativas de implementar boas práticas de PPD desde o desenho de funcionalidades, por exemplo. Seja na coleta de dados utilizados por funcionalidades, ou na

preocupação com a disposição de informações de transparência disponibilizadas ao usuário durante a interação com a interface do sistema. Esforços que deram origem a um repositório interno de boas práticas compartilhadas entre os membros do time de desenvolvimento e engenharia;

(2) Não há fórmula pronta para aplicação da lei em sistemas de software: De acordo com a especialista não há "*how to*[1]" estruturado de como implementar a lei na prática: seja um documento criado pela própria organização em que faz parte, ou mesmo por parte da Autoridade Nacional de Proteção de Dados (ANPD). Até o momento da entrevista, não existiam guias específicos ao contexto de sistemas de software. Apesar da falta, "*há espaço para a experimentação e exploração na implementação da lei na prática*". Em que, a partir da própria prática e dos desafios cotidianos enfrentados por sua equipe de desenvolvimento de software, são desenhadas soluções sempre em referência à LGPD;

(3) Seu papel de especialista na atuação como *Product Owner (PO)*: formação em Direito e especialidade em LGPD são muito utilizadas durante as sessões de *brainstorming* de funcionalidades e reuniões diárias com desenvolvedores;

(4) Atuação no desenvolvimento dos Use Cases (UCs) do sistema: durante a especificação e desenho de UCs do sistema, em que são elencados quais dados serão manipulados (tratados) na implementação de funcionalidades do sistema. Trabalho realizado sempre com o apoio de especialistas técnicos para avaliar a capacidade de implementação do que é desenhado e;

(5) Uso da estrutura dos Casos de Uso (UCs): A utilização das estruturas dos UCs, mas não da forma convencional. Em sua equipe, os Ucs são utilizados para além de registrar a interação entre ator e sistema. O *template* utilizado para registrar os Ucs possuem uma estrutura adicional chamada de "mapa de dados", seção em que são registrados dados, sua origem e tipo utilizados nas funcionalidades desenhadas;

(6) Designers orientados à transparência: há uma constante troca entre a especialista e os profissionais responsáveis pelo desenho e implementação de interface de interação com o usuário. Seu trabalho com PPD conta com o apoio de *Designers* para que o usuário esteja sempre bem-informado

[1] "How to" é um jargão da língua inglesa utilizado para indicar presença ou a falta de procedimentos, passos ou instruções de como fazer ou completar um procedimento ou uma tarefa, por exemplo.

durante a navegação e tomadas de decisão, além de possibilitar que o usuário tenha conhecimento sobre como e quais dados são utilizados pelo sistema. O time possui um trabalho constante na ponderação entre manter o usuário informado e não impedir sua jornada no sistema seja prejudicada por conta da superexposição de informações durante sua navegação;

(7) Documentação dos processos: a especialista demonstra uma preocupação adicional, não apenas por conta da LGPD**,** mas também por conta de o sistema em desenvolvimento ser um sistema especialista, que utiliza inteligência artificial para apresentar resultados às partes envolvidas em uma transação;

(8) Cultura dos desenvolvedores: em sua percepção, os desenvolvedores são orientados à resolução do problema de forma técnica, apenas. Com uma mirada voltada para criação soluções que resolvam os problemas de forma técnica, em que as preocupações com PPD se tornam secundárias. Algo que pode estar relacionado à própria cultura de PPD, neste caso, a falta dela.

Especialista B:

(1) Uso de *Privacy by Design*: o PbD surge como uma boa prática para pensar privacidade e proteção de dados logo no início dos processos de desenvolvimento, similar aos esforços da Especialista A;

(2) Engenharia Reversa para produtos existentes: para sistemas já em produção, ainda não adequados à lei, a especialista descreve um conjunto de perguntas realizadas durante o processo de engenharia reversa dos dados coletados, como *"Quais dados são utilizados? Quero saber o mínimo sobre o meu cliente para promover o serviço"*. Ao olhar o todo, seu objetivo é identificar o que é necessário e essencial, caso contrário, sua sugestão é a remoção;

(3) Processo de garantia de conformidade à lei: *"Não há uma receita de bolo"*. Em sua experiência, é possível explorar a aplicação de conceitos previstos em lei. A especialista cita um recurso chamado de "Mapeamento de fluxo de dados", como um artefato de apoio à etapa. Neste artefato seriam registrados dados pessoais utilizados e quais funcionalidades realizam tratamentos sobre eles. Recurso similar ao apresentado pela Especialista A, nomeado "Mapa de Dados".

2.3 - Considerações finais

Em ambos os relatos, foi possível identificar confluência de práticas e desafios enfrentados pelas especialistas. E, apesar das especialistas atuarem em equipes, organizações e produtos com finalidades distintas, foi possível trazer à superfície detalhes sobre a aplicação da lei (LGPD) em produtos de software.

Apesar do número reduzido de entrevistadas, é possível observar que as especialistas têm aplicado seus conhecimentos para criação de produtos em conformidade à lei. Seja na mentoria aos desenvolvedores ou no apoio a outros profissionais envolvidos, as profissionais têm um papel essencial de contribuir e intervir durante as diversas etapas do desenvolvimento de sistemas de software para disseminar práticas e influenciar o pensamento alinhados com conceitos presentes na LGPD. Os achados possibilitam trazer à superfície detalhes sobre o processo empírico de aplicação da LGPD na prática, que conta com a experiência, repertório e sapiência da especialista na criação de produtos cada vez mais adequados à lei.

3 Fundamentação Teórica: Inspeção de Software

Neste capítulo, são abordados os principais conceitos sobre inspeção de software e suas técnicas. Além de introduzir os principais desafios em relação à implementação da cultura de privacidade e proteção de dados na Engenharia de Software.

3.1 - Inspeção de Software

A inspeção de software é um tipo de verificação visual de um produto que detecta e identifica anomalias, erros e desvios dos padrões e especificações (IEEE, 2008). A inspeção de software possui objetivo de melhorar a qualidade de produtos de software, uma abordagem de baixo custo que reduz o retrabalho (FAGAN, 1976), auxiliando não apenas na detecção, mas também na remoção de defeitos potencialmente negligenciados nas diversas etapas do processo de desenvolvimento de software (SHULL, RUS, *et al.*, 2000).

A utilização de técnicas de inspeção de software pode ocorrer em diversas etapas do processo de desenvolvimento de software, como requisitos (FAGAN, 1976), (PORTER, VOTTA, *et al.*, 1995), às etapas de testes (BOEHM, BASILI, 2001). Publicações detalham resultados positivos relacionados à sua eficácia e eficiência, especialmente quando empregada nas fases iniciais de requisitos (LAITENBERGER, DEBAUD, 2000). Isso se deve ao fato de que ela possibilita uma identificação mais fácil e menos custosa de erros, reduzindo as chances de sua propagação para etapas seguintes (BASILI, GREEN, *et al.*, 1996).

3.1.1 - Processo de Inspeção de Software

O processo de inspeção de software é caracterizado por um processo bem definido. Composto por seis etapas, o processo descreve um conjunto de operações a serem realizadas, desde a escolha do artefato a ser inspecionado ao reajuste do artefato (FAGAN, 1986).

Desde sua proposição por Fagan (1986), o processo de inspeção de software tem passado por diversas revisões e aprimoramentos. Pesquisadores, como Sauer e Jeffery, *et al.* (2000) e Kalinowski *et. al* (2004), têm se baseado na literatura mais atualizada e na geração de evidências para fundamentar melhorias, introduzir novas abordagens organizacionais e realizar adaptações ao processo original de inspeção.

A seguir, apresentam-se detalhes sobre as etapas do processo de inspeção e suas descrições, extraídos de (KALINOWSKI, SPÍNOLA, *et al.*, 2004), disponíveis na Figura 1:

(1) **Planejamento**: etapa em que a seleção da equipe, contexto da inspeção e papéis são definidos.

(2) **Detecção**: etapa em que os inspetores executam o processo de inspeção em busca por defeitos. Ao final, uma lista de discrepância é produzida. Uma discrepância é um possível defeito.

(3) **Coleção**: etapa em que o moderador realiza a sistematização das discrepâncias identificadas pelo inspetor.

(4) **Discriminação**: etapa em que o autor, o inspetor e o moderador discutem discrepâncias identificadas. O objetivo é decidir sobre cada discrepância: descartar as consideradas falsos positivos e adicionar à lista de defeitos as classificadas como defeitos. O tipo de defeito deve ser classificado conforme uma taxonomia conhecida pela equipe.

(5) **Retrabalho**: etapa em que o autor do artefato, em posse da lista de defeitos, realiza a correção dos defeitos no artefato inspecionado.

(6) **Continuação**: etapa em que o moderador decide, após o artefato ser corrigido pelo autor, se há necessidade de uma nova rodada de inspeção.

Figura 1 - Etapas do processo de inspeção - Extraído de (KALINOWSKI, SPÍNOLA, et al., 2004)

A taxonomia de defeitos, apresentada por Travassos, Shull, et al., (1999), disponível na Tabela 5, empregada para classificar os defeitos descobertos durante o processo de inspeção. Seu objetivo é qualificar e fornecer informações adicionais sobre os defeitos identificados na etapa de Discriminação (TRAVASSOS, SHULL, et al., 1999).

Tabela 5 - Taxonomia de defeitos extraída de (TRAVASSOS, SHULL, et al., 1999)

Defeito	Descrição Geral
Omissão	Informação importante que deveria ter sido especificada no artefato, porém foi omitida no mesmo.
Fato incorreto	Informações no artefato de software contradizem informações no documento requisitos ou no conhecimento de domínio geral.
Inconsistência	Informações dentro de uma parte dos artefatos de software são inconsistentes com outras informações no artefato de software.
Ambiguidade	A informação contida no artefato é ambígua, ou seja, passível de mais de uma interpretação.
Informação Estranha	Informação é fornecida, no entanto ela não é necessária ou utilizada no sistema.

3.1.2 - Técnicas para Inspeção de Software

Para Mello (2011), um dos fatores decisivos no planejamento e resultados da inspeção de produtos e projetos de software é a escolha da técnica de inspeção a ser utilizada. Sejam em inspeções *Ad-hoc*, um tipo de inspeção baseada no conhecimento do inspetor, normalmente executada de forma não estruturada (SHULL et al., 1999), com possibilidade de ser executada nos mais diversos tipos de artefatos. Outra abordagem são as técnicas de inspeção baseadas em Checklist, que consistem em perguntas formuladas, tipicamente em formato "Sim/Não". Essas perguntas têm o propósito de orientar e auxiliar o inspetor durante o processo de inspeção de um documento (LAITENBERGER, EMAM, et al., 2001).

Além das técnicas *Ad-hoc* e de checklist, a literatura apresenta uma ampla variedade de abordagens para diferentes objetivos, artefatos ou produtos. A seguir, listaremos algumas dessas técnicas encontradas na literatura:

- ***Defect-based Reading (DBR):*** utilizada para detecção de defeitos em documento de requisitos, a técnica oferece diferentes classes e um conjunto específico de procedimentos que cada revisor executa para encontrar defeitos orientados dentro de classes específicas de defeitos (PORTER, VOTTA, 1994).
- ***Perspective-based Reading (PBR):*** a técnica foca em cenários para detecção de defeitos em documentos de requisitos, descritos em linguagem natural. Seu objetivo é revisar um documento sob diferentes perspectivas, seja um testador, usuário ou designer, realiza um conjunto de procedimentos específicos orientado à perspectiva em questão através de um conjunto de perguntas (BASILI, GREEN, *et al.*, 1996).

- ***Object-Oriented Reading Techniques (OORTs):*** família de técnicas de leitura para apoiar a verificação de diferentes diagramas orientados a objetos baseados em UML (TRAVASSOS, SHULL, et al., 1999).
- **Usage-Based Reading (UBR)**: é uma técnica que utiliza o ponto de vista do usuário para detecção de defeitos severos. Foca nas necessidades do usuário, a inspeção acontece a partir do documento de requisitos, mais especificamente os casos de uso (THELIN, RUNESON, *et al.*, 2002).
- ***OO-PBR - Object Oriented - Perspective Based Reading***: é uma técnica de inspeção de leitura, baseada em perspectiva, para identificação de defeitos em documentos de requisitos escritos em linguagem natural. Fornece um conjunto de perguntas e um procedimento ao inspetor durante o processo de criação de modelos. A técnica de inspeção é composta de diversas questões para avaliar a completeza, clareza, consistência, corretude, concisão e organização adequada. (MAFRA, TRAVASSOS, 2006).
- **ArqCheck: Abordagem para inspeção de documentos arquiteturais:** é uma técnica de inspeção baseada em checklist para detecção de defeitos em documento arquiteturais. Seu objetivo é a melhoria da qualidade da arquitetura de um software, e possibilitar a identificação de defeitos arquiteturais relacionados ao atendimento de requisitos funcionais e requisitos de qualidade. Suas principais características são avaliar a consistência do documento, atendimento aos requisitos, sendo uma abordagem utilizada para atender aos requisitos de qualidade (BARCELOS, TRAVASSOS, 2006).
- **ActCheck - Inspeção do Diagrama de Atividades na Especificação de Requisitos:** é uma técnica de inspeção focada na verificação semântica entre a especificação de requisitos e os diagramas de atividades que descrevem estes requisitos. Esta técnica é composta por três artefatos principais: (1) checklist de inspeção utilizado para apoiar a especificação de requisitos descrita com diagramas de atividades; (2) questionário de caracterização a ser utilizado como apoio à configuração do checklist; (3) tabela de rastreabilidade entre o checklist e os itens do questionário. Além de uma lista de casos discrepantes, material que pode ser utilizado durante o processo de treinamento para utilização e aplicação da técnica (MELLO, PEREIRA, *et al.*, 2010).
- **FMCheck - Verification of Software Product Line Artefacts: A Checklist to Support Feature Model Inspections:** é uma técnica de inspeção baseada em

checklist para apoiar a detecção de defeitos em *feature models* que descrevem linhas de produtos de software (DE MELLO, TEIXEIRA, *et al.*, 2014)

- **BPCheck - A Checklist-Based Inspection Technique for Business Process Models:** é uma técnica de inspeção baseada em *checklist* que oferece suporte à detecção de defeitos em modelos BPMN (*Business Process Model and Notation)*. Seu objetivo é cobrir nove dos elementos semânticos da BPMN. A técnica de inspeção fornece um conjunto de perguntas de inspeção que cobrem um total de 55 itens de verificação. Ademais, há uma lista, não exaustiva, de 109 Casos Discrepantes (DC). Na lista são abordados a consistência entre os elementos do modelo, a clareza de sua descrição e sua correção e completude em relação à descrição textual do processo de negócios (MELLO, MOTTA, *et al.*, 2016).
- **SCENARIOTCHECK**: é uma técnica de inspeção de suporte à qualidade de descrição de cenários de IoT (*Internet of Things*). A técnica é construída com base na técnica de especificação de requisitos SCENARIOT de Da Silva e Travassos (2020). SCENARIOTCHECK possui um checklist com uma série de perguntas de inspeção. Seu objetivo é auxiliar o inspetor na busca por problemas de requisitos nas descrições de cenários produzidos com a técnica de especificação SCENARIOT (DE SOUZA, MOTTA, *et al.*, 2019).

3.2 - Trabalhos Relacionados

Durante a pesquisa para desenvolver uma técnica de inspeção alinhada aos princípios da LGPD, mesmo que de forma *Ad-hoc*, foi possível evidenciar um crescente interesse da comunidade de Engenharia de Software pela Lei Geral de Proteção de Dados Pessoais (LGPD). Durante esse processo, foram identificadas várias abordagens, tanto práticas quanto conceituais, em relação ao conteúdo da lei.

Ainda em 2020, dois anos após a aprovação da LGPD, pesquisadores já se debruçavam sobre os problemas relacionados à modelagem dos principais conceitos de privacidade e proteção de dados presentes na regulação brasileira. Na pesquisa de Martin, Barros, *et al*. (2020), através da aplicação de *Formal Concept Analysis* (FCA), pesquisadores investigam estratégias para determinar estruturas hierárquicas entre os termos e conceitos presentes LGPD. Com FCA, o objetivo é dar suporte a um processo de desenvolvimento de software adequado à LGPD (MARTINS, BARROS, *et al.*, 2020).

Mendes, Viana, *et al*. (2021), em uma abordagem mais prática, disponibilizam uma um corpus de conhecimento sobre a LGPD através de uma técnica de inspeção,

baseada em *checklist*, para a identificação de adequação à lei. A técnica proposta contém um de conjunto 52 itens de *checklist*, originados de atributos de qualidade extraídos da própria lei brasileira, da GDPR, regulação europeia, e revisão bibliográfica. A investigação que deu origem a cinco categorias: *transparência, segurança, consentimento, responsabilidade e direitos dos titulares*. Mais tarde, agrupados em atributos relacionados ao 1) sistema de software; e 2) empresa/controlador (MENDES, VIANA, *et al.*, 2021). Mais tarde, o estudo foi estendido por Pereira, Mendes *et al.* (2022), em que investigadores propuseram adições ao checklist inicial para apoiar a verificação de sistemas baseados em Internet das coisas (IoT).

Ainda em contexto brasileiro, Peixoto *et al.* (2022) investigaram a percepção e relação de desenvolvedores de software sobre privacidade e proteção de dados através de entrevistas semiestruturadas. Os resultados demonstram quais fatores influenciam, de forma positiva ou negativa, desenvolvedores durante o processo de implementação de medidas orientadas à PPD em suas rotinas de desenvolvimento de sistemas de software. Foram identificados nove Fatores Pessoais (PF), cinco Fatores Comportamentais (BF), sete Fatores Ambientais Externos (EF). Os resultados revelam, que, dentro da categoria de Fatores Pessoais (PF), um fator que influencia negativamente decisões é uma confusão terminológica entre os termos privacidade e segurança. Outro fator é a falta de conhecimento formal sobre privacidade, ou noção de que a privacidade não é relevante. Por fim, um cruzamento busca identificar qual fator, dentre as três categorias propostas, oferece algum tipo de influência sobre outro (PEIXOTO, FERREIRA, *et al.*, 2022).

Dias, Angelica, *et al.* (2022) investigam ações tomadas por organizações e times ágeis durante o desenvolvimento de software. A pesquisa revela que os profissionais envolvidos no desenvolvimento de sistemas de software possuem certo conhecimento por parte dos profissionais sobre a LGPD, em especial sobre os princípios. Outro achado relevante da investigação é a identificação de áreas mais afetadas pela LGPD. De acordo com a pesquisa, os times sentem mais impactos nas atividades de requisitos e construção de software. Outro achado relevante, disponível na Tabela 6, é a relação entre o conhecimento dos princípios da LGPD e sua utilização por parte dos profissionais. Evidências foram obtidas por meio de respostas de 53 profissionais, coletadas através de formulário eletrônico e entrevistas semiestruturadas com 10 profissionais (DIAS, ANGELICA, *et al.*, 2022)

Tabela 6 - Relação conhecimento do princípio da LGPD x uso pelas organizações (Extraído de (DIAS, ANGELICA, et al., 2022) adaptada[2])

Princípio LGPD	% conhecem o princípio	% Usou o princípio
Segurança	81.1%	90.6%
Livre acesso	67.9%	43.2%
Qualidade de Dados	66%	54.7%
Prevenção	66%	56.6%
Finalidade	60.4%	56.6%
Transparência	60.4%	58.5%
Necessidade	56.6%	43.4%
Não-discriminação	56.6%	32.1%
Adequação	54.7%	45.3%
Responsabilidade e prestação de contas	52.8%	34%

3.3 - Considerações finais

Na direção de encurtar este distanciamento, a aplicação da LGPD já faz parte do cotidiano dos diferentes times de pesquisa brasileiros (DIAS, ANGELICA, *et al.*, 2022), entretanto, apesar da relevância técnica e dos atributos tratados nas abordagens para aproximar PPD do ciclo de desenvolvimento de software, não foi possível identificar material de apoio à interpretação ou aplicação das leis, principalmente à LGPD, no contexto do desenvolvimento de sistemas de software.

Com o intuito de somar aos resultados previamente obtidos, vislumbramos oportunidades de promover o desenvolvimento de uma tecnologia de software, baseada em evidência, que permita a verificação dos princípios da LGPD em artefatos de software. E assim, contribuir para a orientação da comunidade da prática a interpretar estes princípios e conceitos de PPD no contexto de atividades de desenvolvimento e evolução de software (SHAPIRO, 2010).

[2] Os títulos das colunas e o nome dos princípios da LGPD foram traduzidos do inglês para o português.

4 Desenvolvendo a *LGPDCheck*

Neste capítulo são apresentados os principais passos percorridos e artefatos desenvolvidos durante o desenvolvimento da técnica de inspeção LGPDCheck.

4.1 - Dos Princípios da LGPD à Tecnologia de Inspeção

Com o objetivo de contribuir para a compreensão do conteúdo e auxiliar na instrumentalização dos conceitos de Privacidade e Proteção de Dados (PPD) presentes na LGPD por parte dos profissionais envolvidos no ciclo de desenvolvimento de software, foram realizadas diversas ações, desde a organização do conhecimento em processos até a construção de artefatos de suporte.

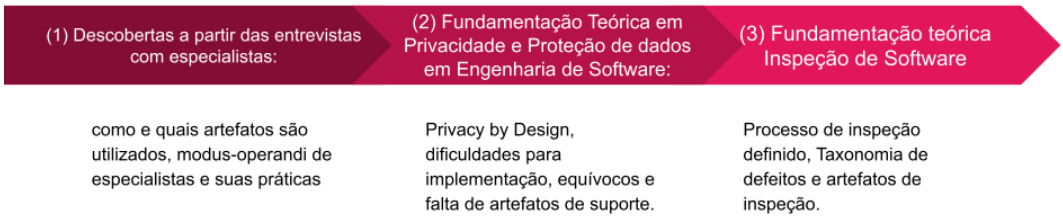

Figura 2 - Visão geral construção da LGPDCheck

Com base no conhecimento acumulado nas três etapas anteriores, que podem ser visualizados na Figura 2, foi possível chegar à proposta da técnica de inspeção *LGPDCheck* à luz dos princípios da LGPD. A *LGPDCheck* consiste em uma técnica de inspeção, baseada em *checklist,* para apoiar a identificação de defeitos (ou não conformidades) em artefatos de software produzidos nas diferentes etapas do ciclo de desenvolvimento de software (TRAVASSOS, SHULL, *et al.*, 1999).

A *LGPDCheck* possui um recorte e enfoque no Capítulo I da LGPD. Este recorte está relacionado às motivações que originam este trabalho e suas inspirações no *modus operandi* de *Privacy by Design* de Cavoukian (2009). Com a *LGPDCheck* almejamos a inclusão dos princípios da LGPD desde as etapas iniciais de criação e construção um produto ou práticas organizacionais.

O arcabouço do *LGPDCheck* oferece artefatos de apoio à verificação por meio de um conjunto de 32 perguntas direcionadas aos dez princípios da LGPD. Estes estão organizados em um processo de inspeção com regras definidas, como sugere Fagan (1986).

Os esforços na proposição do arcabouço que compõem a *LGPDCheck* foram direcionados às tentativas de tornar o conteúdo da lei mais acessível aos profissionais com pouca familiaridade com a lei. Durante a construção da proposta atual da

LGPDCheck, em especial aos achados da etapa de entrevista com especialistas, foi possível compreender que a LGPD nos contextos de software requer um grau de subjetividade, parte do processo de reflexão das especialistas na tomada de decisão baseadas nos limites da lei. Porém, é importante destacar que a *LGPDCheck* também herda certa subjetividade, conforme identificado por Gürses, Trancoso, *et al*. (2011), o que pode representar um desafio para profissionais com nenhuma experiência com PPD.

Esse grau de subjetividade foi mantido de forma intencional, em especial construção das perguntas de inspeção que compõem o *checklist* de inspeção da técnica. Devido aos múltiplos contextos aos quais sistemas de software podem estar inseridos, acreditamos não ser desejável que a técnica possua um caráter rígido e determinístico sobre os dados e práticas que foram, estão e serão utilizadas por indivíduos e organizações.

Diferente de Mendes, Viana, *et al*. (2021), que propuseram abordagens mais alinhadas ao *compliance* e a adequação à LGPD como um todo, a *LGPDCheck* tem propósitos anteriores, justamente por focar nos princípios da LGPD e possuir um recorte apenas no primeiro capítulo da lei.

Assim como sugere Shapiro (2010), a *LGPDCheck* disponibiliza em seu arcabouço ferramentas para execução, por meio de um processo estruturado, com artefatos de suporte. Artefatos estes que contemplam exemplos direcionados aos contextos de sistemas de software, glossário, quadros de apoio com recursos de treinamento.

As seções a seguir descrevem as principais etapas, decisões, artefatos e processos que compõem a primeira versão da *LGPDCheck*.

4.1.1 - Abordagem Multinível de Inspeção

Inicialmente, ao debruçar-se sobre os dez princípios previstos no Art. 6º da LGPD, a primeira hipótese para construção da técnica de inspeção que utilizasse os princípios tinha como objetivo dois artefatos, neste caso, o documento de requisitos e Diagramas de Caso de Uso (UCs). O caminho surge a partir dos relatos das especialistas, baseados em suas práticas cotidianas com a aplicação da lei no ciclo de desenvolvimento de software, presentes no Capítulo 2, na subseção 2.2.4 - Descobertas desta dissertação.

Sob a premissa de identificar defeitos com menor quantidade de esforço, com foco em reduzir o retrabalho, surge a abordagem multinível de inspeção. Na abordagem

proposta, são definidas duas perspectivas de verificação: Nível I - Requisitos e Nível II – Sistemas em execução, cada um com um objetivo e foco em artefatos específicos. Detalhes podem ser visualizados na Tabela 7.

Tabela 7 - Níveis de Inspeção

Nível	Descrição	Objetivos da inspeção
I – Requisitos	A inspeção a ocorre no documento de requisitos do sistema a ser construído ou em construção.	Verificar se dados e seus possíveis tratamentos respeitam as definições dos princípios.
		Verificar a existência ou a falta de normas, práticas organizacionais ou diretrizes da organização detentora do sistema em inspeção, capazes de garantir que os princípios sejam implementados.
II – Sistema em execução	A inspeção ocorre em nível de funcionalidade do sistema em execução.	Verificar a presença de funcionalidades capazes de garantir que os princípios sejam implementados/cobertos.

Após a definição da abordagem multinível, nas etapas seguintes, tornou-se possível distribuir conjuntos de princípios da LGPD a cada um dos níveis. Isso resultou em uma redução significativa no esforço de verificação e, como resultado, na quantidade de itens a serem verificados em um artefato.

4.1.2 - Priorização dos princípios da LGPD por Nível de Inspeção

A partir da proposta de uma abordagem multinível de inspeção e, posteriormente, sua fragmentação em distintas perspectivas de verificação (Requisitos e Sistemas em Execução), os dez princípios da LGPD foram priorizados entre primários e secundários entre os dois níveis de inspeção para compor o arcabouço de verificação da *LGPDCheck*. O processo de priorização teve como objetivo oferecer um conjunto reduzido de princípios para a inspeção em nível de inspeção, tornando mais explícito quais princípios devem receber foco em determinado nível de inspeção. O resultado da priorização por nível de inspeção é disponibilizado na Tabela 9.

