UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Paulo Henrique da Silva

Uma abordagem para o desenvolvimento de soluções computacionais de apoio a engenharia de requisitos com foco na proteção de dados

Florianópolis
2024

Paulo Henrique da Silva

Uma abordagem para o desenvolvimento de soluções computacionais de apoio a engenharia de requisitos com foco na proteção de dados

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do título de mestre em Ciência da Computação.
Orientadora: Prof. Fabiane Barreto Vavassori Benitti, Dra.
Coorientadora: Prof. Michelle Silva Wangham, Dra.

Florianópolis
2024

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Silva, Paulo Henrique da
Uma abordagem para o desenvolvimento de soluções computacionais de apoio a engenharia de requisitos com foco na proteção de dados / Paulo Henrique da Silva ; orientadora, Fabiane Barreto Vavassori Benitti, coorientadora, Michelle Silva Wangham, 2024.
111 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Ciência da Computação, Florianópolis, 2024.

Inclui referências.

1. Ciência da Computação. 2. Engenharia de requisitos. 3. Proteção de dados. 4. LGPD. 5. GDPR. I. Benitti, Fabiane Barreto Vavassori. II. Wangham, Michelle Silva. III. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Ciência da Computação. IV. Título.

Paulo Henrique da Silva

Uma abordagem para o desenvolvimento de soluções computacionais de apoio a engenharia de requisitos com foco na proteção de dados

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof.(a) Patricia Vilain, Dr(a).
Universidade Federal de Santa catarina - UFSC
Prof.(a) Jean Carlo Rossa Hauck, Dr(a).
Universidade Federal de Santa catarina - UFSC

Prof.(a) Emerson Ribeiro de Mello, Dr(a).
Instituto Federal de Santa Catarina - IFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Ciência da Computação.

Documento assinado digitalmente
Marcio Bastos Castro
Data: 06/02/2024 13:40:01-0300
CPF: ***.707.720-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de
Pós-Graduação

Documento assinado digitalmente
Fabiane Barreto Vavassori Benitti
Data: 28/01/2024 17:30:54-0300
CPF: ***.986.440-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Fabiane Barreto Vavassori Benitti,
Dra.
Orientadora

Documento assinado digitalmente
MICHELLE SILVA WANGHAM
Data: 31/01/2024 21:01:47-0300
CPF: ***.535.072-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Michelle Silva Wangham, Dra.
Coorientadora
Universidade do Vale do Itajaí - UNIVALI

Florianópolis, 2024.

À minha esposa Princiani, e aos meus filhos Pedro,
Sarah e Valentina (em memória).

AGRADECIMENTOS

Agradeço à minha esposa Princiani pelo amor, pela resiliência, parceria e por viver este meu sonho como se fosse o dela. Agradeço aos meus filhos Pedro e Sarah pela paciência, carinho, respeito e por me motivarem de uma maneira que eles ainda não compreendem. Às minhas orientadoras, professora Fabiane e professora Michelle, pelas provocações, conselhos e carinho com que conduziram toda esta trajetória, saibam que as vezes que cruzei com o caminho de vocês, saí não só com mais conhecimento, mas também me tornei uma pessoa melhor. Por fim, agradeço à minha mãe Elizabete e à minha querida vó Matilde (em memória), pela dedicação, educação e amor incondicional, que só compreendi quando me tornei pai.

RESUMO

O crescimento tecnológico tem permitido o processamento em larga escala de dados pessoais, dados por vezes tratados para finalidades não previamente consentidas por seus titulares ou sem a devida proteção. A privacidade é um tema crucial que se popularizou com a entrada em vigor de regulamentações como GDPR e LGPD. Pesquisas mostram que aderir a essas regulamentações não é algo trivial para empresas que desenvolvem soluções que tratam dados pessoais. Esse cenário é agravado pelo desconhecimento das equipes de desenvolvimento de software em relação às normas de proteção de dados. Neste contexto, o presente trabalho visou desenvolver uma abordagem para apoiar as equipes na construção de requisitos de software aderentes aos regulamentos de proteção de dados por meio de uma estrutura baseada em fluxo de trabalho e, para tanto, partiu da identificação do problema, projeto de solução e avaliação. A abordagem definida analisa o requisito sob vários pontos de vista relacionados à proteção de dados, indicando pontos de melhoria a serem considerados para a implementação do requisito em questão. Duas avaliações da abordagem foram realizadas: (i) um estudo de caso com avaliação por painel de especialistas; e (ii) uma prova de conceito. A primeira avaliou a entrega de valor da abordagem e a capacidade de se adaptar a diferentes cenários. A prova de conceito teve como objetivo demonstrar a integração da abordagem a uma ferramenta de mercado para avaliar a flexibilidade. Como resultado observado houve a concordância dos especialistas quanto a entrega de valor e à flexibilidade da arquitetura proposta pela abordagem, bem como foi possível demonstrar a flexibilidade da abordagem para diferentes cenários e aderência à ferramenta de mercado.

Palavras-chave: Engenharia de requisitos, Proteção de dados, LGPD, GDPR

ABSTRACT

Technological growth has enabled the large-scale processing of personal data, data that is sometimes processed for purposes not previously consented to by its owners or without proper protection. Privacy is a crucial issue that has become popular with the entry into force of regulations such as GDPR and LGPD. Research shows that adhering to these regulations is not a trivial matter for companies that develop solutions that process personal data. This scenario is exacerbated by software development teams' lack of knowledge of data protection regulations. In this context, this work aimed to develop an approach to support teams in building software requirements that adhere to data protection regulations through a workflow-based structure, starting with problem identification, solution design and evaluation. The defined approach analyzes the requirement from various points of view related to data protection, indicating points of improvement to be considered for the implementation of the requirement in question. Two evaluations of the approach were carried out: (i) a case study with evaluation by a panel of experts; and (ii) a proof of concept. The first assessed the approach's value delivery and its ability to adapt to different scenarios. The proof of concept aimed to demonstrate the integration of the approach with a market tool to assess flexibility. As a result, the experts agreed on the delivery of value and the flexibility of the architecture proposed by the approach, as well as demonstrating the approach's flexibility for different scenarios and adherence to a market tool.

Keywords: Requirements engineering, Data protection, LGPD, GDPR

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CIS Controls	Center for Internet Security Controls
DPIA	Data Protection Impact Assessment
DSM	Design Science Methodology
EDPRL	Enterprise Data Privacy Requirement Language
GDPR	General Data Protection Regulation
GQM	Goals, Questions and Metrics
ICO	Information Commissioner's Office
IOT	Internet Of Things
ISO	International Organization fo Standardization
LGPD	Lei Geral de Proteção de Dados
LLM	Large Language Model
MOM	Message Oriented Middleware
NIST	National Institute of Standards and Technology
PbD	Privacy by Design
PEC 17/19	Proposta de Emenda Constitucional 17/19
PPSI	Programa de Privacidade e Segurança da Informação
RIPD	Relatório de Impacto a Proteção de Dados
SBES	Simpósio Brasileiro de Engenharia de Software
TF-IDF	Term Frequency – Inverse Document Frequency

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica permitiu o desenvolvimento das mais diversas soluções, estas por sua vez incorporaram a capacidade de armazenar, processar e transmitir dados em um volume não antes imaginado (BIONI, 2019). Além disto, o acesso à informação é cada vez mais impulsionado pela economia digital. Soluções como *Internet Of Things (IOT)*, Big Data e Inteligência Artificial fomentam a coleta e o armazenamento de dados em grande escala para serem processados de maneira a atender alguma necessidade da sociedade, empresas ou indivíduos. No entanto, os dados coletados podem conter informações pessoais e serem tratados para objetivos não legítimos ou não informados previamente, violando a privacidade de seus titulares (SYPE *et al.*, 2014).

Segundo a ONU (2018), a privacidade é um direito universal de todo ser humano, mas não há um consenso quanto ao conceito, sendo este abrangente, incluindo liberdade de pensamento, controle sobre as informações pessoais, liberdade de vigilância, direito de proteção à reputação e proteção contra buscas e interrogatórios (SOLOVE; WASHINGTON, 2008).

No Brasil, a importância foi legalmente dada na Constituição Federal de 1988, que contém, dentre outros pontos, o direito à inviolabilidade da vida privada e intimidade (BRASIL, 1988). Entretanto, o tema ganhou mais força com a Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018 que, possuindo forte influência do *General Data Protection Regulation (GDPR)* ou Regulamento Geral de Proteção de Dados europeu, também estabelece regras para o tratamento de dados pessoais, trazendo mais proteção para os titulares dos dados e penalidades para aqueles que não seguirem as regras (BRASIL, 2018).

Fortalecendo cada vez mais o tema, um pouco mais recente, a Proposta de Emenda Constitucional 17/19 (PEC 17/19) foi aprovada e incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais dos cidadãos (SENADO, 2021).

Contudo, vazamentos de dados pessoais ainda representam uma parcela significativa das consequências de incidentes, representando metade dos que foram catalogados pela Verizon em 2023 (VERIZON, 2023). Para além disto, os custos com vazamento de dados também aumentaram em cerca de 15,3% em relação a 2020, segundo relatório disponibilizado pela IBM (IBM, 2023).

Ainda segundo a IBM (2023), apenas um terço dos vazamentos de dados são identificados pela própria empresa, o que fortalece a necessidade de mais investimento na área. Para apoiar isto, é preciso considerar frameworks e boas práticas que possam orientar as equipes no tratamento de dados pessoais.

O conjunto de recomendações da norma International Organization fo Standardization (ISO) 27000 são padrões internacionais para a promoção de qualidade no que

se refere à segurança da informação, o objetivo é orientar organizações, de qualquer setor, por meio de recomendações de boas práticas para a gestão da segurança da informação (DIAMANTOPOULOU *et al.*, 2020).

Igualmente relevante, são as orientações fornecidas pelo *Center for Internet Security Controls (CIS Controls)* e pelo Framework *National Institute of Standards and Technology (NIST)*. O CIS Controls oferece um conjunto de boas práticas de segurança cibernética detalhadas (CENTER FOR INTERNET SECURITY (CIS), 2021), enquanto o NIST é amplamente reconhecido por suas diretrizes de gerenciamento de risco em segurança cibernética (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2018). Ambas as abordagens oferecem maneiras adicionais de aprimorar a segurança de dados e sistemas.

Com o grande crescimento de novas soluções que processam dados pessoais, aumentam-se as exigências para que equipes de desenvolvimento estejam preparadas, engajadas e se sintam responsáveis por implementar softwares que garantam a proteção de dados pessoais (BEDNAR *et al.*, 2019). Não é mais aceitável que estas equipes não priorizem ou não possuam conhecimento suficiente sobre as tecnologias e processos que preservem a privacidade dos usuários e protejam seus dados pessoais (HADAR *et al.*, 2018).

Neste cenário, outra abordagem que ganha relevância é o *Privacy by Design (PbD)*, que visa mitigar ameaças à privacidade desde a concepção do projeto, criando um processo que assegura que apenas dados pessoais necessários serão processados para cada propósito específico. O PbD tem como base 7 princípios, a saber (CAVOUKIAN, 2010):

1. Proativo, e não reativo; preventivo, e não corretivo: antecipar e prevenir situações que possam comprometer a privacidade;

2. Privacidade como padrão: o usuário não deve ter que realizar nenhuma ação para manter sua privacidade ao acessar um sistema;

3. Privacidade incorporada ao design: a privacidade não deve ser acrescentada como algo adicional no sistema, ela deve estar incorporada às tecnologias, processos, operações e arquiteturas da informação;

4. Funcionalidade total: conhecida também como soma positiva, tem como objetivo garantir que as funcionalidades essenciais do sistema cheguem a todos, evitando falsos dilemas, ou seja, garantir que não seja necessário abrir mão da privacidade em troca de mais funcionalidades no sistema ou projeto;

5. Segurança ponta a ponta e proteção durante todo o ciclo de vida dos dados: medidas de segurança são essenciais e é preciso garantir que os dados serão

armazenados com segurança e também destruídos com segurança no fim do ciclo de vida do dado;

6. Visibilidade e transparência: estas são fundamentais para estabelecer responsabilização e confiança; e
7. Respeito pela privacidade do usuário: as informações devem garantir integridade, confidencialidade e disponibilidade, com padrões fortes de privacidade, informações claras, notificações apropriadas e opções *user-friendly* que empoderem os usuários de forma que estes tenham um gerenciamento ativo sobre seus próprios dados.

A Engenharia de requisitos é um processo que determina o que os usuários realmente precisam, documentando tais necessidades de maneira que possa ser efetivamente comunicada para o cliente e para o time de desenvolvimento (PRESSMAN, 2009).

A preocupação com a privacidade desde a concepção está alinhada com tal processo, uma vez que esta inicia justamente na concepção, definindo o escopo e a natureza do problema a ser solucionado e, por fim, verifica se as restrições do software foram atendidas (SOMMERVILLE, 2011). Com isto, faz sentido que estas restrições contenham as demandas impostas pelos regulamentos de proteção de dados pessoais.

Contudo, a especificação de requisitos é uma atividade complexa. As diferentes necessidades, subjetividade na compreensão e interpretação podem impactar na qualidade do software se mal entendidos por analistas ou desenvolvedores durante a implementação (NASCIMENTO *et al.*, 2018).

Neste contexto, a contribuição deste trabalho está em apoiar soluções computacionais de gestão de requisitos por meio de uma abordagem que estimule a proteção de dados pessoais durante a especificação de requisitos de software.

1.1 PROBLEMA DE PESQUISA

Durante a análise e especificação dos requisitos de um sistema, os analistas responsáveis podem focar em priorizar apenas itens que estejam diretamente associados a entregas de valor perceptíveis pelos usuários e deixar requisitos relacionados com segurança e proteção de dados em segundo plano. Tal comportamento pode ser devido aos prazos de entrega não compatíveis com a capacidade da equipe ou pela falta de conhecimento dessas áreas. O fato é que muitas vezes os requisitos relacionados à proteção de dados são negligenciados (CAMACHO *et al.*, 2016) (SACHDEVA; CHUNG, 2017), voltando a serem discutidos apenas quando um incidente de vazamento de dados ocorre.

Com o objetivo de promover a proteção de dados pessoais estão os regulamentos GDPR e LGPD, que apesar das diferenças, têm como ponto de intersecção, regulamentar o uso de dados dos cidadãos europeus e brasileiros, respectivamente, por organizações que pretendem ou que já utilizam dados pessoais em seus produtos ou processos (MASSENO, 2019). Com isto, desde a entrada em vigor desses regulamentos, empresas ao redor do mundo precisam se adequar, caso tenham a intenção de processar dados pessoais dos cidadãos.

Por conta dos atuais regulamentos de proteção de dados, os usuários estão mais preocupados com seus dados pessoais. Estudo conduzido pela kpmg (2020) com 101.162 consumidores de 27 países, aponta que 98% dos entrevistados disseram estar preocupados com seus dados pessoais e o que acontece com eles. No Brasil, em 2019, 96% dos brasileiros já concordavam que as empresas deveriam fazer mais para mantê-los protegidos (IBM, 2019).

No entanto, o processo de adequação não é trivial, regulamentos de proteção de dados impõem uma série de desafios, seja pelas obrigações impostas, que obrigam a adequação, não só de softwares que serão desenvolvidos, mas também, em desenvolvimento ou já finalizados, seja pela dificuldade de leitura e interpretação de textos normalmente ambíguos, muitas vezes difíceis de entender para quem não possui conhecimento jurídico, sendo este um problema comum em empresas de pequeno porte (C. TIKKINEN-PIRI; MARKKULA, 2017) ou ainda, a adaptação a esses regulamentos pode ser desafiadora em países que não possuem uma cultura consolidada de proteção de dados (CUNHA; AL., 2021).

De acordo com a ABES Software (2020), 95% das empresas responsáveis pela produção de software no Brasil são de pequeno porte e, além dos desafios já abordados até aqui, elas precisarão lidar com o fato de que muitos desenvolvedores não priorizam a proteção de dados pessoais devido à falta de conhecimento, compreensão sobre o conceito ou desconhecimento de tecnologias que possibilitam essa proteção (HADAR *et al.*, 2018). Para além disso, as próprias empresas também apresentam dificuldades em definir e explicar as razões para garantir o tratamento adequado dos dados (CANEDO *et al.*, 2020).

Para amenizar este cenário desafiador, existem trabalhos com propostas para apoiar a proteção de dados (BREAUX *et al.*, 2009) (LANGHEINRICH, 2001) (CAVOUKIAN, 2012) e como padrões internacionais que promovem a segurança e a privacidade, como é o caso das ISO 27001, ISO 27002 e ISO 27701.

A implantação da ISO 27001 implica um alto comprometimento com a proteção da informação, o que representa um nível de conforto considerável para as organizações que interagem com a entidade certificada (LOPES *et al.*, 2019), sendo a diferença entre a 27002 o nível de detalhe. Enquanto a ISO 27001 descreve brevemente cada controle, a ISO 27002 detalha cada um, fornecendo diretrizes e boas práticas para a

sua implementação (DIAMANTOPOULOU *et al.*, 2020), (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), 2022).

Assim como a ISO 27002, a ISO 27701 é uma extensão da 27001, contudo, especifica os requisitos e fornece as diretrizes para garantir a privacidade dos dados pessoais (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), 2022).

Ainda, propostas apresentadas por Morales-Trujillo *et al.* (2019) no estudo "A Systematic Mapping Study on Privacy by Design in Software Engineering" oferecem possibilidades para auxiliar equipes de desenvolvimento a incorporar mais proteção de dados em seus softwares. No entanto, observa-se que a maioria das soluções se concentra na modelagem ou tratam-se de requisitos e padrões de privacidade (RAMADAN *et al.*, 2018), (ALSHAMMARI; SIMPSON, 2018), (ROWAN; DEHLINGER, s.d.), (JUTLA *et al.*, 2013). Além disso, muitas delas são soluções computacionais bem específicas, para marketplaces ou sistemas para área da saúde (GUERRIERO *et al.*, s.d.) (ANTIGNAC; LE MÉTAYER, 2015). O estudo não relata abordagens ou ferramentas que ofereçam suporte a sistemas independentemente de sua natureza, ou estudos que usem requisitos de software como base para gerar alertas relacionados à proteção de dados ou a regulamentos de privacidade. Por fim, os próprios autores destacam a necessidade de abordagens que aumentem a conscientização sobre a privacidade na engenharia de software.