4.1.2.1 - Processo de priorização dos princípios ao nível de Inspeção

O processo de priorização contou com dois passos principais. O primeiro, a partir da definição dos princípios da LGPD presentes em seu Art. 6º, foi realizada uma análise conceitual com objetivo de identificar quais princípios estavam mais próximos conceitualmente.

Após a conclusão do primeiro passo, os princípios foram agrupados da seguinte maneira, como demonstrado na Tabela 8:

Tabela 8 - Grupo de princípios da LGPD

Grupo	Princípios da LGPD
A	Finalidade, Adequação e Necessidade
B	Segurança, Prevenção, Não discriminação, e Responsabilização e Prestação de contas
C	Livre acesso, Qualidade dos dados e Transparência

A seguir, é possível ver em detalhes como os grupos de princípios foram organizados em seus respectivos grupos. Além disso, é apresentado uma breve explanação de como os princípios estão relacionados nos contextos de sistemas de software.

Grupo A (Nível de Inspeção I – Requisitos): os princípios classificados como primários são *Finalidade, Adequação e Necessidade*: foi identificado uma proximidade muito forte entre os três princípios. Uma vez que seus objetivos estão relacionados à relação entre o titular de dados, seus dados pessoais e a responsabilidade dos agentes de tratamento. Outro fator que reforça a inclusão dos princípios no Nível I – Requisitos é a maior probabilidade de dados e seus tratamentos poderem ser identificados ainda nas etapas mais iniciais do desenvolvimento de sistemas de software, em especial no documento de requisitos, alinhados com os princípios e *modus operandi* de PbD.

A relação entre os princípios Finalidade, Adequação e Necessidade fica mais evidente ao imaginar uma situação hipotética de tratamento qualquer, uma vez que:

1. Ao realizar uma operação de tratamento sobre dados pessoais é indispensável a existência de uma finalidade(s) (princípio I). Ter uma finalidade significa ter uma motivação legítima, específica, explícita e informada ao titular sobre a realização daquele tipo de tratamento, sempre observando os limites previstos em lei;
2. Ao existir finalidade – ou finalidades – para o tratamento, a adequação (princípio II), busca garantir o cumprimento do primeiro princípio para que não exista violação ou contradição em relação aos tratamentos realizados e as finalidades. Uma tentativa de garantir que apenas o informado seja de fato executado.
3. O princípio da necessidade (princípio III) com objetivos de manter simetria e justiça na coleta de dados e outros tratamentos realizados nos dados pessoais titular. Para qualquer tipo de operação de tratamento de dados, deve ser

coletado o mínimo necessário para realização de finalidades. E assim, garantir que, ao existir uma coleta de dados pessoais, ela não seja abusiva e desproporcional ao tratamento a ser realizado.

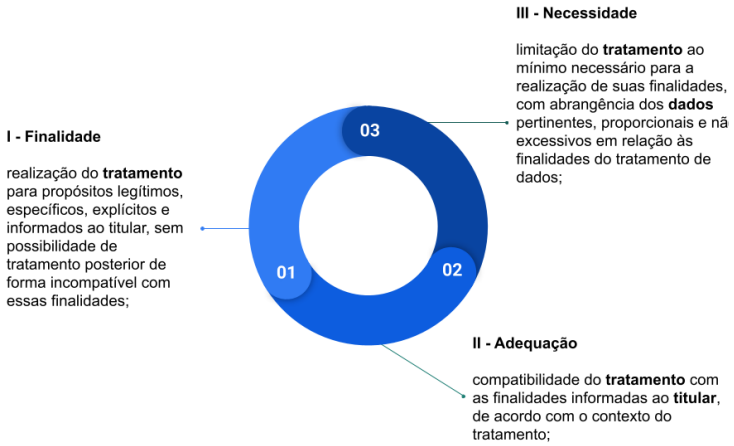

Figura 3 - Relação finalidade, necessidade e adequação

Grupo B (Nível de Inspeção I – Requisitos): os princípios classificados como primários são Segurança, Prevenção, Não discriminação e Responsabilização e Prestação de contas. Os quatro princípios têm seu foco nas práticas, rotinas e políticas de uma organização ao tratar dados pessoais de seus usuários-titulares de dados. Em uma organização, os princípios podem ser relacionados à existência – ou a falta – de recursos técnicos ou administrativos apropriados para efetivação dos princípios em relação aos dados tratados do usuário-titular. Em termos de capacidade da organização, promover medidas técnicas e administrativas em relação à segurança e prevenção de incidentes com os dados tratados do usuário-titular, políticas e práticas de não-discriminação, e capacidade do agente de tratamento demonstrar sua adequação à própria lei.

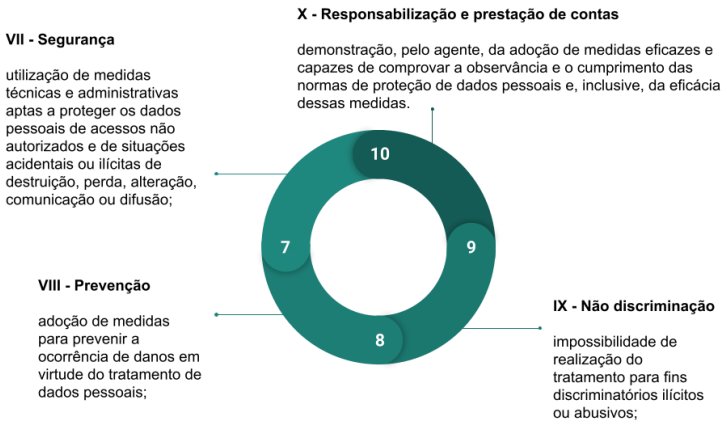

Figura 4 - Relação dos princípios Segurança, Prevenção, Não discriminação e Responsabilização e prestação de contas

Grupo C (Nível de Inspeção II – Sistemas em Execução): os princípios classificados como primários são *Livre acesso, Qualidade dos Dados, Transparência*. Os três princípios estão relacionados à disponibilização de recursos ao usuário, em relação aos dados pessoais coletados e tratados. Em uma organização, normalmente, são utilizados sistemas para efetivação desses princípios. Sua efetivação pode ocorrer por meio da disponibilização de funcionalidades ao usuário-titular. Para que usuários-titulares tenham acesso aos dados tratados e tratamentos realizados, a possibilidade de acesso às informações sobre a qualidade e corretude dos seus dados, e informações transparentes sobre como seus dados são tratados.

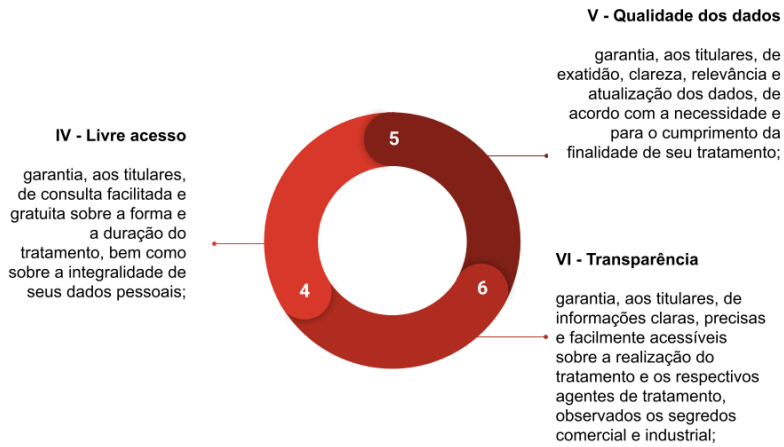

Figura 5 - Relação dos princípios Livre acesso, Qualidade dos dados, Transparência

No passo seguinte, os princípios foram classificados como primário ou secundário através da seguinte premissa: "*com base nos objetivos dos níveis de*

inspeção e artefatos a serem verificados, qual grupo de princípio oferece melhor cobertura para o nível de inspeção em questão?". Este passo resultou na priorização entre primário e secundário dos dez princípios da LGPD em seus respectivos níveis de inspeção. O resultado desta etapa pode ser visualizado na Tabela 9.

Tabela 9 - Princípios da LGPD VS Nível de Inspeção VS Priorização

Grupo	Princípio	Nível I: Requisitos	Nível II: Sistemas em Execução
A	Finalidade	PRIMÁRIO	SECUNDÁRIO
	Adequação	PRIMÁRIO	SECUNDÁRIO
	Necessidade	PRIMÁRIO	SECUNDÁRIO
B	Segurança	PRIMÁRIO	SECUNDÁRIO
	Prevenção	PRIMÁRIO	SECUNDÁRIO
	Não discriminação	PRIMÁRIO	SECUNDÁRIO
	Responsabilização e prestação de contas	PRIMÁRIO	SECUNDÁRIO
C	Livre acesso	SECUNDÁRIO	PRIMÁRIO
	Qualidade dos dados	SECUNDÁRIO	PRIMÁRIO
	Transparência	SECUNDÁRIO	PRIMÁRIO

Se faz relevante ressaltar que a principal diferença entre o conjunto de princípios do A e B (Requisitos) e C (Sistemas em Execução) está na forma em que o usuário usufrui ou experiencia esse conjunto de princípios. No primeiro, normalmente, o usuário experimenta de forma direta através de funcionalidades de um sistema, por exemplo. No segundo, o usuário experimenta de forma indireta, uma vez que os princípios influenciam na existência e implementação de práticas, políticas internas e regimentos internos, normalmente, não transparentes ao usuário-titular.

Durante o processo de priorização, foi possível identificar que os princípios classificados como primários podem ser considerados mais prováveis de serem cobertos ao respectivo nível de inspeção. Ao focar nos princípios priorizados, é possível oferecer um conjunto menor e mais focado de itens de verificação ao inspetor durante o processo de verificação. Já os princípios classificados como secundários, são considerados menos prováveis de serem cobertos pelo nível de inspeção em comparação aos classificados como primários.

É importante destacar que os princípios classificados como secundários não são descartáveis ao nível de inspeção, pelo contrário. Os princípios podem ser considerados caso o inspetor identifique tal necessidade. A decisão deve ser tomada baseada nas necessidades da organização e artefatos em verificação.

4.2 - Artefatos de Apoio à Verificação da *LGPDCheck*

Nas seções a seguir são apresentados e descritos os principais artefatos desenvolvidos durante a elaboração da *LGPDCheck*. Dentro de cada seção e

subsecção é possível encontrar a descrição do artefato, detalhes sobre sua estrutura, campos, além da relevância do artefato para a composição do arcabouço de verificação da *LGPDCheck*.

4.2.1 - Material de Apoio

O Material de Apoio (ver Apêndice B) é um artefato desenvolvido com o propósito de tornar mais acessíveis os conceitos de Privacidade e Proteção de Dados (PPD) aos profissionais envolvidos no desenvolvimento de sistemas de software. Este material busca remover possíveis ambiguidades do vocabulário jurídico. Seu objetivo é aproximar os princípios e conceitos de PPD presentes na LGPD aos contextos de sistemas de software utilizando uma linguagem familiar e exemplos alinhados às experiências comuns dos profissionais envolvidos no desenvolvimento de sistemas de software.

O material de apoio é composto por duas seções: a primeira contém o Glossário de termos de Privacidade e Proteção de Dados para Sistemas de Software; a segunda, apresenta os Quadros de Princípios da LGPD para Sistemas de Software.

4.2.1.1 - O Glossário de Termos de Privacidade e Proteção de Dados para Sistemas de Software

O Glossário é composto de alguns dos principais conceitos da LGPD, em especial do Art. 6º, como Tratamento de dados, Titular de dados, Agentes de tratamentos, Dados pessoais e Anonimização. O glossário conta com definições alternativas adaptadas aos contextos de sistemas de software. Seu objetivo é apresentar o temo presente na LGPD com uma definição mais próxima e familiar ao profissional envolvido no ciclo de desenvolvimento de software sem que haja a necessidade de recorrer ao vocabulário jurídico da LGPD.

4.2.1.2 - Quadros dos Princípios da LGPD para Sistemas de Software

Os Quadros dos Princípios da LGPD para Sistemas de Software compõem a segunda metade do Material de apoio. Foram desenvolvidos dez quadros, um para cada um dos dez princípios da LGPD. Os quadros foram elaborados a partir das definições dos princípios presentes no Art.6 da LGPD. O objetivo de cada quadro é estruturar, em um documento único, diversas informações relevantes sobre a LGPD, porém, adaptados e exemplificados aos contextos de sistemas de software.

Um quadro é composto de cinco seções, dividido conceitualmente em duas partes. A primeira, I - Apresentação do princípio da LGPD, dedicadas a apresentar o princípio ao inspetor que possui pouco ou nenhum conhecimento sobre o universo da

LGPD e PPD. Contém informações auxiliares para compreensão dos princípios, sempre que possível, criando paralelos da linguagem jurídica para os contextos de sistemas de software.

A segunda, denominada II – Checklist de Treinamento, é composta por um checklist de inspeção direcionado ao treinamento do inspetor. Este checklist de treinamento inclui um conjunto de perguntas acompanhadas de seus gabaritos, proporcionando ao inspetor um conjunto de exemplos práticos. As perguntas contidas nesse checklist de treinamento são parte do checklist de inspeção da *LGPDCheck* (ver Apêndice E). A seguir uma descrição detalhada de cada uma das seis seções que compõem o material de treinamento:

Parte I: Apresentação do princípio da LGPD

- **Seção 1**: Identificação do princípio e nome do princípio como definidos em lei.
- **Seção 2 -** Interpretação do princípio para sistemas de software: ao utilizar definições descritas no Art. 6º, para cada um dos dez princípios foram elaboradas interpretações alternativas e expandidas, para auxiliar na compreensão do significado dos princípios.
- **Seção 3 - ação esperada pela organização**: ao utilizar definições descritas no Art. 6º, de forma alternativa, foram elaborados exemplos e expectativas para auxiliar na compreensão da responsabilidade atribuída à organização e/ou indivíduo que mantém o sistema ou produto verificado.
- **Seção 4 - exemplo de violação ao princípio em sistemas de software**: foram elaborados exemplos para exemplificar uma violação do princípio, considerando, quando possível, particularidades encontradas em sistemas de software.

Parte II: Checklist de treinamento

- **Seção 5 - Perguntas de identificação de discrepâncias:** foram elaboradas perguntas para identificar violações, adequações ou inadequações em relação à implementação dos princípios da LGPD no artefato em inspeção. Perguntas são respondidas no formato “Sim/Não”. As respostas são registradas no campo 5.A do respectivo Quadro de princípio da LGPD.
- **5.B - Classificação de discrepância:** a classificação é realizada para cada uma das discrepâncias identificadas no respectivo Quadro de princípio da

LGPD. O inspetor deve atribuir uma classificação utilizando a taxonomia de defeitos de Shull (1999): *omissão, fato incorreto, ambiguidade, inconsistência e informação estranha.*

4.2.2 - Formulário de Discrepâncias

O Formulário de Discrepâncias (Apêndice C), adaptado de Mello e Massollar, *et al.*, (2011), é um artefato de suporte ao processo de verificação da *LGPDCheck*. Artefato desenhado para que nele sejam registradas todas as discrepâncias (possíveis defeitos) encontradas durante o processo de verificação da *LGPDCheck* pelo inspetor.

O formulário possui uma estrutura simples, dividido em duas partes. Na primeira, são registradas informações sobre data em que a inspeção foi realizada, identificação do inspetor responsável, horário de início e fim da verificação. Na segunda, são registradas informações sobre as discrepâncias encontradas durante o processo de verificação e detalhes adicionais sobre a discrepância, como o nome do artefato inspecionado, a descrição da discrepância identificada, classificação da discrepância e sua localização.

4.3 - Instrumentalização da *LGPDCheck*

Para colocar em prática o conhecimento organizado e os artefatos desenvolvidos durante a concepção da proposta da *LGPDCheck*, um processo foi proposto. Este processo, composto por cinco passos, é visualmente representado na Figura 6, que apresenta os principais passos para conduzir inspeções com a *LGPDCheck*.

4.3.1 - Processo de Verificação da *LGPDCheck*

O processo de verificação da *LGPDCheck* (Figura 6) possui cinco passos, cada passo possui um conjunto de ações a serem executadas pelo inspetor durante o processo de verificação. O processo foi desenhado para ser executado de forma sequencial, iniciando pelo Passo 1 e finalizando no Passo 5, independentemente do nível de inspeção.

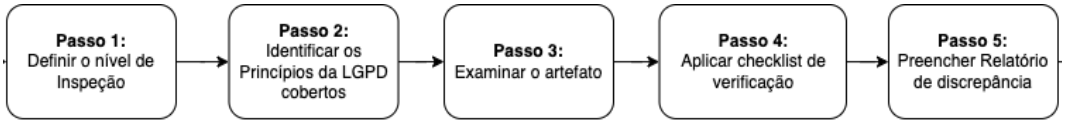

Figura 6 – Fluxo de Inspeção *LGPDCheck*

A seguir detalhes dos cinco passos do fluxo geral de inspeção da *LGPDCheck* podem ser vistos a seguir:

- **Passo 1 - Definir o nível de inspeção:** decisão com base nos objetivos definidos em cada um dos níveis de inspeção e com base no artefato a ser inspecionado.
- **Passo 2 - Identificar os princípios da LGPD cobertos:** o inspetor deve identificar os quadros de acordo com o nível de inspeção.
- **Passo 3 - Examinar o artefato:** O inspetor deve ler o artefato de acordo com o objetivo do nível de inspeção e suas instruções específicas, quando existentes.
- **Passo 4 - Aplicar checklist de verificação:** o inspetor deve executar a verificação através das perguntas presentes nos Quadros de Apoio da *LGPDCheck* (ver Apêndice B).
- **Passo 5 - Preencher o formulário de discrepância:** Para cada item de verificação do checklist em que a resposta for “Não”, uma discrepância foi identificada. O inspetor deve registrar a discrepância identificada no Formulário de Discrepância (Apêndice C) e classificá-la de acordo com a taxonomia de Shull (1999). O passo deve ser repetido até que as perguntas do checklist sejam esgotadas para o artefato em verificação, detalhes do subfluxo estão representados na Figura 7.

Informações complementares às ações, detalhe, descrições, objetivos e princípios priorizados por nível de inspeção podem ser vistos na Figura 7.

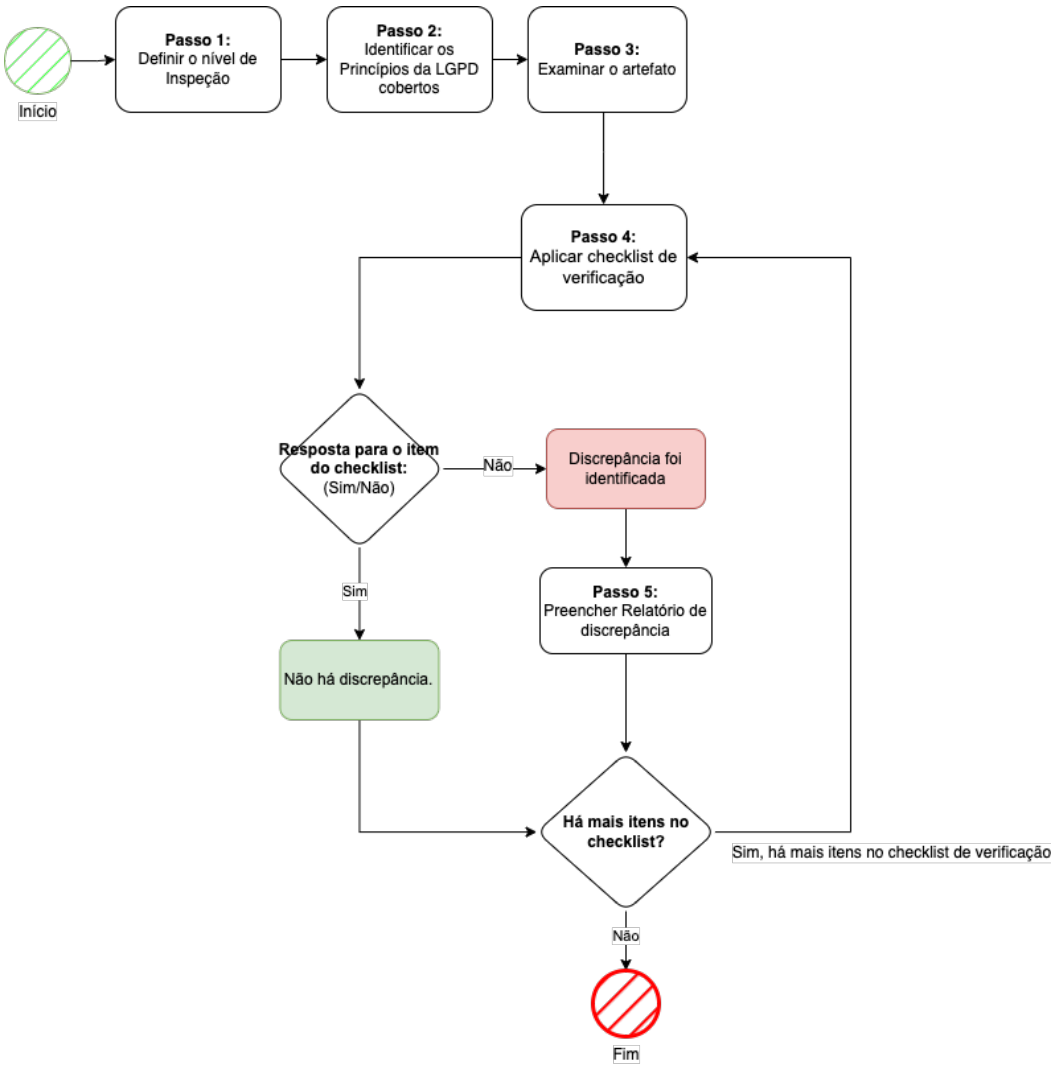

Figura 7 - Processo de Inspeção *LGPDCheck* expandido

Tabela 10 - Níveis de Inspeção, descrição, objetivos e princípios priorizados

Nível de Inspeção	Grupo	Princípios primários	Descrição	Objetivo
Nível I: Requisitos	A	Finalidade; Adequação; Necessidade;	A inspeção ocorre no documento de requisitos do sistema a ser construído ou em construção;	Verificar se dados e seus tratamentos respeitam as definições dos princípios priorizados no nível de inspeção
	B	Segurança; Prevenção; Não-discriminação; Responsabilização e prestação de contas		Verificar a existência ou a falta de normas, práticas organizacionais ou diretrizes da organização detentora do sistema em inspeção, capazes de garantir que os princípios sejam implementados.
Nível II: Sistemas em Execução	C	Livre acesso; Qualidade dos dados; Transparência	A inspeção ocorre em nível de funcionalidade do sistema em execução.	Verificar a presença de funcionalidades capazes de garantir que os princípios sejam implementados/cobertos.

4.3 - Considerações finais

A *LGPDCheck* representa um esforço significativo na construção de um marco referencial sobre a qualidade de artefatos de software à luz da LGPD. Entretanto, a técnica não deve ser encarada como um instrumento de *compliance* jurídico, mas sim como um arcabouço orientador.

É importante destacar que a LGPD possui um escopo maior do que o presente na *LGPDCheck*. E, apesar de existirem termos e conceitos de PPD importantes que não fazem parte da técnica e seu arcabouço, como Bases de Tratamentos, Dados Sensíveis, Coleta de Dados de Crianças e Adolescentes, estes não foram abordados por uma questão de limitação do próprio escopo da técnica, a incorporação destes temas geraria maior complexidade, que extrapola o escopo deste trabalho.

Após investigar o *modus operandi* de especialistas, compreendemos a necessidade de empacotar níveis de subjetividade. A interpretação da lei e os contextos jurídicos não são facilmente traduzidos em conjuntos regras baseadas em *"If-then-else"* como em uma linguagem de programação.

Por fim, a *LGPDCheck* deve ser encarada como o primeiro passo, seja ao nível individual ou organizacional, para participação efetiva na cultura de privacidade e proteção de dados. Esperamos que o glossário, quadros de princípios, exemplos e perguntas de verificação sirvam para auxiliar na construção de referenciais não apenas em artefatos de software, mas também possam fomentar a cultura de privacidade e proteção de dados.

5 Estudo de Viabilidade *LGPDCheck*

Neste capítulo são apresentados o estudo experimental para avaliação da LGPDCheck, e os resultados obtidos após a sua aplicação.

As próximas seções deste capítulo apresentam o desenho geral do estudo de viabilidade utilizado para avaliar a viabilidade da técnica de inspeção *LGPDCheck*. O estudo proposto é baseado no estudo executado de Mello, Teixeira, *et al.*, (2014), que buscou caracterizar a viabilidade de uma outra técnica de inspeção também baseada em checklist. Por fim, são apresentados os resultados qualitativos, obtidos no estudo de viabilidade, e quantitativos, coletados através do formulário de avaliação.

5.1 - Planejamento

O estudo foi desenhado no formato dois fatores, dois tratamentos. Os participantes receberam documentos contendo a especificação de requisitos de dois módulos distintos de um Sistema Web com funcionalidades diferentes, mesmo domínio, de complexidade equivalente.

Após a etapa de desenho do estudo e seu protocolo, com base no modelo GQM de Basili, Caldiera, *et al.*, (1994), o objetivo deste estudo foi definido da seguinte forma:

***Analisar*:**	a inspeção de recursos de privacidade e proteção de dados em artefatos de software usando técnicas *Ad-hoc* e *LGPDCheck*
Com o propósito de:	caracterizar
***Em relação*:**	a eficácia (defeitos identificados/total de defeitos existentes) e eficiência (defeitos identificados/tempo) da *LGPDCheck* na detecção de defeitos à luz dos princípios da LGPD
***Do ponto de vista*:**	de pesquisadores em Engenharia de Software
No contexto:	de profissionais de software (representados por alunos de Graduação, Mestrado e Doutorado em Engenharia de Sistemas e Computação da Universidade Federal do Rio de Janeiro (UFRJ), discentes de uma disciplina de Engenharia de Software Experimental da pós-graduação.

Durante esta etapa também foram elaborados todos os artefatos utilizados durante o estudo (ver Apêndice A-J), desde o formulário de caracterização, Termos de Consentimento (TCLE) e artefatos de suporte, como checklists e Quadros de apoio

LGPDCheck e Formulários de Discrepâncias, utilizados durante ambas rodadas do experimento.

5.1.1 - Formação dos Grupos

Inicialmente, foi realizado o processo de caracterização dos participantes (ver Apêndice G), dividido em três dimensões: (I) Formação Geral, II - Desenvolvimento de Software e III - Contextos diferentes. Todos os 14 participantes foram identificados através de identificador único de participante de S1 a S14 (ver Tabela 11). Para registrar a experiência dos participantes, foi utilizada uma escala de 5 pontos, organizada da seguinte maneira:

1 = Nenhum

2 = Estudei em aula ou em livro

3 = Pratiquei em 1 projeto em sala de aula

4 = Utilizei em 1 projeto na indústria

5 = Utilizei em vários projetos na indústria

Para as questões relacionadas a outros contextos, foi utilizada uma escala de 3 pontos, organizada da seguinte maneira:

1 = Eu não tenho familiaridade com a área. Eu nunca fiz isto.

3 = Eu utilizo isto algumas vezes, mas não sou um especialista.

5 = Eu sou muito familiar com esta área. Eu me sentiria confortável fazendo isto.

Através do formulário, foram coletados dados utilizados na estratégia de definição dos grupos do experimento. Para formação de grupos equilibrados, foram utilizados critérios como a experiência em requisitos de software, experiência prática, experiência teórica em desenvolvimento de sistemas, experiência no planejamento e execução de inspeções de software, por fim, conhecimento prévio em Privacidade e Proteção de Dados de regulações como LGPD (PPD/LGPD).

Em conjunto aos dados previamente coletados, os grupos foram ajustados com base no atual nível de instrução em que cada participante se encontra, abrangendo bacharelado (Bsc), mestrado (Msc) e doutorado (Dsc). O critério para equilibrar o escopo das inspeções foi a experiência prévia do participante com PPD e LGPD.

Tabela 11 - Caracterização dos participantes do estudo de viabilidade *LGPDCheck*

ID	Exp. anterior Desenvolvimento de Software (Prática)	Experiência Requisitos	Experiência Inspeção de Software	Experiência Planejamento de Inspeções	Experiência PPD/ LGPD	Instrução
S01	4	5	4	2	1	Msc
S02	4	3	3	2	3	Msc
S03	4	5	1	1	1	Msc
S04	4	3	2	1	1	Msc
S05	4	2	1	2	1	Dsc
S06	1	1	2	2	3	Dsc
S07	4	1	2	2	3	Bsc
S08	4	3	2	1	3	Msc
S09	4	3	1	1	1	Bsc
S10	4	3	3	1	1	Msc
S11	4	3	2	1	5	Msc
S12	4	2	1	1	1	Msc
S13	4	3	1	1	3	Msc
S14	1	1	1	1	1	Msc

A etapa de caracterização resultou na composição de dois grupos, G1 e G2, disponível na Tabela 12, cada um formado por 7 participantes, seguindo um critério de balanceamento de perfis.

Tabela 12 - Grupos e participantes

Grupo	Participante
G1	S01
G1	S02
G1	S03
G1	S07
G1	S10
G1	S11
G1	S12
G2	S04
G2	S05
G2	S06
G2	S08
G2	S09
G2	S13
G2	S14

5.2 - Execução

O estudo de viabilidade, inicialmente, contou com 14 participantes, todos alunos de uma disciplina graduação e pós-graduação da Universidade Federal do Rio de Janeiro, UFRJ. O experimento foi conduzido durante o mês de agosto de 2023, com uma semana entre a rodada T1 e T2. Após a etapa de formação dos grupos, apenas 13 dos 14 participantes avançaram para a etapa de execução do estudo. O participante S09 abandonou o estudo, reduzindo o número de participantes do G1, de sete para seis participantes. É importante ressaltar que a saída do participante S09 não modificou o arranjo dos grupos G1 e G2, uma vez que os grupos estavam suficientemente balanceados.

Ambas as tentativas (T1 e T2) foram realizadas no documento de visão e requisitos do **Sistema Integrado de Gerência de Informações Contábeis,** um sistema real e em produção. Entre seus distintos módulos disponíveis, dois foram disponibilizados para o estudo:

- **Módulo de Solicitações (MSL):** módulo responsável pela gestão das solicitações contábeis realizadas pelos diversos clientes. Através desse módulo essas solicitações são criadas e acompanhadas pelos próprios clientes. Por outro lado, os colaboradores ficam responsáveis por avaliar essas solicitações e prosseguir com o processamento delas.
- **Módulo de Gestão Usuários (MGU):** módulo responsável pela administração dos usuários, bem como pela definição das funcionalidades as quais esses usuários terão acesso.

Tabela 13 - Resumo do Experimento

(T1) Ad-hoc:

- Os participantes receberam um treinamento via vídeo com duração aproximada de 30 minutos de Introdução à Lei Geral de Proteção de Dados Pessoais (LGPD)[3].
- Cada grupo realizou a inspeção *Ad-hoc* no artefato designado (ver Tabela 14)
- Cada participante preencheu seu relatório individual de discrepâncias encontradas durante a verificação com *Ad-hoc*.

(T2) *LGPDCheck*:

- Os participantes receberam treinamento[4] via vídeo com duração aproximada de 30 minutos. Durante o treinamento foram abordados como utilizar[5] a *LGPDCheck* para inspecionar artefatos de software.
- Cada grupo realizou a inspeção com *LGPDCheck* no artefato designado (ver Tabela 14)
- Cada participante preencheu seu relatório individual de discrepâncias encontradas durante a verificação com a técnica *LGPDCheck*.
- Cada participante preencheu o formulário de avaliação e aceitação da tecnologia.

Durante a primeira rodada (T1), os dois grupos receberam instruções sobre a LGPD e seus princípios através de um treinamento em vídeo, que abordou os seguintes temas: **I – Contexto Geral da Lei e escopo de aplicação, II – Principais termos e definições, III – Princípios da LGPD**. Ademais, também receberam instruções sobre inspeção de software e tipos de defeitos através de um treinamento. Após o treinamento, os participantes realizaram as inspeções *Ad-hoc* individualmente, relatando as discrepâncias identificadas em um formulário.

Tabela 14 – Grupos, Rodadas, e Artefatos Inspecionados

Grupo (tamanho)	T1	Módulo	T2	Módulo
G1 (6)	Ad-hoc	MSL	*LGPDCheck*	MGU
G2 (7)	Ad-hoc	MGU	*LGPDCheck*	MSL

[3] Vídeo “Introdução à Lei Geral de Proteção de Dados Pessoais (LGPD)” <https://youtu.be/AhXvvTr9Bqo>
[4] Vídeo “treinamento LGPDCheck”: <https://youtu.be/zOuke8U3NbY>
[5] Vídeo de explicação do material de apoio e seus artefatos: < https://youtu.be/EhF7bBqeb94>

Após a rodada T1, os participantes participaram de mais uma sessão de treinamento. Nesta sessão, eles foram apresentados à *LGPDCheck* e seus recursos, essenciais para a rodada T2.

Na segunda rodada (T2), os participantes de cada grupo foram designados para realizar inspeções usando a *LGPDCheck* em um módulo do sistema que ainda não inspecionaram, mas que foram inspecionados *Ad-hoc* por outros participantes na rodada T1. Como na primeira rodada, os participantes relataram as discrepâncias identificadas em uma folha de relatório de discrepâncias. Porém, desta vez deveriam associar cada discrepância relatada a um item do checklist *LGPDCheck,* também indicar o tipo de discrepância (**O – Omissão, FI – Fato incorreto, IN – Inconsistência, A – Ambiguidade e IE – Informação Estranha**) e fornecer informações adicionais sobre como e onde encontrar a discrepância relatada. A distribuição dos grupos (G1 e G2) e seus participantes, Tentativas (T1 e T2) e seus respectivos módulos podem ser vistos na Tabela 15.

Tabela 15 - Distribuição dos participantes

Grupo	Participante	Módulo (T1)	Módulo (T2)
G1	S01	MGU	MSL
G1	S02	MGU	MSL
G1	S03	MGU	MSL
G1	S07	MGU	MSL
G1	S10	MGU	MSL
G1	S11	MGU	MSL
G1	S12	MGU	MSL
G2	S04	MSL	MGU
G2	S05	MSL	MGU
G2	S06	MSL	MGU
G2	S08	MSL	MGU
G2	S09	MSL	MGU
G2	S13	MSL	MGU
G2	S14	MSL	MGU

Após a rodada T2, cada participante foi provido com um questionário de avaliação LGPDCheck (ver Apêndice H). Este formulário de avaliação abrange um conjunto de 16 perguntas, que englobam tanto questões abertas quanto fechadas. O propósito é capturar a percepção dos participantes após o experimento, com os resultados sendo detalhados na seção 5.3 - Resultados Quantitativos e 5.4 - Resultados Qualitativos deste capítulo. Todos os dados obtidos na execução do estudo de viabilidade foram posteriormente tabelados e preparados para etapa de análise

quantitativa e qualitativa. Os resultados das análises são detalhados a seguir na seção de Resultados Quantitativos.

5.3 - Resultados Quantitativos

Nesta seção, os dados coletados durante as rodadas *Ad-hoc* (T1) e *LGPDCheck* (T2) são apresentados. Estes dados subsidiam os resultados gerais (Ad-Hoc/*LGPDCheck*), tempo e duração da inspeção, número de discrepâncias (DC)[6], falsos positivos (FP)[7], defeitos (ND)[8], Defeitos LGPD (ND_LGPD)[9], eficiência (EFF)[10] e eficácia (EFC)[11].

Nas seções a seguir são explorados os resultados tanto por rodada (T1 e T2), por módulo, por participante.

5.3.1 - Etapa de Discriminação de Defeitos

Esta seção tem como objetivo oferecer detalhes sobre o processo conduzido durante a etapa de discriminação. Durante esta fase, os moderadores executam o processo de classificação de cada uma das Discrepâncias (ND), determinando se estas devem ser confirmadas como Defeitos (DEF) ou descartadas como Falsos Positivos (FP).

Os exemplos foram coletados durante as rodadas T1 e T2 através dos formulários de discrepâncias, preenchidos pelos participantes no estudo de viabilidade. Nas seções subsequentes, são apresentados exemplos (cenários) com base nos relatados individuais dos participantes durante as etapas do estudo de viabilidade da *LGPDCheck*.

5.3.1.2 - Defeito (ND)

Cenário: os participantes relataram a falta de informações relacionadas aos papeis ou informações consideradas necessárias para compreensão e construção de regras de negócio relacionadas ao domínio do sistema em inspeção. Exemplos podem ser vistos a seguir:

---

[6] Discrepâncias (DC) são todas as inconformidades relatadas pelo inspetor durante o processo de inspeção.
[7] Falso Positivo (FP) são discrepâncias consideradas válidas pelo moderador, porém não se confirmaram como um defeito.
[8] Defeitos (DEF) os moderadores decidem, caso a caso, quais discrepâncias são confirmadas como um defeito (DEF) durante a etapa de discriminação.
[9] Defeito LGPD é uma categorização dos defeitos interna, realizada durante a etapa de discriminação pelos moderadores.
[10] Eficiência é o tempo médio (em minutos) para detectar um único defeito.
[11] Eficácia é a razão entre o número de defeitos encontrados pelo participante e o número total de defeitos distintos encontrados por cada participante

- *“Não especificado no caso de uso”*
- *“Não é definido quais são as funcionalidades públicas.”*
- *“Cita reenviar a senha, a mesma?”*
- *“Não é descrito qual dado será usado para identificar o usuário.”*
- *“Ausência de definição de PF (Pessoa Física).”*

5.3.1.3 - Defeito LGPD (DEF_LGPD)

Foram criadas duas categorias internas para os defeitos LGPD e não LGPD. Posteriormente, essa categorização permitiu traçar um comparativo entre as duas rodadas em relação aos defeitos do tipo LGPD identificados. Sempre que um defeito era confirmado, ele também era avaliado se se encaixava na categoria Privacidade e Proteção de Dados (LGPD), possibilitando distinguir entre defeitos gerais (ND) e defeitos específicos LGPD (DEF_LGPD).

Cenário 1: Coleta de dados sem justificativa ou excessiva.

- *“O dado pessoal “Localização” se refere ao endereço de residência? Se sim, para quê?”*
- *“F14. Para quê a localização?”*
- *“Informação do telefone e localização não são necessárias.”*
- *“Faltam processos para avaliar a proporcionalidade.”*

Cenário 2: falta de definição de práticas de segurança e políticas de acesso nos documentos inspecionados:

- *“Não há menção a criptografia.”*
- *“não há indicação de medidas para redução de dados em caso de acesso indevido aos dados do usuário.”*
- *“Não foram definidas práticas para vazamento de dados pessoais.”*
- *“Não são descritas medidas de segurança ou anonimização.”*

Cenário 3: Falta de transparência com o usuário sobre os tratamentos realizados sobre seus dados pessoais:

- *“Não é evidente se o usuário tem acesso à justificativa dos tratamentos de seus dados, nem se notificado quando de alterações.”*

- *“Deve garantir a autorização por parte do titular que teve seus dados tratados.”*

5.3.1.4 - Falso Positivo (FP)

Cenário 1: o participante identificou uma discrepância, na situação relatada, uma sigla incorreta. O participante reportou a mesma discrepância inúmeras vezes. Nesse caso, quando confirmado o defeito, apenas uma ocorrência foi considerada, o restante descartado do montante total como FP.

Cenário 2: os participantes relataram discrepâncias que eram contraditórias às informações presentes nos documentos fornecidos, logo, foram descartadas.

Exemplos:

- *“Funcionalidade não está na Fig. 3.”*
- *“O software não apresenta restrições de visibilidade para substitutos.”*
- *“Não está claro a finalidade de armazenar esses dados.”*

5.3.2 - Resultados gerais

Foram identificados um total de 230 discrepâncias, 157 (cerca de 68%) foram confirmadas como defeitos durante a etapa de discriminação (ver Figura 1), sendo 44 na rodada Ad-hoc (T1) e 113 na rodada *LGPDCheck* (T2) (ver Tabela 16).

Tabela 16 - Números gerais das rodadas

Métrica	**Ad-hoc**	***LGPDCheck***	**Total**
Total de Discrepâncias (DC)	89	141	230
Total de Defeitos (ND)	44	113	157
Falsos Positivos (FP)	63	28	91
Total defeitos LGPD (DEF_LGPD)	23	103	126

Do montante de defeitos confirmados após a etapa de discriminação, aproximadamente 72% dos defeitos confirmados foram identificados pela *LGPDCheck*, enquanto cerca de 28% pela Ad-hoc (ver Tabela 17).

Tabela 17 - Porcentagem de defeitos por rodada

Rodada	**Porcentagem de defeitos confirmados**
Ad-hoc	28,03%
LGPDCheck	71,97%

Em relação aos defeitos confirmados do tipo LGPD (DEF_LGPD), dos 44 defeitos confirmados durante a rodada **Ad-hoc (T1)**, cerca de 52% (23) dos defeitos confirmados. Enquanto a ***LGPDCheck* (T2)**, dos 113 defeitos confirmados, cerca de 91% (103) são do tipo LGPD, os resultados podem ser vistos em detalhes na Tabela 18.

Tabela 18 - Eficiência Ad-hoc x *LGPDCheck*

Técnica	Duração média de inspeção (minutos)	Total de defeitos	Eficiência (Defeito por minuto)
LGPDCheck	60,9	113	1,85
Ad-Hoc	51,3	44	0,86

Em termos de Eficácia (Efc), ou confirmação entre discrepâncias válidas e confirmação em defeitos, Ad-Hoc tem 49,4% de confirmação de defeitos, 89 discrepâncias para 44 defeitos, enquanto a *LGPDCheck* tem 80%, 141 discrepâncias para 113 defeitos.

Em termos de Eficiência (Eff), foi utilizado a média de duração do tempo de inspeção em minutos por rodada. A duração média do tempo de inspeção para Ad-Hoc foi 51,3 minutos, enquanto a *LGPDCheck* a média foi de 60,9 minutos. A verificação com *LGPDCheck* teve uma média de duração de inspeção de cerca de 18,7% mais longa, em uma média de 9,6 minutos. A eficácia da rodada Ad-Hoc foi de 0,86 defeitos por minuto, enquanto na *LGPDCheck* 1,85 defeitos por minuto. Quando comparada a Ad-Hoc, a *LGPDCheck* foi cerca de 116% mais eficiente na detecção de defeitos por minuto de inspeção.

5.3.3 - Resultados por Inspetores

Nesta seção, são apresentados os resultados individuais dos participantes, destacando as diferenças notadas durante uma rodada, os defeitos confirmados e os falsos positivos (FP) identificados no estudo. Cada resultado individual inclui a duração da inspeção em minutos, o quão eficiente (Eff) foi o inspetor em detectar defeitos, sua eficácia (Efc) na confirmação de defeitos, e, por fim, a porcentagem de FP do participante em uma rodada específica. A intenção é oferecer uma visão mais detalhada do desempenho único de cada participante durante a inspeção e a rodada correspondente.

Tabela 19 - Resultados Ad-hoc por Inspetores

ID	Módulo	Discrepâncias	Defeitos	FP	DEF_LGPD	Duração (min)	Eff	Efc	% FP
S01	MGU	3	1	2	1	45	45,0	33,3	66,7
S02	MGU	5	5	0	4	50	10,0	100,0	0,0
S03	MGU	13	2	11	1	45	22,5	15,4	84,6
S04	MSL	5	2	3	2	66	33,0	40,0	60,0
S05	MSL	8	4	4	0	59	14,8	50,0	50,0
S06	MSL	8	8	0	7	67	8,4	100,0	0,0
S07	MGU	2	0	2	0	60	N/A	0,0	100,0
S08	MSL	6	3	3	2	59	19,7	50,0	50,0
S10	MGU	4	3	1	2	50	16,7	75,0	25,0
S11	MGU	10	3	7	0	69	23,0	30,0	70,0
S12	MGU	10	3	7	0	62	20,7	30,0	70,0
S13	MSL	9	6	3	4	45	7,5	66,7	33,3
S14	MSL	6	4	2	0	41	10,3	66,7	33,3

É importante mencionar que, durante a rodada Ad-hoc, 18 discrepâncias foram descartadas, pois o inspetor S14 relatou a mesma discrepância, em diversas partes do documento. Nesse caso, apenas uma única entrada foi considerada como defeito, o restante desconsiderado do montante elegível à categoria de defeitos. O mesmo não ocorreu na rodada LGPDCheck, em que nenhuma discrepância foi descartada, uma vez que, na grande maioria, os inspetores associaram a discrepância a uma pergunta do checklist, tornando mais explicita a análise individual durante a etapa de discriminação.

Ao consultar a Tabela 19, é possível obter uma visão abrangente dos resultados dos participantes durante a rodada Ad-hoc (T1). Ao observar os dados individualmente por inspetor:

- Quantidade de Defeitos (DEF)**:** Os inspetores S02, S04 e S05 se destacam, cada um com 5, 4 e 4 defeitos, respectivamente. Em contraste, S07 não identificou nenhum defeito durante a inspeção.
- Falsos Positivos (% FP): S02 e S06 alcançaram 0% de falsos positivos, indicando uma precisão notável na identificação de defeitos. Em contrapartida, S03 e S07 apresentaram percentagens elevadas de falsos positivos, atingindo 84,6% e 100%, respectivamente.
- Eficiência (Eff): S02, S06, S13 e S14 obtiveram as melhores taxas de eficiência na identificação de defeitos por tempo de inspeção.

- Eficácia (Efc): S02, S05, S06 e S07 atingiram 100% de eficácia na confirmação de defeitos. No entanto, a maioria dos participantes manteve uma eficácia abaixo de 50%.

Durante a etapa de verificação, cada discrepância identificada foi classificada[12] pelos inspetores entre Omissão (O), Fato Incorreto (FI), Inconsistência (IN), Ambiguidade (A) e Informação Estranha (IE).

Tabela 20 - Resultados Ad-hoc por inspetores e tipos de defeito

ID	Módulo	Defeitos	Def_O	Def_IE	Def_A	Def_IN	Def_FI
S01	MGU	1	1	0	0	0	0
S02	MGU	5	2	0	3	0	0
S03	MGU	2	0	1	1	0	0
S04	MSL	2	2	0	0	0	0
S05	MSL	4	1	2	1	0	0
S06	MSL	8	8	0	0	0	0
S07	MGU	0	0	0	0	0	0
S08	MSL	3	1	0	2	0	0
S10	MGU	3	3	0	0	0	0
S11	MGU	3	1	0	2	0	0
S12	MGU	3	1	0	2	0	0
S13	MSL	6	5	0	1	0	0
S14	MSL	4	1	0	0	3	0
Total		44	26	3	12	3	0

Ao observar a Tabela 20, uma visualização complementar aos resultados da Tabela 19, os resultados anteriores são expandidos para visualizar o tipo dos defeitos identificados pelos inspetores durante a rodada. A visualização permite destacar as seguintes informações:

- Inspetor S06 apresenta um número maior de defeitos em comparação com outros inspetores.
- O defeito do tipo Omissão (O) é o tipo de defeito mais comum, com Inspetores S06, S13 e S02 liderando no número de defeitos identificados.

[12] Detalhes sobre a taxonomia de defeitos podem ser encontrados na seção 3.1 - Inspeção de Software.

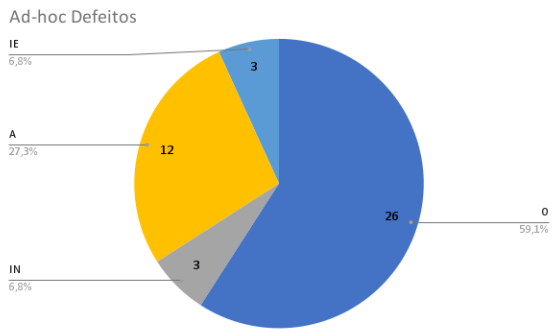

Figura 8 - Defeitos Ad-hoc

O gráfico disponível na Figura 8 oferece uma representação visual da distribuição dos tipos de defeitos identificados durante a rodada Ad-hoc. Em destaque, observamos que a Omissão (O) lidera com 59.1% das ocorrências, seguida pela Ambiguidade (A) com 27.3%. Empatados em terceiro lugar com 6.8%, Informação Estranha (IE) e Inconsistência (IN).

Tabela 21 - Resultados *LGPDCheck* por inspetores e tipos de defeito

ID	Módulo	Discrepâncias	Defeitos	FP	DEF_ LGPD	Duração	Eff	Efc	% FP
S01	MSL	9	7	2	6	73	10,4	77,8	22,2
S02	MSL	12	6	6	6	71	11,8	50,0	50,0
S03	MSL	18	15	3	15	54	3,6	83,3	16,7
S04	MGU	19	17	2	17	53	3,1	89,5	10,5
S05	MGU	2	2	0	0	52	26,0	100,0	0,0
S06	MGU	17	15	2	15	68	4,5	88,2	11,8
S07	MSL	5	4	1	2	77	19,3	80,0	20,0
S08	MGU	12	6	6	5	74	12,3	50,0	50,0
S10	MSL	7	6	1	5	50	8,3	85,7	14,3
S11	MSL	20	19	1	18	54	2,8	95,0	5,0
S12	MSL	6	6	0	5	66	11,0	100,0	0,0
S13	MGU	11	9	2	9	56	6,2	81,8	18,2
S14	MGU	3	1	2	0	44	44,0	33,3	66,7

Ao fazer referência à Tabela 21, obtemos uma visão dos resultados dos participantes durante a rodada *LGPDCheck* (T2). Ao analisar os dados de cada inspetor separadamente podemos observar:

- Quantidade de Defeitos (DEF): O inspetor S11 apresenta a maior quantidade de defeitos (19), seguido pelos Inspetores S03 e S06 (15 cada).

- Falsos Positivos (% FP): os inspetores S05, S10 e S12 apresentam 0% de falsos positivos, indicando com aproveitamento de 100% na identificação de defeitos. A maior taxa de FP é do inspetor S14 com 66,7%.
- Eficiência (Eff): S03, S04, S06 e S11 respectivamente obtiveram as melhores taxas de eficiência na identificação de defeitos por tempo de inspeção.

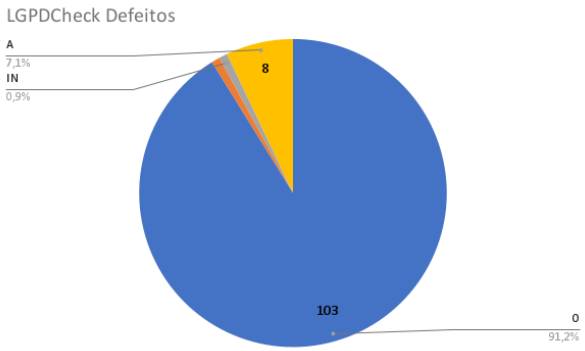

Figura 9 - *LGPDCheck* defeitos

O gráfico disponível na Figura 9 apresenta de forma visual a distribuição dos tipos de defeitos identificados durante a rodada *LGPDCheck*. Em primeiro lugar, destaca-se a Omissão (O) com 91.2% das ocorrências, seguida por Ambiguidade (A) com 7.1%. Em terceiro lugar, Fato Incorreto (FI) e Inconsistência (IN), ambos com 0.9%.

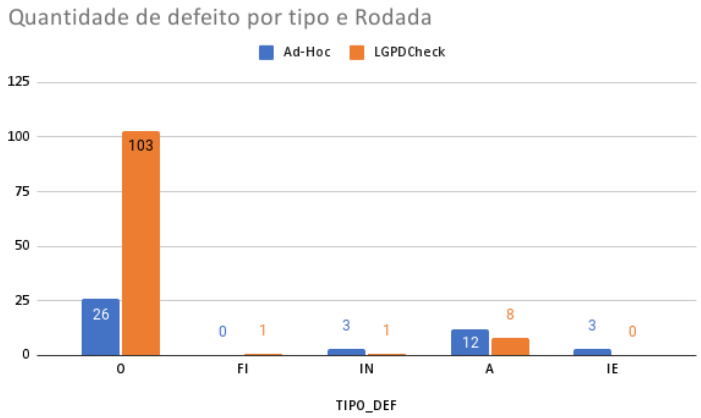

Figura 10 - Comparativo defeitos gerais Ad-hoc x *LGPDCheck* por tipo de defeito

Considerando os gráficos presentes nas Figura 8, Figura 9 e Figura 10 é notável que, embora a *LGPDCheck* identifique e confirme um maior número total de defeitos, a técnica tende a sobressair na identificação de defeitos do tipo omissão. Por outro lado, a Ad-hoc, mesmo apresentando uma quantidade total menor de defeitos e uma taxa de

confirmação inferior, quando comparada a *LGPDCheck*, a rodada Ad-hoc demonstrou identificar defeitos de tipos mais variados.

5.3.4 - Resultados por Módulo e Rodada

A classificação permitiu a análise dos defeitos encontrados entre as rodadas Ad-hoc (T1) e *LGPDCheck* (T2) e módulos verificados (MSL/MGU).

Tabela 22 - Resultados gerais x Tipo de Defeito

Rodada	Módulo	DEF_O	DEF_FI	DEF_IN	DEF_A	DEF_IE
MGU	*Ad-hoc*	8	0	0	8	1
MGU	*LGPDCheck*	44	1	1	4	0
MSL	*Ad-hoc*	18	0	3	4	2
MSL	*LGPDCheck*	59	0	0	4	0

Ao analisar a tabela acima, é possível observar os resultados e o número de defeitos por módulo dos sistemas verificados MSL e MGU e sua respectiva taxonomia de defeitos associada para as rodadas (T1) e (T2), para ambos os módulos MGU e MSL.