Considerando o exposto até o momento, o presente projeto tem como questão de pesquisa: Como auxiliar na especificação de requisitos de software com foco na proteção de dados?

1.2 SOLUÇÃO PROPOSTA

Visando responder a questão de pesquisa, este projeto propõe uma abordagem que possa ser implementada, no todo ou em parte, por equipes de desenvolvimento que precisam de apoio ferramental para auxiliar na definição de requisitos aderentes aos regulamentos de proteção de dados pessoais.

Contudo, há de se ter em vista que cada organização desenvolvedora de software possui um processo específico de desenvolvimento e, portanto, requer ferramentas aderentes às especificidades de cada empresa ou processo. Por exemplo, artefatos de especificação de requisitos podem contemplar histórias de usuário, casos de uso, cenários, dentre outros (SCHÖN *et al.*, 2017). Por outro lado, regulamentos e boas práticas de proteção de dados contém, em sua maioria, pontos que tendem a se manter iguais independentemente do segmento da organização, pois são definidos em legislação ou normas.

Ainda, é preciso considerar que para determinar a aderência aos regulamentos

de proteção de dados, é necessário analisar diversos aspectos antes de identificar a base legal que justifica o tratamento de um dado pessoal. Tomando a GDPR como exemplo, para cada dado é necessário analisá-lo quanto a licitude, finalidade, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade, o que somado a dinamicidade do ciclo de vida de um software, força a criação de um processo para garantir que etapas essenciais na verificação da adequação aos regulamentos sejam executadas caso haja alteração ou adição de um novo dado.

Considerando o cenário até aqui descrito, a abordagem proposta contempla três visões, como apresentado na figura 1: (i) visão dos Requisitos: parte flexível que se comunica com um *workflow* e pode ser adaptada para permitir a inclusão de novas formas de especificar requisitos; (ii) visão do Workflow: parte responsável por conduzir o requisito de software através de etapas que se comunicam com serviços especializados para que requisitos e seus dados sejam analisados; e (iii) visão dos Serviços: parte comum a todas as empresas e processos, suporta serviços de regulamentos, boas práticas e outros.

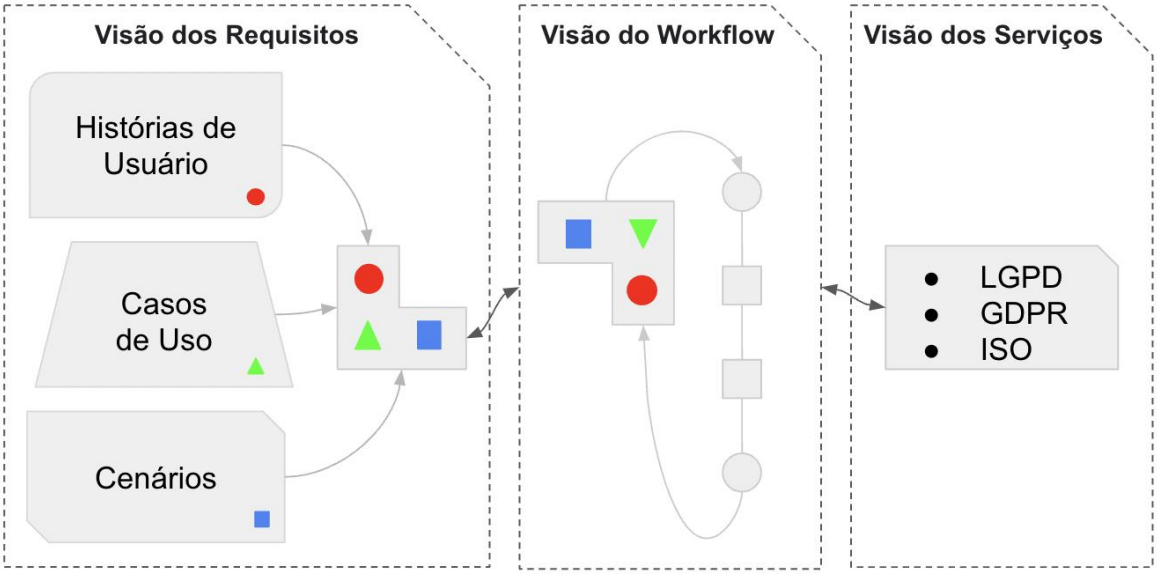


Figura 1 – Visão geral conceitual da abordagem proposta

1.2.1 Visão dos Requisitos

A visão dos rRequisitos consiste em um modelo conceitual que seja flexível para comportar artefatos de especificação de requisitos independente do formato como por exemplo, histórias de usuário e casos de uso. Para tanto, é preciso que esta visão defina padrões para estabelecer a comunicação com o Workflow ao mesmo tempo que mantenha sua flexibilidade, assegurando desta forma que as soluções que pretendem aderir a abordagem possam adaptá-la sem que prejudique a comunicação com a Visão Workflow e muito menos alterem a forma como trabalham.

Ao contrário das outras visões, esta visão é a única que precisa estar incorporada ao sistema aderente[1] de alguma maneira, seja por meio de biblioteca a ser importada, por meio de um *plugin* que seja acoplado ou ainda, codificando a visão diretamente no sistema. Com isto, espera-se facilitar a inclusão de novas formas de especificar requisitos de software com foco em proteção de dados, dado a característica adaptável aos diferentes processos de desenvolvimento.

1.2.2 Visão do Workflow

A visão do workflow conduz um requisito através de um fluxo customizável que utiliza etapas para analisá-lo com diferentes objetivos como por exemplo, verificar se possui dados pessoais sensíveis à luz de algum regulamento, sugerir boas práticas ou apontar itens na lei relevantes para o contexto. É importante destacar que essas etapas tem o objetivo de enriquecer a análise, a incrementando para levar informação cada vez mais relevante para as etapas subsequentes, de maneira a aumentar a capacidade de um parecer final sobre a adequação do requisito de software com relação à proteção de dados.

1.2.3 Visão dos Serviços

A visão dos serviços prevê serviços com funcionalidades para gerenciar regulamentos de proteção de dados como a LGPD, guias e catálogos de boas práticas como a ISO 27002 e ISO 27701, e outros serviços cujo foco seja apoiar a proteção de dados. Esta é uma visão considerada comum a todas as organizações, pois trata de aspectos que, indiferente do segmento de mercado da empresa ou organização, o conteúdo pode facilitar o processo de adequação aos regulamentos de proteção de dados.

As três visões juntas, habilitam a solução aderente a usufruir da abordagem proposta, bastando definir a forma como será incorporada à solução o modelo conceitual proposto pela visão de requisitos e implementá-la. Por exemplo, é possível criar um plugin que implemente a visão de requisitos para estabelecer a comunicação com o Workflow como apresentado na Figura 2 - cenário 1, ou desenvolver uma solução de gerenciamento de requisitos que já integre a visão de requisitos, como mostra a Figura 2 - cenário 2.

É importante que a visão dos Requisitos seja desenvolvida a partir de um modelo conceitual[2] pois isto irá permitir uma leitura padronizada de suas classes e relacionamentos, facilitando a interpretação na hora de implementar a solução.

[1] Entende-se como “sistema aderente” a solução atualmente utilizada pela organização para especificar os requisitos, como por exemplo, Jira, Trello, etc; e que se deseja incorporar a este sistema o apoio à proteção de dados pessoais por meio da presente abordagem.

[2] A modelagem conceitual objetiva abstrair um modelo do mundo real e identificar o que e como deve ser modelado (FURIAN *et al.*, 2015).

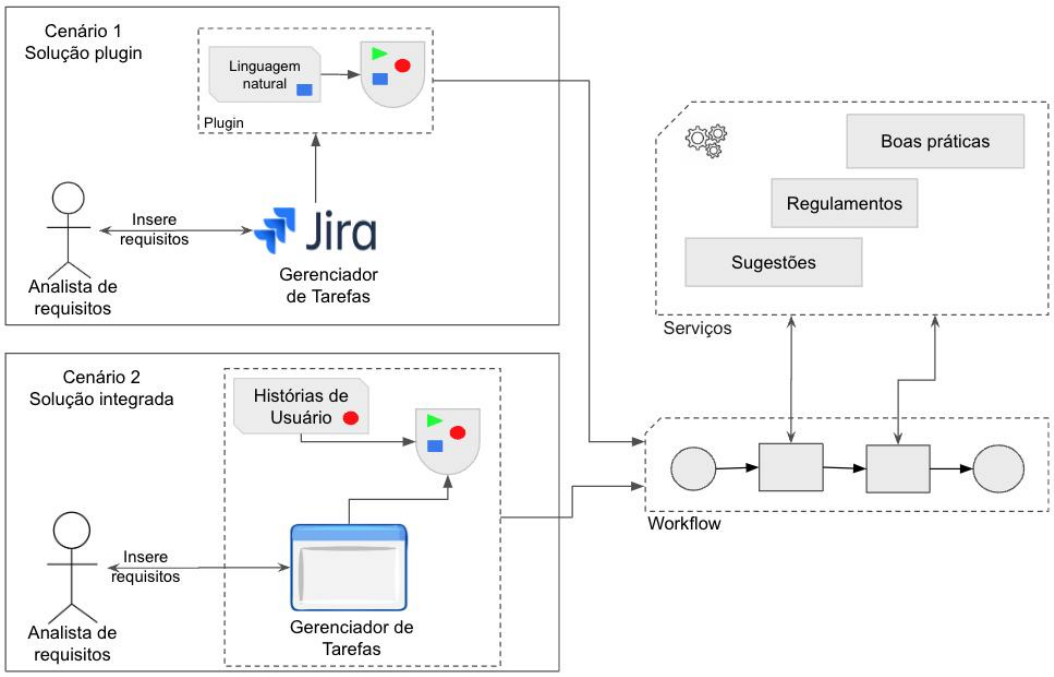


Figura 2 – Cenários de Implementação da Solução Proposta

Pode-se observar que em ambos cenários ilustrados na Figura 2, plugin ou solução integrada, tanto a visão do Workflow quanto dos Serviços permanecem inalteradas. Assim, propõe-se, devido a natureza desacoplada e domínio bem definido, que a visão dos Serviços seja implementada por meio de micro-serviços e que a visão do Workflow permita que seu fluxo seja customizável de maneira a poder definir novas etapas, bem como acoplar novos serviços dependendo do objetivo do fluxo/etapa em questão.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Apoiar a definição de requisitos de software alinhados à proteção de dados, por meio de uma abordagem que possa ser implementada por ferramentas de gerenciamento de requisitos.

1.3.2 Objetivos Específicos

1. Definir um modelo conceitual que especifique aspectos essenciais para ferramentas de gestão de requisitos englobarem proteção de dados pessoais.
2. Definir um workflow que permita customizar etapas e acoplar serviços que processem requisitos de software em prol da proteção de dados.
3. Desenvolver um conjunto de serviços que apoiem a adesão aos regulamentos de proteção de dados pessoais.

4. Avaliar a viabilidade de uso da abordagem, sua capacidade de adaptação e entrega de valor.

1.4 DELIMITAÇÃO DO ESCOPO

Considerando que há diversos regulamentos com foco na proteção de dados, no contexto deste projeto foi considerada a LGPD e alguns artefatos essenciais previstos, como o Relatório de Impacto a Proteção de Dados (RIPD) e o mapa dos dados, ambos tratados no capítulo 2.

Ainda, considerando como foco a LGPD, muitos são os serviços que podem ser desenvolvidos para auxiliar na adequação a lei. Este projeto busca identificar os serviços que podem ser desenvolvidos. Contudo, visando demonstrar a viabilidade da abordagem proposta, apenas um sub-conjunto desses serviços foi desenvolvido.

1.5 METODOLOGIA

1.5.1 Metodologia da Pesquisa

Como metodologia de pesquisa foi utilizada a *Design Science Methodology (DSM)* que, conforme Wohlin e Runeson (2021), fornece orientação prescritiva e frameworks. No entanto, Wohlin e Runeson (2021) destacam que várias instâncias de DSM são propostas e usadas em diferentes campos de pesquisa. Neste trabalho, será adotado o processo de pesquisa descrito por Offermann *et al.* (2009) que propoem um modelo de processo linear, com algumas iterações, o qual foi instanciado e adaptado para o projeto aqui em questão, conforme ilustrado na Figura 3. De acordo com Wohlin e Runeson (2021), a DSM, conforme formulada por Offermann *et al.* (2009), se alinha bem com a pesquisa de engenharia de software e o ciclo geral de pesquisa.

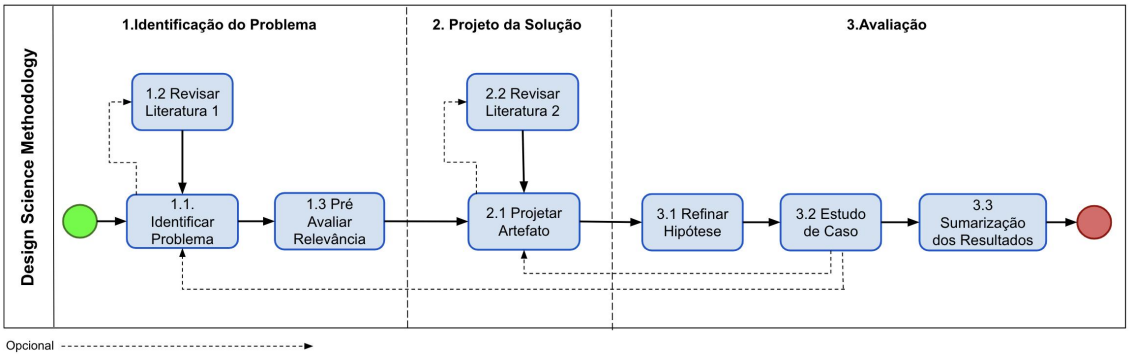


Figura 3 – Design Science Methodology

1.5.2 Procedimentos Metodológicos

Os métodos e resultados esperados com o emprego da metodologia apresentada na Figura 3 podem ser visualizados na Tabela 1.

Etapa	Atividades (OFFERMANN *et al.*, 2009)	Métodos	Resultados
Etapa 1. Identificação do problema	- 1.1 Identificar o problema - 1.2 Revisar a literatura - 1.3 Pré-avaliar a relevância	Mapeamento sistemático da literatura (KITCHENHAM; CHARTERS, 2007) (PETERSEN *et al.*, 2015)	- Capítulo Introdução, incluindo: • descrição do problema (atividade 1.1) • proposta de solução (atividade 1.3) - Capítulo Mapeamento sistemático • análise do estado da arte (atividade 1.2)
Etapa 2. Projeto da solução	- 2.1 Projetar artefato - 2.2 Revisar literatura	- Pesquisa bibliográfica • Proteção de dados (LGPD) - Especificação da abordagem: • modelo conceitual (FURIAN *et al.*, 2015) • arquitetura / serviços (NEWMAN, 2015)	- Capítulo Fundamentação teórica (atividade 2.2) - Capítulo Abordagem proposta (atividade 2.1)
Etapa 3. Avaliação	- 3.1 Refinar hipóteses - 3.2 Estudo de caso	- Implementação da abordagem - GQM (BASILI *et al.*, 1994)	- Capítulo Implementação (atividade 3.2) - Capítulo Avaliação (atividade 3.2)

Tabela 1 – Design Science Methodology

2 FUNDAMENTAÇÃO TEÓRICA

A Verizon, empresa de telecomunicações e comunicações globais que já catalogou mais de 953 mil incidentes, indicou em seu relatório que de todos os incidentes catalogados em 2023, cerca de 50% indicaram violação de dados pessoais (VERIZON, 2023). Ainda, segundo a IBM (2023), a cada 3 vazamentos de dados apenas 1 é identificado pela equipe interna das empresas, o que aponta para a necessidade de um maior investimento nesta área.

Sabendo que as pessoas são avaliadas tendo como base os seus dados pessoais (BIONI; DIAS, 2020), a importância de regulamentos como a LGPD e GDPR para garantir que os dados pessoais sejam devidamente tratados se mostra ainda mais relevante.

Neste cenário, é preciso que empresas incorporem boas práticas e recomendações em seus processos para diminuir as chances ou minimizar o impacto de violações de dados pessoais. Padrões internacionais como a ISO 2700, recomendações trazidas pelo CIS Controls ou o Framework Nist devem ser considerados.

Outro conceito recomendado como boa prática para assegurar a proteção da privacidade e o cumprimento das leis de proteção de dados é o PbD. Introduzido na década de 1990, o PbD propõe a incorporação de medidas de privacidade desde o design inicial do desenvolvimento, garantindo que esteja em todo processo de criação do software (CAVOUKIAN, 2011).

A ideia de considerar a privacidade do usuário desde o início do desenvolvimento do software é tão valorizada que é mencionada no artigo 25º da GDPR, em vigor desde maio de 2018 (EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016). A GDPR estabelece normas para a proteção de dados pessoais, visando proteger os direitos e liberdades fundamentais dos indivíduos, definindo requisitos para organizações que processam dados pessoais de residentes na União Europeia.

No contexto brasileiro, a LGPD foi promulgada em 2020 para assegurar a privacidade dos brasileiros em uma sociedade cada vez mais digital. A LGPD estabelece diretrizes para o tratamento de dados pessoais, buscando evitar que dados pessoais e dados pessoais sensíveis sejam comercializados e que sejam utilizados para os fins diferentes dos coletados, desta forma assegurando a segurança física e moral dos titulares dos dados (SCHRAMM, 2019).

Embora a LGPD não mencione explicitamente o termo PbD, os princípios e requisitos estabelecidos pela legislação brasileira estão alinhados com os fundamentos do PbD. Isto porque, apesar das diferenças entre essas regulamentações e seus contextos legais, tanto a GDPR quanto a LGPD compartilham a visão de que a proteção de dados e a privacidade devem ser consideradas como elementos essenciais desde o início do desenvolvimento de sistemas e serviços, cumprindo, assim, o conceito central

do PbD.