Uma outra forma de visualizar os resultados acima é por rodada (T1/Ad-hoc) ou (T2/*LGPDCheck*), que engloba os números obtidos por cada um dos módulos MSL e MGU, como visto na Tabela 22.

5.3.4.1 - Resultados dos Defeitos tipo LGPD por Rodada

Ao analisar resultados obtidos por módulo dos sistemas verificados MSL e MGU (ver Tabela 23), é possível compreender que na rodada Ad-hoc (T1), no módulo MGU foram confirmados 17 defeitos, desses defeitos 8 são do tipo LGPD (aprox. 47%). Enquanto para o módulo MSL foram confirmados 27 defeitos, em que 15 são defeitos do tipo LGPD (aprox. 55%). Enquanto na rodada *LGPDCheck* (T2), no módulo MGU foram confirmados 50 defeitos, desse montante, 46 são do tipo LGPD (aprox. 92%). Enquanto para o módulo MSL foram confirmados 63 defeitos, dos quais 57 são defeitos do tipo LGPD (aprox. 90%).

Tabela 23 - Resultados por Módulo e Defeitos LGPD

Módulo	Rodada	Total DEF	Total DEF_LGPD	% DEF_LGPD
MGU	*Ad-hoc*	17	8	47,06
MGU	*LGPDCheck*	50	46	92,00
MSL	*Ad-hoc*	27	15	55,56
MSL	*LGPDCheck*	63	57	90,48

Em relação aos defeitos vinculados à LGPD, ao observar os dados da Tabela 24, é possível examinar os resultados obtidos em ambas as rodadas, incluindo as classificações atribuídas aos defeitos específicos relacionados à LGPD.

Tabela 24 - Defeitos por tipo LGPD por TIPO (O, FI, IN, A, IE)

Rodada	Módulo	DEF_LGPD_O	DEF_LGPD _FI	DEF_LGPD _IN	DEF_LGPD _A	DEF_LGPD _IE	Total
MGU	Ad-Hoc	4	0	0	3	1	8
MGU	*LGPDCheck*	44	0	0	2	0	46
MSL	Ad-Hoc	13	0	0	2	0	15
MSL	*LGPDCheck*	56	0	0	1	0	57

Os gráficos presentes nas Figura 11, Figura 12 e Figura 13 funcionam como apoios visuais, seu objetivo é auxiliar na visualização da distribuição dos defeitos associados à LGPD e seus tipos, porém, visualizados por rodada.

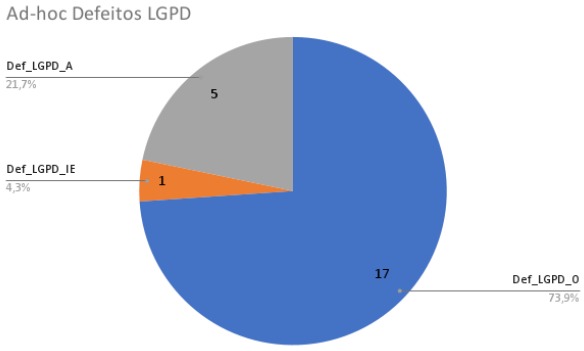

Figura 11 - Ad-hoc defeitos tipo LGPD

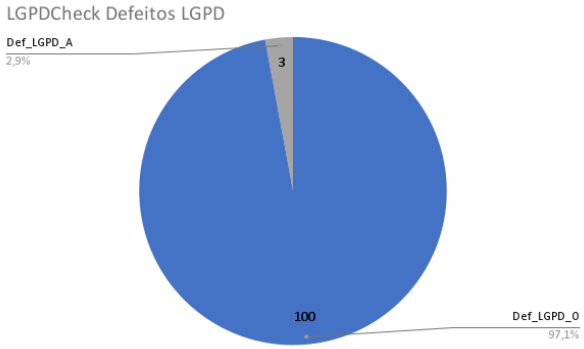

Figura 12 - *LGPDCheck* defeitos tipo LGPD

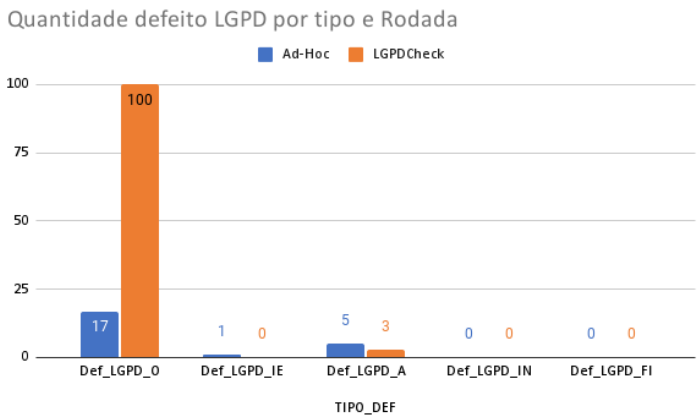

Figura 13 - Comparativo defeitos associados à LGPD Ad-hoc x *LGPDCheck* por tipo de defeito

Os defeitos associados à LGPD, em sua maioria, são predominantemente do tipo Omissão (O), representando 97% ou 100 defeitos na *LGPDCheck*, enquanto para Ad-hoc, aproximadamente 73%, totalizando 17 defeitos. Os resultados estão visualmente apresentados nos gráficos das Figura 11, Figura 12 e Figura 13, refletindo as informações detalhadas na Tabela 24.

Ainda para Ad-hoc, foram identificados cinco defeitos do tipo Ambiguidade (A), enquanto para a *LGPDCheck*, esse número foi de três. Por fim, os defeitos do tipo Informação Estranha (IE), foram exclusivamente identificados na rodada Ad-hoc, totalizando um defeito, enquanto nenhum defeito foi detectado na *LGPDCheck*.

5.3.5 - Defeitos únicos

Os dados foram examinados em busca de outliers, e a normalidade e a homocedasticidade foram verificadas usando os testes de Shapiro-Wilk e Levene. Testes não paramétricos ou paramétricos, como os testes t de Wilcoxon e Student, foram aplicados conforme apropriado (ver Apêndice I).

Antes que os testes fossem realizados, os defeitos (DEF) e (DEF_LGPD) identificados e confirmados passaram por uma nova rodada de análise com objetivo de identificar defeitos únicos em ambas as rodadas (T1) e (T2), foram incluídos todos os inspetores, em ambas rodadas, que tiveram ao menos um defeito identificado.

Com um total de 12 inspetores para Ad-hoc (T1) e 13 para *LGPDCheck* (T2), uma rodada de classificação de defeitos dos defeitos (DEF) foi realizada por módulo. O processo de identificação ocorreu da seguinte forma:

- Cada defeito foi analisado pelos moderadores de acordo com a descrição, tipo de defeito e localização informada pelo inspetor e, quando aplicável, a pergunta do checklist;
- Cada defeito foi associado a um identificador exclusivo que inclui o prefixo do módulo onde o defeito foi identificado, seguido por dois dígitos. Os identificadores seguem o formato MSLn ou MGUn, indicando se o defeito pertence ao módulo MSL ou MGU, seguido pelo número específico do defeito (n).
- Ao iniciar o processo de identificação de defeitos no mesmo módulo, independentemente da rodada em que foram descobertos, cada defeito recebia um identificador exclusivo. Posteriormente, ao encontrar um defeito semelhante, os moderadores revisavam cuidadosamente a resposta do inspetor relativa a esse defeito para determinar se já havia sido relatado anteriormente. Quando se confirmava que o defeito era único e ainda não havia sido identificado, um novo identificador era atribuído. No entanto, se o defeito já tivesse sido identificado anteriormente, o identificador do defeito era repetido.

Durante a avaliação do módulo MSL (*Ad-hoc/LGPDCheck*), foram identificados, no total, 53 defeitos únicos. Na fase de inspeção *Ad-hoc* (T1), com 16 defeitos únicos identificados, e na etapa subsequente, inspeção *LGPDCheck* (T2), com 30 defeitos únicos identificados, observou-se que 7 defeitos foram comuns às duas rodadas de inspeção. Os resultados detalhados podem ser visualizados na Figura 14.

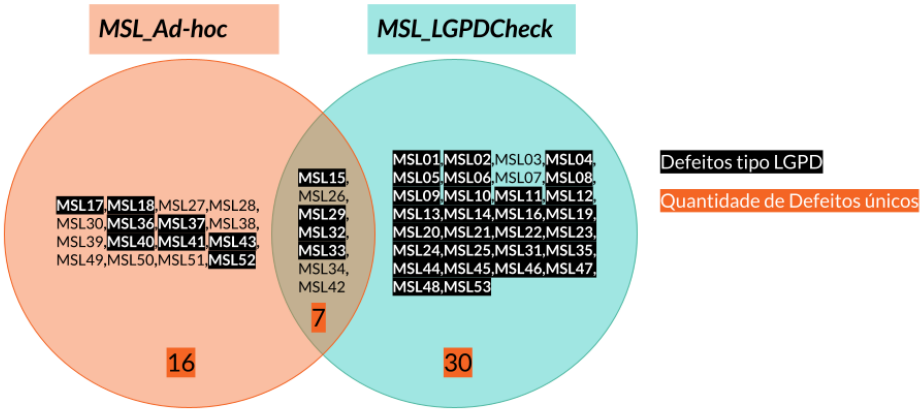

Figura 14 - Defeitos únicos MSL (Ad-hoc e LGPDCheck)

Quanto ao módulo MGU (*Ad-hoc/LGPDCheck),* 45 defeitos únicos foram identificados no total. Durante a inspeção *Ad-hoc (T1)*, foram encontrados 10 defeitos únicos, enquanto na fase subsequente, na inspeção LGPDCheck (T2), identificou-se um

total de 33 defeitos únicos. Destaca-se que 2 defeitos foram comuns a ambas as rodadas de inspeção. Os resultados detalhados podem ser visualizados na Figura 15.

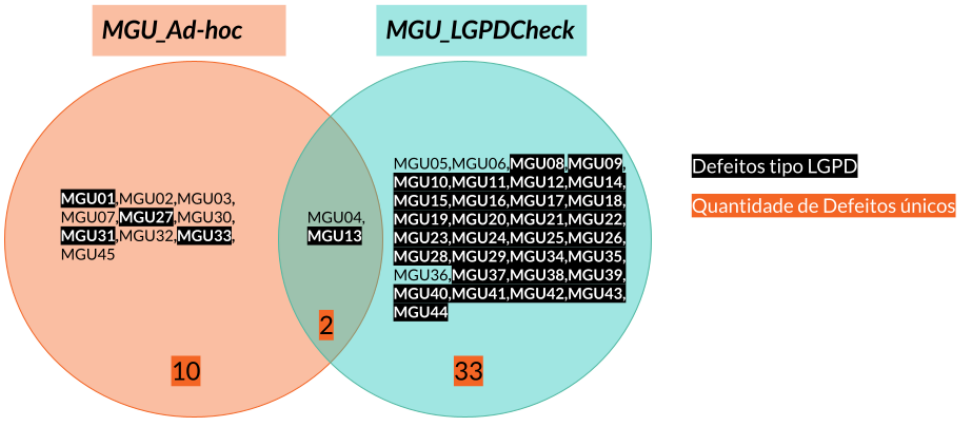

Figura 15 - Defeitos únicos MGU (Ad-hoc e LGPDCheck)

Os resultados por participantes estão disponíveis na Tabela 25 para a rodada *Ad-hoc*, e na Tabela 26 para a *LGPDCheck*.

Tabela 25 - Defeitos únicos Ad-hoc

ID	Técnica	Módulo	Defeitos	Duração (seg.)	DEF_ LGP	DEF_O	DEF_ FI	DEF_ IN	DEF_ A	DEF_IE
S01	*Ad-hoc*	MGU	**1**	2700	1	MGU01				
S02	*Ad-hoc*	MGU	**5**	3000	4	MGU31			MGU03 , MGU07	
S03	*Ad-hoc*	MGU	**2**	2700	1					MGU01
S04	*Ad-hoc*	MSL	**2**	3960	2	MSL32, MSL36				
S05	*Ad-hoc*	MSL	**4**	3540	0					
S06	*Ad-hoc*	MSL	**8**	4020	7	MSL17, MSL18, MSL29, MSL37, MSL40, MSL41, MSL52				
S08	*Ad-hoc*	MSL	**3**	3540	2				MSL33, MSL42	
S10	*Ad-hoc*	MGU	**3**	3000	2	MGU13, MGU27				

S11	*Ad-hoc*	MGU	**3**	4140	0					
S12	*Ad-hoc*	MGU	**3**	3720	0					
S13	*Ad-hoc*	MSL	**6**	2700	4	MSL15, MSL33, MSL34, MSL43				
S14	*Ad-hoc*	MSL	**2**	2460	0					

Tabela 26 - Defeitos únicos *LGPDCheck*

ID	Técnica	Módulo	Defeitos	Duração (seg.)	DEF_ LGPD	DEF_O	DEF_ FI	DEF_ IN	DEF_ A	DEF_ IE
S01	*LGPDCheck*	MSL	**7**	4380	6	MSL01, MSL02, MSL03, MSL04, MSL05, MSL06				
S02	*LGPDCheck*	MSL	**6**	4260	6	MSL02, MSL08, MSL09, MSL10, MSL11, MSL16				
S03	*LGPDCheck*	MSL	**15**	3240	15	MSL01, MSL02, MSL11, MSL12, MSL13, MSL14, MSL16, MSL19, MSL20, MSL21, MSL22, MSL23, MSL29, MSL31, MSL32				
S04	*LGPDCheck*	MGU	**14**	3180	14	MGU08, MGU09, MGU11, MGU12, MGU19, MGU24, MGU25, MGU26, MGU34, MGU35, MGU38, MGU39, MGU40, MGU41				

S05	*LGPDCheck*	MGU	**2**	3120	0					
S06	*LGPDCheck*	MGU	**15**	4080	15	MGU09, MGU10, MGU11, MGU12, MGU13, MGU14, MGU15, MGU16, MGU17, MGU18, MGU19, MGU20, MGU21, MGU22, MGU41				
S07	*LGPDCheck*	MSL	**4**	4620	2	MSL33, MSL45				
S08	*LGPDCheck*	MGU	**6**	4440	5	MGU08, MGU11, MGU23, MGU26, MGU41				
S10	*LGPDCheck*	MSL	**6**	3000	5	MSL02, MSL23, MSL25, MSL26, MSL32				
S11	*LGPDCheck*	MSL	**19**	3240	17	MSL01, MSL02, MSL04, MSL11, MSL12, MSL14, MSL15, MSL16, MSL19, MSL29, MSL31, MSL32, MSL35, MSL44, MSL46, MSL47, MSL48				
S12	*LGPDCheck*	MSL	**6**	3960	5	MSL02, MSL25, MSL53, MSL32			MSL29	
S13	*LGPDCheck*	MGU	**9**	3360	9	MGU23, MGU24, MGU25, MGU28,			MGU44	
S14	*LGPDCheck*	MGU	**1**	2640	0					

Nas seções a seguir, serão apresentados os resultados obtidos durante os testes realizados, seguidos por uma breve conclusão dos resultados obtidos.

5.3.5.1 - Defeitos por técnica (rodada)

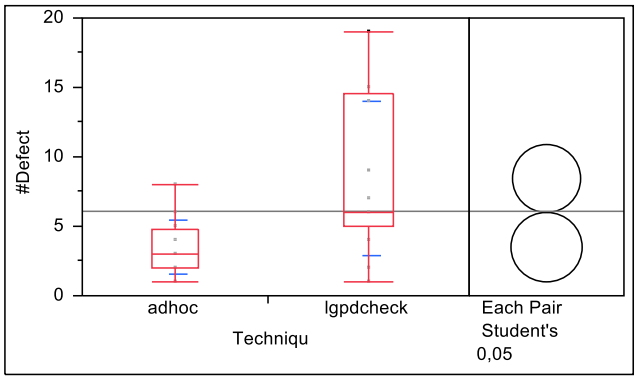

Figura 16 - Oneway Analysis of #Defects By Technique

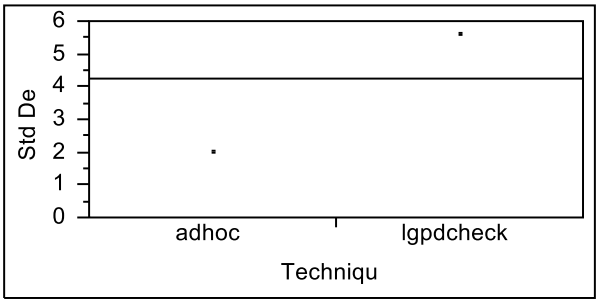

Figura 17 – Teste de variância

Level	Count	Std Dev	MeanAbsDif to Mean	MeanAbsDif to Median
Ad-hoc	12	1,977142	1,500000	1,333333
LGPDCheck	13	5,562005	4,568047	4,153846

Test	F Ratio	DFNum	DFDen	p-Value
O'Brien[.5]	6,7639	1	23	0,0160*
Brown-Forsythe	4,5604	1	23	0,0436*
Levene	11,6502	1	23	0,0024*
Bartlett	9,8813	1	.	0,0017*
F Test 2-sided	7,9138	12	11	0,0017*

Welch's Test
Welch Anova testing Means Equal, allowing Std Devs Not Equal

F Ratio	DFNum	DFDen	Prob > F
9,0990	1	15,2	0,0086*

t Test
3,0165

Means Comparisons
Comparisons for each pair using Student's t
Confidence Quantile

t	**Alpha**
2,06866	0,05

LSD Threshold Matrix

Abs(Dif)-LSD	***LGPDCheck***	***Ad-hoc***
LGPDCheck	-3,4434	1,4471
Ad-hoc	1,4471	-3,5840

Positive values show pairs of means that are significantly different.

Existe diferença entre o número de defeitos encontrados com *LGPDCheck* quando comparado com Ad-hoc. No cenário do estudo aplicado, a *LGPDCheck* é capaz de encontrar uma quantidade muito maior de defeitos durante o processo de inspeção.

5.3.5.2 - Defeitos por técnica por tempo (segundos)

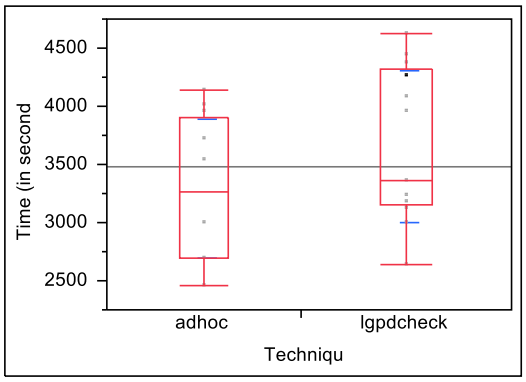

Figura 18 - Oneway Analysis of Time (in seconds) By Technique

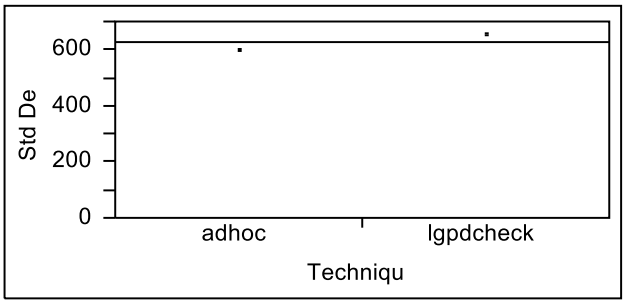

Figura 19 - Teste de variância

Level	**Count**	**Std Dev**	**MeanAbsDif to Mean**	**MeanAbsDif to Median**
Ad-hoc	12	596,6269	530,0000	530,0000
LGPDCheck	13	652,8989	585,7988	572,3077

Test	F Ratio	DFNum	DFDen	p-Value
O'Brien[.5]	0,3128	1	23	0,5814
Brown-Forsythe	0,1005	1	23	0,7541
Levene	0,3727	1	23	0,5475
Bartlett	0,0890	1	.	0,7655
F Test 2-sided	1,1975	12	11	0,7722

Welch's Test
Welch Anova testing Means Equal, allowing Std Devs Not Equal

F Ratio	DFNum	DFDen	Prob > F
2,1377	1	22,999	0,1573

t Test
1,4621

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
Ad-hoc	12	129,500	156,000	10,7917	-1,417
LGPDCheck	13	195,500	169,000	15,0385	1,417

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
129,5	-1,41721	0,1564

1-way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
2,0865	1	0,1486

Embora se possa ver uma leve variação a menos na média, podemos concluir com os resultados apresentados que não há diferença significativa no tempo de inspeção entre Ad-hoc e *LGPDCheck*.

5.3.5.3 - Defeitos por técnica, tempo e módulo

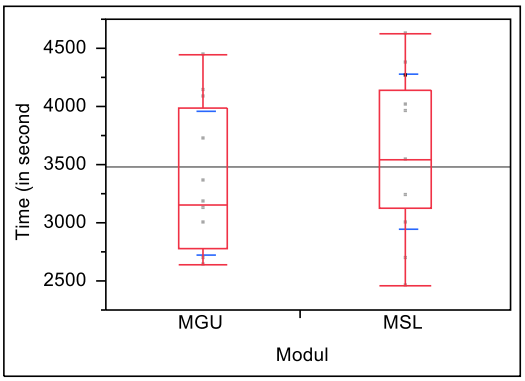

Figura 20 - Oneway Analysis of Time (in seconds) By Module

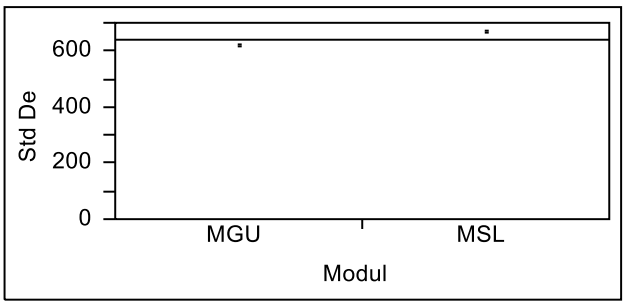

Figura 21 - Teste de variância

Level	Count	Std Dev	MeanAbsDif to Mean	MeanAbsDif to Median
MGU	12	614,7283	506,6667	480,0000
MSL	13	661,7459	545,3254	540,0000

Test	F Ratio	DFNum	DFDen	p-Value
O'Brien[.5]	0,1150	1	23	0,7376
Brown-Forsythe	0,1542	1	23	0,6982
Levene	0,0870	1	23	0,7707
Bartlett	0,0596	1	.	0,8072
F Test 2-sided	1,1588	12	11	0,8140

Welch's Test
Welch Anova testing Means Equal, allowing Std Devs Not Equal

F Ratio	DFNum	DFDen	Prob > F
1,1121	1	22,998	0,3026

t Test
1,0546

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
MGU	12	137,000	156,000	11,4167	-1,008
MSL	13	188,000	169,000	14,4615	1,008

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
137	-1,00840	0,3133

1-way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
1,0726	1	0,3004

Após a análise dos resultados acima, podemos verificar que não há diferença em tempo de inspeção entre os módulos.

5.3.5.4 - Defeitos LGPD por técnica

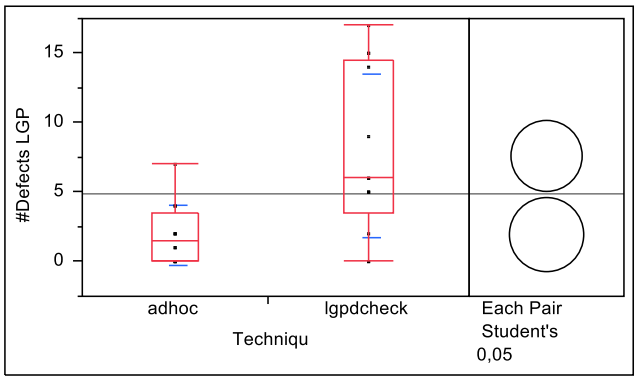

Figura 22 - Oneway Analysis of #Defects LGPD By Technique

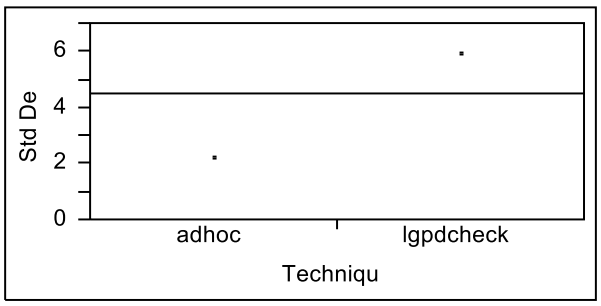

Figura 23 - Teste de variância

Level	Count	Std Dev	MeanAbsDif to Mean	MeanAbsDif to Median
Ad-hoc	12	2,151462	1,583333	1,583333
LGPDCheck	13	5,867118	4,911243	4,538462

Test	F Ratio	DFNum	DFDen	p-Value
O'Brien[.5]	9,3033	1	23	0,0057*
Brown-Forsythe	6,2001	1	23	0,0204*
Levene	13,2076	1	23	0,0014*
Bartlett	9,3722	1	.	0,0022*
F Test 2-sided	7,4367	12	11	0,0022*

Welch's Test
Welch Anova testing Means Equal, allowing Std Devs Not Equal

F Ratio	DFNum	DFDen	Prob > F
10,7050	1	15,394	0,0050*

t Test
3,2719

Means Comparisons
Comparisons for each pair using Student's t
Confidence Quantile

t	Alpha
2,06866	0,05

LSD Threshold Matrix

Abs(Dif)-LSD	***LGPDCheck***	***Ad-hoc***
LGPDCheck	-3,6444	1,9792
Ad-hoc	1,9792	-3,7932

Positive values show pairs of means that are significantly different.

Estatisticamente, os resultados demonstram que técnica *LGPDCheck* possui desempenho superior, quando comparado a Ad-hoc, na detecção de defeitos do tipo LGPD (DEF_LGPD).