2.1 FUNDAMENTOS E PRINCÍPIOS DA LGPD

A LGPD possui fundamentos com o objetivo de garantir a proteção dos dados pessoais, princípios que são essenciais para proteger a privacidade dos indivíduos e promover a transparência nas práticas de tratamento de dados. Os 10 princípios que norteiam o tratamento de dados pessoais são (BRASIL, 2018):

1. Finalidade: O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos e explícitos, informados ao titular dos dados.
2. Adequação: O tratamento de dados deve ser limitado ao mínimo necessário para o cumprimento da finalidade pretendida, evitando-se o tratamento excessivo ou desnecessário.
3. Necessidade: A coleta e o tratamento de dados pessoais devem ser estritamente necessários para a finalidade pretendida, levando em consideração os meios disponíveis e os riscos envolvidos.
4. Livre acesso: Deve ser garantido ao titular dos dados o acesso facilitado às informações sobre o tratamento de seus dados, incluindo a forma e a duração do tratamento, os agentes de tratamento envolvidos e os direitos do titular.
5. Qualidade dos dados: Os dados pessoais devem ser corretos, completos e atualizados, de acordo com a necessidade e a finalidade para a qual foram coletados.
6. Transparência: O titular dos dados deve ser informado de forma clara, adequada e ostensiva sobre o tratamento de seus dados pessoais, incluindo os agentes de tratamento envolvidos, a finalidade do tratamento, os direitos do titular e as informações de contato do controlador.
7. Segurança: Devem ser adotadas medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acesso não autorizado, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
8. Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos aos titulares dos dados, como a implementação de sistemas internos de governança e de proteção de dados.
9. Não discriminação: O tratamento de dados pessoais não pode ser utilizado para fins discriminatórios ilícitos ou abusivos.

10. Responsabilização e prestação de contas: O controlador de dados é responsável pelo cumprimento da LGPD e deve adotar medidas internas para garantir o cumprimento dos princípios e das obrigações previstas na lei.

2.1.1 Dados Pessoais

Segundo Brasil (2018), dados pessoais são informações que se referem a uma pessoa física identificada ou identificável, ou seja, informações que permitem identificar uma pessoa de forma direta ou indireta são consideradas como dados pessoais. Isso abre muitas possibilidades de informações como nome, endereço, número de telefone, endereço de e-mail, identificação fiscal e outros dados que podem ser usados para identificar uma pessoa específica, como por exemplo: localização ou até mesmo uma postagem na internet. A definição de dados pessoais é fundamental, uma vez que a LGPD visa proteger essas informações contra uso indevido (CNPD, 2023).

2.1.2 Dados Pessoais Sensíveis

Dados Pessoais Sensíveis são uma categoria de dados pessoais que requer uma atenção mais rigorosa, uma vez que seu uso indevido representa um maior risco a privacidade das pessoas. Esses dados incluem informações sobre a origem racial ou étnica, convicções religiosas, opiniões políticas, orientação sexual, informações genéticas e dados de saúde (TSE; ANPD, 2021).

2.1.3 Agentes de Tratamento de Dados

Agentes de Tratamento de Dados desempenham papéis específicos na gestão e processamento de dados pessoais e, neste caso, podendo ser pessoas naturais ou jurídicas, públicas ou privadas que tratam dados pessoais. Os agentes de tratamento podem ser divididos em duas categorias: Controlador e Operador (TSE; ANPD, 2021).

O Controlador é responsável por determinar as finalidades e meios de tratamento de dados pessoais, de maneira geral é ele quem que toma as decisões referentes ao tratamento do dado pessoal. O Operador é quem realiza o tratamento em nome do controlador, seguindo suas orientações e em conformidade com a LGPD (TSE; ANPD, 2021).

2.1.4 Bases Legais

A LGPD traz no texto da lei, mais especificamente no artigo 7, capítulo 2, que se refere ao tratamento de dados pessoais, dez hipóteses que justificam o tratamento de dados pessoais, são elas (BRASIL, 2018):

1. Mediante o fornecimento de consentimento pelo titular;

2. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
3. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
4. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
5. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
6. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
7. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
8. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
9. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou ainda
10. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A escolha da base legal adequada é fundamental, uma vez que determina a legitimidade do tratamento de dados.

2.1.5 Artefatos da LGPD

A LGPD sugere alguns artefatos para apoiar as empresas no caminho para a adequação. Os principais artefatos são: (i) Mapa de Dados; (ii) Aviso de privacidade; (iii) Termo de consentimento; (iv) Política de Segurança da Informação; e (v) Relatório de Impacto à Proteção de Dados.

No apoio ao levantamento do tratamento dos dados pessoais um documento que se destaca é o Mapa dos Dados ou Inventário dos dados. Segundo o artigo 37 da LGPD, "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse"(BRASIL, 2018). Amparado nisto, o governo por meio do Programa Programa de Privacidade e Segurança da Informação (PPSI) e inspirado em modelos

propostos pelas autoridades de proteção de dados da França, Bélgica e Inglaterra, desenvolveu um guia para elaboração do inventário de dados pessoais onde indica as informações mínimas a serem coletadas, são elas (MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, 2023):

1. Identificação do serviço/processo;
2. Identificação dos agentes de tratamento e encarregado;
3. Finalidade do tratamento dos dados pessoais;
4. Categoria de dados pessoais;
5. Categoria dos dados pessoais sensíveis;
6. Categoria de titulares de dados pessoais;
7. Compartilhamento de dados pessoais;
8. Medidas de privacidade e segurança da informação;
9. Transferência internacional de dados pessoais.

Além disto, o guia destaca a importância da manutenção /atualização do inventário e aponta que o Inventário dos Dados contém informações que subsidiam a elaboração do RIPD, essencial para avaliação da conformidade com a LGPD.

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), cuja função é assegurar a conformidade com a LGPD (NASCIMENTO, 2018), o RIPD desempenha um papel fundamental na demonstração do tratamento de dados pessoais em conformidade com a LGPD e na garantia dos direitos dos titulares de dados (PROTEÇÃO DE DADOS (ANPD), 2023). O RIPD é um documento que avalia os riscos e impactos potenciais que o tratamento de dados pessoais pode ter sobre os direitos e liberdades dos titulares dos dados, e é recomendado que seja elaborado antes mesmo do início do tratamento dos dados pessoais.

A GDPR também tem um documento que compartilha alguns conceitos e propósitos com o objetivo de avaliar os riscos e impactos à proteção de dados, o *Data Protection Impact Assessment (DPIA)*. A *Information Commissioner's Office (ICO)*, órgão responsável por proteger as informações pessoais no Reino Unido e encarregado de fazer cumprir a GDPR na União Europeia (ICO, 2023), apresenta em seu guia quais informações são necessárias para o DPIA (ICO, 2022). No Brasil, a ANPD também aponta quais dados são necessários para compor o RIPD (PROTEÇÃO DE DADOS (ANPD), 2023):

1. Identificação dos agentes de tratamento e do encarregado;

2. Outras partes interessadas/envolvidas;
3. Justificativa da necessidade de elaboração do relatório;
4. Projeto/Processo que justifica a elaboração do RIPD;
5. Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;
6. Tratamento de dados;
7. Análise de hipótese legal;
8. Análise de princípios da LGPD;
9. Riscos identificados ao titular;
10. Resultado apurado com base na metodologia utilizada pelo agente de tratamento;
11. Medidas, salvaguardas e mecanismos de mitigação de risco;
12. Comentários e aprovações.

Para o item 6, tratamento dos dados, a ANPD ainda determina que devem conter as seguintes informações: i. Descrição do tratamento; ii. Dados pessoais; iii. Dados pessoais sensíveis; iv. Categorias de titulares; v. Dados de crianças e adolescentes; vi. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento; vii. Fonte de coleta; viii. Finalidade do tratamento; ix. Informar quais são os compartilhamentos internos e externos; e x. Política de armazenamento.

2.1.6 Considerações

Os conceitos apresentados nesta seção, relacionados à LGPD, são cruciais para compreender a relação entre a proteção de dados pessoais e sua aplicação no contexto deste trabalho. Ao implementar um software que leve em consideração a privacidade do usuário, é importante reconhecer que existem várias opções e abordagens possíveis.

É fundamental ter em mente que, durante o desenvolvimento de software, nem sempre é uma realidade que analistas de sistemas, analistas de requisitos, desenvolvedores e outros membros da equipe possuam o conhecimento necessário para considerar todas as complexidades relacionadas à privacidade dos dados. Além disso, muitas empresas, especialmente as de pequeno e médio porte, podem não ter uma estrutura adequada para oferecer suporte do ponto de vista legal e de proteção de dados, o que torna o processo de integração da privacidade no desenvolvimento mais desafiador.

Compreender os princípios e requisitos da LGPD é crucial, pois eles fornecem as bases legais e conceituais para garantir a proteção dos dados pessoais em um software. Reconhecendo as limitações de conhecimento e recursos dentro das equipes de desenvolvimento e das empresas, é possível explorar estratégias e soluções para enfrentar os desafios da privacidade de dados de forma eficaz.

Em resumo, incorporar um processo de levantamento de requisitos que inclua as informações apresentadas nesta seção pode facilitar a adequação aos regulamentos, como a LGPD, e, como consequência, proporcionar mais privacidade aos usuários do software.

3 MAPEAMENTO SISTEMÁTICO DA LITERATURA

No estudo, “A Systematic Mapping Study on Privacy by Design in Software Engineering”, (MORALES-TRUJILLO *et al.*, 2019) investigaram a proteção de dados no ciclo de desenvolvimento de software. Contudo, o contexto está mais relacionado a trabalhos que utilizam PbD, ou seja, por um lado está restrito à abordagem por PbD e, por outro, é mais genérico por considerar toda área de engenharia de software. Ainda, a execução da pesquisa foi realizada em 2017, anterior ao início da vigência das leis e regulamentações.

Assim, o presente estudo mapeou as abordagens de engenharia de requisitos que tem apoiado o desenvolvimento de soluções com foco na proteção de dados pessoais. Para tanto, tomou-se como base as orientações de Kitchenham e Charters (2007).

3.1 MÉTODO

3.1.1 Questões de Pesquisa

O objetivo deste mapeamento foi identificar processos, métodos, técnicas e ferramentas para engenharia de requisitos de software que apoiam a proteção de dados pessoais, respondendo às seguintes questões:

1. Quais abordagens de engenharia de requisitos contribuem para a proteção de dados pessoais?
2. Quais normas/regulamentos embasam cada abordagem identificada?
3. As abordagens foram desenvolvidas para algum domínio específico?
4. As abordagens foram empregadas/avaliadas em contexto real (em empresas)?
5. Como as soluções propostas foram avaliadas?

3.1.2 Processo de Busca

Para a construção da *string* executada nos mecanismos de busca foram considerados dois critérios como ponto de partida: (i) a área de engenharia de requisitos; e (ii) termos, normas, leis e regulamentos relacionados à proteção de dados pessoais. Com base nestas duas partes-chaves foi realizada a construção da *string* de busca, por meio da união dos termos e do uso de sinônimos, conforme segue:

(“software requirements” OR “engineering requirements” OR “functional requirements” OR “privacy requirements” OR “non-functional requirements”) AND (“LGPD” OR “GDPR” OR “data privacy” OR “27701” OR “privacy protection” OR “data protection” OR “privacy by design”)

A *string* foi adaptada para os mecanismos de busca da IEEE Xplore [1], ACM Digital Library [2] e SCOPUS [3]; este último indexa várias bases de dados, como por exemplo: Elsevier, Wiley e Springer.

3.1.3 Critérios de inclusão e exclusão

Os critérios de inclusão e exclusão aplicados foram:

1. Estudos que respondem às perguntas de pesquisa **(Inclusão)**: Deverá conter no estudo analisado, posicionamento dos autores, de maneira clara, de que se trata de uma abordagem da engenharia de requisitos com foco em proteção de dados;
2. Estudos publicados a partir de 2018 **(Inclusão)**: considerando que os regulamentos de proteção de dados foram propostos a partir do mencionado ano;
3. Estudos duplicados **(Exclusão)**; e
4. Livros, editoriais, tutoriais, painéis, sessões de posters, prefácios, opiniões, resumos, cartas, apresentações de slides, relatórios técnicos, dissertação, tese, trabalho com menos de 5 páginas, ou qualquer trabalho classificado como Grey Literature[4] **(Exclusão)**;

3.1.4 Procedimento de seleção

A Figura 4 apresenta o fluxo para o procedimento de seleção dos estudos, em seguida são detalhados os passos executados.

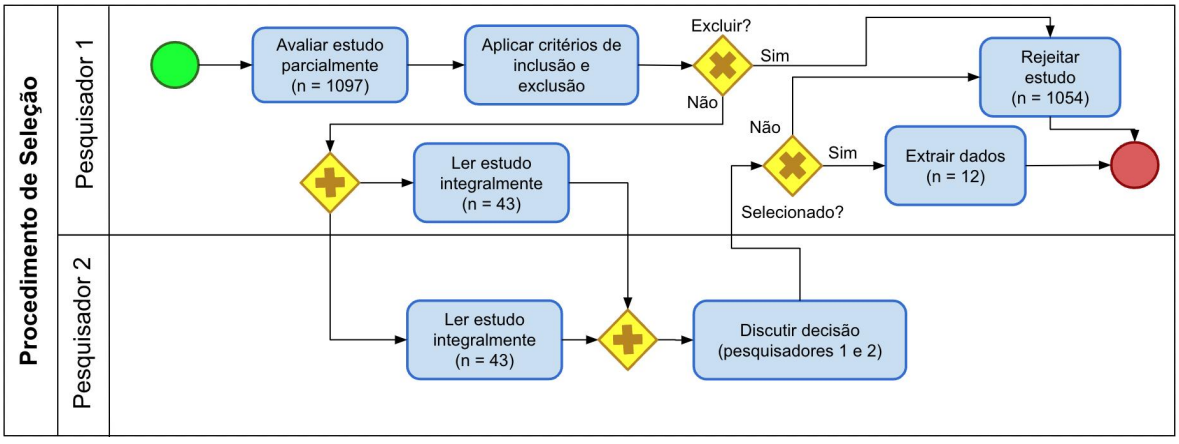


Figura 4 – Fluxo para o Procedimento de Seleção dos Estudos

[1] https://ieeexplore.ieee.org/
[2] https://dl.acm.org
[3] https://www.scopus.com/
[4] Publicações consideradas não convencionais e não comerciais, difíceis de encontrar em canais tradicionais de distribuição e com controle bibliográfico ineficaz, demandando mais pesquisa para recuperá-las, sendo comum não serem incluídas em bibliografias e catálogos(BOTELHO; CRUZ DE OLIVEIRA, 2008).

1. **Avaliar estudo parcialmente**: Leitura de título, resumo e conclusão - realizado pelo pesquisador 1;
2. **Aplicar critérios de inclusão e exclusão**: Aplicação dos critérios de inclusão e exclusão, definidos na seção 3.1.3 - realizado pelo pesquisador 1;
3. **Ler estudo integralmente**: Leitura integral do texto do estudo - realizado pelos pesquisadores 1 e 2;
4. **Discutir decisão**: Discussão quanto a pareceres divergentes - realizado pelos pesquisadores 1 e 2;
5. **Extrair dados**: Extração dos dados do estudo de forma que sirvam para contextualizar as respostas às questões de pesquisa - realizado pelo pesquisador 1 e revisado pelo pesquisador 2; e
6. **Rejeitar estudo**: Etapa que remove o estudo do processo.

Em setembro de 2021, as strings de busca foram executadas nas fontes de busca selecionadas para o mapeamento. A Tabela 2 apresenta os resultados do processo de seleção.

Fonte	Resultado busca	Selecionados
Scopus	500	8
IEEE	229	1
ACM	368	3

Tabela 2 – Resultados do processo de seleção

A coluna “Resultado Busca” contém os estudos obtidos na execução da *string* nos mecanismos de busca, sendo que um total de 1097 estudos foram retornados. Dos estudos encontrados, 91 foram rejeitados por serem duplicados, 963 foram excluídos devido aos critérios de inclusão e exclusão (em uma primeira rodada com leitura parcial). Os 43 restantes passaram pela etapa de leitura integral de dois pesquisadores. Por fim, 12 estudos foram selecionados para o processo de extração dos dados.

3.1.5 Extração dos Dados

Para cada estudo selecionado, buscou-se extrair os dados apresentados na Tabela 3 para responder às questões de pesquisa. Após a extração dos dados, os resultados foram organizados em tabelas para facilitar a análise.

Id	**Descrição**
Título	Título do estudo
Ano	Ano de publicação
País	País de publicação
Classificação	Journal, conferência ou Workshop
Regulamento	LGPD, GDPR ou outros regulamentos
Padrões	ISO27701, ISO27002 ou outros
Solução	Técnica, Ferramenta, Catálogo e etc.
Abordagem	Nome da abordagem
Descrição	Breve descrição da abordagem
Domínio	Qual o domínio da abordagem (Ex:Saúde, Educação)
Aplicação	Abordagem aplicada no meio acadêmico ou empresa?
Avaliação	Como foi realizada a avaliação
Método	Questionário, Estudo de caso e etc.
Estudo de caso	Caso realizado um estudo de caso, qual o contexto?
Input e Output	Para cada solução, quais artefatos de entrada e saída?

Tabela 3 – Campos do formulário de extração de dados

A Tabela 4 apresenta os estudos incluídos no mapeamento, uma classificação do tipo de solução apresentada e o nome (quando existente). A coluna Id indica a referência de cada estudo.