5.3.5.5 - Análise defeitos Ad-hoc

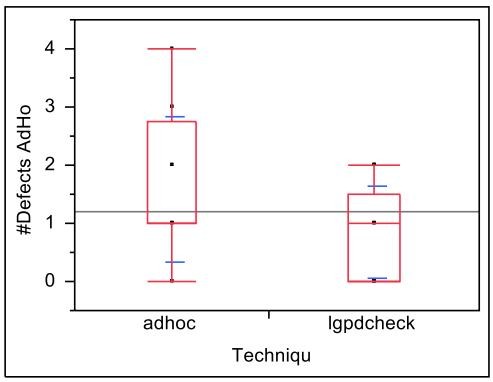

Figura 24 - Oneway Analysis of #Defects *Ad-hoc* By Technique

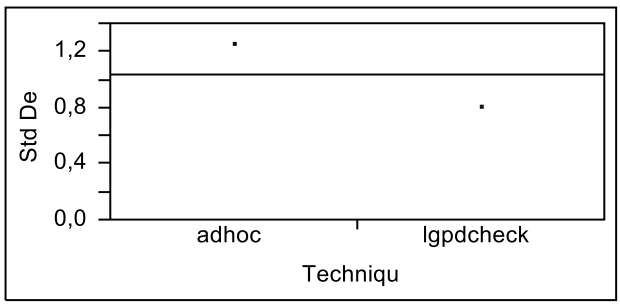

Figura 25 - Teste de variância

Level	**Count**	**Std Dev**	**MeanAbsDif to Mean**	**MeanAbsDif to Median**
Ad-hoc	12	1,240112	1,013889	0,9166667
LGPDCheck	13	0,800641	0,650888	0,6153846

Test	**F Ratio**	**DFNum**	**DFDen**	**p-Value**
O'Brien[.5]	2,5295	1	23	0,1254
Brown-Forsythe	0,9310	1	23	0,3447
Levene	2,7952	1	23	0,1081
Bartlett	2,0669	1	.	0,1505
F Test 2-sided	2,3991	11	12	0,1481

Welch's Test
Welch Anova testing Means Equal, allowing Std Devs Not Equal

F Ratio	DFNum	DFDen	Prob > F
3,0622	1	18,573	0,0966

t Test
1,7499

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
Ad-hoc	12	182,500	156,000	15,2083	1,485
LGPDCheck	13	142,500	169,000	10,9615	-1,485

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
182,5	1,48501	0,1375

1-way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
2,2909	1	0,1301

Com base nos resultados apresentados acima, é possível afirmar que *Ad-hoc* encontra mais defeitos comuns (DEF) do que *LGPDCheck* com a perspectiva de inspeção voltada para LGPD.

5.4 - Resultados Qualitativos

O questionário de avaliação, disponível no Apêndice H, desempenhou um papel crucial na coleta de percepções acerca da aceitação, utilidade e uso da tecnologia de inspeção *LGPDCheck*. O questionário é composto de 16 perguntas, doze fechadas e quatro abertas. Todas as perguntas do questionário foram desenhadas com 4 pontos na escala *Likert*, sendo a menor avaliação possível “Discordo Totalmente” ou “Muito Baixo”, e avaliação mais alta “Concordo Totalmente” ou “Muito Alto”.

Após a etapa de aplicação da rodada (T2) *LGPDCheck*, os participantes preencheram o formulário de avaliação. Posteriormente, os dados foram transformados da escala *Likert* para valores numéricos, de acordo com os valores correspondentes na

Tabela 27. Os resultados, percepções e devolutivas dos participantes são apresentadas nas seções a seguir.

Tabela 27 - Escala Likert do questionário de avaliação pontos e valores

Pontos da escala	Valor
Discordo totalmente ou Muito Baixo	0
Discordo Parcialmente ou Baixo	1
Concordo Parcialmente ou Alto	2
Concordo Totalmente ou Muito Alto	3

5.4.1 - Avaliação dos Participantes

O questionário de avaliação foi estruturado para coletar questões abertas e fechadas, sua organização pode ser observada a seguir:

- Questões de 1, 2, 3 e 4: Facilidade de uso da *LGPDCheck*;
- Questões 5, 6 e 7: Utilidade da *LGPDCheck*;
- Questões 8 e 9: Intenção de uso e recomendação;
- Questão 10: Impressões gerais sobre a *LGPDCheck* (formato aberto);
- Questão 11: Sugestões de melhorias para a *LGPDCheck* (formato aberto);
- Questão 12: Conhecimento sobre PPD nos contextos de sistemas de software: pergunta 12;
- Questão 13: Conhecimento sobre domínio MGU;
- Questão 14: Conhecimento sobre domínio MSL;
- Questão 15: Percepção geral sobre a participação no estudo (formato aberto);
- Questão 16: Sugestões gerais de melhorias ao estudo (formato aberto).

Uma vez transformados na escala numérica, foi realizada a mediana por cada uma das questões. O questionário é baseado no modelo *Technology Acceptance Model (TAM)* ou Modelo de Aceitação de Tecnologia (DAVIS, BAGOZZI, *et al.*, 1989). Os resultados são organizados em três grandes categorias: Facilidade de Uso, Percepção de Utilidade e Intenção de Uso.

Tabela 28 - Resultados gerais questionário de avaliação

	Facilidade de Uso				Utilidade			Intenção de Uso	
Questão	Técnica	Perguntas	Material de Apoio	Relatório	Técnica	Perguntas	Material de Apoio	Próprio Inspetor	Recomendar
Mediana	**2**	**2**	**3**	**2**	**3**	**3**	**3**	**3**	**3**

5.4.1.1 - Visualização dos resultados por questão

Nesta seção, são apresentados os resultados da etapa de avaliação da técnica de inspeção *LGPDCheck*. Os resultados são apresentados para cada uma das 16 perguntas presentes no formulário de avaliação.

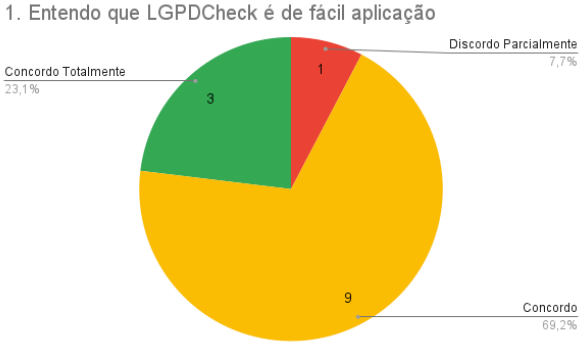

Figura 26 - Percepção dos participantes sobre a facilidade de aplicação da *LGPDCheck*

Quando questionados sobre a facilidade de aplicação da *LGPDCheck*, como pode ser visualizado Figura 26, quatro participantes indicaram "Concordo", três participantes indicaram "Concordo Totalmente" e apenas um participante indicou "Discordo Parcialmente" da afirmação.

Figura 27 - Percepção dos participantes sobre a facilidade de compreender as perguntas do Checklist da *LGPDCheck*

Para a questão dois, sobre o quão fácil é compreender perguntas presentes no checklist de inspeção da *LGPDCheck*, em detalhes na Figura 27, cinco participantes “Concordo Totalmente”, seis participantes sinalizaram “Concordo Parcialmente”, apenas

dois participantes sinalizaram “Discordo Parcialmente” da afirmação. A mediana para as questões um e dois foi 2 pontos, que apesar de alta, é o menor valor presente na avaliação geral da *LGPDCheck* e seus artefatos.

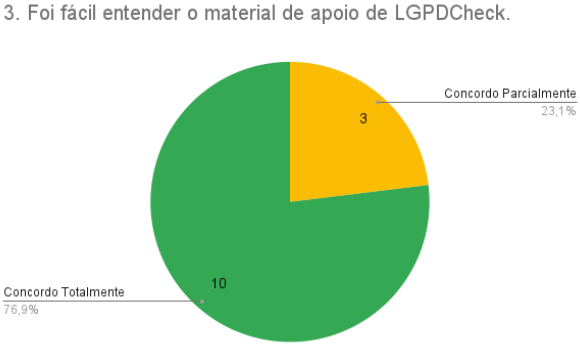

Figura 28 - Percepção dos participantes sobre a facilidade de compreender o material de apoio da *LGPDCheck*

Na questão quatro, em detalhes na Figura 28, abordou o quão fácil foi entender o material de apoio da *LGPDCheck*. Dez participantes sinalizaram “Concordo Totalmente” e três participantes “Concordo Parcialmente”. A mediana para a questão foi máxima, obtendo três pontos. Os resultados obtidos indicam que o material de apoio, composto do compilado dos dez princípios da LGPD, exemplos de violações orientados aos contextos de software foi bem aceito e fácil de ser utilizado pelos participantes.

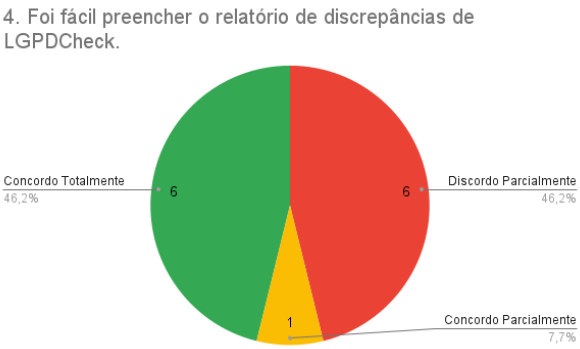

Figura 29 - Percepção dos participantes sobre a facilidade de preencher o formulário de discrepâncias da *LGPDCheck*

Na questão quatro, com mediana de 2 pontos, quando perguntados sobre quatro sobre o quão fácil foi preencher o relatório de discrepâncias da *LGPDCheck* (Apêndice C), seis participantes sinalizaram “Concordo Totalmente”, seis participantes sinalizaram “Discordo Parcialmente” e apenas um participante sinalizou “Concordo” para a afirmação, em detalhes na Figura 29.

O resultado da mediana auxilia na percepção de um aspecto negativo sobre o formulário de discrepâncias. A pontuação mais baixa sugere que o formulário é o

artefato que apresenta o maior nível de dificuldade percebida durante o processo de inspeção utilizando a LGPDCheck. Dificuldade que também foi relatada por outros participantes nas questões dez e onze, em que dois participantes expressam: “S08: Foi cansativo preencher os artefatos (Checklist e formulários) simultaneamente”, reforçados por *“S07: Pensar em maneira de otimizar o número de perguntas ao fim da inspeção, o inspetor pode ser pela fadiga, deixar de passar discrepâncias importantes.”*

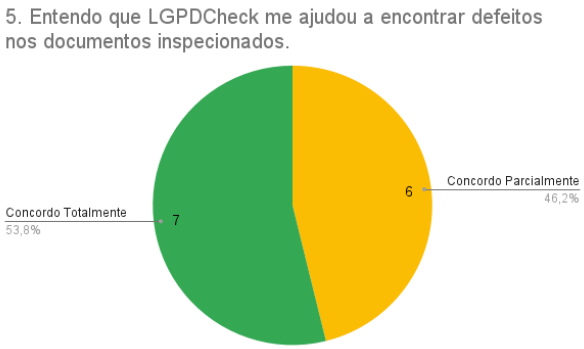

Figura 30 - Percepção dos participantes sobre se a LGPDCheck os auxiliou a encontrar defeitos

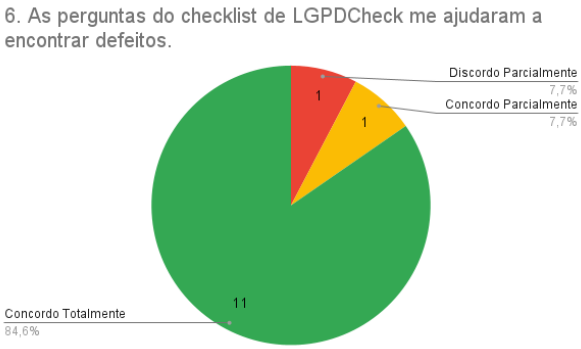

Figura 31 - Percepção dos participantes se o checklist da LGPDCheck os auxiliou a encontrar defeitos

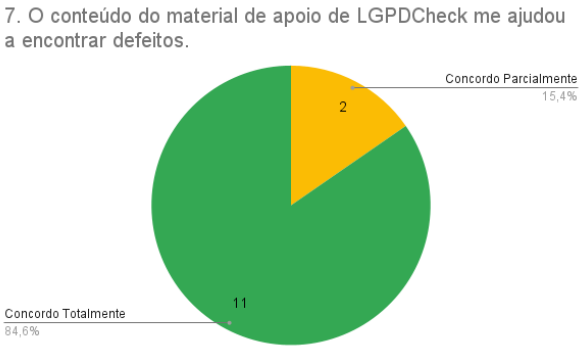

Figura 32 - Percepção dos participantes sobre se o Material de Apoio da *LGPDCheck* os auxiliou a encontrar defeitos

Através das questões cinco, seis e sete, foram capturadas as percepções dos participantes sobre a utilidade da LGPDCheck, do Checklist de verificação e dos Materiais de apoio à inspeção. Com mediana 3, nota máxima para as três questões, os resultados podem ser vistos individualmente nas Figura 30, Figura 31 e Figura 32.

O resultado auxilia a compreender que na experiência dos participantes, em sua grande maioria, compreendem que a *LGPDCheck* e seus materiais os auxiliaram no processo de identificação de defeitos. Os resultados são suportados não apenas pela avaliação dos inspetores no formulário de avaliação, mas também pelos números gerais obtidos com a utilização da *LGPDCheck*, em comparação com *Ad-hoc*, seja na quantidade de discrepâncias identificadas ou na taxa de confirmação de discrepância em defeito.

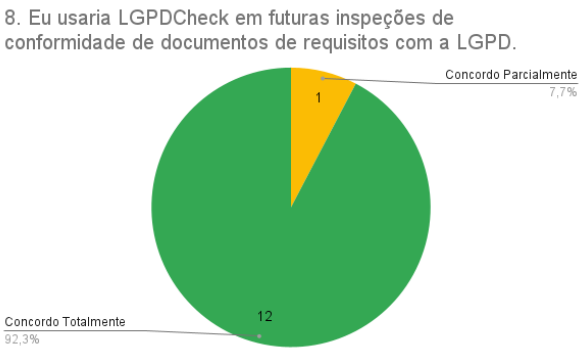

Figura 33 - Percepção dos participantes sobre usos futuros da *LGPDCheck*

Figura 34 - Percepção dos participantes sobre recomendação da *LGPDCheck* para outros profissionais

Sobre a intenção de uso, através da questão oito (ver Figura 33), foram capturadas as intenções dos participantes em usar a *LGPDCheck* em oportunidades futuras. E na questão nove (ver Figura 34), se recomendariam a técnica utilizada para outros profissionais. Com mediana 3, nota máxima para ambas as questões, doze participantes responderam "Concordo Totalmente", um participante respondeu "Concordo Parcialmente".

O resultado nos leva a compreender que, apesar de um estudo controlado e de pequeno escopo e de contexto acadêmico, há uma percepção geral de utilidade da técnica e materiais para além experimentos em que os participantes fizeram parte. Através da análise, é possível interpretar que os participantes compreendem que a *LGPDCheck*, seus recursos e materiais podem ser utilizados por outros profissionais envolvidos na construção de sistemas de software.

Ademais, através das questões dez, onze, quinze e dezesseis, foi possível obter sugestões de possíveis melhorias, devolutivas em geral sobre a *LGPDCheck*, impressões sobre a participação no estudo e, por fim, sugestões de melhorias para o estudo.

Na questão dez, os participantes foram convidados a compartilhar suas principais impressões sobre a experiência de uso da *LGPDCheck*. Ao analisar as devolutivas dos participantes sobre suas experiências no estudo, é possível avaliar que, a grande maioria, relatou ter experiências positivas durante a participação no estudo. Em especial quando comparado com rodada (T1/Ad-Hoc), em que os participantes sentiram falta de instrumentos que dessem apoio ao processo. Enquanto para (T2/*LGPDCheck*), ao analisar as impressões dos participantes, fica evidente que os participantes se perceberam mais bem orientados durante o processo de verificação, dada a disponibilidade de artefatos de apoio. A seguir, são apresentadas as respostas

individuais de cada um dos participantes, todas identificadas por seus códigos internos de identificação no estudo:

- *S01: “Apesar de ter gostado das perguntas e do material de apoio, tive dificuldades em responder algumas das perguntas com as informações do material inspecionado.”*
- *S02: “Sinto que foi uma experiência mais tranquila e guiada reler o documento com perspectivas distintas (em função dos princípios ajudou bastante).”*
- *S03: “O método evidencia as falhas e brechas da legislação a que se refere, mesmo nos casos de aplicação mais simples.”*
- *S04: “Muito bem, indo questão a questão, é possível cobrir todos os aspectos da lei mesmo sem conhecimento profundo dela, e não só criticar os requisitos errados, mas identificar omissões.”*
- *S05: “Um guia para identificar inconsistências em software com relação a LGPD. Apresentou uma sistematização na inspeção em relação à LGPD.”*
- *S06: “O uso do LGPDCheck me ajudou a identificar discrepâncias que antes, de maneira Ad-hoc não consegui identificar, principalmente pelo fato de não ser especialista na LGPD.”*
- *S07: “Achei o método elucidativo de olhar para o artefato em paralelo com a descrição dos fatores a serem levados em consideração.”*
- *S08: ”Uma boa técnica que direcionou a inspeção e foi um bom guia para a leitura dos requisitos, entretanto, foi cansativo preencher os artefatos (Checklist e formulários) simultaneamente.”*
- *S10: “No início, achei um pouco complicado o uso da técnica, no sentido de que seria necessário o conhecimento da totalidade dos requisitos da aplicação para a aplicação de cada pergunta da checklist, mas pareceu mais tranquilo após a leitura do documento de visão e a posterior tentativa de uso.”*
- *S11: “Achei a LGPDCheck de fácil entendimento e bem didático, o mesmo contém os principais pontos de cada princípio da LGPD e seus questionamentos são bem pertinentes do que se deve ter em cada um deles, de um modo geral a experiência em sua utilização foi bem satisfatória.”*

– *S12: “Bom material de estudo (vídeo e texto).”*

– *S13: “É difícil espelhar exemplos da LGPDCheck em todos os requisitos, ainda que seja bom.”*

Na questão onze, os participantes foram convidados a compartilhar sugestões de melhorias a técnica *LGPDCheck*. Os feedbacks recebidos sobre a *LGPDCheck* destacam sugestões significativas para melhorias gerais. Houve a sugestão de adicionar novas opções de resposta ao checklist, por exemplo. A necessidade de um direcionamento mais claro para a utilização do checklist também foi mencionada, assim como a importância de otimizar o número de perguntas para evitar fadiga durante a verificação. Além disso, foram feitas sugestões para unir artefatos para tornar a inspeção menos cansativa foi destacada. A solicitação por mais exemplos foi ressaltada como uma maneira de enriquecer a compreensão da técnica como um todo.

A seguir, são apresentadas as respostas individuais de cada um dos participantes, todas identificadas por seus códigos internos de identificação no estudo:

– *S01: “Talvez fosse positivo adicionar, para além das respostas "Sim", "Não", "Não se aplica", uma opção: "não respondido" / "não informado.”*

– *S04: “Incluiria no questionário um campo de texto livre sobre sugestões de melhorias ao sistema em estudo.”*

– *S05: “Entendo, que deveria ser melhor direcionado que para cada feature usar as perguntas do checklist.”*

– *S06: “Pensar em maneira de otimizar o número de perguntas ao fim da inspeção, o inspetor pode, pela fadiga, deixar de passar discrepâncias importantes.”*

– *S07: “Não possuo prática com documentos de especificação, talvez seja interessante acrescentar uma descrição sobre o nível de detalhes a serem analisados.”*

– *S08: “Algumas perguntas do checklist ficaram confusas. Ex. 26 e 4. - Acredito que se desse para juntar os dois artefatos a inspeção poderia ser menos cansativa.”*

– *S12: “Mais exemplos”.*

Na questão doze, treze e quatorze, os participantes puderam fazer autoavaliação relacionada às suas habilidades com privacidade e proteção de dados em sistemas de

software, além do nível de conhecimento prévio sobre os domínios específicos de cada módulo dos sistemas avaliados durante o experimento.

Para a questão doze, sobre seus conhecimentos sobre privacidade e proteção de dados em sistemas de software, em detalhes na Figura 35, sete participantes se autoavaliaram com um nível “Alto” de conhecimento, cinco participantes sinalizaram Baixo”, apenas um participante sinalizou “Muito Baixo” da afirmação. A mediana para as questões um e dois foi 2 pontos.

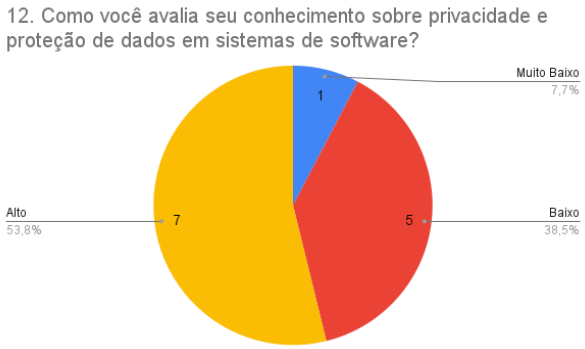

Figura 35 - Autoavaliação dos participantes sobre seus conhecimentos em Privacidade e proteção de dados pessoais em sistemas de software

Para a questão treze, sobre seus conhecimentos prévios relacionados ao domínio do Módulo de Gestão de Usuários (MGU), em detalhes na Figura 36, um participante sete se autoavaliaram com um nível “Muito Alto” de conhecimento, dois participantes se autoavaliaram com um nível “Alto” de conhecimento, cinco participantes sinalizaram “Baixo”, e cinco participantes sinalizaram “Muito Baixo” da afirmação. A mediana para a questão foi de 1 ponto.

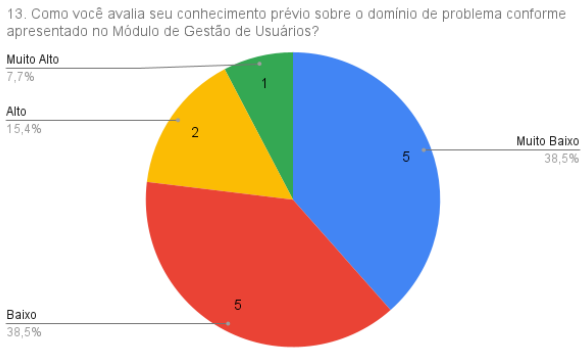

Figura 36 - Autoavaliação dos participantes sobre o domínio do problema no Módulo de Gestão de Usuários (MGU)

Para a questão quatorze, sobre seus conhecimentos prévios relacionados ao domínio do Módulo de Solicitações (MSL), em detalhes na Figura 37, dois participantes

se autoavaliaram com um nível “Alto” de conhecimento, sete se autoavaliaram com um nível “Baixo” de conhecimento, quatro participantes sinalizaram Baixo”. A mediana para a questão foi de 1 ponto.

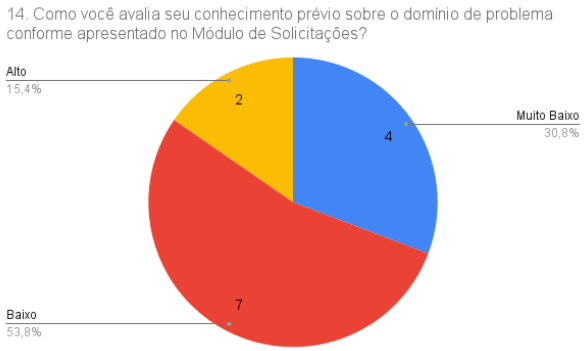

Figura 37 - Autoavaliação dos participantes sobre o domínio do problema no Módulo de Solicitações (MSL)

A questão de autoavaliação doze, que obteve mediana de 2, os participantes indicam que possuem algum grau de conhecimento sobre PPD nos contextos de sistemas de software. Já para as questões treze e quatorze, ambas obtiveram mediana de 1 ponto, demonstrando que os participantes, de modo geral, possuem conhecimentos baixos sobre os sistemas aos quais executaram a verificação.

Enquanto na questão quinze, os participantes puderam oferecer suas principais impressões sobre a experiência de participação nas diferentes etapas e atividades do estudo. Alguns participantes apreciaram o direcionamento proporcionado pela técnica *LGPDCheck* em comparação com abordagens *Ad-hoc*. A experiência foi geralmente considerada satisfatória, proporcionando entendimento prático sobre inspeções em artefatos de software. Quanto às sugestões, foram propostas soluções como: perguntas condicionais, mais contato com a documentação do *LGPDCheck*. Outras observações incluíram a falta de profundidade na definição dos requisitos nos documentos apresentados.

A seguir, são apresentadas as respostas individuais de cada um dos participantes, todas identificadas por seus códigos internos de identificação no estudo:

– *S01: “Por ter avaliado módulos de um grande sistema, fiquei inseguro quanto ao comportamento do módulo junto de outros. Por exemplo, apesar do coordenador poder alterar documentos de uma PF no MSL, a PF (Pessoa Física) pode também alterá-los no MGU?”*

- *S02: “Senti que os documentos apresentados careciam de profundidade na definição dos requisitos.”*
- *S03: “Foi muito mais cansativa que a primeira inspeção solta. Foi difícil concentrar a busca nos princípios da LGPD (Ad-hoc). Nessa (“LGPDCheck”) foi bem mais fácil identificar as imprecisões.”*
- *S04: ”No primeiro estudo (“Ad-hoc”) só consegui identificar ambiguidades e requisitos já presentes no texto. Neste (LGPDCheck) foi possível identificar muito mais defeitos e omissões de forma fácil.”*
- *S05: ”Excelente para entender na prática como é produzido inspeções em artefatos de software”.*
- *S06: “Achei bastante proveitoso para entendimento prático dos temas abordados na aula.”*
- *S07: “Eu tive a impressão de visualizar melhor a prática seguindo a técnica de inspeção (LGPDCheck). A forma Ad-hoc parece abrir mais à subjetividade.”*
- *S08: “Foi interessante participar, especialmente notar as diferenças de uma inspeção Ad-hoc e seguindo uma técnica (LGPDCheck)”.*
- *S10: “Foi interessante participar do estudo, sobretudo a observação do maior direcionamento quando se usa a LGPDCheck, o que não ocorreu no trial Ad-hoc, que me senti um pouco perdido.”*
- *S11: ”Foi uma experiência muito satisfatória, tendo em vista que todas as etapas foram bem explicadas e muito bem elaboradas, o que permitiu com que houvesse pouca/nenhuma dúvida de como prosseguir com as etapas seguintes.”*
- *S13: “Foi difícil extrair defeitos de forma Ad-hoc, porém a experiência foi interessante. Foi interessante entender melhor sobre inspeções. Os vídeos também instruíram bastante.”*

Na questão dezesseis, os participantes puderam expressar suas sugestões para melhoria do estudo em que participaram. Os participantes não apenas devolutivas sobre o estudo, mas também à LGPDCheck. Suas sugestões foram:

- *S02: ” Dar uma tabela com definição dos tipos de erros de inspeção”.*

– *S03: “Acho que a inadequação completa gera muitas respostas "não" e "N/A". Talvez sejam necessárias perguntas condicionais para serem aplicadas quando existe a finalidade.”*

– *S05: ”Na segunda fase usando a LGPD, seria interessante maior contato com a documentação do LGPDCheck.”*

– *S12: “Na primeira atividade, embora a apresentação da LGPD, não ficou claro para mim que era para inspecionar em relação à LGPD.”*

É importante destacar que apesar da sugestão do participante S02, todos os participantes recebem, junto com o formulário de discrepância (ver Apêndice C), que contém toda a taxonomia de defeitos e suas siglas no cabeçalho do documento. A taxonomia de defeitos também esteve presente no treinamento que todos os participantes receberam durante a etapa de treinamento. Diferente do que foi relatado pelo participante S05, durante a rodada (T2), os participantes receberam, além dos vídeos de treinamentos, os seguintes artefatos impressos: (1) APÊNDICE B – MATERIAL DE APOIO; (2) APÊNDICE C – FORMULÁRIO DE DISCREPÂNCIAS ; (3) APÊNDICE E – CHECKLIST DE VERIFICAÇÃO .