Id	**Autor**	**Ano**	**Tipo de solução**	**Nome da solução**
[3]	(LI *et al.*, 2018)	2018	Ferramenta	Coconut
[8]	(AYALA-RIVERA; PASQUALE, 2018)	2018	Processo	GuideME
[12]	(SILVA JUNIOR *et al.*, 2018)	2018	Método	Método para Elicitação de Requisitos de Privacidade em Computação Ubíqua
[9]	(SILVA *et al.*, 2018)			
[1]	(BARTOLINI *et al.*, 2019)	2019	Ferramenta	Plugin Eclipse
[7]	(STACH; STEIMLE, 2019)	2019	Ferramenta	EPICUREAN
[10]	(MANNA *et al.*, 2019)	2019	Linguagem	EDPRL
[2]	(BALDASSARRE *et al.*, 2020)	2020	Ferramenta	VIS-PRIZE
[6]	(ZINSMAIER *et al.*, 2020)	2020	Processo	Processo de Zinsmaier et al.
[11]	(KNEUPER, 2020)	2020	Técnica	Técnica de Kneuper
[5]	(FERREYRA *et al.*, 2020)	2020	Método	PDP-ReqLite
[4]	(ANSARI *et al.*, 2021)	2021	Método	P-STORE

Tabela 4 – Estudos primários selecionados

3.2 RESULTADOS

Esta seção responde às questões de pesquisa apresentadas na Seção 3.1.1, a partir da análise dos 12 estudos listados na Tabela 4.

3.2.1 Quais abordagens de engenharia de requisitos contribuem para a proteção de dados pessoais?

Observa-se na Tabela 4 que dentre os estudos encontrados há quatro ferramentas, três métodos, dois processos, uma técnica e uma linguagem. As abordagens propostas são brevemente descritas nas seções seguintes.

3.2.1.1 Coconut

Coconut é um plug-in para o Android Studio que ajuda os desenvolvedores a lidar com os requisitos de privacidade, engajando os desenvolvedores a pensar sobre privacidade durante o processo de desenvolvimento de aplicativos móveis e fornecendo feedback em tempo real sobre possíveis problemas de privacidade (LI *et al.*, 2018).

3.2.1.2 GuideMe

GuideMe é uma abordagem sistemática que apoia a elicitação de requisitos de software e os vincula às obrigações de proteção de dados da GDPR. O processo consiste em seis passos para passar as demandas abstratas impostas no regulamento GDPR para requisitos técnicos que podem ser implementados em sistemas. Focada na GDPR, tem como ponto de partida uma auditoria dos dados que serão ou que estão sendo tratados, entregando ao fim um documento de especificação de requisitos de privacidade (AYALA-RIVERA; PASQUALE, 2018).

3.2.1.3 Método para Elicitação de Requisitos de Privacidade em Computação Ubíqua

Em (SILVA JUNIOR *et al.*, 2018), os autores propõem um método de elicitação de requisitos de privacidade em computação ubíqua que leva em conta as expectativas e desejos dos usuários. O método é composto de sete passos, nos quais são utilizadas variadas técnicas e ferramentas, a saber: (1) desenvolvimento e aplicação de questionário; (2) desenvolvimento de personas; (3) desenvolvimento de cenários; (4) seleção de usuários; (5) apresentação e discussão do cenário; (6) re-design do cenário e construção de protótipos; e (7) aplicação de questionário pós-experimento. Em (SILVA *et al.*, 2018), os autores apresentam a utilização do método em um cenário diferente; a identificação de erros ou barreiras enfrentadas pelos participantes na aplicação do método; e a observação da percepção e sentimento de utilidade do método para os participantes.

3.2.1.4 Plugin Eclipse

Os autores (BARTOLINI *et al.*, 2019) descrevem uma solução baseada em um modelo legal do GDPR para enriquecer processos de negócios modelados em

BPMN com anotações que expressam requisitos de proteção de dados. Para avaliar a viabilidade da abordagem proposta, a metodologia foi prototipada em um plug-in Eclipse desenvolvido utilizando BPMN2 *Modeler*.

3.2.1.5 EPICUREAN

Usa técnicas de modelagem e mineração de dados para determinar e recomendar configurações de privacidade apropriadas ao usuário. Para tanto, os autores (STACH; STEIMLE, 2019) (i) estabeleceram um processo de 3 fases para elicitação de requisitos de privacidade, denominado EPICUREAN; (ii) introduziram uma técnica de modelagem hierárquica para descrever qual conhecimento pode ser derivado de quais dados brutos (fase de preparação); (iii) apresentaram um processo para especificar configurações de privacidade e saber quais configurações de privacidade são relevantes para qual usuário (fase de treinamento); (iv) descreveram um processo para encontrar configurações de privacidade adequadas aos requisitos dos usuários e sugerir outras configurações de privacidade (fase de aplicação); e (v) integraram EPICUREAN ao PATRON (sistema de privacidade para aplicações IoT que maximiza as funcionalidades de uma aplicação, enquanto minimiza os dados privados divulgados).

3.2.1.6 EDPRL

Em (MANNA *et al.*, 2019) é descrito o projeto de uma linguagem para a especificação de requisitos de privacidade de dados, denominada *Enterprise Data Privacy Requirement Language (EDPRL)*. O objetivo da linguagem é auxiliar na especificação automatizada dos requisitos de privacidade e na identificação subsequente dos controles de privacidade. A linguagem é baseada em JSON e suas construções estão em conformidade com os requisitos específicos de ativos da norma ISO 29151:2017, de modo a refletir as melhores práticas do setor.

3.2.1.7 VIS-PRIZE

Trata-se de uma base de conhecimento, a Privacy Knowledge Base (PKB), e o protótipo VIS-PRISE (Visually Inspection to Support Privacy and Security), uma ferramenta visual que auxilia na decisão dos desenvolvedores de integrar os requisitos de privacidade e segurança em todas as fases de desenvolvimento de software. A base de conhecimento PKB formaliza os relacionamentos entre 5 elementos-chave de privacidade: Privacidade por Design, Estratégias de Design de Privacidade, Padrão de Privacidade, Vulnerabilidades e Contexto (BALDASSARRE *et al.*, 2020).

3.2.1.8 Processo de Zinmaier et al.

Esta é uma abordagem de engenharia de requisitos focada em privacidade que tem como ponto de partida um modelo de ameaças produzido pelo método STRIDE, e que envolve os *stakeholders* desde o início do projeto com o objetivo de compilar um documento detalhado de especificação de requisitos. A abordagem inclui a aplicação de metodologias de classificação de risco e ameaça, uma técnica para derivar requisitos técnicos de textos legais, uma etapa para evitar a redundância de requisitos e uma forma de garantir a conformidade com a GDPR, mantendo a rastreabilidade dos requisitos (ZINSMAIER *et al.*, 2020).

3.2.1.9 Técnica de Kneuper

(KNEUPER, 2020) traduz os requisitos resultantes dos princípios da GDPR para requisitos de software. A proposta lista uma série de requisitos de software agrupados pelos princípios da GDPR com objetivo de apoiar tanto desenvolvedores de software quanto analistas de requisitos. A proposta traz requisitos que devem ser considerados para qualquer sistema, contudo, ainda é preciso uma análise por especialistas de maneira a considerar as especificidades de cada sistema, como por exemplo, a finalidade do sistema que está sendo desenvolvido (KNEUPER, 2020).

3.2.1.10 PDP-ReqLite

A PDP-ReqLite é uma metodologia para elicitar requisitos de privacidade e proteção de dados, propondo que seja possível também garantir adequação à GDPR. A metodologia permite como *input* do processo: (i) o RDFD (Diagrama de Fluxo de Dados de Requisitos), que descreve os requisitos relacionados ao processamento e armazenamento de dados e os fluxos de informações entre esses requisitos; (ii) o PID (Diagrama de Informações Pessoais), que identifica quais dados dos *stakeholders* serão processados pelo sistema e as relações entre esses dados; e (iii) também aceita os artefatos de entrada do ProPAn (Problem-based Privacy Analysis), método a partir do qual foi inspirado (FERREYRA *et al.*, 2020).

3.2.1.11 P-STORE

Trata-se de uma metodologia sistemática de 10 passos que envolve os *stakeholders* na definição dos requisitos de privacidade, possuindo também técnicas para definir, categorizar e priorizar as ameaças encontradas para, então, gerar um documento de especificação de requisitos focados em privacidade (ANSARI *et al.*, 2021).

3.2.2 Quais normas/regulamentos embasam cada abordagem identificada?

Seis estudos explicitaram que utilizaram como embasamento a GDPR, conforme pode-se observar na Tabela 5. Observou-se que um dos estudos utilizou a norma ISO 29151:2017 como referencial. A ISO/IEC 29151:2017 estabelece objetivos de controle, controles e diretrizes para implementação de controles, para atender aos requisitos identificados por uma avaliação de risco e impacto relacionado à proteção de dados de identificação pessoal.

Id	Autor	Nome da solução	Embasamento
[3]	(LI *et al.*, 2018)	Coconut	-
[8]	(AYALA-RIVERA; PASQUALE, 2018)	GuideME	GDPR
[12]	(SILVA JUNIOR *et al.*, 2018)	Método para Elicitação de Requisitos de	-
[9]	(SILVA *et al.*, 2018)	Privacidade em Computação Ubíqua	
[1]	(BARTOLINI *et al.*, 2019)	Plugin Eclipse	GDPR
[7]	(STACH; STEIMLE, 2019)	EPICUREAN	GDPR
[10]	(MANNA *et al.*, 2019)	EDPRL	ISO 29151
[2]	(BALDASSARRE *et al.*, 2020)	VIS-PRIZE	-
[6]	(ZINSMAIER *et al.*, 2020)	Processo de Zinsmaier et al. A	GDPR
[11]	(KNEUPER, 2020)	Técnica de Kneuper	GDPR
[5]	(FERREYRA *et al.*, 2020)	PDP-ReqLite	GDPR
[4]	(ANSARI *et al.*, 2021)	P-STORE	-

Tabela 5 – Embasamento dos estudos selecionados

3.2.3 As abordagens foram desenvolvidas para algum domínio específico?

O EPICUREAN (STACH; STEIMLE, 2019) foi concebido para atuar juntamente com o PATRON, que é um sistema para privacidade em ambientes de IOT. Contudo, os autores informam que o conceito pode ser transferido para qualquer sistema de privacidade. Neste mesmo contexto, de computação ubíqua, tem-se o método para elicitação de requisitos de privacidade proposto por (SILVA JUNIOR *et al.*, 2018) (SILVA *et al.*, 2018). Já Coconut, descrito em (LI *et al.*, 2018), tem como foco a privacidade no contexto de aplicativos móveis. Todas as demais soluções se propõem serem de domínio geral, sem focar em domínios específicos.

3.2.4 As abordagens foram empregadas/avaliadas em contexto real (em empresas)?

A Tabela 6 demonstra que oito soluções foram avaliadas em ambientes acadêmicos e apenas uma solução foi avaliada em ambiente real, ou seja, no contexto de uma empresa. Dois estudos não reportaram aplicação. O único estudo avaliado em

contexto real, envolveu 10 desenvolvedores juniores (sem conhecimentos e competências específicas sobre segurança e privacidade), funcionários de uma *spin-off* da universidade.

Id	Contexto	Estudo de Caso
[3]	Academia	App previsão do tempo
[8]	Academia	* Sistema de controle de acesso biométrico * Sistema de informacão acadêmico
[12][9]	Academia	* Sistema de sensoriamento domiciliar de consumo de água e energia elétrica * Aplicativo de compartilhamento de viagens
[1]	Academia	Serviço de entrega por terceiros
[7]	Academia	Serviços inteligentes de saúde
[10]	-	-
[2]	Empresa	Re-engenharia de dois sistemas legados
[6]	Academia	Setor de Logística
[11]	-	-
[5]	Academia	Smart Grid
[4]	Academia	Sistema de gerenciamento para área da saúde

Tabela 6 – Contexto de avaliação dos estudos selecionados

3.2.5 Como as soluções propostas foram avaliadas?

Conforme demonstra a Figura 5, dez dos doze estudos foram avaliados por meio de estudos de caso, sendo que seis contaram com análise por especialistas, três aplicaram um questionário após o estudo e um realizou avaliação de usabilidade. Os dois restantes foram soluções propostas e não realizaram avaliação.

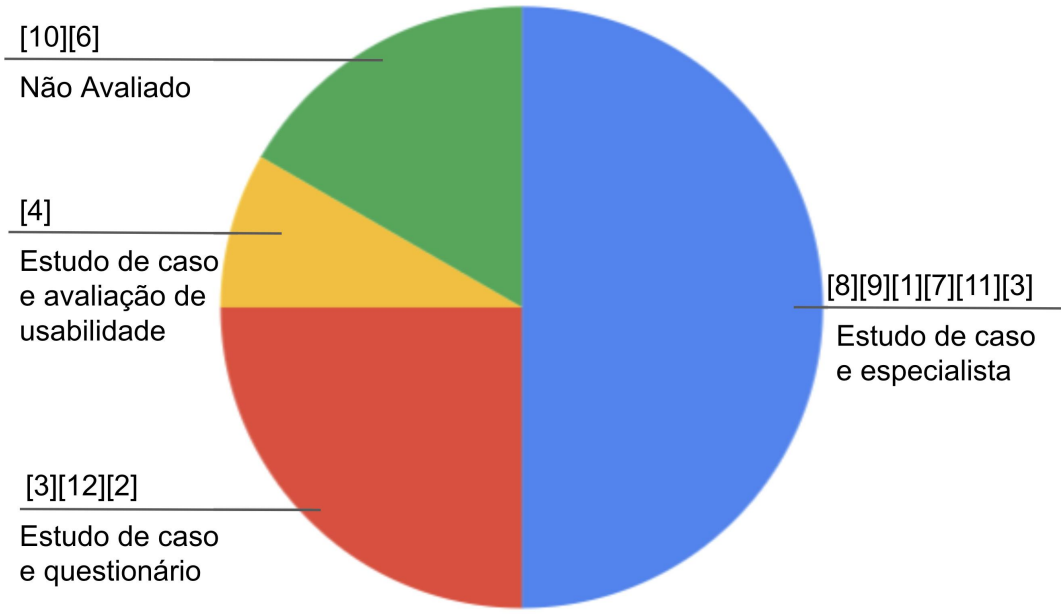


Figura 5 – Método de Avaliação dos Estudos

Importante também considerar os critérios de avaliação abordados pelos diferentes estudos, pois podem ser referencial para futuras pesquisas:

- Coconut (LI *et al.*, 2018): A avaliação explorou princípios de privacidade relacionados a granularidade da localização, comunicação de dados com terceiros/-provedor de serviço, monetização (integração de anúncio utilizando a biblioteca AdMob do Google) e análises de histórico de localização.
- GuideMe(AYALA-RIVERA; PASQUALE, 2018): Foi aplicado o questionário de avaliação SMART que verifica se os requisitos estavam corretos em termos de como eles foram formulados.
- Método para Elicitação de Requisitos de Privacidade em Computação Ubíqua (SILVA JUNIOR *et al.*, 2018): Explorou princípios de privacidade como compartilhamento e retenção de dados de consumo domiciliar com terceiros, presença física de sensores, conflito entre utilidade do sistema e a proteção dos dados pessoais.
- EPICUREAN (STACH; STEIMLE, 2019): Descreve 6 requisitos focados na simplicidade, no que se refere ao envolvimento dos usuários em mecanismos de elicitação de requisitos de privacidade.
- VIS-PRIZE(BALDASSARRE *et al.*, 2020): A avaliação buscou: (i) identificar os princípios de PbD violados pela vulnerabilidade; (ii) identificar as estratégias de PbD a serem implementadas no sistema para respeitar os princípios; (iii) identificar os padrões de privacidade que fundamentam as estratégias de PbD; (iv) identificar o Componente de Estratégias de Dados a ser implementado na arquitetura-alvo para reengenharia do sistema do ponto de vista da privacidade; (v) identificar as Estratégias de Componentes de Processos a serem implementadas na arquitetura-alvo para reprojetar o sistema do ponto de vista da privacidade. Cada tarefa foi avaliada com aplicação do questionário SUS (System Usability Scale) para avaliar a usabilidade da solução.
- Processo de Zinsmaier et al. (ZINSMAIER *et al.*, 2020): Propuseram identificar os interesses das partes em relação aos princípios de segurança - confidencialidade, integridade e disponibilidade, bem como os princípios de privacidade - transparência, desvinculação (*unlinkability*), minimização de dados e intervenção do titular dos dados. Os cenários de ameaça foram avaliados de acordo com os riscos associados, usando a metodologia DREAD.
- P-STORE (ANSARI *et al.*, 2021): avaliado por um estudo de caso de um projeto de sistema de saúde digital. Além disso, usaram a técnica fuzzy AHP com fuzzy TOPSIS para a avaliação de usabilidade de diferentes requisitos de privacidade.

O estudo demonstrou que a abordagem P-STORE tem a capacidade de obter requisitos de privacidade mais eficientes e permite que o engenheiro de software organize os requisitos de privacidade de forma eficaz.

3.3 DISCUSSÃO

Pode-se observar pelos estudos selecionados que não há uma predominância entre as abordagens pesquisadas, ou seja, tem-se tanto abordagens baseadas em métodos e processos para auxiliar na elicitação de requisitos de privacidade, quanto ferramentas consistindo em soluções com algum nível de automatização. Contudo, quando a opção dos pesquisadores é por desenvolver uma ferramenta, observa-se que plugins tem se destacado (LI *et al.*, 2018)(BARTOLINI *et al.*, 2019).

Importante também observar (vide Figura 6) que a maioria das soluções propõem como entrada necessidades específicas, especificações ou dados; e como saída predominante tem-se requisitos de privacidade. Na análise do gráfico da Figura 6, observou-se como entradas:

- Código-fonte: considerando chamadas de API e Java *Annotations* (LI *et al.*, 2018).
- Dados: especificação de informações sobre o dado, como por exemplo, tipo do dado, contexto e formato (AYALA-RIVERA; PASQUALE, 2018).
- Necessidades específicas: categoria que abrange técnicas diversas para obter requisitos de usuário, como por exemplo, modelos mentais (SILVA *et al.*, 2018)(SILVA JUNIOR *et al.*, 2018), interesses dos *stakeholders* (ZINSMAIER *et al.*, 2020) e objetivos do sistema (ANSARI *et al.*, 2021).
- Especificação: abrange algum artefato de modelagem, como por exemplo, modelagem de negócio (BARTOLINI *et al.*, 2019) ou Requirements Data-Flow Diagram (RDFD) e Personal Information Diagram (PID) (FERREYRA *et al.*, 2020).
- Requisitos de privacidade propriamente dito.
- Vulnerabilidades.
- GDPR (o próprio regulamento).

As saídas das soluções, em sua maioria, são requisitos de privacidade (SILVA *et al.*, 2018)(SILVA JUNIOR *et al.*, 2018)(MANNA *et al.*, 2019)(ZINSMAIER *et al.*, 2020)(FERREYRA *et al.*, 2020). Algumas pesquisas têm focado em fornecer recomendações sobre gerenciamento de dados de acordo com o GDPR (BARTOLINI *et al.*, 2019) ou de configurações de privacidade (STACH; STEIMLE, 2019) ou ainda alertas em tempo de programação (LI *et al.*, 2018). Observa-se também pesquisas mais amplas, tendo como saída um documento, como por exemplo, plano de implementação

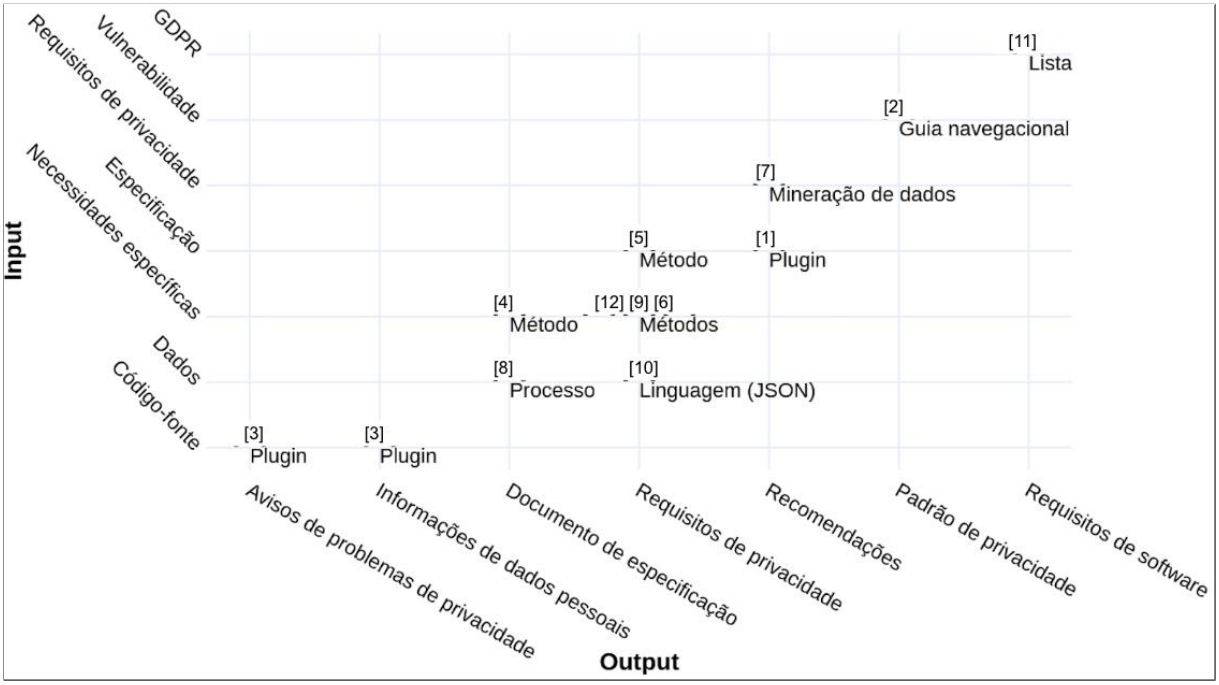


Figura 6 – Análise dos input e output de cada solução

(AYALA-RIVERA; PASQUALE, 2018) ou documento de especificação de requisitos de segurança (ANSARI *et al.*, 2021).

Contudo, há de se ressaltar que a aplicação das soluções tem ficado restrita ao ambiente acadêmico, com apenas um estudo aplicado - apenas para avaliação - em um ambiente real (BALDASSARRE *et al.*, 2020). Este fato aponta para a necessidade de amadurecimento das pesquisas ou maior proximidade academia-empresa, para que as soluções pesquisadas de fato colaborem para aumento da privacidade e proteção de dados das soluções de mercado.

No que tange o amadurecimento das pesquisas, observou-se que estudo de caso é a forma predominante de avaliação. Ressalta-se, neste aspecto, não haver sinergia entre os procedimentos de avaliação. Pode-se observar pelo listado na Seção 3.2.5 que há diferentes instrumentos e critérios empregados nas avaliações. Neste ponto, esta pesquisa colabora em apontar que a elaboração de um método de avaliação na área de privacidade e proteção de dados é uma oportunidade de pesquisa em aberto.

Observa-se também que os estudos de caso escolhidos para aplicação das soluções são bastante distintos (ver Tabela 6). Este fato, analisado em conjunto com a predominância de soluções de domínio geral (Seção 3.2.3), demonstra que, apesar de requisitos de privacidade e proteção de dados serem analisados no contexto da aplicação, as pesquisas buscam soluções genéricas, em sua maioria, sem focar em domínios específicos. Mesmo quando a pesquisa tem um foco específico, ainda assim são de contextos bem genéricos, como por exemplo, aplicativos móveis (LI *et al.*, 2018) ou computação ubíqua (SILVA *et al.*, 2018) (STACH; STEIMLE, 2019). Não foram

encontrados estudos apenas para domínios específicos, como por exemplo, redes sociais e saúde digital. Deste fato, levanta-se o questionamento se soluções mais específicas não seriam de mais fácil aplicabilidade.

3.4 AMEAÇAS À VALIDADE

Com relação às ameaças sobre a validade do estudo, (PETERSEN *et al.*, 2015) destacam alguns tipos de validades a serem enfatizadas sobre os estudos de mapeamento sistemático: descritiva, teórica, de generalização e interpretativa.

A validade descritiva está relacionada ao fato das informações obtidas com um mapeamento serem descritas de maneira precisa e objetiva. Para reduzir essa ameaça, os dados extraídos pelo pesquisador 1 foram revisados pelo pesquisador 2. Sendo assim, as ameaças à validade descritiva relacionadas ao mapeamento deste trabalho são consideradas sob controle.

A validade teórica aborda questões relacionadas à capacidade de obtenção das informações que são pretendidas ao realizar o MSL. Por exemplo, a seleção de informações que são contrárias às pretendidas pelo mapeamento pode afetar a validade do estudo. Com o intuito de amenizar essa possível ameaça de validade, termos relevantes foram selecionados e as chaves de busca foram elaboradas de acordo os temas envolvidos (Engenharia de Requisitos e Privacidade). O planejamento do mapeamento foi elaborado pelo pesquisador 1 e revisado por 2 especialistas (um da área de Engenharia de Software e outro da área de Segurança), ambos com experiência em mapeamentos sistemáticos. Dessa maneira, as ameaças referentes à validade teórica também puderam ser minimizadas.

A validade relacionada à generalização se baseia nos aspectos de formalização dos documentos utilizados para registro nos processos de planejamento. Ameaças possíveis relacionadas à validade interpretativa também foram reduzidas neste trabalho devido ao fato das etapas de planejamento e execução serem elaboradas e executadas pelo pesquisador 1 e, posteriormente, revisadas pelos 2 pesquisadores com experiência em estudos sistemáticos.

Em relação à replicabilidade do processo de mapeamento sistemático, todo o processo foi documentado em um relatório detalhado, com descrição dos estágios e suas entradas e saídas, assim como todos os registros das informações extraídas dos trabalhos abordados nesse mapeamento (trabalhos recuperados, excluídos e incluídos) estão armazenadas em uma ferramenta especializada para apoio a estudos sistemáticos, a citar, a ferramenta StArt [5].

[5] `http://lapes.dc.ufscar.br/tools/start_tool`

3.5 CONSIDERAÇÕES FINAIS

Esta seção apresentou um mapeamento sistemático que teve como objetivo investigar soluções da área de Engenharia de Requisitos para apoio a proteção de dados pessoais. O mapeamento também gerou um artigo publicado em outubro de 2022 intitulado *How Has Requirements Engineering Supported Data Protection* (DA SILVA *et al.*, 2022b).

Um conjunto de 1097 publicações foi analisado, sendo 12 selecionados como publicações relevantes para o objetivo do mapeamento. Foram apresentadas 11 soluções distintas, abordando um conjunto de 7 categorias de artefatos de entrada e 7 categorias de saída. As pesquisas tem como entradas predominantes necessidades específicas para sistemas de diversos domínios. Já a saída predominante das soluções pesquisadas são requisitos de privacidade.

Considerando os resultados obtidos, algumas oportunidades no campo da proteção de dados e engenharia de software se destacaram. Primeiramente, constatou-se a ausência de ferramentas que ofereçam suporte à proteção de dados a partir dos requisitos de software, especialmente em conformidade com regulamentações como o GDPR e a LGPD. Além disso, não foram encontradas ferramentas que auxiliem diretamente na conformidade com a LGPD a partir da perspectiva dos requisitos de software. Também é evidente a falta de uma abordagem genérica que possa ser customizada para se adaptar às particularidades de diversos segmentos ou às constantes evoluções das regulamentações.

Diante disto, o presente trabalho colabora ao propor uma abordagem de engenharia de software que permite ser customizada. Essa abordagem utiliza requisitos de software como *input* para conduzir e orientar membros da equipe de desenvolvimento com relação à proteção de dados, gerando alertas e sugestões que visam aprimorar e adequar esses requisitos à proteção de dados antes mesmo de serem implementados. A contribuição do trabalho reside na capacidade de preencher lacunas existentes, fornecendo uma estrutura que apoia o desenvolvimento de software em conformidade com regulamentações de proteção de dados.

4 ABORDAGEM PROPOSTA

4.1 VISÃO GERAL

Como já apresentado no Capítulo 1, a abordagem proposta por este trabalho tem como base três visões que são apresentadas na Figura 7. Para recapitular, a Visão dos Requisitos define um modelo conceitual que deve ser adotado por sistemas que gerenciam requisitos e desejam seguir a abordagem proposta, tal modelo define como submeter um requisito para ser analisado e como receber as análises geradas na Visão do Workflow.

A Visão do Workflow é dotada de um fluxo customizável que transporta um requisito de software por etapas que executam análises específicas e que vão propagando esta análise até que chegue ao fim do fluxo e, para isto, contam com apoio da Visão de Serviços, que disponibiliza um conjunto de micro-serviços com objetivos bem definidos e que podem ser utilizados pelas etapas da visão do Workflow.

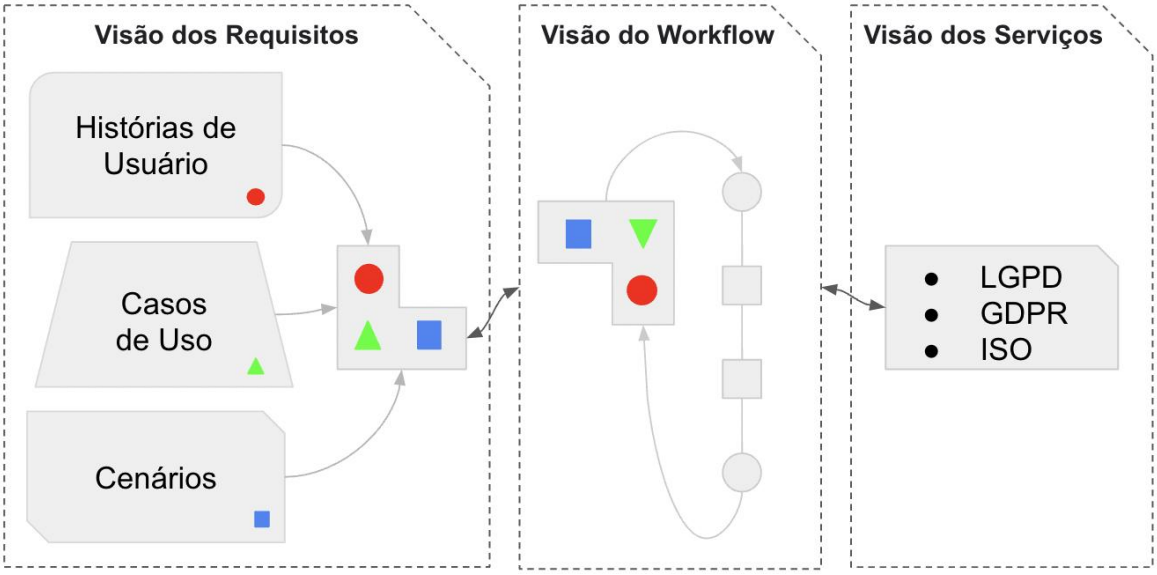


Figura 7 – Visão geral conceitual da abordagem proposta

Para cada uma destas visões algumas definições são necessárias, como: 1) Qual modelo conceitual será disponibilizado para as soluções que pretendem aderir à abordagem?; 2) Quais etapas do Workflow serão implementadas?; e 3) Quais serviços serão desenvolvidos para suportar as etapas previstas para o Workflow? Para tanto, estas definições são elaboradas nas próximas seções.

4.2 VISÃO DOS REQUISITOS

Esta visão é responsável por estabelecer a comunicação entre o sistema aderente e a Visão do Workflow. É por meio do modelo proposto nesta visão que o requisito de software é encaminhado ao workflow para análise. Além disto, o modelo define uma

forma de tratar os eventos gerados no workflow. A Figura 8 apresenta o modelo conceitual que deve ser implementado pelo sistema que deseja aderir à abordagem.

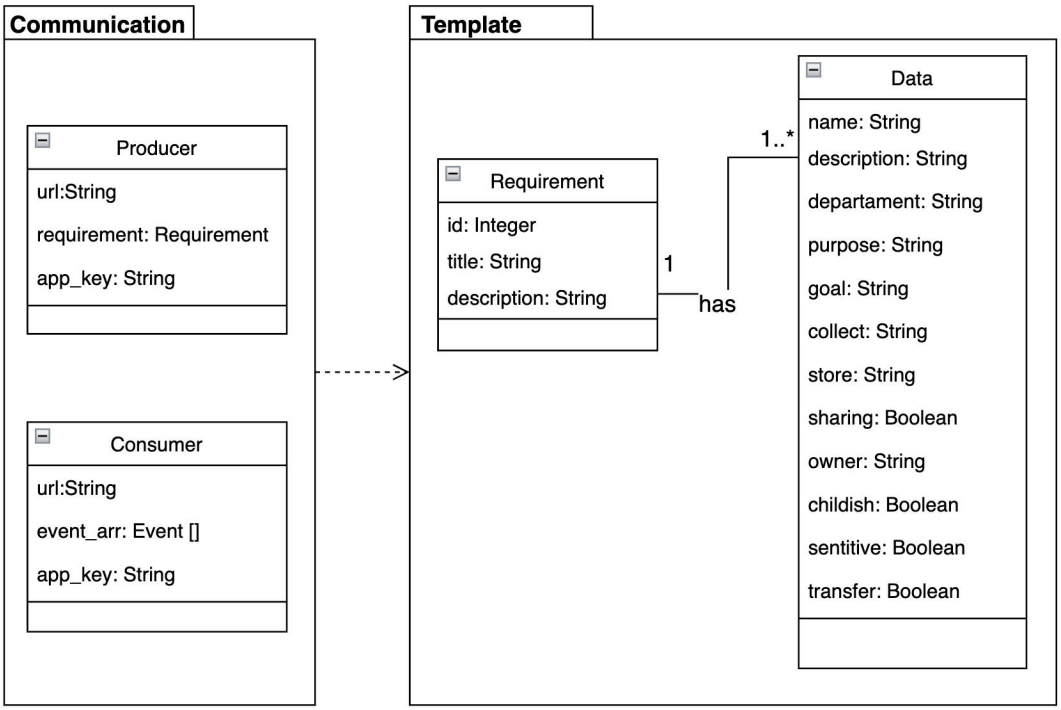


Figura 8 – Diagrama a ser implementado na visão de requisitos

Como pode ser observado na Figura 8, dois pacotes são apresentados: *Template* e *Communication*. O pacote *Template* define o formato que o requisito deve possuir para ser enviado para a Visão do Workflow. Nele estão definidos campos essenciais esperados pela Visão do Workflow para que esta possa processar as ações para proteção de dados pessoais, campos estes que observam as definições dos artefatos apresentadas na subseção 2.1.5. O formato esperado pela Visão do Workflow é uma estrutura em Json (*JavaScript Object Notation*) que deve refletir as classes do pacote *Template*, como apresentado no trecho 4.2.1.