5.5 - Considerações Finais

Com base nos resultados quantitativos, foi possível identificar que a *LGPDCheck,* quando comparada a *Ad-hoc,* obteve resultados superiores, tanto na quantidade de discrepâncias identificadas, quanto na quantidade na confirmação destes em defeitos. Em ambas as rodadas foi possível identificar defeitos do tipo LGPD, mas a *LGPDCheck*, por oferecer orientação, artefatos e materiais de suporte orientados à LGPD, foi capaz de identificar uma quantidade superior de defeitos, tanto comuns quanto do tipo LGPD. Ao mesmo tempo em que *LGPDCheck* possui uma eficiência na detecção de defeito por minuto de inspeção superior a *Ad-hoc*.

Embora a *LGPDCheck* tenha demonstrado superioridade quantitativa em quase todos os aspectos analisados na seção anterior, a inspeção do tipo *Ad-hoc* destacou-se por sua capacidade de identificar uma variedade mais ampla de tipos de defeitos, abrangendo categorias como Omissão (O), Fato Incorreto (FI), Inconsistência (IN), Ambiguidade (A) e Informação Estranha (IE) na taxonomia de defeitos, enquanto na *LGPDCheck*, o defeito do tipo Omissão foi predominante. Um outro aspecto importante dos resultados obtidos na rodada *Ad-hoc* é que os inspetores conseguiram identificar defeitos relacionados à LGPD durante a avaliação, mesmo que em uma quantidade inferior.

Em relação aos resultados qualitativos, ao analisar as medianas sob a perspectiva da escala (TAM), as respostas ao formulário de avaliação foram bem positivas e os participantes se sentiram à vontade para expressar críticas sobre a técnica e experimento. De fato, os participantes indicaram suas maiores dificuldades. As medianas menores indicam que o maior desafio para a *LGPDCheck* foi o artefato relatório de discrepâncias. Com base nas devolutivas, é possível que a estrutura ou a formulação do próprio documento possa ser responsável. Vale ressaltar que os participantes receberam diversos artefatos, separados para realizar o processo de verificação com a *LGPDCheck*.

E, em algumas das devolutivas há uma percepção de que o processo de verificação foi cansativo, que pode estar conectado à quantidade de documentos em que o participante teve que lidar durante o processo de verificação. A introdução de processos digitais, apoiados por ferramentas de terceiros ou um sistema próprio de suporte à verificação, poderia potencialmente melhorar o desempenho e a aceitação do estudo e das ferramentas.

6 Conclusão

Este capítulo discute os principais resultados do estudo de viabilidade conduzido para avaliar a proposta da técnica de inspeção LGPDCheck, bem como as considerações finais deste estudo. Também são apresentadas as contribuições e perspectivas futuras.

6.1 - Conclusão

Ao observar desafios relacionados à compreensão e implementação de regulações em sistemas de software, nasce a proposta da *LGPDCheck*: uma tecnologia de inspeção à luz dos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD). Com foco na LGPD, a técnica de inspeção *LGPDCheck* com propósito de reduzir as distâncias entre os profissionais envolvidos na construção de sistemas de software e conceitos de PPD previstos na LGPD. Lacunas encontradas na literatura e reforçada por achados obtidos em forma de relatos durante a o desenvolvimento dessa dissertação. É importante ressaltar que essa dificuldade na interpretação e tangibilidade das leis não é algo exclusivo à LGPD, mas um desafio comum às regulações ao redor do mundo, mas é identificada como um grande desafio aos profissionais que atuam na construção de sistemas de software (GÜRSES, TRONCOSO, DIAZ et al., 2011, 2015).

Assim como sugere Shapiro (2010), por meio de instrumentos e processos bem definidos, a *LGPDCheck* oferece um arcabouço de recursos àqueles que buscam a implementação de instrumentos regulatórios em sistemas de software. A *LGPDCheck* tem ênfase na oferta de recursos auxiliares para dar mais tangibilidade e concretude aos conceitos e definições presentes na LGPD.

Na atual proposta da *LGPDCheck*, o foco está na disponibilização de artefatos e instrumentos. Além disso, apresenta um fluxo de verificação que incorpora os conceitos e definições da LGPD, presentes no primeiro capítulo da lei, mas com linguagem e exemplos adaptados aos contextos de sistemas de software.

Os artefatos que compõem a *LGPDCheck* são tentativas de redução das barreiras e lacunas na compreensão dos conceitos e princípios presentes na lei. A exemplo, o Material de Apoio (Apêndice B), composto do Glossário de termos de Privacidade e Proteção de Dados para Sistemas de Software e Quadros de Princípios. Dois recursos essenciais da *LGPDCheck*, sempre que possível, equiparando conceitos presentes na lei com os conceitos de sistemas de software.

Em uma primeira avaliação, a *LGPDCheck* não apenas obteve um ótimo desempenho em termos de identificação de defeitos, mas também uma ótima aceitação e utilidade percebida por parte dos participantes no estudo. Os elementos mencionados nos levam à conclusão de que a *LGPDCheck* pode ser uma aliada nos desafios diários enfrentados por esses profissionais, ao mesmo tempo que pode contribuir para a redução ou estreitamento das lacunas anteriormente mencionadas.

Almejamos que os materiais, descobertas e artefatos resultantes desta dissertação representem um passo significativo na contribuição para a redução das lacunas identificadas. Esperamos que o conhecimento acumulado, bem como as ferramentas e fluxos desenvolvidos, possam servir como fontes valiosas de orientação sobre como textos jurídicos, leis e regulamentações podem ser adaptados aos contextos de sistemas de software. E que, em futuro próximo, a *LGPDCheck* contribua para cultura de Privacidade e Proteção de Dados Pessoais à medida que profissionais estejam capacitados para compreender e integrar o PPD em seu pensamento, práticas individuais e organizacionais, resultando em sistemas que, por padrão e desde sua concepção, respeitem e garantam aos cidadãos e usuários seus direitos à privacidade e proteção de dados.

6.2 - Contribuições

Com a proposta, descobertas, experimentação e publicação deste trabalho, vislumbramos de forma objetiva as seguintes colaborações:

(1) Mapeamento e exposição das práticas e *modus operandi* de profissionais que aplicam a LGPD em sistemas de software. Destaque para os desafios e práticas das especialistas com formação em Direito e seu envolvimento na construção de software.

(2) Oferta estruturada de uma técnica de inspeção, fluxos, artefatos e recursos para apoiar a identificação de possíveis violações ou inconformidades à LGPD em artefatos de software. Destaque ao Material de Apoio, que caracteriza e diferencia a *LGPDCheck* de outras tecnologias de inspeção disponíveis. O Material Apoio de consiste em um único documento que estrutura os conceitos da LGPD, utilizando uma linguagem mais acessível e perguntas de verificação direcionadas aos contextos de sistemas de software. Esses esforços visam preencher uma lacuna existente na implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) em sistemas de software, proporcionando um guia sobre como as regulamentações podem ser incorporadas de maneira eficiente e eficaz.

(3) Atuação na lacuna da privacidade e proteção de dados desde a concepção, garantindo que a privacidade e proteção de dados sejam consideradas desde a construção dos sistemas.

6.3 - Ameaças à Validade

Validade de construto: destacamos o pequeno número de sujeitos submetidos ao estudo, e o número limitado de domínios inspecionados (um sistema, dois módulos), porém, uma combinação limitada de grupos (dois). No entanto, vale ressaltar que nenhum participante deverá inspecionar o mesmo módulo mais de uma vez. Além disso, não podemos garantir que os módulos sejam comparáveis em número de defeitos e complexidade. Para mitigar essa ameaça, compusemos um subconjunto equilibrado de funcionalidades para inspecionar em cada módulo.

Validade externa: os sujeitos são no mínimo alunos do 3º ano de graduação a alunos de pós-graduação (mestrado e doutorado), com diferentes níveis de experiência em engenharia de software e inspeção.

Validade Interna: dada a novidade e escassez de materiais com foco em PPD para engenharia de software, foram preparados treinamentos para que cada participante adquira conhecimento sobre o assunto.

Conclusão Validade: os resultados iniciais não podem ser generalizados. No entanto, eles contribuirão para a evolução do *LGPDCheck* para posterior avaliação e uso.

6.4 - Limitações da Pesquisa

Embora os participantes tenham demonstrado um nível de conhecimento e prática na construção e desenvolvimento de software em um sistema real, o estudo de viabilidade foi conduzido em um ambiente acadêmico, envolvendo um número limitado de participantes (13). No entanto, a técnica *LGPDCheck*, desenvolvida nesta dissertação, poderia se beneficiar de mais rodadas do estudo de viabilidade, especialmente em projetos de maior escala que envolvam um grande volume de coleta e processamento de dados pessoais de usuários.

Deve-se destacar que não foi possível realizar a validação com especialistas da técnica proposta e seus artefatos, seja em termos de sua utilidade prática ou de sua fidelidade às interpretações dos conteúdos da LGPD nos contextos de sistemas de software. A ausência desse processo de validação impede uma avaliação crítica dos artefatos desenvolvidos e sua adequação às exigências da lei.

Por fim, é preciso destacar que todos os recursos da *LGPDCheck* foram utilizados de forma analógica, sem suporte computacional, e requer uma grande quantidade de esforço para geração dos resultados aqui apresentados. A ausência desse suporte para a automação da técnica *LGPDCheck* evidencia a necessidade de ferramentas mais eficientes, como formulários, planilhas digitais ou sistemas. Essa limitação compromete a escalabilidade da técnica e restringe sua aplicação a contextos fora do ambiente acadêmico.

6.5 - Publicações

O artigo intitulado "*Um checklist para inspeção de privacidade e proteção de dados pessoais em artefatos de software*" foi apresentado e publicado nos Anais do XXVI Congresso Ibero-Americano em Engenharia de Software (CibSE 2023), que teve lugar no Uruguai.

- Cerqueira, D. A., de Mello, R. M., & Travassos, G. H. (2023). Um checklist para inspeção de privacidade e proteção de dados pessoais em artefatos de software. Anais Do XXVI Congresso Ibero-Americano Em Engenharia de Software (CIbSE 2023), 206–213. https://doi.org/10.5753/cibse.2023.24704

O plano do estudo intitulado *"Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law*" foi aceito para apresentação na 17º *ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (ESEM) 2023, em Nova Orleans, Louisiana (EUA). O estudo representa um passo fundamental no processo de avaliação desta dissertação de mestrado, uma vez que busca investigar a eficácia da técnica *LGPDCheck* na busca por conformidade de sistemas de software com à Lei Geral de Proteção de Dados do Brasil (LGPD).

Este estudo foi submetido à trilha de *Registered Reports* (RR)[13] da conferência ESEM 2023, em conjunto com o *Empirical Software Engineering j*ournal (EMSE). A inclusão do estudo na RR da conferência ESEM 2023 confere ao trabalho a oportunidade de ter seu protocolo de pesquisa revisado por pares, aumentando a confiança no rigor científico empregado no trabalho.

O RR foi publicado no ArXiv (arXiv:2308.14874) e apresentado em 26 de outubro de 2023, durante a conferência do ESEM 2023. Até maio de 2024, os resultados obtidos durante a execução do estudo serão submetidos em formato de artigo ao Journal EMSE.

[13] Informações adicionais disponíveis em: </https://conf.researchr.org/details/esem-2023/esem-2023-registered-reports/2/Experimental-Evaluation-of-a-Checklist-Based-Inspection-Technique-to-Verify-the-Compl>

- Cerqueira, D. A., de Mello, R. M., & Travassos, G. H. (2023). Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law. http://arxiv.org/abs/2308.14874

6.6 - Perspectivas Futuras

Pretendemos realizar um segundo estudo aplicando a *LGPDCheck* em um projeto externo. Nesse próximo estudo, avaliaremos o desempenho da técnica e aceitação de profissionais em projetos que estejam fora do escopo acadêmico. Se os resultados forem positivos, promoveremos o *LGPDCheck* como uma técnica recomendada para a proteção da privacidade em artefatos de sistemas de software. Caso contrário, usaremos os resultados para identificar as deficiências da técnica e trabalharemos em sua evolução.

Vislumbramos avaliar a construção de uma infraestrutura de apoio computacional para *LGPDCheck*, com objetivo de melhorar a usabilidade dos materiais e reduzir a quantidade de recursos físicos necessários e trabalho manual durante as etapas de coleta e processamento de dados. Além disso, é relevante considerar a potencial adaptação do trabalho e do arcabouço desenvolvido para outros contextos além do brasileiro, como o da GDPR, a lei europeia sobre Proteção de Dados Pessoais. Isso abre portas para investigações futuras, explorando possíveis ajustes e extensões do estudo, especialmente no âmbito da adaptação para a GDPR, abrindo novas perspectivas de aplicabilidade e relevância internacional.

Por último, reconhecemos a relevância da criação de um oráculo de inspeção *LGPDCheck* para facilitar futuras aplicações e reproduções de estudos de viabilidade. Esse oráculo de inspeção pode incluir informações sobre o processo de moderação, papéis e responsabilidades, assim como detalhar a identificação minuciosa de defeitos, falsos positivos e defeitos LGPD.

Referências

ALSHAMMARI, M., SIMPSON, A. "Towards a principled approach for engineering privacy by design", **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**, v. 10518 LNCS, p. 161–177, 2017. DOI: 10.1007/978-3-319-67280-9_9. Disponível em: http://link.springer.com/10.1007/978-3-319-67280-9_9.

BARCELOS, R. F., TRAVASSOS, G. H. "ArqCheck: Uma abordagem para inspeção de documentos arquiteturais baseada em checklist". 29 maio 2006. **Anais** [...] [S.l.], Sociedade Brasileira de Computação - SBC, 29 maio 2006. p. 174–188. DOI: 10.5753/sbqs.2006.15608. Disponível em: https://sol.sbc.org.br/index.php/sbqs/article/view/15608.

BASILI, V. R., CALDIERA, G., ROMBACH, H. D. "The goal question metric approach", **Encyclopedia of Software Engineering**, v. 2, p. 528–532, 1994. DOI: 10.1.1.104.8626. Disponível em: http://maisqual.squoring.com/wiki/index.php/The Goal Question Metric Approach.

BASILI, V. R., GREEN, S., LAITENBERGER, O., *et al.* "The empirical investigation of Perspective-Based Reading", **Empirical Software Engineering**, v. 1, n. 2, p. 133–164, 1996. DOI: 10.1007/BF00368702. Disponível em: http://link.springer.com/10.1007/BF00368702.

BOEHM, B., BASILI, V. R. "Software Defect Reduction Top 10 List", **Computer**, v. 34, n. 1, p. 135–137, 2001. DOI: 10.1109/2.962984. .

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018:Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 fev. 2022.

CAVOUKIAN, A. "Privacy by Design - The 7 foundational principles", **Information and Privacy Commissioner of Ontario, Canada**, p. 5, 2009. Disponível em: http://jpaulgibson.synology.me/ETHICS4EU-Brick-SmartPills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf.

CAVOUKIAN, A. **Privacy by design [leading edge]**. **IEEE Technology and Society Magazine**. [S.l: s.n.]. Disponível em: http://ieeexplore.ieee.org/document/6387956/. , 2012

DA SILVA, V. M., TRAVASSOS, G. H. "ScenarIoT: Support for Scenario Specification of Internet of Things-based Software Systems". 19 out. 2020. **Anais** [...] [S.l.],

Sociedade Brasileira de Computação - SBC, 19 out. 2020. p. 195–209. DOI: 10.5753/cbsoft_estendido.2020.14628. Disponível em: https://sol.sbc.org.br/index.php/cbsoft_estendido/article/view/14628.

DAVIS, F. D., BAGOZZI, R. P., WARSHAW, P. R. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", **Management Science**, v. 35, n. 8, p. 982–1003, ago. 1989. DOI: 10.1287/mnsc.35.8.982. Disponível em: https://pubsonline.informs.org/doi/10.1287/mnsc.35.8.982.

DE MELLO, Rafael Maiani, MOTTA, R. C., TRAVASSOS, G. H., "A Checklist-Based Inspection Technique for Business Process Models". **Lecture Notes in Business Information Processing**, [S.l: s.n.], 2016. v. 260. p. 108–123. DOI: 10.1007/978-3-319-45468-9_7. Disponível em: http://link.springer.com/10.1007/978-3-319-45468-9_7.

DE MELLO, Rafael Maiani, TEIXEIRA, E. N., SCHOTS, M., *et al.* "Verification of Software Product Line artefacts: A checklist to support feature model inspections", **Journal of Universal Computer Science**, v. 20, n. 5, p. 720–745, 2014. .

DE SOUZA, B. P., MOTTA, R. C., DE O. COSTA, D., *et al.* "An IoT-based Scenario Description Inspection Technique". 28 out. 2019. **Anais** [...] New York, NY, USA, ACM, 28 out. 2019. p. 20–29. DOI: 10.1145/3364641.3364644. Disponível em: https://dl.acm.org/doi/10.1145/3364641.3364644.

DIAS, E., ANGELICA, C., SEIDEL, T., *et al.* "Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation", **Requirements Engineering**, n. 0123456789, 2022. DOI: 10.1007/s00766-022-00391-7. Disponível em: https://doi.org/10.1007/s00766-022-00391-7.

EDUARDO, J., PIMENTEL, D. E. S. "Introdução Ao Direito Digital", **Revista Jurídica ESMP-SP**, p. 16–39, 2018. .

ENGSTRÖM, E., STOREY, M. A., RUNESON, P., *et al.* "How software engineering research aligns with design science: a review", **Empirical Software Engineering**, v. 25, n. 4, p. 2630–2660, 2020. DOI: 10.1007/s10664-020-09818-7. .

FAGAN, M. E. "Advances in software inspections", **IEEE Transactions on Software Engineering**, v. SE-12, n. 7, p. 744–751, jul. 1986. DOI: 10.1109/TSE.1986.6312976. Disponível em: http://ieeexplore.ieee.org/document/6312976/.

FAGAN, M. E. "Design and code inspections to reduce errors in program development", **IBM Systems Journal**, v. 15, n. 3, p. 182–211, 1976. DOI: 10.1147/sj.153.0182. Disponível em: http://ieeexplore.ieee.org/document/5387093/.

GUIMARÃES, M. **LGPD: Tudo sobre a Lei Geral de Proteção de Dados**. 2021. Disponível em: https://direito.idp.edu.br/blog/direito-digital/lgpd-lei-geral-de-protecao-

de-dados/.

GÜRSES, S., TRONCOSO, C., DIAZ, C. "Engineering: Privacy by design", **Computers, Privacy & Data Protection**, v. 317, n. 5842, p. 1178–1179, 2011. .

GÜRSES, S., TRONCOSO, C., DIAZ, C. "Engineering privacy by design reloaded", **Amsterdam Privacy Conference**, n. 610613, p. 1–21, 2015. Disponível em: https://iapp.org/resources/article/engineering-privacy-by-design-reloaded/.

HADAR, I., HASSON, T., AYALON, O., *et al.* "Privacy by designers: software developers' privacy mindset", **Empirical Software Engineering**, v. 23, n. 1, p. 259–289, fev. 2018. DOI: 10.1007/s10664-017-9517-1. Disponível em: http://link.springer.com/10.1007/s10664-017-9517-1.

IEEE. "1028-2008 - IEEE Standard for Software Reviews and Audits", **IEEE Std 1028-2008**, v. 2008, n. August, p. 1–53, 2008. DOI: 10.1109/IEEESTD.2008.4601584. Disponível em: https://ieeexplore.ieee.org/document/4601584.

KALINOWSKI, M., SPÍNOLA, R. O., TRAVASSOS, G. H. "Infra-estrutura Computacional para Apoio ao Processo de Inspeção de Software". 31 maio 2004. **Anais** [...] [S.l.], Sociedade Brasileira de Computação - SBC, 31 maio 2004. p. 117–131. DOI: 10.5753/sbqs.2004.16188. Disponível em: https://sol.sbc.org.br/index.php/sbqs/article/view/16188.

KALINOWSKI, M., TRAVASSOS, G. H. "A computational framework for supporting software inspections". 2004. **Anais** [...] Linz, Austria, IEEE, 2004. p. 46–55. DOI: 10.1109/ASE.2004.1342723. Disponível em: http://ieeexplore.ieee.org/document/1342723/.

LAITENBERGER, O., DEBAUD, J.-M. "An encompassing life cycle centric survey of software inspection", **Journal of Systems and Software**, v. 50, n. 1, p. 5–31, jan. 2000. DOI: 10.1016/S0164-1212(99)00073-4. Disponível em: https://linkinghub.elsevier.com/retrieve/pii/S0164121299000734.

LAITENBERGER, O., EMAM, K. El, HARBICH, T. G. "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. DOI: 10.1109/32.922713. .

LEMOS, R., DOUDEK, D., LANGENEGGER, N., *et al.* **GDPR: a nova legislação de proteção de dados pessoais da Europa**. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018. Acesso em: 9 set. 2022.

MAFRA, S. N., TRAVASSOS, G. H. "Leitura Baseada em Perspectiva: A Visão do Projetista Orientada a Objetos". 29 maio 2006. **Anais** [...] [S.l.], Sociedade Brasileira

de Computação - SBC, 29 maio 2006. p. 144–158. DOI: 10.5753/sbqs.2006.15606. Disponível em: https://sol.sbc.org.br/index.php/sbqs/article/view/15606.

MARCH, S. T., SMITH, G. F. "Design and natural science research on information technology", **Decision Support Systems**, v. 15, n. 4, p. 251–266, dez. 1995. DOI: 10.1016/0167-9236(94)00041-2. Disponível em: https://linkinghub.elsevier.com/retrieve/pii/0167923694000412.

MARTINS, A. D. F., BARROS, P. V. da S., MONTEIRO, J. M., *et al.* "LGPD: A Formal Concept Analysis and its Evaluation". 28 set. 2020. **Anais** [...] [S.l.], Sociedade Brasileira de Computação - SBC, 28 set. 2020. p. 259–264. DOI: https://doi.org/10.5753/sbbd.2020.13651. Disponível em: https://sol.sbc.org.br/index.php/sbbd/article/view/13651.

MELLO, Rafael M. de, MASSOLLAR, J. L., TRAVASSOS, G. H. "Técnica de Inspeção Baseada em Checklist para Identificação de Defeitos em Diagramas de Atividades". 6 jun. 2011. **Anais** [...] [S.l.], Sociedade Brasileira de Computação - SBC, 6 jun. 2011. p. 119–133. DOI: 10.5753/sbqs.2011.15391. Disponível em: https://sol.sbc.org.br/index.php/sbqs/article/view/15391.

MELLO, Rafael Maiani de. **TÉCNICA PARA INSPEÇÃO DE DIAGRAMAS DE ATIVIDADES**. 2011. 181 f. Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, 2011. Disponível em: https://www.cos.ufrj.br/uploadfile/1300459712.pdf.

MELLO, Rafael Maiani de, PEREIRA, W. M., TRAVASSOS, G. H. "Activity Diagram Inspection on Requirements Specification". set. 2010. **Anais** [...] [S.l.], IEEE, set. 2010. p. 168–177. DOI: 10.1109/SBES.2010.29. Disponível em: http://ieeexplore.ieee.org/document/5629595/.

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". 27 set. 2021. **Anais** [...] New York, NY, USA, ACM, 27 set. 2021. p. 263–268. DOI: 10.1145/3474624.3477069. Disponível em: https://dl.acm.org/doi/10.1145/3474624.3477069.

MORALES-TRUJILLO, M. E., MATLA-CRUZ, E. O., GARCÍA-MIRELES, G. A., *et al.* "A systematic mapping study of Privacy by Design", **Avances en Ingenieria de Software a Nivel Iberoamericano, CIbSE 2018**, v. 22, n. 1, p. 107–120, 2018. .

ONU. "Declaração Universal dos Direitos Humanos", p. 7, 1948. Disponível em: https://brasil.un.org/pt-br/download/50044/91601.

OTTO, P. N., ANTON, A. I. "Addressing Legal Requirements in Requirements Engineering". out. 2007. **Anais** [...] [S.l.], IEEE, out. 2007. p. 5–14. DOI: 10.1109/RE.2007.65. Disponível em: http://ieeexplore.ieee.org/document/4384161/.

PARLAMENTO EUROPEU E DO CONSELHO. "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho". , 2016, p. 1–119.

PEIXOTO, M., FERREIRA, D., CAVALCANTI, M., *et al.* "The perspective of Brazilian software developers on data privacy", **Journal of Systems and Software**, v. 195, p. 111523, jan. 2022. DOI: 10.1016/j.jss.2022.111523. Disponível em: https://doi.org/10.1016/j.jss.2022.111523.

PEREIRA, I., MENDES, J., VIANA, D., *et al.* "Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal", n. 13, p. 28–31, 2022. DOI: 10.5753/cbsoft_estendido.2022.226679. .

PORTER, A. A., VOTTA, L. G. "An experiment to assess different defect detection methods for software requirements inspections". 1994. **Anais** [...] [S.l.], IEEE Comput. Soc. Press, 1994. p. 103–112. DOI: 10.1109/ICSE.1994.296770. Disponível em: http://ieeexplore.ieee.org/document/296770/.

PORTER, A. A., VOTTA, L. G., BASILI, V. R. "Comparing detection methods for software requirements inspections: a replicated experiment", **IEEE Transactions on Software Engineering**, v. 21, n. 6, p. 563–575, jun. 1995. DOI: 10.1109/32.391380. Disponível em: http://ieeexplore.ieee.org/document/391380/.

SAUER, C., JEFFERY, D. R., LAND, L., *et al.* "The effectiveness of software development technical reviews: a behaviorally motivated program of research", **IEEE Transactions on Software Engineering**, v. 26, n. 1, p. 1–14, 2000. DOI: 10.1109/32.825763. Disponível em: http://ieeexplore.ieee.org/document/825763/.

SERASA EXPERIAN. **Pesquisa LGPD (Lei Geral de Proteção de Dados Pessoais): Como as empresas se preparam para atender à nova regulamentação**. . [S.l: s.n.], 2020. Disponível em: https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf.

SHAPIRO, S. S. "Privacy by design: Moving from Art to Practice", **Communications of the ACM**, v. 53, n. 6, p. 27–29, jun. 2010. DOI: 10.1145/1743546.1743559. Disponível em: https://dl.acm.org/doi/10.1145/1743546.1743559.

SHULL, F. J. **Developing Techniques for Using Software Documents: A Series of Empirical Studies**. 1998. University of Maryland, 1998.

SHULL, F, TRAVASSOS, G. H., CARVER, J., *et al.* "Evolving a Set of Techniques for OO Inspections", p. 1–36, 1999. .

SHULL, Forrest, RUS, I., BASILI, V. "How perspective-based reading can improve requirements inspections", **Computer**, v. 33, n. 7, p. 73–79, jul. 2000. DOI: 10.1109/2.869376. Disponível em: https://ieeexplore.ieee.org/document/869376/.