O pacote *Communication*, por sua vez, é responsável por intermediar a comunicação com o Workflow. Nele são definidas duas classes *Producer* e *Consumer*, que devem ser implementadas para o envio dos requisitos e para reagir a eventos gerados durante a execução das etapas, respectivamente.

```
{
    "id":"Requirement Id",
    "title":"Requirement Title",
    "description":"Requirement Description",
    "data":[
        [ {"name":"value"}, {"description":"value"},
         {"department":"value"}, {"purpose":"value"},
         {"goal":"value"}, {"collect":"value"},
         {"store":"value"}, {"sharing":"value"},
         {"owner":"value"}, {"childish":"value"},
         {"sensitive":"value"} ,{"transfer":"value"},
        ]
    ],
}

```

Listing 4.2.1 – Estrutura JSON do pacote de Template

Após a criação do requisito de software, o usuário o encaminha para análise por meio da classe *Producer*. Ao chegar no Workflow, é determinada a etapa pela qual o requisito deve passar. Em seguida, o requisito é analisado para determinar a etapa que deve seguir, que compreende quais serviços devem ser invocados para apoiar a análise. Este ciclo persiste até a conclusão da análise ou que ocorra um erro que requeira intervenção do usuário. A figura 9 ilustra essa dinâmica:

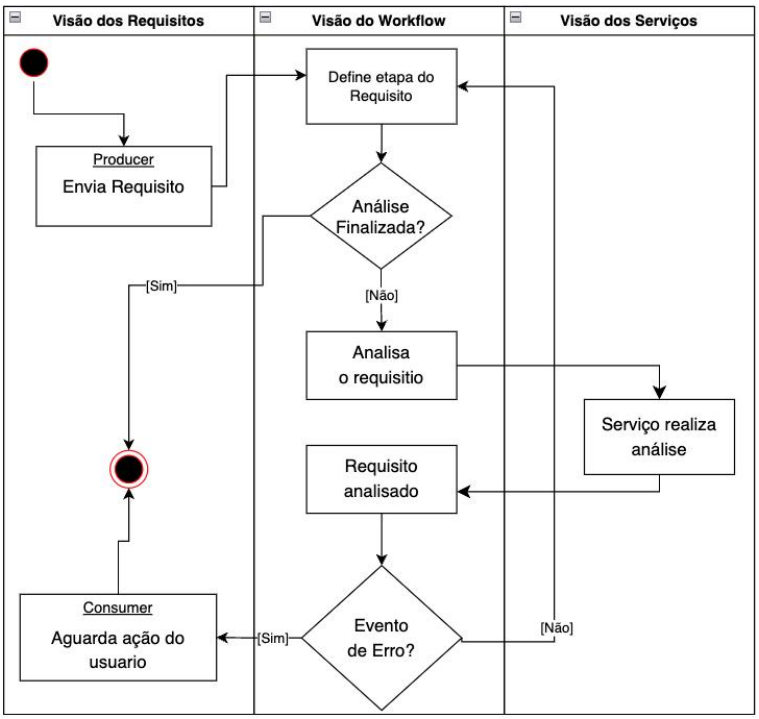


Figura 9 – Fluxo Visão dos Requisitos - Produto - Workflow - Consumidor

4.3 VISÃO DO WORKFLOW

4.3.1 Proposta das etapas

Para iniciar o desenvolvimento do workflow é necessário definir as etapas pelas quais um requisito de software pode passar e, para tanto, amparou-se nos artigos 8 capítulo 1 e 38 capítulo 3 da LGPD, que definem uma série de informações mínimas para a elaboração do RIPD, relatório este que pode ser solicitado a qualquer momento pela autoridade nacional e requer que algumas informações mínimas sejam incorporadas a ele (BRASIL, 2018).

Além das informações apontadas no texto da LGPD, também foi utilizado o guia e template disponibilizado pelo governo federal para elaboração do RIPD (FEDERAL, 2022), como descrito na subseção 2.1.5 sobre artefatos da LGPD, o que resultou nas seguintes informações a serem coletadas durante as etapas do workflow: (i) descrição dos tipos de dados coletados; (ii) métodos da coleta do dado; (iii) garantia de segurança; (iv) análise das salvaguardas; (v) mecanismo de mitigação de risco; (vi) compartilhamento com terceiros; (vii) prazo para tratamento e retenção; (viii) bases legais e (ix) finalidade do tratamento e contexto.

Observando as informações que devem ser coletadas, estas foram agrupadas para definir as etapas abaixo, ilustradas pela Figura 10:

- Análise inicial do dado: tem como objetivo validar o requisito de software recebido e as informações esperadas para cada dado pessoal associado ao requisito;
- Regulamentos: tem como objetivo apoiar especialistas na justificativa legal para o tratamento dos dados e, para isto, considera o requisito de software e a análise das etapas anteriores para sugerir trechos da LGPD que possam ser relevantes no momento da análise de justificativas para o uso;
- Análise de risco: disponibiliza meios para que análises de salvaguardas e mecanismos de mitigação de riscos sejam criadas; e
- Boas práticas para mitigar riscos: tem o objetivo de sugerir boas práticas de desenvolvimento para mitigação de riscos e para tanto, utiliza-se de recomendações trazidas pela ISO 27002, ISO 27701, NIST e CIS Controls v8 Privacy Companion Guide.

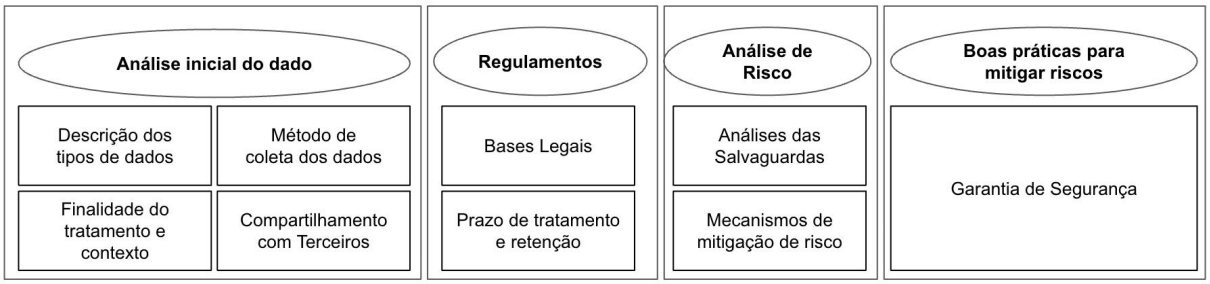


Figura 10 – Agrupamento das informações necessárias para gerar o RIPD

4.3.2 Ciclo de vida do workflow

O Workflow é uma esteira composta por etapas em que cada etapa executa suas regras de negócio chamando os serviços existentes na visão dos Serviços e, ao final envia o resultado para a próxima etapa da esteira. As regras de negócio são particulares de cada etapa que, por sua vez, possuem objetivos distintos e utilizam os serviços disponibilizados pela visão de Serviços para alcançá-los.

Como apresenta a Figura 11, a etapa Initial Data Analysis é a "porta de entrada" para o workflow, por ser responsável pelo recebimento e validação da "matéria-prima" da abordagem - o dado pessoal, e após realizar a validação do requisito e dos dados associados a este, o resultado é enviado para a etapa de *Regulations*.

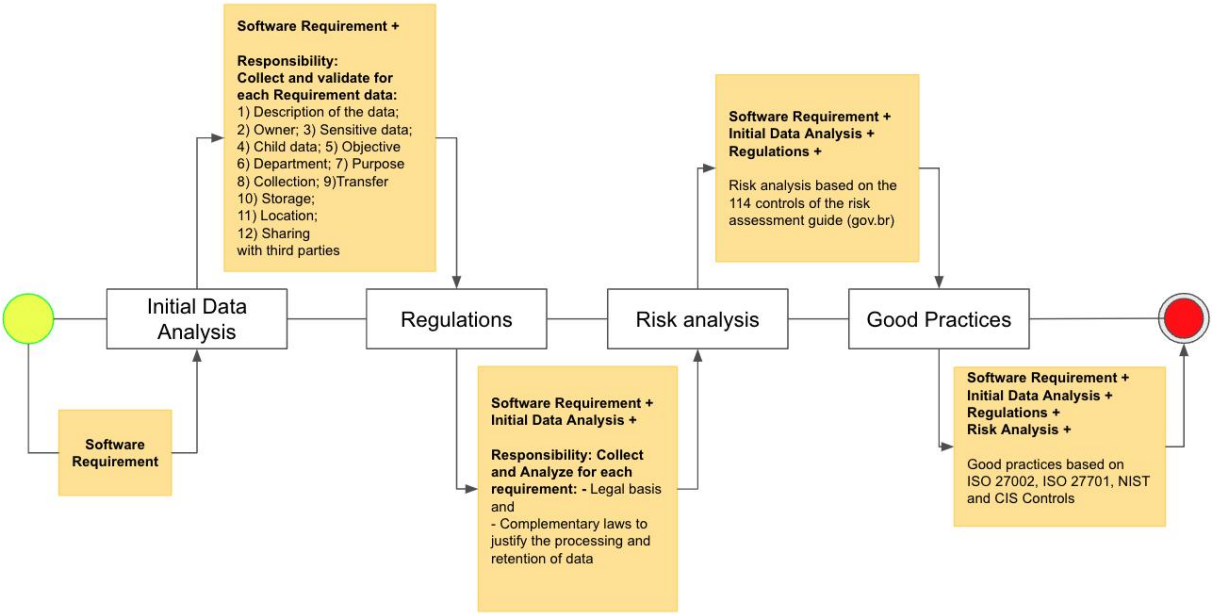


Figura 11 – Etapas do Workflow

A etapa de Regulations, por sua vez, utilizando os dados e análises vindos da etapa anterior, realiza análise específica para sugerir trechos da LGPD que possam apoiar um posicionamento acerca da (i) retenção dos dados; (ii) prazo de tratamento; e (iii) base legal e sua justificativa antes de enviar para a etapa de Risk Analysis. Essa etapa, de maneira similar, disponibiliza meios para que a análise de risco seja

realizada e então, finalmente enviar para etapa de Good Practices que irá sugerir boas práticas disponíveis em normas, como a ISO 27002 e ISO 27701 ou em conjuntos de diretrizes como NIST e CIS Controls, para que o desenvolvimento do requisito em questão considere os riscos identificados na etapa anterior.

Contudo, é preciso prever que alguns eventos podem acontecer durante a análise dos dados, como a necessidade de informações adicionais, falha durante as validações ou até mesmo exceções que bloqueiem a análise. Por exemplo: durante a etapa Initial Data Analysis , pode-se identificar que um dado associado ao requisito não teve suas informações obrigatórias corretamente enviadas, sendo necessário um ajuste antes do requisito passar para próxima etapa. Por isto, a arquitetura do workflow deve prever mecanismos para permitir que a análise continue.

4.3.3 Arquitetura do workflow

Como já visto, o requisito de software tramita por etapas do Workflow, onde é analisado e pode necessitar de interações para que siga o fluxo e então, chegue ao final da análise. Para tanto, a própria arquitetura desta visão precisa fornecer meios para inserção de requisitos para análise, identificar que um requisito está bloqueado no fluxo e verificar se a análise chegou ao fim.

Como forma de facilitar a identificação de eventos que podem acontecer no workflow e manter a flexibilidade da abordagem, permitindo que outras etapas e serviços sejam desenvolvidos, propõem-se uma arquitetura orientada a mensagens/eventos, na qual eventos gerados na visão do Workflow são adicionados em uma estrutura para que possam ser consumidos pela visão dos Requisitos e então, ações sejam tomadas de acordo com a necessidade do sistema aderente.

Para viabilizar a arquitetura proposta, esta foi separada em três componentes, *Orchestrator*, *Broker* e *Consumers*, que podem ser visualizados na figura 12.

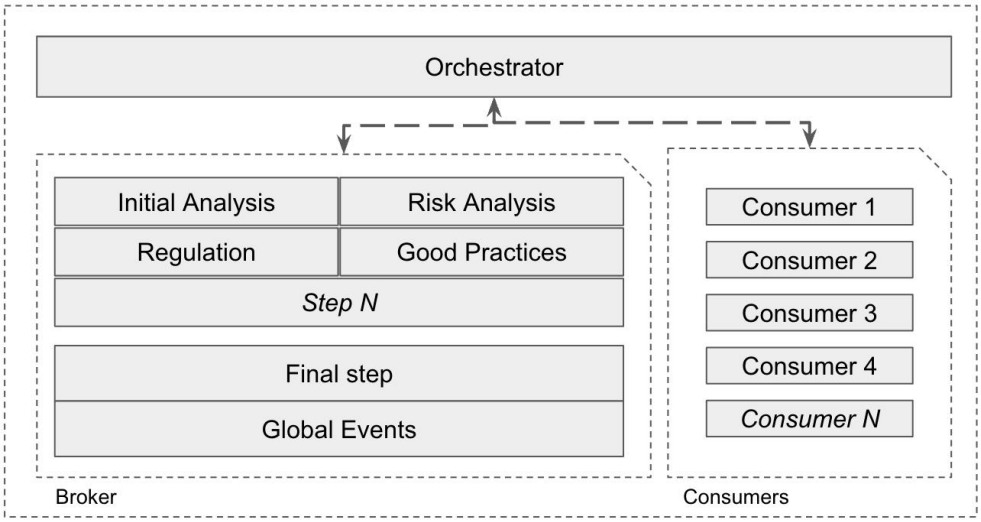


Figura 12 – Arquitetura do Workflow

O *Orchestrator* é uma API que centraliza e disponibiliza as informações necessárias para o correto funcionamento do Workflow. Informações como fluxos, etapas, serviços que as etapas devem consumir, ordem que devem consumir, são tipos de informações disponibilizadas, bem como disponibiliza meio de enviar requisito para análise, obter seu status e obter status de requisitos já analisados.

O componente *Broker* é o responsável pelo gerenciamento das etapas definidas, para tanto sugere-se o uso de um *Message Broker*, que é uma aplicação utilizada em sistemas distribuídos, mais especificamente em sistemas tipo *Message Oriented Middleware (MOM)*(YONGGUO *et al.*, 2019). O *Message Broker* fornece uma camada de comunicação onde componentes do sistema se conectam para enviar e receber mensagens, eventos ou requisições.

Os *Consumers* são consumidores que se conectam ao broker para “escutar” mensagens das filas de sua responsabilidade. Para cada etapa no *Broker*, há um consumidor correspondente que pega as mensagens, verifica quais serviços deve chamar e o que fazer em caso de sucesso e erro, consultando o *Orchestrator*.

Tal proposta empresta flexibilidade à *abordagem*, permitindo que serviços e etapas sejam melhorados ou novos sejam desenvolvidos sem que haja necessidade de alterações no sistema aderente e nem alterações que envolvam desenvolvimento do Workflow.

Ainda de encontro com a flexibilidade esperada para esta visão, sugere-se que eventos gerados pela Visão do Workflow possuam os campos descritos abaixo com seus respectivos objetivos:

1. *Timestamp*: identificar hora e data que o evento ocorre;
2. *Service Name*: identificar o nome do serviço;
3. *Level*: indicar se o evento é de: (i) erro (error); (ii) requer mais atenção (warn); ou se é (iii) apenas um acompanhamento (info);
4. *Action*: sugererir ações possíveis para o evento, podendo ser: (i) nada a fazer (nothing); (ii) refazer o processo (retry); (iii) realizar ajuste (adjustment);
5. *Requirement Id*: Identificar numericamente o requisito associado ao evento; e
6. *Message*: Retornar feedback descritivo, por exemplo: "Quando o dado é pessoal, é preciso informar se é compartilhado".

4.4 VISÃO DOS SERVIÇOS

Esta visão concentra os serviços que serão utilizados pelas etapas para alcance dos objetivos. Seu uso não é restrito a apenas uma etapa específica, ou seja, os

serviços aqui contidos podem ser utilizados mais de uma vez e por qualquer etapa, bastando que para isto sejam devidamente cadastrados e configurados na Visão do Workflow.

Considerando as etapas e seus objetivos definidos na seção anterior, foram definidos os serviços listados abaixo, a Figura 13 ilustra a utilização dos serviços por etapa.

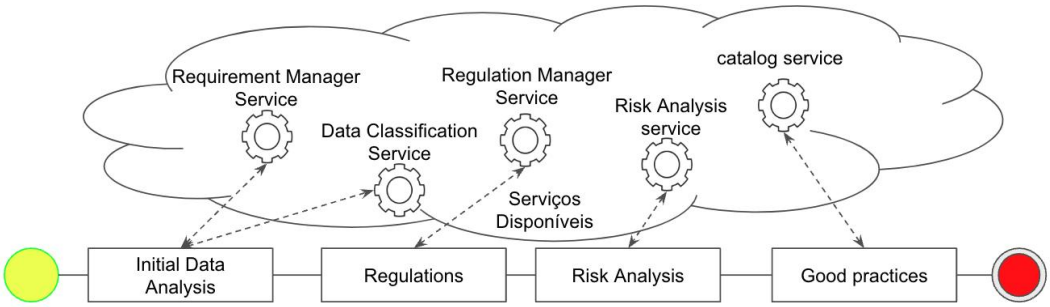


Figura 13 – Visão dos Serviços por etapa

1. **Requirement Manager Service:** é indicado para etapa *Initial Data Analysis* e tem o objetivo de realizar a validação e verificação de cada dado pessoal enviado com o requisito de software de acordo com a LGPD.

2. **Data Classification Service:** é sugerido para etapa *Initial Data Analysis* e tem o objetivo de verificar indícios de dados pessoais e dados pessoais sensíveis. Para tanto, uma proposta é que este serviço implemente um banco de sinônimos baseado em palavras apontadas como sensíveis, segundo a LGPD, em conjunto com a métrica de Levenshtein [1] para identificar possíveis diferenças que indiquem erros ortográficos e um algoritmo de processamento natural de linguagem.

3. **Regulation Manager Service:** propõe-se o uso na etapa *Regulations* com o objetivo de sugerir trechos da lei que possam ser relevantes durante o desenvolvimento do software. Uma possibilidade é o serviço utilizar a técnica Term Frequency – Inverse Document Frequency (TF-IDF)[2] para apoiar na sugestão de trechos da LGPD;

4. **Risk Analysis service:** é sugerido para etapa *Risk Analysis*, tendo como objetivo identificar os riscos de incidentes que geram impacto potencial sobre os titulares dos dados pessoais, analisar as salvaguardas e identificar os mecanismos de mitigação de riscos. Uma possibilidade é que nesta etapa haja uma interação

[1] Distância de Levenshtein é uma métrica de string para medir a diferença entre duas sequências (PONCELET *et al.*, 2008).

[2] A técnica TF-IDF calcula a relevância estatística de uma palavra em um conjunto de documentos (QAISER; ALI, 2018).

com o usuário, permitindo que este aponte dentre os dados do requisito o risco associado em uma possível violação de dados, bem como a sua criticidade; e

5. **Catalog service:** é indicado para a etapa *Good practices* para identificar controles que possam ser usados para mitigar os riscos. Uma proposta para esta etapa, é a utilização de um modelo de machine learning como o Large Language Model (LLM) em conjunto com informações oriundas da ISO 27002 e ISO 27701. Este tipo de modelo permite a utilização de grande quantidade de texto para treinamento e tem dentre as possibilidades a geração de textos automáticos em um formato legível para o usuário (RADFORD *et al.*, 2018). Com isto, seria possível utilizar o retorno da etapa *Risk Analysis* como input para o modelo treinado, gerando uma resposta para apoiar sugestões de controles para mitigar riscos.

O serviço pode ser desenvolvido em qualquer linguagem, contanto que permita seu consumo por meio do protocolo HTTP e ser acessível pela Visão do Workflow e seus *consumers*. Além disto, é de suma importância que os serviços respondam com os dados (i)*action* que indica uma sugestão do serviço para uma ação a ser realizada; (ii)*level*, o nível de atenção que a abordagem deve dar para a análise; (iii)*requirement id*, o ID do requisito que foi analisado pelo serviço; (iv)*timestamp*, data e hora que o serviço realizou a análise; (v) *service name*, nome do serviço; e, (vi) *Message*, análise realizada. Por fim, o serviço precisa entregar sua resposa no formato json, como exemplificado a seguir:

```
{
    "action": "nothing",
    "level": "info",
    "requirement_id": "152529",
    "timestamp": "12/09/2023",
    "service_name": "requirement-manager-service",
    "message": "example"
}
```

Listing 4.4.1 – JSON template para a resposta dos serviços

4.5 CONSIDERAÇÕES FINAIS

Em resumo a abordagem é baseada em três visões interconectadas: Visão dos Requisitos, Visão do Workflow e Visão dos Serviço, para fornecer suporte à proteção de dados pessoais no contexto de gerenciamento de requisitos de software. As visões são fundamentadas em um modelo conceitual para a comunicação entre o sistema aderente e o Workflow, um fluxo customizável para análise de requisitos e um conjunto de micro-serviços com objetivos específicos.

5 IMPLEMENTAÇÃO

Com foco na avaliação da abordagem proposta, as visões definidas no capítulo anterior foram implementadas em uma ferramenta. Esta seção apresenta o conjunto de requisitos que foram definidos bem como, as tecnologias utilizadas na implementação. Por fim, um cenário de exemplo utilizando a ferramenta desenvolvida é apresentado.

5.1 REQUISITOS FUNCIONAIS

Nesta seção são definidos os requisitos funcionais das implementações da abordagem realizadas para uso nos exemplos e avaliações deste trabalho.

5.1.1 Visão dos Requisitos

5.1.1.1 FHGR

Os requisitos listados abaixo especificam as funcionalidades básicas que uma ferramenta de gestão de requisitos deve possuir para viabilizar o uso da abordagem. Desta forma, tais requisitos foram implementados inicialmente na ferramenta FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos), ferramenta apresentada no capítulo de avaliação 6:

1. O sistema deve possibilitar aos usuários a criação de requisitos de software, permitindo a inserção de título e descrição para cada requisito;
2. O sistema deve permitir ao usuário editar e remover requisitos cadastrados no sistema; e
3. O sistema deve permitir ao usuário a visualização e listagem de todos os requisitos cadastrados, facilitando a análise global e gerencial por parte dos usuários;

Os requisitos especificados abaixo foram implementados para atender o modelo conceitual proposto (seção 4.2):

1. O sistema deve permitir o envio de um ou mais requisitos para análise;
2. O sistema deve permitir o cadastro de um ou mais dados e associá-lo a um requisito cadastrado, garantindo que o usuário insira as informações previstas pelo modelo conceitual proposto na seção 4.2;
3. O sistema deve permitir listar, remover e editar dados associados a um requisito;
4. O sistema deve apresentar as análises de requisitos realizadas pelo Workflow;

5. O sistema deve disponibilizar alerta visual na página de listagem quando a análise do requisito retornar erro; e
6. O sistema deve apresentar o mapeamento dos dados.

5.1.2 Visão do Workflow

5.1.2.1 Orchestrator

1. A API deve disponibilizar *endpoint* para o envio do requisito de software para análise;
2. A API deve disponibilizar *endpoint* que permita recuperar todas informações dos dados pessoais; e
3. A API deve disponibilizar *endpoint* para recuperar detalhes de um requisito, contendo todas as análises realizadas.

5.1.2.2 Consumidores

1. O sistema deve permitir configurar a URL da API Orchestrator, que indica quais serviços devem ser consumidos; e
2. O sistema deve permitir configurar a fila a qual deve consumir as mensagens;

5.1.3 Visão dos Serviços

5.1.3.1 Requirement Manager Service

1. O serviço deve disponibilizar *endpoint* para análise do requisito;
2. O serviço deve validar se o requisito de software enviado contém dados pessoais associados e validar se os dados possuem as informações obrigatórias segundo a LGPD; e
3. O serviço deve implementar o protocolo de resposta de acordo com a seção 4.4

5.1.3.2 Data Classification Service

1. O serviço deve disponibilizar *endpoint* para análise do requisito;
2. O serviço deve verificar indícios de dados pessoais sendo utilizados no requisito de software considerando o título, descrição e os dados pessoais associados ao requisito e classificá-los quanto a dado pessoal ou dado pessoal sensível; e
3. O serviço deve implementar o protocolo de resposta de acordo com a seção 4.4

5.1.3.3 Regulation Manager Service

1. O serviço deve disponibilizar *endpoint* para análise do requisito;
2. O serviço deve sugerir trechos da LGPD com base no requisito enviado, bem como com base nos parâmetros enviados por outras etapas ou serviços; e
3. O serviço deve implementar o protocolo de resposta de acordo com a seção 4.4

Na sequência são especificados aspectos não-funcionais e arquiteturais da implementação da ferramenta, observando a abordagem proposta.

5.2 VISÃO DE REQUISITOS

Para visão dos requisitos foi desenvolvida uma aplicação web utilizando a biblioteca *front-end* React do javascript. Além disto, foi utilizado o framework react-admin, que facilita a criação de interfaces administrativas para web.

Originalmente, a aplicação permitiu a criação, recuperação, edição e exclusão de requisitos de software. Para viabilizar essas funcionalidades foi desenvolvida uma API em Python, especificamente projetada para esse propósito. Para facilitar, o framework Flask foi utilizado e para armazenamento dos dados, o Postgres foi a escolha adotada.

Após o desenvolvimento da aplicação Web e API para o gerenciamento dos requisitos de software, foi então implementado na aplicação desenvolvida em React o modelo conceitual apresentado no capítulo anterior, com isto, a aplicação incorporou a capacidade de enviar o requisitos para análise e recuperar eventos produzidos na visão do Workflow (conforme especificado na seção 5.1.1) .

5.3 VISÃO DO WORKFLOW

A Figura 14 apresenta os componentes implementados para a visão do Workflow, como pode ser observado, tem-se os componentes API, Consumidores/Produtores e Filas, estas últimas agrupadas dendro de uma estrutura chamada Broker. De maneira geral, as API's disponibilizam interfaces a serem utilizadas por outras aplicações que possuem interesse no que o serviço disponibiliza. As filas, por sua vez, servem para enfileirar mensagens recebidas e, por fim, consumidores/produtores tem o objetivo de pegar ou colocar mensagens em uma fila.

A API e os consumidores da visão do Workflow foram desenvolvidos utilizando a linguagem de programação Python. Essa escolha oferece uma ampla gama de recursos e bibliotecas disponíveis na comunidade Python, facilitando o desenvolvimento e a manutenção do código.

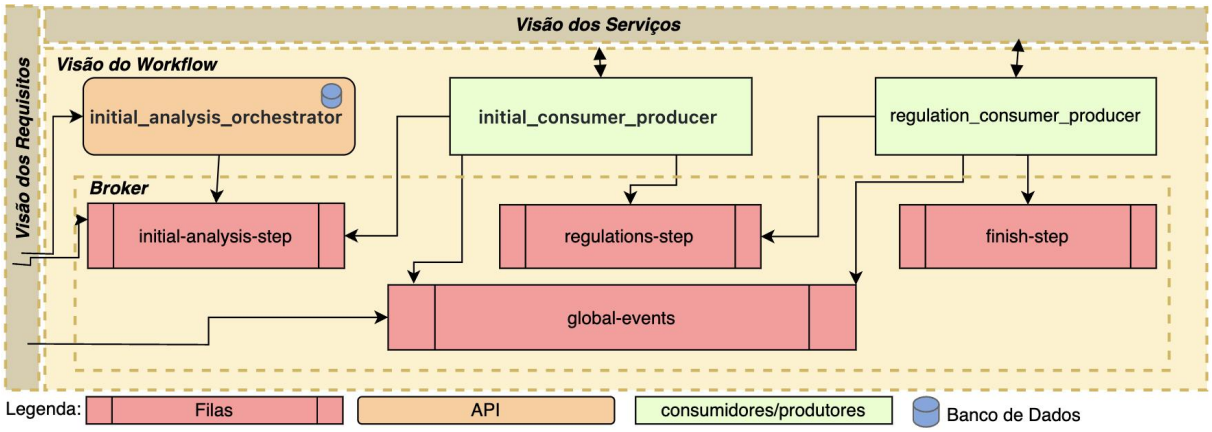


Figura 14 – Componentes Implementados da Visão dos Workflow

Além disso, para agilizar o processo de desenvolvimento da API, foi utilizado o framework. Flask. O Flask é escrito em Python e oferece uma abstração simplificada para criação de APIs, permitindo uma implementação mais eficiente e organizada.

No que diz respeito ao armazenamento de dados, optou-se pelo uso do banco de dados PostgreSQL. O PostgreSQL é um sistema de gerenciamento de banco de dados relacional que oferece performance, segurança e confiabilidade. Essa escolha permite atender às necessidades das aplicações em relação ao armazenamento de forma eficiente e escalável.

Para a implementação da mensageria ou *broker*, fundamental para o funcionamento da Visão do Workflow, foi adotado o software RabbitMQ. O RabbitMQ é um software de mensagens de código aberto que utiliza o protocolo AMQP *(Advanced Message Queuing Protocol)*. A utilização do RabbitMQ traz várias vantagens importantes, dentre elas:

1. Confiabilidade: Garantindo que as mensagens sejam entregues aos destinatários corretos, assegurando um fluxo de comunicação confiável.

2. Escalabilidade: Com a capacidade de lidar com grandes volumes de mensagens, o RabbitMQ permite que o sistema seja dimensionado conforme necessário, acompanhando o crescimento da demanda.

3. Mensageria assíncrona: O que melhora a eficiência e o desempenho, especialmente em ambientes distribuídos.

5.4 VISÃO DE SERVIÇOS

Os microsserviços implementados na Visão dos Serviços foram três: 1) *Requirement Manager Service*, 2) *Data Classification Service* e 3) *Regulation Manager Service*. Ambos microsserviços foram desenvolvidos utilizando a linguagem de programação

Python e framework Flask, que facilita a criação de API's. Abaixo são detalhadas características específicas de cada um dos serviços implementados.

5.4.1 Requirement Manager Service

Este microserviço atende a primeira etapa "*Initial Data Analysis*" e tem como objetivo verificar se os dados que estão sendo enviados junto ao requisito de software possuem as informações obrigatórias, segundo a LGPD, conforme explicitado na figura 11. Além de verificar a existência das informações associadas aos dados, o microserviço também valida a estrutura do json enviado em busca de dados faltantes, nulos ou em branco.

Este serviço é bloqueante, ou seja, caso alguma falha seja percebida o serviço envia um evento de erro para o Workflow, impedindo que a análise continue.

5.4.2 Data Classification Service

Este microserviço também é dedicado à primeira etapa "*Initial Data Analysis*" e visa identificar dados pessoais comuns e sensíveis presentes nos requisitos de software analisados. Para isso, utiliza a distância de Levenshtein, que é útil para identificar similaridades entre palavras, corrigir erros de digitação ou encontrar correspondências aproximadas. Ademais, simplifica as palavras ao remover as *stop words*[1] e reduzi-las à sua forma radical por meio do processo de *Stemming*[2]. O algoritmo deste microserviço também incorpora um dicionário[3] para identificar palavras indicativas de dados, tanto comuns quanto sensíveis.

Este microserviço não foi implementado para ser bloqueante. Contudo, sempre que identifica um dado no requisito, seja no texto ou no próprio dado, adiciona um evento de alerta para que o usuário decida o que fazer.

5.4.3 Regulation Manager Service

Este microserviço atende a etapa de "*Regulations*' e visa fornecer trechos relevantes da LGPD que possam estar relacionados ao requisito do software analisado. Para alcançar esse objetivo, o microserviço possui um processo de preparação do texto da LGPD e um processo de recuperação dos trechos da lei.

Para o processo de preparação do texto, algumas etapas se fizeram necessárias, sendo a implementação do algoritmo TF-IDF a principal delas. O *TF-IDF (Term Frequency-Inverse Document Frequency)* é um método estatístico utilizado no proces-

[1] Palavras comuns, que não fornecem informações relevantes (SOLKA, 2008).

[2] Processo de normalização linguística onde o termo é reduzido a uma forma comum denominada stem ou radical, removendo suas variações (MORAIS; AMBRÓSIO, 2007).

[3] Disponível na URL `https://codigos.ufsc.br/masters-degree/data_classification_service/-/blob/main/data_classification_service/controller/analyse_controller.py`

samento de linguagem natural e na recuperação de informação, o qual utiliza-se para avaliar a importância de uma palavra em um documento dentro de um conjunto de documentos (YANG, 2017). A Figura 15 apresenta as etapas realizadas neste processo de preparação do texto da LGPD.

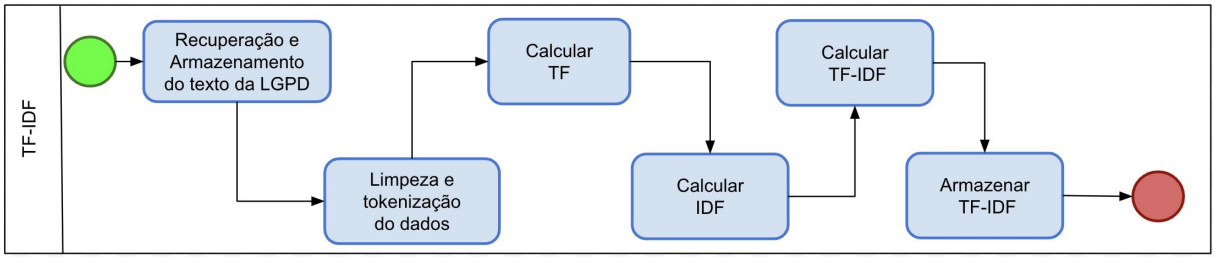


Figura 15 – Preparação do texto da LGPD

1. Recuperação e Armazenamento do texto da LGPD: Primeiramente o texto é armazenado no banco de dados do microserviço de forma a permitir recuperar a informação para limpeza e tokenização dos dados, bem como recuperar o texto original no processo de recuperação dos trechos da lei.

2. Limpeza e tokenização dos dados: Com o texto armazenado são então retiradas as acentuações, caracteres especiais, removidos os *stop words*, transformada as palavras em minúsculas e então as frases são tokenizadas, ou seja, quebrando as frases em palavras.

3. Calcular TF: Esta etapa mede quantas vezes um token aparece no documento.

4. Calcular IDF: Nesta etapa, o objetivo é verificar o quão comum o token é em todos os documentos, ou seja, quanto determinado token aparece em todos os documentos. A ideia é que quanto mais raro um termo mais informativo este pode ser.

5. Calcular TF-IDF: Nesta etapa o TF e IDF são multiplicados e os termos com pontuação mais alta são considerados mais importantes no contexto do texto analisado.

6. Armazenar TF-IDF: Por fim, o cálculo do TF-IDF é armazenado no banco de dados para que possa ser recuperado em posterior consulta.

Com este processo realizado, é possível que as análises dos requisitos sejam realizadas. Ao ser acionado, o serviço então realiza alguns passos para indicar um trecho da lei, são eles (Figura 16):

1. Limpeza e tokenização do requisito: São retiradas as acentuações, caracteres especiais, removidos os *stop words*, transformada as palavras em minúsculas e

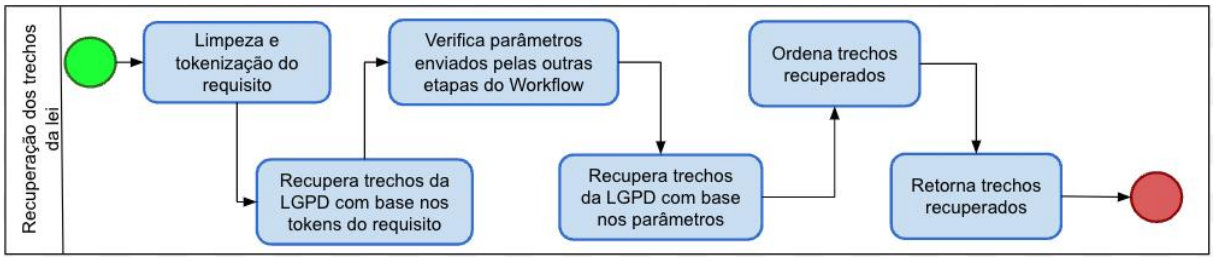


Figura 16 – Recuperação dos trechos da LGPD

tokenizadas todo o requisito enviado, processo similar ao realizado na preparação do texto.

2. Recupera trechos da LGPD com base nos tokens do requisito: Nesta etapa são recuperados os valores de TF-IDF para cada token gerado para o requisito na etapa anterior;

3. Verifica parâmetros enviados pelas outras etapas do Workflow: É verificado se o requisito possui indicação explícita de alguma característica específica entre os dados. Como por exemplo, dados pessoais "sensíveis", "infantis", "compartilhados"entre outras que podem ser apontadas pelas etapas do Workflow.

4. Recupera trechos da LGPD com base nos parâmetros: Recupera trechos da LGPD armazenados no banco de dados utilizando como parâmetro as características específicas identificas na etapa anterior, por exemplo, "infantil".

5. Ordena trechos recuperados: Ordena resultados de ambas recuperações do banco de dados de foma crescente, considerando o score do TF-IDF.

6. Retorna trechos recuperados: Por fim, retorna os dados para a etapa que realizou a requisição.

5.5 INFRAESTRUTURA

Como pode ser observado na Figura 17, a abordagem adotada consiste em vários componentes interconectados. Essa estrutura oferece flexibilidade, permitindo a atualização dos componentes existentes ou a adição de novos sem interromper o funcionamento da abordagem. No entanto, essa abordagem também pode apresentar desafios na configuração do ambiente.

Para simplificar essa complexidade, foram utilizadas as ferramentas Docker e Compose. O Docker é uma plataforma de virtualização que permite empacotar os componentes em contêineres independentes, garantindo a portabilidade e a consistência do ambiente de execução. Já o Compose é uma ferramenta do Docker que facilita a definição e a execução de múltiplos contêineres de forma coordenada, por meio de um arquivo YAML.