THELIN, T., RUNESON, P., WOHLIN, C., *et al.* "How much information is needed for usage-based reading? A series of experiments". 2002. **Anais** [...] [S.l.], IEEE Comput. Soc, 2002. p. 127–138. DOI: 10.1109/ISESE.2002.1166932. Disponível em: http://ieeexplore.ieee.org/document/1166932/.

TRAVASSOS, G., SHULL, F., FREDERICKS, M., *et al.* "Detecting defects in object-oriented designs", **ACM SIGPLAN Notices**, v. 34, n. 10, p. 47–56, out. 1999. DOI: 10.1145/320385.320389. Disponível em: https://dl.acm.org/doi/10.1145/320385.320389.

UN. **The right to privacy in the digital age : resolution / adopted by the Human Rights Council on 23 March 2017**. . Geneva, [s.n.], 2017. Disponível em: https://digitallibrary.un.org/record/1307661/files/A_HRC_RES_34_7-EN.pdf?ln=en.

UN. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. . Geneva, [s.n.], 2022. Disponível em: https://digitallibrary.un.org/record/3985679?ln=en.

APÊNDICE A – COLETA DE INFORMAÇÕES COM ESPECIALISTAS AS ESPECIALISTAS

Eixo 1: Histórico com a LGPD:

- Solicitar ao especialista que conte sobre a sua experiência e relação com a LGPD;

Eixo 2: LGPD no desenvolvimento de Software

- Como você aplica a LGPD no seu contexto? Pode contar como é o processo?
- Do ponto de vista do ciclo de desenvolvimento, como isso chega até você?

Perguntas de sequência e continuidade

- É o mesmo processo para produtos existentes ("no mercado") e produtos novos (em desenvolvimento)?
- É correto pensar, aos olhos da LGPD que:
    a. para produtos existentes existe um processo de Adequação e
    b. para novos produtos e para funcionalidades existe um processo de conformidade?
- A LGPD se aplica para todos os casos? Todos os sistemas/produtos?
- Como garantir que o produto está em conformidade e/ou adequado à lei?
- Quais as ações para lidar com o problema de não-conformidade uma vez identificado?

APÊNDICE B – MATERIAL DE APOIO

(1) Glossário de termos de Privacidade e Proteção de Dados para Sistemas de Software

- **Usuário**: o termo usuário será utilizado como sinônimo para o papel do Titular de Dados nos contextos de sistemas de software. Um usuário é uma Pessoa Física (PF), responsável, em grande maioria, por realizar interações com o sistema de software.
- **Sistema:** será utilizado como sinônimo para exemplificar situações em que o usuário realiza interações, sejam passivas ou ativas, com sistemas de software.
- **Organização**: será utilizado como sinônimo para "Agentes de Tratamento" ao descrever o papel de detentora e/ou mantenedora do sistema de software, em desenvolvimento ou em distribuição, com o qual o usuário realiza suas interações.
- **Dados Pessoais:** são informações, características, ou até mesmo metadados, que possibilitam que um usuário possa ser identificado ou identificável dentro e fora do contexto de sistemas de software. Entretanto, dentro do contexto de sistemas de software, os dados pessoais representam o ativo manipulado, armazenado ou acessado de um usuário pelo sistema de software.
- **Tratamento de dados pessoais:** o termo tratamento de dados será utilizado como sinônimo para o termo operações de tratamento no contexto de sistemas de software. Um tratamento de dados é qualquer verbo com noção de ação, realizada ou planejada sob os dados pessoais do usuário. Desta forma, um tratamento de dados é qualquer atividade sistêmica realizada com os dados pessoais do usuário. Um CRUD, acrônimo em sistemas de software para operações de *Criar, Ler, Atualizar e Apagar (Create*, *Read*, *Update*, *Delete)*, é um exemplo de tratamento de dados.
- **Anonimização** (ou anonimização de dados): técnica desenvolvida e utilizada por organizações para tornar um dado pessoal (ou um conjunto de dados pessoais) em não pessoal, removendo as características do dado pessoal que permitem a identificação do usuário. Seu objetivo é preservar, proteger e oferecer maior segurança ao usuário proprietário dos dados. A anonimização deve ser executada sempre que for necessário remover características de identificação de um conjunto de dados pessoais. Exemplos de técnicas de

anonimização são: 1) remoção de sobrenomes; 2) Agregação de dados pessoais; ou qualquer técnica que impossibilite que o usuário seja identificado ou identificável, e os dados pessoais possam ser publicados sem danos ou prejuízos ao usuário.

(2) Quadros dos princípios da LGPD para Sistemas de Software

I - FINALIDADE
1. Definição da lei
Realização do tratamento dos dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
2. Interpretação do princípio para sistemas de software
Deve existir uma **finalidade** explícita para a **execução de uma funcionalidade com um dado pessoal no sistema**. Muitas vezes são necessários não apenas um dado pessoal para cumprimento de uma finalidade**,** mas sim um conjunto de dados pessoais, como um e-mail, nome, CPF e outros. Uma **finalidade** no contexto de sistemas de software representa uma justificativa legítima e específica por parte da organização para realizar operações e manipular os dados pessoais de seus usuários, necessários para cumprir com objetivo de fornecer um **serviço** ou nova **funcionalidade**. Esta **funcionalidade** ou **serviço** deve estar atrelada a uma **justificativa** para a realização do tratamento de dados pessoais do usuário. No contexto de sistemas de software, ainda pode ser necessária a utilização de recursos, sejam interfaces gráficas, mensagens ou alertas que auxiliem o usuário na compreensão das razões organizacionais para o tratamento de dados pessoais. As finalidades informadas ao usuário devem, na medida do possível, ser as mesmas durante todo o ciclo de vida do sistema de software. Em caso de existir a necessidade de desenvolver ou implementar novas funcionalidades (mais tratamentos de dados pessoais), diferente do informado inicialmente, o usuário deverá ser notificado da alteração da finalidade de coleta e tratamento dos dados pessoais. Nesses casos é **necessário** informar e **repactuar** com o usuário sobre os tratamentos a serem realizados pela organização/sistema em seus dados pessoais.
3. Ação esperada
A organização deve ser capaz de informar a(s) finalidade(s) do(s) tratamento(s) de dados pessoais. A finalidade não deve ser ampla, genérica ou ambígua. A finalidade deve ser compatível com a informação fornecida ao usuário. Se não há finalidade explícita e justificada para o tratamento dos dados pessoais de um usuário, não há adequação à lei.
4. Exemplos de violação ao princípio em sistemas de software
Ao usar os dados pessoais de CPF e identificação do usuário para o tratamento de dados pessoais relacionado à emissão de uma cobrança (boleto) via sistema, sua finalidade é a emissão de cobrança. Deste modo, o conjunto de dados pessoais de identificação deve ser utilizado apenas para este fim.

O princípio é violado quando o dado pessoal é utilizado para outra finalidade, como a aprovação de crédito com um banco parceiro, sem autorização do usuário.		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação defeito**
(1) Existe alguma razão explícita e não genérica que justifique cada tratamento de dados pessoais?	Não	Omissão
(2) As finalidades dos tratamentos de dados pessoais são informadas ao usuário?	Não	Omissão
(3) A descrição da(s) finalidade(s) permite o claro entendimento do tratamento de dados pessoais realizada pelo sistema/organização?	Não	Ambiguidade
(4) A finalidade do tratamento de dados pessoais foi modificada e informada ao usuário?	Não	Inconsistência

II - ADEQUAÇÃO
1. Definição da lei
Compatibilidade do tratamento de dados pessoais com as finalidades informadas ao usuário, de acordo com o contexto e a finalidade do tratamento.
2. Interpretação do princípio para sistemas de software
O sistema de software e suas funcionalidades devem, além de ter uma finalidade explícita, possuir tratamentos de dados pessoais **compatíveis** com a finalidade informada ao usuário. É preciso cumprir o princípio da finalidade, realizando **apenas** o que foi informado ao usuário dentro do contexto de atuação da organização. Em um sistema de software espera-se que o dado pessoal coletado para uma finalidade seja apenas utilizado para esta finalidade.
3. Ação esperada
As operações de tratamento de dados pessoais realizadas pela organização devem ser compatíveis com as informadas ao usuário. Qualquer modificação ou adição de novas finalidades para os tratamentos de dados pessoais deve ser comunicada ao usuário para garantir a conformidade com o princípio.
4. Exemplos de violação ao princípio em sistemas de software
Considere o uso do CPF e outros dados pessoais de identificação associados à finalidade de emissão de faturas ou cobranças em um sistema de software. O princípio é violado quando no sistema de software há tratamentos de dados pessoais diferentes ou adicionais aos informados ao usuário para um determinado dado pessoal ou conjunto de dados pessoais. Por exemplo, coletar e armazenar o CPF e outros dados de identificação para verificar ou calcular o *score* de crédito do usuário. Espera-se que o dado pessoal seja utilizado **única e exclusivamente** para finalidade inicialmente informada ao usuário. Sua utilização para qualquer outra finalidade configura uma inadequação às finalidades iniciais e viola o princípio da adequação.

5. Perguntas de inspeção ao Especialista/Inspetor	(5.A) Resposta esperada (Sim/Não)	(5.B) Classificação defeito
(5) A organização está realizando operações de **tratamento de dados pessoais compatíveis com as finalidades** informadas ao usuário?	Não	Fato Incorreto
(6) O dado pessoal é tratado em diferentes partes do sistema de software ou organização? Se sim, sua **finalidade continua** consistente com a informada ao usuário?	Não	Inconsistência

III – NECESSIDADE		
1. Definição da lei		
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;		
2. Interpretação do princípio para sistemas de software		
Um sistema de software deve coletar apenas os dados pessoais necessários e específicos para alcançar as finalidades funcionais do sistema. Deve existir proporcionalidade entre o objetivo da funcionalidade projetada e os dados pessoais coletados para alcançar tal objetivo. Ao projetar as funcionalidades, organizações devem focar em ter sob seu domínio **apenas** o conjunto de dados pessoais considerado essencial para alcançar o objetivo da funcionalidade esperada.		
3. Ação esperada		
A coleta de dados pessoais organização deve levar em consideração a proporcionalidade e a necessidade da coleta dos dados para a finalidade do tratamento de dados pessoais visando reduzir a quantidade de dados pessoais coletados, evitando assim ocorrer uma coleta abusiva e desnecessária dos dados pessoais.		
4. Exemplos de violação ao princípio		
Algumas regras de negócio de um sistema de software financeiro dependem da avaliação de crédito do usuário. Para que seja realizada uma consulta em um sistema externo de avaliação de crédito é necessário utilizar um conjunto de dados pessoais de identificação, como CPF, endereço e dados de renda. O princípio é violado quando há uma coletada baseada na máxima de “coletar o máximo que posso, apenas porque posso”, ao coletar e armazenar dados sem nenhuma utilidade, ou seja, necessário para o cumprimento da funcionalidade desenhada. Por exemplo, para realizar uma avaliação de crédito (finalidade), não é correto e necessário a coleta de dados pessoais relacionados à orientação sexual ou gênero que, além de dados sensíveis, são desnecessários ou desproporcionais à finalidade(s) do tratamento.		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação defeito**
(7) A coleta de dados pessoais é consistente, coerente e adequada para cumprir com um serviço ou funcionalidade (finalidade) desejada no sistema de software?	Não	Inconsistência

(8) É possível reduzir ou excluir algum dos dados pessoais coletados sem prejuízo a execução da funcionalidade?	Não	Informação Estranha
(9) Existem processos para avaliar a proporcionalidade na coleta dos dados pessoais?	Não	Omissão

IV - LIVRE ACESSO		
1. Definição da lei		
Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.		
2. Interpretação do princípio para sistemas de software		
Um sistema de software necessita oferecer mecanismos ou funcionalidades para que os usuários possam obter informações sobre quais e como seus dados pessoais estão sendo tratados pela organização. O sistema de software deve oferecer ao usuário recursos para que ele possa conhecer informações relacionadas aos tratamentos realizados sobre seus dados. O acesso livre às informações sobre os dados pessoais não necessariamente precisa ser sistêmico, ele pode ser feito através de canais alternativos, incluindo meios não digitais ou até mesmo intermediado por humanos e não apenas outros sistemas de software.		
3. Ação esperada		
Deve ser oferecido acesso às informações sobre os tratamentos de dados pessoais ao usuário, assim como a duração do tratamento para a finalidade informada.		
4. Exemplos de violação ao princípio		
Durante a realização de um processo seletivo, a coleta de dados pessoais **possui um período determinado**, que varia entre a abertura da vaga (publicação/publicização da oportunidade), até sua finalização (contratação). Ao finalizar o processo seletivo é esperado que exista a finalização dos tratamentos de dados coletados para fins do processo seletivo. O princípio é violado quando a organização não é capaz de oferecer informações sobre os tratamentos dos dados pessoais realizados e sua duração. Ou mesmo em situações em que a organização é **incapaz** de garantir que o usuário tenha acesso às informações sobre como e quais dos seus dados pessoais estão sendo tratados. Ao tratar dados pessoais de endereço como o CEP, se o dado estiver desatualizado, coletado ou inferido de uma outra base, ou até mesmo através de uma coleta consentida, pode fazer com que o usuário tenha um serviço negado, oferecendo prejuízos ao titular.		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação do defeito**
(10) São oferecidos mecanismos para que o usuário possa acessar informações sobre como é realizado o tratamento de seus dados pessoais?	Não	Omissão
(11) São oferecidos mecanismos para que o usuário possa acessar informações sobre a	Não	Omissão

duração do tratamento de seus dados pessoais?		

V - QUALIDADE DE DADOS		
1. Definição da lei		
Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;		
2. Interpretação do princípio para sistemas de software		
Um sistema de software **necessita oferecer mecanismos ou funcionalidades** para que os usuários possam obter informações sobre a corretude dos tratamentos de seus dados pessoais. A organização deve disponibilizar funcionalidades para que o usuário possa, quando necessário, modificar ou atualizar seus dados pessoais para garantir a correção funcional, assegurando que os dados pessoais estejam corretos e atualizados.		
3. Ação esperada		
A organização deve garantir a qualidade dos dados pessoais durante a realização dos tratamentos de dados pessoais do usuário.		
4. Exemplos de violação ao princípio em sistemas de software		
Ao realizar uma operação de avaliação ou consulta de perfil de crédito é importante garantir que os dados pessoais do usuário estejam atualizados. Caso contrário, a avaliação pode ser baseada em dados pessoais desatualizados, o que pode resultar em decisões equivocadas. O princípio é violado **quando não há possibilidade de o** usuário consultar, e quando necessário, corrigir seus dados pessoais para fim do cumprimento da funcionalidade de uma avaliação do crédito que leve em consideração sua vida financeira atual. A ocorrência de erros na consulta de bases de dados ou durante o processo de transformação de dados pessoais durante sua coleta, a falta de validação em um campo ou mudança de tipo de dados, permitem a coleta e armazenamento de dados imprecisos.		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta (Sim/Não)**	**(5.B) Classificação defeito**
(12) É possível garantir que os dados pessoais já coletados e tratados estão atualizados?	Não	Omissão
(13) Existem mecanismos que permitam ao usuário verificar se seus dados pessoais estão atualizados e corretos?	Não	Omissão
(14) Existem mecanismos que permitam ao usuário atualizar ou solicitar a atualização/correção de seus dados pessoais?	Não	Omissão
(15) Existem mecanismos que permitam ao usuário informar sobre inconsistência em seus dados pessoais?	Não	Omissão

VI - TRANSPARÊNCIA		
1. Definição da lei		
Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;		
2. Interpretação do princípio para sistemas de software		
Um sistema de software **necessita oferecer mecanismos ou funcionalidades** para que os usuários possam obter informações sobre **quem são os responsáveis,** e quais tratamentos de seus dados pessoais são realizados. A organização deve disponibilizar informações sobre os tratamentos de dados pessoais e seus respectivos responsáveis em uma linguagem simples e sem jargões, facilitando, na medida do possível, a compreensão por um usuário leigo do conteúdo disponibilizado.		
3. Ação esperada		
A organização deve oferecer mecanismos para que o usuário possa acessar com simplicidade informações sobre como e quais tratamentos são realizados sobre seus dados pessoais, assim como as organizações têm acesso e realizam estes tratamentos.		
4. Exemplos de violação ao princípio para sistemas de software		
Ao realizar tratamentos de dados pessoais relacionados à concessão de crédito, o sistema de software precisará, em casos em que esse serviço não seja interno, compartilhar dados pessoais e informações com sistemas externos para que a organização informe ao seu usuário o crédito solicitado. Exemplos de tratamentos de dados são: (I) **Solicitação de Empréstimo:** onde é avaliada a liberação ou não de um empréstimo junto a uma instituição financeira; (II) **Solicitação de aumento de limite de cartão de crédito:** onde é avaliado se o limite de crédito do usuário será aumentado ou não; O princípio é violado quando a organização falha em oferecer informações ao usuário sobre quais tratamentos de dados pessoais e quem os realiza, mediante pedido ou solicitação do usuário. É essencial que o usuário, na medida do possível, possa estar ciente do que ocorre com seus dados pessoais. A disponibilização de *logs ou* fórmulas matemáticas, a depender do tipo de usuário do sistema, pode ainda configurar uma violação, uma vez que o recurso é atípico para uma grande parcela de usuários, devido às informações especializadas e escritas em linguagem técnica.		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação defeito**
(16) Existem mecanismos que informam ao usuário quem possui acesso aos seus dados pessoais?	Não	Omissão
(17) O mecanismo de transparência disponibilizado possui linguagem adequada ao tipo de usuário?	Não	Ambiguidade
(18) Através do mecanismo de transparência o usuário pode verificar quem são os responsáveis pelos tratamentos de dados pessoais realizados?	Não	Omissão

(19) O mecanismo existente oferece acesso às decisões e critérios utilizados para chegar ao resultado do tratamento de dados pessoais?	Não	Omissão

VII - SEGURANÇA
1. Definição da lei
Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
2. Interpretação do princípio para sistemas de software
Um sistema de software deve manifestar este princípio por meio da implementação de práticas técnicas ou administrativas para proteger os dados pessoais em tratamento. Estas medidas podem ser políticas de acesso baseadas em permissões ou níveis, medidas de segurança da informação ao nível de infraestrutura e governança institucional, ou uso de técnicas de criptografia na transmissão e armazenamento de dados pessoais.
3. Ação esperada
A organização deve implementar medidas técnicas e administrativas para manter a segurança dos dados pessoais do usuário.
4. Exemplos de violação ao princípio em sistemas de software
Em sistemas de software o princípio de segurança é violado quando: **(1) Controle de acesso:** não há uma política de acesso aos dados armazenados. A violação acontece ao armazenar os dados em um banco de dados, físico ou digital, em que os dados pessoais armazenados são compartilhados entre diversos setores de uma organização sem que exista qualquer tipo de controle de acesso ou mesmo acessos parciais, permitindo que um funcionário possa acessar dados pessoais tratados, porém desnecessários para sua atuação ou rotina de trabalho. A não utilização de medidas de controle de acesso cria uma lacuna para que os dados pessoais dos usuários possam ser expostos ou explorados fora do contexto (finalidades) para qual os dados pessoais foram coletados. **(2) Criptografia: a** falta do uso de técnicas de criptografia durante o tratamento de dados pessoais é uma clara violação ao princípio de segurança, uma vez que a informação coletada da relação usuário e sistema pode ser interceptada por terceiros. **(3) Criptografia no armazenamento:** a falta da utilização de criptografia para armazenamento de dados, mesmo os não considerados pessoais, podem trazer riscos aos usuários em casos de vazamento ou acessos indevidos aos dados. O armazenamento de dados em formato simples e descriptografados aumenta o risco de danos ao usuário em casos de acesso indevido ou vazamento de dados. **(4) API sem autenticação e/ou permissivas**: é comum aos sistemas de software possuir APIs (*Aplication Programming Interfaces*) para troca de dados entre sistemas ou para utilização e consumo por desenvolvedores. Podem existir casos em que não proteger APIs com autenticação pode configurar acessos excessivos ou abusivos aos dados pessoais **do usuário.**

5. Perguntas de inspeção ao Especialista/Inspetor	(5.A) Resposta esperada (Sim/Não)	(5.B) Classificação do defeito
(20) Existem medidas administrativas implementadas para proteger os dados pessoais de acessos não autorizados?	Não	Omissão
(21) Existem medidas técnicas implementadas para proteger os dados pessoais de acessos não autorizados?	Não	Omissão
(22) A organização possui alguma medida para reduzir os danos decorrentes do acesso indevido aos dados pessoais?	Não	Omissão

VIII – PREVENÇÃO
1. Definição da lei
Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
2. Interpretação do princípio para sistemas de software
O princípio da prevenção está relacionado às práticas de prevenção a eventuais danos que possam ocorrer por conta do tratamento dos dados pessoais do usuário. Em um sistema de software o princípio está relacionado às medidas de prevenção adotadas pela organização, que podem se manifestar em forma de funcionalidades sistêmicas disponibilizadas ao usuário ou medidas e/ou práticas organizacionais da detentora do sistema para prevenir ou combater possíveis danos ao usuário durante o tratamento de seus dados pessoais.
3. Exemplos de violação ao princípio em sistemas de software
Em sistemas de software o princípio de segurança é violado quando: (1) **Danos ao usuário por falta de segurança:** o sistema é projetado para coletar e armazenar dados de geolocalização, parte de um mecanismo interno de antifraude. Quando o usuário realiza uma transação no sistema, sua localização é coletada, processada e armazenada. Seu armazenamento é justificado para fins de conferência e auditoria. Os dados de histórico permanecem armazenados junto aos registros de tentativas e compras do usuário. O sistema sofreu um ataque, seu banco de dados foi exposto por uma falha de segurança. Os dados de compra e localização dos usuários foram divulgados. O princípio é violado quando não há implementação de medidas de prevenção como criptografia ou anonimização para prevenir danos maiores ao usuário. (2) **Transformação de dados pessoais:** após coletados, dados são utilizados em cálculos em diversas partes do sistema. O princípio é violado quando não há medidas para validação ou transformação dos dados, transformando o dado em um valor diferente do informado pelo usuário. O usuário pode sofrer danos por conta da má transformação ou coleta do dado informado. (3) **Divulgação de dados anonimizados**: dados anonimizados não são considerados dados pessoais. É comum, por parte de instituições, a publicação de informações com fins legítimos de transparência, até mesmo com interesse em promover melhorias em condições trabalhistas ou do próprio ambiente de trabalho. Nesses casos é recomendada a utilização de técnicas de anonimização (não confundir com criptografia).

O princípio é violado quando, em uma empresa de pequeno porte, o sistema realiza um processo de anonimização sobre dados de funcionários para fins de melhoria de saúde no ambiente de trabalho. Na lista divulgada foram removidos os campos idade, nome e departamento, porém mantidos dados de comorbidade e faixa etária. A lista é processada pelo sistema e enviada de forma automática para o fornecedor de saúde laboral e internamente para alguns funcionários. O princípio é violado quando, apesar da lista estar tecnicamente anonimizada, o processo de anonimização é ineficaz. No contexto em que a empresa possui poucos funcionários, ao combinar o dado da comorbidade com a faixa etária é muito provável ser possível identificar o funcionário.

5. Ação esperada

A organização deve implementar medidas de prevenção aos possíveis danos relacionados ao tratamento dos dados pessoais.

Devem ser criadas políticas institucionais, padrões e processos para prevenção de danos que possam vir a ser causados. Não apenas medidas aplicadas após a ocorrência de danos, mas também para a prevenção de danos aos usuários. É necessário também uma posição proativa na realização de mapeamento de possíveis danos relacionados aos tratamentos de dados realizados, como verificação de impacto sobre possíveis danos que possam vir a ser causados ao realizar tratamentos de dados pessoais do usuário.

5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação do defeito**
(23) Existem práticas que busquem identificar ou reduzir chances de danos ao usuário em tratamentos de dados pessoais?	Não	Omissão
(24) Existem práticas estabelecidas para a prevenção à perda dos dados pessoais do usuário?	Não	Omissão
(25) Existem práticas estabelecidas em casos de acesso indevido e/ou vazamento de dados pessoais?	Não	Omissão
(26) A técnica de anonimização de dados pessoais é adequada?	Não	Omissão

IX - NÃO DISCRIMINAÇÃO

1. Definição da lei

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

2. Interpretação do princípio para sistemas de software

Sistemas de software devem ser projetados para evitar qualquer tipo de tratamento de dados pessoais que possam causar danos aos usuários de forma direta ou indireta.

É necessário posicionar o usuário do sistema no centro, em busca de práticas responsáveis, sejam mecanismos ou funcionalidades que reduzam as possibilidades de sistemas causarem danos aos usuários.

3. Ação esperada
O agente de tratamento deve implementar processos, oferecer soluções e realizar mapeamentos relacionado aos tratamentos de dados pessoais do usuário, a fim de reduzir e/ou eliminar riscos de discriminação que possam a vir ser causados por tratamentos realizados.
4. Exemplos de violação ao princípio para sistemas de software
Por meio de um aplicativo e um aparelho inteligente (pulseira ou relógio), são coletados e armazenados dados sobre a saúde do usuário e sua atividade física. Com isso é possível fornecer dicas sobre melhorias de saúde e rotina baseado nos dados de saúde coletados diariamente do usuário. O sistema possui diversos modos de visualização sobre as informações sobre sua evolução e saúde física. O princípio é violado quando, a partir da rotina de monitoramento das atividades do usuário, são realizadas predições relacionadas à sua saúde, como a **predição** de doenças, comorbidades, criando um perfil de risco de saúde para o usuário (***profiling***). Também é violado ao: (1) coletar a informação sobre o gênero do usuário para fins de perfil **e personalização de rotinas de saúde (finalidade)**, não é aceitável que esses dados sejam utilizados para cobrar mais caro ou negar um serviço baseado em um risco de saúde calculado ou comorbidade; (2) coletar dados sobre o cep e geolocalização do usuário com objetivo de inferir perfis demográficos e socioeconômicos do usuário, com o objetivo de inferir raça, classe ou qualquer outro dado sensível e utilizá-los para realização de cobranças diferenciadas, juros mais altos ou a negação de serviços.

5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta (Sim/Não)**	**(5.B) Classificação defeito**
(27) Existem práticas para prevenir a existência de discriminações que possam causar danos ao usuário?	Não	Omissão
(28) Existem práticas organizacionais que utilizem dados pessoais sensíveis como variáveis de decisão?	Não	Fato Incorreto

X - RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS
1. Definição da lei
Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, da eficácia dessas medidas.
2. Interpretação do princípio para sistemas de software
Um sistema de software deve adotar, e se necessário, disponibilizar mecanismos que auxiliem o usuário a compreender que seus dados pessoais e seus respectivos tratamentos estão sendo realizados de acordo com a lei**.**
3. Ação esperada
O agente de tratamento, seja no nível de produto de software, processos ou organizacional, deve informar quais são os mecanismos e medidas utilizados para proteger os dados pessoais do usuário.

4. Exemplos de violação ao princípio para sistemas de software		
O princípio é violado quando a organização falha em implementar práticas (técnicas ou administrativas) que auxiliem o usuário a compreender que seus dados pessoais estão sendo tratados em conformidade com a LGPD. Documentação de práticas: casos em que a organização e seus sistemas não possuem documentação de suas práticas, tornando incapaz demonstrar que os tratamentos de dados pessoais são sistematicamente executados como informado ao usuário. Casos em que a organização não possui registros sobre como as funcionalidades realizam os tratamentos de dados. Em sistemas de software diversas dessas informações podem estar contidas em documentos e artefatos produzidos no ciclo de desenvolvimento de software (requisitos, diagramas, dentre outros).		
5. Perguntas de inspeção ao Especialista/Inspetor	**(5.A) Resposta esperada (Sim/Não)**	**(5.B) Classificação defeito**
(29) Existem artefatos, recursos e processos que auxiliem na demonstração de cumprimento da lei?	Não	Omissão
(30) Os artefatos disponibilizados possuem linguagem facilitada e acessível a usuários leigos e não especialistas?	Não	Ambiguidade
(31) Os artefatos são de fácil acesso ao usuário? ***Levar em consideração a quantidade de passos necessários para acessar. Quanto menor a quantidade de cliques/passos, melhor para o usuário.*	Não	Omissão

APÊNDICE C – FORMULÁRIO DE DISCREPÂNCIAS

LGPDCHECK

Formulário de Discrepâncias

Revisor #: _____ **Data:** _____
Início (hh:mm): _____ **Fim (hh:mm):** _____

Utilize este formulário para relatar eventuais discrepâncias que você identificar durante a inspeção de artefatos de requisitos utilizando a *LGPDCheck*. Ao identificar uma discrepância, indique:

- o número da discrepância,
- o tipo da discrepância (vide abreviações abaixo),
- o local em que foi identificada a discrepância (Ex.: **RF12**, **Pág. 5**, **Glossário etc.**),
- o horário em que a discrepância foi identificada (Ex.: 16:55),
- a pergunta da técnica que levou à identificação da discrepância, caso pertinente (Ex.: **15, 22,** etc.), e
- uma descrição da discrepância, sucinta e concisa, mas que permita ao autor do documento corrigi-la.

Para o relato do tipo da discrepância, utilize as seguintes abreviações:

O - Omissão
IE - Informação Estranha
A - Ambiguidade
IN - Inconsistência
FI - Fato Incorreto

Num.	Tipo	Local.	Hora (hh:mm)	Pergunta	Descrição da Discrepância
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
19.					
20.					

APÊNDICE D – FORMULÁRIO DE DISCREPÂNCIAS AD-HOC

Revisor #: _____ **Data:** _____
Início (hh:mm): _____ **Fim (hh:mm):** _____

Utilize este formulário para relatar eventuais discrepâncias que você identificar durante a inspeção *Ad-hoc* de artefatos de projeto tendo em vista a LGPD. Ao identificar uma discrepância, indique:

- o número da discrepância,
- o tipo da discrepância (vide abreviações abaixo),
- o local em que foi identificada a discrepância (Ex.: **RF12**, **Pág. 5**, **Glossário etc.**),
- o horário em que a discrepância foi identificada (Ex.: 16:55), e
- uma descrição da discrepância, sucinta e concisa, mas que permita ao autor do documento corrigi-la.

Para o relato do tipo da discrepância, utilize as seguintes abreviações:

O - Omissão
IE - Informação Estranha
A - Ambiguidade
IN - Inconsistência
FI - Fato Incorreto

Num.	**Tipo**	**Local.**	**Hora (hh:mm)**	**Descrição da Discrepância**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				

APÊNDICE E – CHECKLIST DE VERIFICAÇÃO *LGPDCHECK*

Verificação da Lei Geral de Proteção de Dados Pessoais em Artefatos e Sistemas de Software

Utilize este checklist durante a inspeção de artefatos de requisitos utilizando a *LGPDCheck*. Utilize o Material de Apoio, composto pelo Glossário de Termos e Quadros dos princípios da LGPD.

Nº	Questão			
	I - FINALIDADE	**Sim**	**Não**	**N/A**
1	Existe alguma razão explícita e não genérica que justifique cada tratamento de dados pessoais?			
2	As finalidades dos tratamentos de dados pessoais são informadas ao usuário?			
3	A descrição da(s) finalidade(s) permite o claro entendimento do tratamento de dados pessoais realizada pelo sistema/organização?			
4	A finalidade do tratamento de dados pessoais foi modificada e informada ao usuário?			
	II - ADEQUAÇÃO	**Sim**	**Não**	**N/A**
5	A organização está realizando operações de tratamento de dados pessoais compatíveis com as finalidades informadas ao usuário?			
6	O dado pessoal é tratado em diferentes partes do sistema de software ou organização? Se sim, sua finalidade continua consistente com a informada ao usuário?			
	III - NECESSIDADE	**Sim**	**Não**	**N/A**
7	A coleta de dados pessoais é consistente, coerente e adequada para cumprir com um serviço ou funcionalidade (finalidade) desejada no sistema de software?			
8	É possível reduzir ou excluir algum dos dados pessoais coletados sem prejuízo a execução da funcionalidade?			
9	Existem processos para avaliar a proporcionalidade na coleta dos dados pessoais?			
	IV - LIVRE ACESSO	**Sim**	**Não**	**N/A**
10	São oferecidos mecanismos para que o usuário possa acessar informações sobre como é realizado o tratamento de seus dados pessoais?			
11	São oferecidos mecanismos para que o usuário possa acessar informações sobre a duração do tratamento de seus dados pessoais?			
	V - QUALIDADE DE DADOS	**Sim**	**Não**	**N/A**
12	É possível garantir que os dados pessoais já coletados e tratados estão atualizados?			
13	Existem mecanismos que permitem ao usuário verificar se seus dados pessoais estão atualizados e corretos?			

14	Existem mecanismos que permitam ao usuário atualizar ou solicitar a atualização/correção de seus dados pessoais?			
15	Existem mecanismos que permitam ao usuário informar sobre inconsistência em seus dados pessoais?			
	VI - TRANSPARÊNCIA	**Sim**	**Não**	**N/A**
16	Existem mecanismos que informam ao usuário quem possui acesso aos seus dados pessoais?			
17	O mecanismo de transparência disponibilizado possui linguagem adequada ao tipo de usuário?			
18	Através do mecanismo de transparência o usuário pode verificar quem são os responsáveis pelos tratamentos de dados pessoais realizados?			
19	O mecanismo existente oferece acesso às decisões e critérios utilizados para chegar ao resultado do tratamento de dados pessoais?			
	VII - SEGURANÇA	**Sim**	**Não**	**N/A**
20	Existem medidas administrativas implementadas para proteger os dados pessoais de acessos não autorizados?			
21	Existem medidas técnicas implementadas para proteger os dados pessoais de acessos não autorizados?			
22	A organização possui alguma medida para reduzir os danos decorrentes do acesso indevido aos dados pessoais?			
	VIII - PREVENÇÃO	**Sim**	**Não**	**N/A**
23	Existem práticas que busquem identificar ou reduzir as chances de danos ao usuário em tratamentos de dados pessoais?			
24	Existem práticas estabelecidas para a prevenção à perda dos dados pessoais do usuário?			
25	Existem práticas estabelecidas em casos de acesso indevido e/ou vazamento de dados pessoais?			
26	A técnica de anonimização de dados pessoais é adequada?			
	IX - NÃO DISCRIMINAÇÃO	**Sim**	**Não**	**N/A**
27	Existem práticas para prevenir a existência de discriminações que possam causar danos ao usuário?			
28	Existem práticas organizacionais que utilizem dados pessoais sensíveis como variáveis de decisão?			
	X - RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	**Sim**	**Não**	**N/A**
29	Existem artefatos, recursos e processos que auxiliem na demonstração do cumprimento da lei?			
30	Os artefatos disponibilizados possuem linguagem facilitada e acessível a usuários leigos e não especialistas?			
31	Os artefatos são de fácil acesso ao usuário? **Levar em consideração a quantidade de passos necessários para acessar. Quanto menor a quantidade de cliques/passos, melhor para o usuário.			

APÊNDICE F – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Eu declaro ter mais de 18 anos de idade e que concordo em participar em estudos conduzidos pelo Prof. Guilherme Horta Travassos, como parte das atividades do curso CPS820 - Engenharia de Software Experimental, oferecido no 2o trimestre de 2023, no Programa de Engenharia de Sistemas e Computação da COPPE/UFRJ. Estes estudos visam compreender a viabilidade de diferentes tecnologias de software utilizadas na construção de sistemas de software contemporâneos.

PROCEDIMENTO

Diferentes tecnologias de software poderão ser apresentadas. Eu entendo que serei ensinado como a tecnologia pode ser aplicada durante o curso e serei solicitado a utilizá-la em exercícios distribuídos ao longo do curso e realizados por times de trabalho organizados pelo pesquisador. Nestes exercícios alguns métodos experimentais serão aplicados por mim visando permitir pensar sobre seu uso e avaliá-los. Eu entendo que, uma vez o curso tenha terminado, os trabalhos que desenvolvi, representando alguns dos exercícios do curso, serão estudados visando entender a eficiência dos procedimentos e técnicas que me foram ensinadas.

Eu entendo que estes exercícios preenchem parte dos requisitos do curso e serão avaliados como tal. O pesquisador conduzirá o estudo consistindo na coleta, análise e relato dos dados dos exercícios. Eu entendo que não tenho obrigação alguma em contribuir com informação sobre meu desempenho nos exercícios, e que posso solicitar a retirada de meus resultados do estudo a qualquer momento e sem qualquer penalidade ou prejuízo. Eu entendo que não existirá nenhum crédito ou benefício extra por participar deste estudo, e que não haverá qualquer impacto negativo em minha avaliação por não participar do estudo. Eu entendo também que quando os dados forem coletados e analisados, meu nome será removido dos dados e que este não será utilizado em nenhum momento durante a análise ou quando os resultados forem apresentados.

CONFIDENCIALIDADE

Toda informação coletada neste estudo é confidencial, segue os princípios da LGPD, e meu nome não será identificado em momento algum. Da mesma forma, me comprometo a não comunicar os meus resultados enquanto não terminar o estudo, bem como manter sigilo das técnicas e documentos apresentados e que fazem parte do experimento.

BENEFÍCIOS, LIBERDADE DE DESISTÊNCIA

Eu entendo que o estudo não impõem qualquer risco pessoal e que os benefícios que receberei deste estudo são limitados ao aprendizado do material que é distribuído e ensinado visando atender os requisitos do curso, 'independente de participar ou não deste estudo, mas que os pesquisadores esperam aprender mais sobre quão eficiente é a identificação de defeitos e os benefícios trazidos por este estudo para o contexto da Engenharia de Software.

Eu entendo que sou livre para realizar perguntas a qualquer momento ou solicitar que qualquer informação relacionada a minha pessoa não seja incluída no estudo. Eu entendo que minha participação no estudo não afetará minha nota final de qualquer forma, e que participo de livre e espontânea vontade com o único intuito de contribuir para o avanço e desenvolvimento de técnicas e processos para a Engenharia de Software.

PROFESSOR RESPONSÁVEL

Prof. Guilherme Horta Travassos
Programa de Engenharia de Sistemas e Computação / COPPE/UFRJ

APÊNDICE G – FORMULÁRIO DE CARACTERIZAÇÃO DOS PARTICIPANTES

Caracterização do Participante

TAG: _____ Nível (Bsc/Msc/Dsc): ____

Formação Geral

Por favor, estime sua habilidade em utilizar material de trabalho em inglês:
__ Eu falo, leio e escrevo fluentemente.
__ Considero o Inglês como sendo uma linguagem onde (Por favor, complete)
Minhas habilidades de leitura e compreensão de textos:
__ poderiam ser melhores
__ são moderadas
__ são altas
__ são muito altas

Minha capacidade de trabalhar/seguir instruções escritas em inglês:
__ poderiam ser melhores
__ são moderadas
__ são altas
__ são muito altas

Qual é sua experiência anterior com desenvolvimento de software na prática? (marque aqueles itens que melhor se aplicam)
__ nunca desenvolvi software.
__ tenho desenvolvido software para uso próprio.
__ tenho desenvolvido software como parte de uma equipe, relacionado a um curso.
__ tenho desenvolvido software como parte de uma equipe, na indústria.

Por favor, explique sua resposta. Inclua o número de semestres ou número de anos de experiência relevante em desenvolvimento (E.g. “Eu trabalhei por 10 anos como programador na indústria”)

Experiência em Desenvolvimento de Software
Por favor, indique o grau de sua experiência nesta seção seguindo a escala de 5 pontos abaixo:
1 = nenhum
2 = estudei em aula ou em livro
3 = pratiquei em 1 projeto em sala de aula
4 = usei em 1 projeto na indústria
5 = usei em vários projetos na indústria

Experiência com Requisitos

- Experiência escrevendo requisitos 1 2 3 4 5
- Experiência escrevendo casos de uso 1 2 3 4 5
- Experiência revisando requisitos 1 2 3 4 5
- Experiência revisando casos de uso 1 2 3 4 5
- Experiência modificando requisitos para manutenção 1 2 3 4 5

Experiência em Projeto

- Experiência em projeto de sistemas 1 2 3 4 5
- Experiência em desenvolver projetos a partir de requisitos e casos de uso 1 2 3 4 5

- Experiência criando projetos Orientado a Objetos 1 2 3 4 5
- Experiência lendo projetos Orientado a Objetos 1 2 3 4 5
- Experiência com Unified Modeling Language (UML) 1 2 3 4 5
- Experiência alterando projeto para manutenção 1 2 3 4 5

Outras Experiências

- Experiência com gerenciamento de projeto de software? 1 2 3 4 5
- Experiência com inspeções de software? 1 2 3 4 5
- Experiência com planejamento de inspeções de software? 1 2 3 4 5
- Experiência com testes de integração de software? 1 2 3 4 5

Experiência em Contextos Diferentes

Nós usaremos esta seção para compreender quão familiar você está com vários sistemas que poderão ser utilizados como exemplos ou para exercícios durante o curso.

Por favor, indique o grau de experiência nesta seção seguindo a escala de 3 pontos abaixo:
1 = Eu não tenho familiaridade com a área. Eu nunca fiz isto.
3 = Eu utilizo isto algumas vezes, mas não sou um especialista.
5 = Eu sou muito familiar com esta área. Eu me sentiria confortável fazendo isto.

Quanto você sabe sobre…

- Controle de atividades diárias em hospitais? 1 3 5
- Utilizar Métricas para Gerenciar Projetos de Software? 1 3 5
- Gerenciar Processos de Manutenção de Equipamentos? 1 3 5
- Lei Geral de Proteção Dados Pessoais Brasileira? 1 3 5

APÊNDICE H – QUESTIONÁRIO DE AVALIAÇÃO *LGPDCHECK*

REVISOR: _____

Estudo *LGPDCheck*

1. **Entendo que *LGPDCheck* é de fácil aplicação.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

2. **Foi fácil entender as perguntas apresentadas no checklist de *LGPDCheck*.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

3. **Foi fácil entender o material de apoio de *LGPDCheck*.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

4. **Foi fácil preencher o relatório de discrepâncias de *LGPDCheck*.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

5. **Entendo que *LGPDCheck* me ajudou a encontrar defeitos nos documentos inspecionados.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

6. **As perguntas do checklist de *LGPDCheck* me ajudaram a encontrar defeitos.**
   ( ) Discordo totalmente
   ( ) Discordo parcialmente
   ( ) Concordo parcialmente
   ( ) Concordo totalmente

7. **O conteúdo do material de apoio de *LGPDCheck* me ajudou a encontrar defeitos.**
   ( ) Discordo totalmente

( ) Discordo parcialmente
( ) Concordo parcialmente
( ) Concordo totalmente

8. Eu usaria *LGPDCheck* em futuras inspeções de conformidade de documentos de requisitos com a LGPD.

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Concordo parcialmente
( ) Concordo totalmente

9. Eu recomendaria o uso de *LGPDCheck* para profissionais que verifiquem a conformidade de documentos de requisitos com a LGPD.

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Concordo parcialmente
( ) Concordo totalmente

10. Por favor, aponte suas principais impressões sobre a experiência de uso de *LGPDCheck*.

11. Caso possua, por favor indique sugestões de melhoria para *LGPDCheck*.

12. Como você avalia seu conhecimento sobre privacidade e proteção de dados em sistemas de software?

( ) Muito baixo ( ) Baixo ( ) Alto ( ) Muito alto

13. Como você avalia seu conhecimento prévio sobre o domínio de problema conforme apresentado no Módulo de Gestão de Usuários do SIGIC?

( ) Muito baixo ( ) Baixo ( ) Alto ( ) Muito alto

14. Como você avalia seu conhecimento prévio sobre o domínio de problema conforme apresentado no Módulo de Solicitações do SIGIC?

( ) Muito baixo ( ) Baixo ( ) Alto ( ) Muito alto

15. Por favor, aponte suas principais impressões sobre a experiência de participação nas diferentes atividades deste estudo.

16. Caso possua, por favor indique sugestões de melhoria para futuras execuções deste estudo.

APÊNDICE I – PROTOCOLO DO ESTUDO DE VIABILIDADE *LGPDCHECK*

1) Objetivo específico

Com base no modelo GQM de (BASILI, CALDIERA, *et al.*, 1994), o objetivo deste estudo foi definido da seguinte forma:

***Analisar*:** a inspeção de recursos de privacidade e proteção de dados em artefatos de software usando técnicas *Ad-hoc* e *LGPDCheck*
Com o propósito de: caracterizar
Em relação: a eficácia (defeitos identificados/total de defeitos existentes) e eficiência (defeitos identificados/tempo) do *LGPDCheck* na detecção de defeitos à luz dos princípios da LGPD
***Do ponto de vista*:** de pesquisadores em Engenharia de Software
***No contexto*:** de profissionais de software (representados por alunos de Graduação, Mestrado e Doutorado em Engenharia de Sistemas da Universidade Federal do Rio de Janeiro (UFRJ), discentes de uma disciplina de Engenharia de Software Experimental da pós-graduação.

2) Questões e métricas

- *Pergunta: Quanto tempo levaram as inspeções?*
- *Métrica: tempo dedicado à inspeção (em minutos) e eficiência de cada inspeção.*
- *Pergunta: Qual técnica de inspeção (LGPDCheck ou Ad-hoc) permite que os inspetores detectem mais defeitos?*
- *Métrica: número de defeitos detectados, eficácia da inspeção.*

3) Hipóteses

$H_0 1$: Não há diferença entre a eficiência das inspeções realizadas com o *LGPDCheck* e as inspeções *Ad-hoc.*

$H_A 1$: A eficiência das inspeções realizadas com o *LGPDCheck* é superior à eficiência das *Ad-hoc.*

$H_0 2$: Não há diferença entre a eficácia das inspeções realizadas com o *LGPDCheck* e as inspeções *Ad-hoc*.

$H_A 2$: A eficácia das inspeções realizadas com o *LGPDCheck* é maior do que as *Ad-hoc*.

a) Variáveis

- **Variáveis independentes**: experiência do participante em inspeções e conhecimento prévio em Privacidade e Proteção de Dados de regulações como LGPD e GDPR. Todas essas variáveis serão coletadas por meio de

um questionário de caracterização dos sujeitos, seguindo os tipos de escala apresentados na Tabela 29.

Tabela 29 - Descrição das variáveis independentes

Nome (abreviação)	Descrição	Escala (tipo)
Experiência com Desenvolvimento de Software (SDExp)	Experiência anterior do participante com atividades de desenvolvimento de software em geral em termos de autoavaliação, anos e número de projetos	Escala Likert de 5 níveis (próprio), numérico
Experiência com inspeção de software (SIExp)	Experiência anterior do participante na realização de inspeções de software em termos de autoavaliação, anos e número de projetos	Escala Likert de 5 níveis (próprio), numérico
Conhecimento sobre PPD (PPDPK)	Autoavaliação do participante sobre seu nível de conhecimento sobre Privacidade e Proteção de Dados (PPD)	Nominal: ou o participante tem experiência anterior ou não
Experiência com LGPD (LGPDEx)	Experiência anterior do participante na aplicação da LGPD em projetos de software em termos de autoavaliação, anos e número de projetos	Escala Likert de 5 níveis (próprio), numérico

- **Variáveis dependentes:** número de defeitos e falsos positivos, tempo gasto na realização da inspeção, eficiência e eficácia. A descrição das variáveis dependentes é apresentada na Tabela 30.

Tabela 30 - Descrição das variáveis dependentes

Nome (abreviação)	Descrição	Escala (tipo)
Número de discrepâncias (DC)	Discrepâncias (DC) são todas as inconformidades relatadas pelo inspetor durante o processo de inspeção.	Numérico
Número de Defeitos (ND)	número de defeitos identificados durante a inspeção pelo participante	Numérico
Falso positivos (FP)	número de candidatos a defeito descartados	Numérico
Duração da Inspeção (ID)	tempo gasto pelo participante para realizar a inspeção (em minutos)	Numérico
Eficiência (Eff)	o tempo médio (em minutos) para detectar um único defeito.	Numérico (Ratio)
Eficácia (Efc)	a razão entre o número de defeitos encontrados pelo participante e o número total de defeitos distintos encontrados por cada participante	Numérico (Ratio)

4) Participantes

Este estudo será realizado com 14 alunos da Universidade Federal do Rio de Janeiro, UFRJ com diferentes níveis de instrução entre Graduação, Mestrado e Doutorado em Engenharia de Sistemas da Universidade Federal do Rio de Janeiro (UFRJ).

Ambas as tentativas (T1 e T2) foram realizadas no documento de visão e requisitos do Sistema Integrado de Gerência de Informações Contábeis, um sistema

real e em produção. Entre seus distintos módulos disponíveis, dois foram disponibilizados para o estudo:

- **Módulo de Solicitações (MSL):** módulo responsável pela gestão das solicitações contábeis realizadas pelos diversos clientes. Através desse módulo essas solicitações são criadas e acompanhadas pelos próprios clientes. Por outro lado, os colaboradores ficam responsáveis por avaliar essas solicitações e prosseguir com o processamento delas.
- **Módulo de Gestão Usuários (MGU):** módulo responsável pela administração dos usuários, bem como pela definição das funcionalidades as quais esses usuários terão acesso.

Os dois módulos, MSL e MGU, do sistema serão inspecionados no quasi-experimento. Para isso, um subconjunto equilibrado de funcionalidades será selecionado para ser examinado para cada módulo. O critério para equilibrar o escopo das inspeções será, primeiramente a experiência prévia do participante com PPD e LGPD, coletada no formulário de caracterização dos participantes do experimento. Nenhum defeito será semeado. Os defeitos reais serão verificados após a coleta dos relatórios dos participantes.

5) Plano de execução

Após a assinatura de um termo de consentimento e de uma ficha de caracterização, cada grupo de alunos (G1, G2) realizará duas rodadas (T1 e T2) sobre combinações distintas de módulos (MSL, MGU) do sistema de software (ver Tabela 31). O quasi-experimento será realizado na sala de aula do curso, na qual cada participante tem acesso a um único módulo.

Na primeira tentativa (T1), os três grupos receberão instruções sobre a LGPD e seus princípios. Eles também receberão instruções sobre inspeção de software e tipos de defeitos. Após o treinamento, os participantes realizarão as inspeções *Ad-hoc* individualmente, relatando as discrepâncias identificadas em um formulário.

Tabela 31 - Grupos, Rodadas, e Artefatos Inspecionados

Grupo (tamanho)	T1	Escopo	T2	Escopo
G1	Ad-hoc	MSL	*LGPDCheck*	MGU
G2	Ad-hoc	MGU	*LGPDCheck*	MSL

Após a rodada T1, os participantes participarão da sessão de treinamento. Nesta sessão, eles serão apresentados ao *LGPDCheck* e seus recursos. Na segunda rodada (T2), os participantes de cada grupo serão designados para realizar inspeções usando

o *LGPDCheck* em outros módulos do sistema que ainda não inspecionaram, mas já foram inspecionados *Ad-hoc* por outro grupo. Como na primeira rodada, os participantes relatarão as discrepâncias identificadas em uma folha de relatório de discrepâncias. Porém, também devem associar cada discrepância a um item do checklist *LGPDCheck*.

6) Análise de Dados

Os seguintes mecanismos serão usados para a análise dos dados coletados:

- Comparação entre o desempenho de cada participante nas duas rodadas.
- Cálculo da variância do defeito e desvio padrão.
- Cálculo do tempo gasto com as inspeções.
- Eliminação de outliers e verificação da normalidade dos dados (Shapiro-Wilk) e homocedasticidade (Levene).
- Aplicação de um teste não paramétrico (*Wilcoxon*) ou paramétrico (Student's), conforme cada caso.

7) Ameaças à Validade (Threats to Validity)

Validade de construto: destacamos o pequeno número de sujeitos submetidos ao estudo, e o número limitado de domínios inspecionados (um sistema, dois módulos), porém, uma combinação limitada de grupos (dois). No entanto, vale ressaltar que nenhum participante deverá inspecionar o mesmo módulo mais de uma vez. Além disso, não podemos garantir que os módulos sejam comparáveis em número de defeitos e complexidade. Para mitigar essa ameaça, compusemos um subconjunto equilibrado de funcionalidades para inspecionar em cada módulo.

Validade externa: os sujeitos são no mínimo alunos do 3º ano de graduação a alunos de pós-graduação (mestrado e doutorado), com diferentes níveis de experiência em engenharia de software e inspeção.

Validade Interna: dada a novidade e escassez de materiais com foco em PPD para engenharia de software, estamos preparando treinamentos para que cada participante adquira conhecimento sobre o assunto.

Conclusão Validade: os resultados iniciais não podem ser generalizados. No entanto, eles contribuirão para a evolução do LGPDCheck para posterior avaliação e uso.

8) Custos do Estudo

a) Custos de Planejamento

- **Plano propriamente dito**: não aplicável;
- **Instrumentação**: termo de consentimento, questionário de caracterização dos participantes, *LGPDCheck*, modelo de relatório de inspeção;
- **Material de treinamento**: gravação de vídeo;
- **Avaliação do Plano**: não aplicável;

b) Custos de Execução

- **Despesas de viagem:** aplicação local;
- **Treinamento:** será ministrado aos alunos treinamento sobre os principais conceitos de Privacidade e Proteção de Dados da LGPD e *LGPDCheck*;
- **Recursos Humanos:** alunos de graduação e pesquisadores;
- **Recursos materiais:** formulários, artefatos de software, computadores, software.

c) Custos de Análise

- não aplicável;

d) Custos de Embalagem

- não aplicável;

e) Escrita e publicação

- inscrição na conferência e taxas de acesso aberto.

ANEXO I – Outras definições da LGPD (Art. 5º)

- **XIV – eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **XIII – bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- **XV - transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- **XVI - uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- **XVII - relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- **XVIII - órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.
- **XIX - autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.