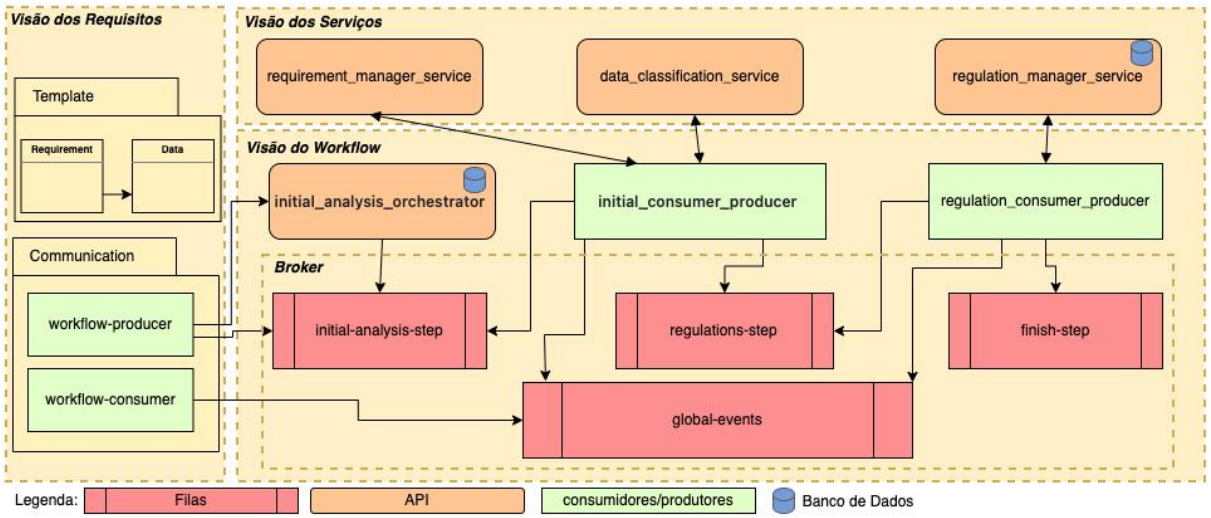


Figura 17 – Componentes da Abordagem

Dessa forma, cada componente da abordagem possui um arquivo YAML dedicado, o que facilita a configuração de forma unificada. Além disso, foi utilizada a função de submódulos do GIT para agrupar os componentes essenciais em um único repositório, permitindo a criação de um arquivo YAML principal que faz referência aos demais arquivos YAML de cada componente.

Essa estratégia baseada em Docker e Compose simplifica a gestão do ambiente, tornando mais ágil a configuração e o controle dos componentes utilizados. Com o uso dos arquivos YAML, pode-se centralizar e automatizar a configuração dos componentes de forma coesa. Isso proporciona uma estratégia eficiente para lidar com a complexidade da configuração, propiciando um ambiente consistente e controlado.

No que diz respeito ao Workflow e aos Serviços, foi utilizado o ambiente fornecido pela Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação, conhecida como SETIC. A SETIC presta suporte às atividades dos programas de pós-graduação da Universidade Federal de Santa Catarina (UFSC) e disponibilizou um ambiente acessível por meio do endereço[4] `http://psiu.inf.ufsc.br/`, o projeto se encontra no servidor dentro da pasta `/psiu/user_privacy_framework`. Além disso, os códigos-fonte da abordagem estão armazenados em um sistema de controle de versões também fornecido pela SETIC e acessível pela URL `https://codigos.ufsc.br/masters-degree/user_privacy_framework`.

5.6 EXEMPLO

Nesta seção é apresentado um exemplo prático baseado num cenário fictício para demonstrar o uso ponta a ponta da abordagem proposta. No exemplo somente as duas primeiras etapas da Visão do Workflow são demonstradas, ou seja, as etapas

[4] Para acessar o endereço o usuário precisa estar logado na VPN da UFSC

de “*Initial Data Analysis*” e “*Regulations*”.

Considera-se uma empresa de desenvolvimento que utiliza uma ferramenta para gestão dos seus requisitos, aqui nomeada FHGR (Ferramenta Hipotética de Gestão de Requisitos). Com a vigência da LGPD, a empresa precisa promover a proteção dos dados pessoais de seus sistemas. Dentre outros produtos, a empresa é responsável por um software de gestão escolar que trata de diversos dados pessoais, incluindo dados de crianças e adolescentes.

Como apoio na adequação à LGPD, a empresa decide utilizar a abordagem aqui proposta integrando-a à FHGR, objetivando não alterar a forma como os requisitos são atualmente propostos e obter um auxílio automatizado no tratamentos dos dados pessoais.

Suponha-se uma nova demanda solicitada ao time responsável: *"Como secretário escolar preciso inserir a foto da criança no sistema para poder identificá-la nas dependências da escola"*. Este requisito de software é então cadastrado na FHGR (agora com a abordagem proposta integrada - Figura 18) e irá passar pelas etapas previstas na Visão do Workflow.

5.6.1 Etapa “*Initial Data Analysis*”

5.6.1.1 Perspectiva do usuário

Ao enviar o requisito para análise, o usuário recebe um feedback, conforme Figura 18.

Após realizar os ajustes indicados, ou seja, após o preenchimento das informações obrigatórias do dado "foto", o requisito é novamente enviado para a Visão do Workflow, que percebendo a existência e corretude das informações obrigatórias, avança na análise e aponta a existência de dados sensíveis (Figura 18b).

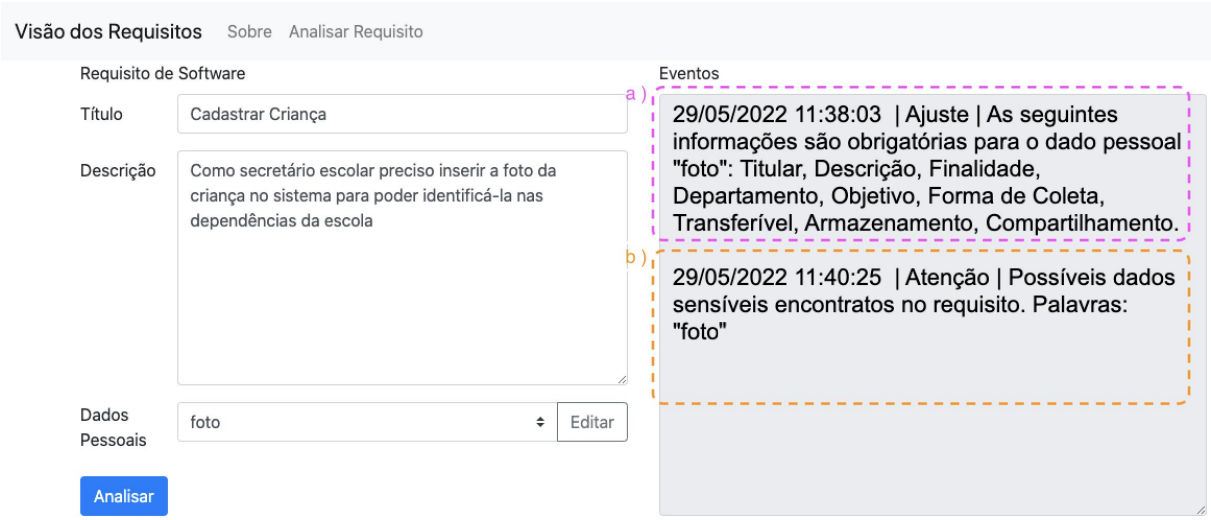
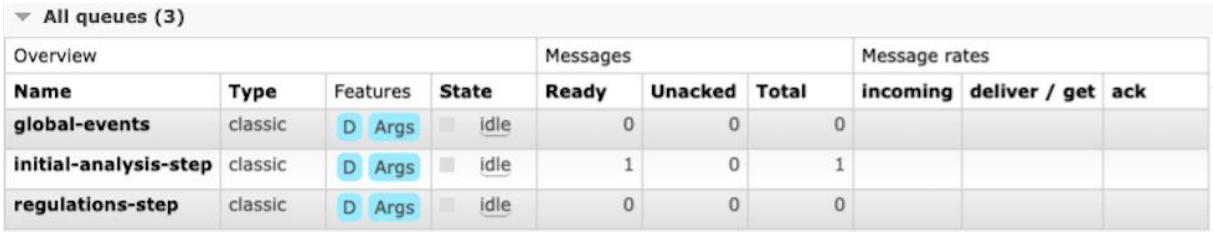


Figura 18 – Alerta de Dados Sensíveis

5.6.1.2 Perspectiva interna

O requisito é recebido pela primeira etapa da Visão do Workflow, etapa "*Initial Data Analysis*", no formato JSON com a estrutura descrita na seção 4.2 que propõem a Visão dos Requisitos. O workflow possui como apoio uma estrutura de fila que recebe todos os requisitos enviados para a análise (Figura 19). Estando o requisito na etapa inicial, estará na fila identificada na coluna "Name" como "initial-analysis-step".



All queues (3)

Overview				Messages			Message rates		
Name	**Type**	Features	**State**	**Ready**	**Unacked**	**Total**	**incoming**	**deliver / get**	**ack**
global-events	classic	D Args	idle	0	0	0			
initial-analysis-step	classic	D Args	idle	1	0	1			
regulations-step	classic	D Args	idle	0	0	0			

Figura 19 – Filas do Workflow

Ao identificar que o requisito está na estrutura de fila mencionada, a visão do Workflow chama o "*Requirement Manager Service*", disponibilizado pela visão dos serviços, que após análise responde alertando a falta de informações obrigatórias (segundo a LGPD referente ao dado pessoal "foto"). Assim, um evento bloqueante (adjustment) é gerado e adicionado à fila de eventos globais, identificado na Figura 19 como *global-events*. A ferramenta FHGR deve tratar o evento, apresentando um retorno ao usuário (Figura 18a).

Sendo o requisito novamente enviado para a Visão do Workflow, e estando correto em relação às informações obrigatórias, o "*Data Classification Service*" é acionado e, utilizando as técnicas já mencionadas na seção 4.4, aponta sobre a possível existência de dados sensíveis considerando a LGPD, como apresenta os eventos da Figura 18b.

5.6.2 Etapa "*Regulation*"

O requisito, estando com os dados corretamente descritos, avança para a etapa de Regulamentos.

5.6.2.1 Perspectiva do usuário

Nesta etapa, o usuário recebe recomendações de trechos da LGPD que se aplicam ao tipo de dado processado, conforme visualizado na Figura 20. No exemplo em questão, as recomendações trazem trechos da Lei que alertam tanto para o uso de dados sensíveis, uma vez que foi identificado o dado sensível "foto", quanto para o tratamento de dados de menores, já que no texto do requisito havia o termo "criança".

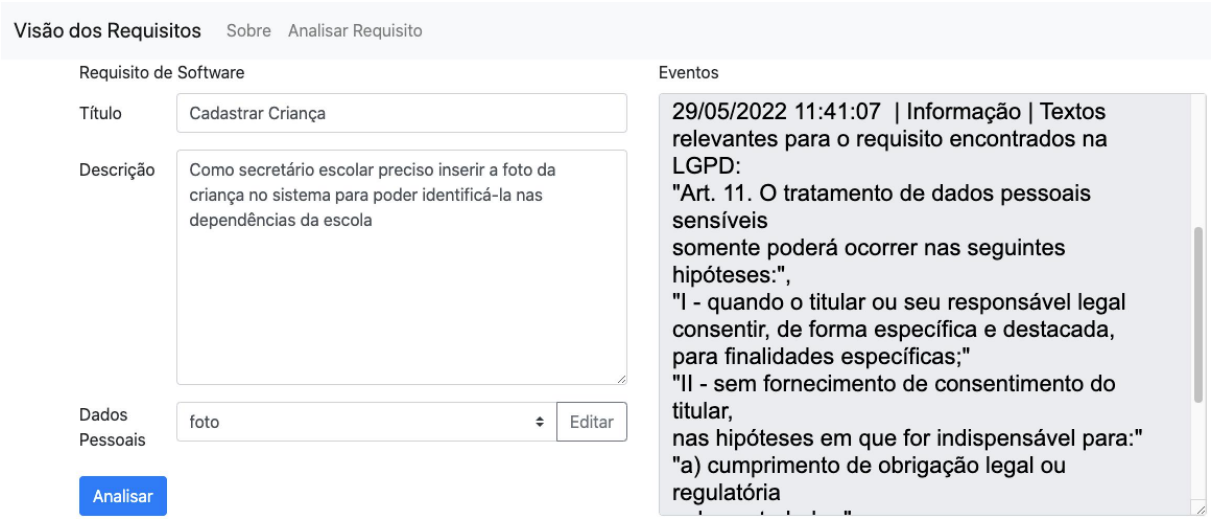


Figura 20 – Informação dos textos relevantes para o requisito analisado

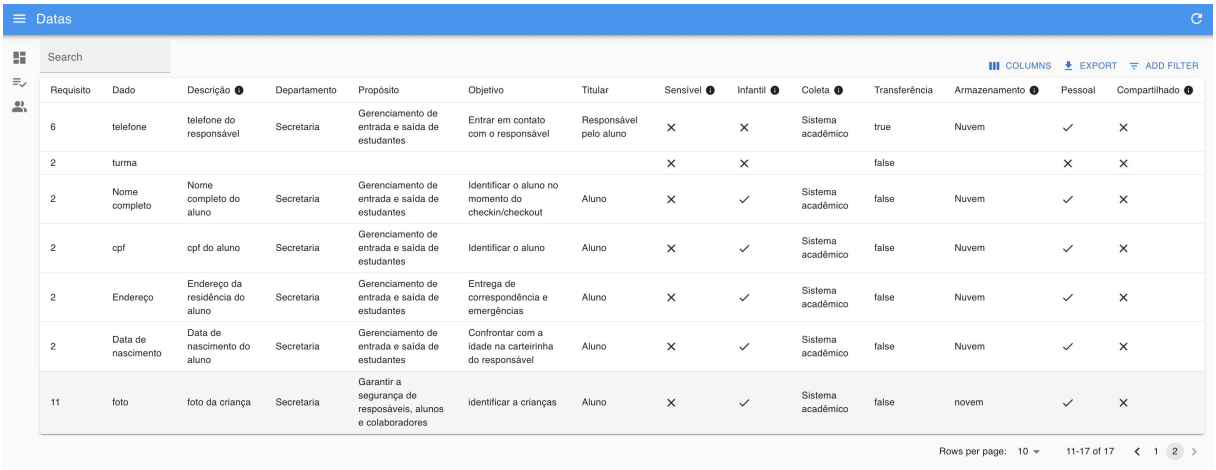
5.6.2.2 Perspectiva interna

Ao passar pela etapa de "*Initial Data Analysis*", o requisito é encaminhado para a etapa "*Regulation*" que possui apoio da estrutura de fila (identificada na Figura 19 como *regulations-step*). A Visão do Workflow, então, consulta o "*Regulation Manager Service*" que retorna os trechos da LGPD que devem ser considerados ao implementar o requisito. A ideia é que a resposta enviada pelo serviço sirva como alerta e insumo para uma possível justificativa para o uso do dado, informação também essencial na construção do RIPD. O JSON abaixo apresenta uma parte do retorno recebido:


```
"action": "nothing",
"level": "info",
"message": [ {
    "sensitive_rule": {
        "Foto":
            [ "Art. 11. O tratamento de dados pessoais
            sensiveis somente podera ocorrer nas seguintes
            hipoteses:",
            "I – quando o titular ou seu responsavel legal
            consentir, de forma especifica e destacada,para
            finalidades especificas;"
            "II – sem fornecimento de consentimento do titular,
            nas hipoteses ..."
            ]
    }}],
    "requirement_id": "01",
    "service_name": "regulation_manager_service",
```

"timestamp": "2022-05-29 11:41:07.751377"

Uma vez que não há mais etapas para o requisito passar, considera-se a análise como concluída. A partir desse momento, é possível acessar no sistema todos os dados associados aos requisitos que já foram analisados, conforme ilustrado na Figura 21.



Requisito	Dado	Descrição	Departamento	Propósito	Objetivo	Titular	Sensível	Infantil	Coleta	Transferência	Armazenamento	Pessoal	Compartilhado
6	telefone	telefone do responsável	Secretaria	Gerenciamento de entrada e saída de estudantes	Entrar em contato com o responsável	Responsável pelo aluno	×	×	Sistema acadêmico	true	Nuvem	✓	×
2	turma						×	×		false		×	×
2	Nome completo	Nome completo do aluno	Secretaria	Gerenciamento de entrada e saída de estudantes	Identificar o aluno no momento do checkin/checkout	Aluno	×	✓	Sistema acadêmico	false	Nuvem	✓	×
2	cpf	cpf do aluno	Secretaria	Gerenciamento de entrada e saída de estudantes	Identificar o aluno	Aluno	×	✓	Sistema acadêmico	false	Nuvem	✓	×
2	Endereço	Endereço da residência do aluno	Secretaria	Gerenciamento de entrada e saída de estudantes	Entrega de correspondência e emergências	Aluno	×	✓	Sistema acadêmico	false	Nuvem	✓	×
2	Data de nascimento	Data de nascimento do aluno	Secretaria	Gerenciamento de entrada e saída de estudantes	Confrontar com a idade na carteirinha do responsável	Aluno	×	✓	Sistema acadêmico	false	Nuvem	✓	×
11	foto	foto da criança	Secretaria	Garantir a segurança de responsáveis, alunos e colaboradores	identificar a crianças	Aluno	×	✓	Sistema acadêmico	false	novem	✓	×

Figura 21 – Mapeamento dos Dados

5.7 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram implementadas as três visões propostas neste trabalho: a Visão de Requisitos, Visão do Workflow e Visão dos Serviços, apresentando detalhes sobre cada uma das visões, suas peculiaridades, arquitetura e funcionamento. Ainda, os três serviços desenvolvidos para suportar as etapas implementadas foram explorados, trazendo detalhes sobre seu funcionamento e implementação.

Além disto, um exemplo prático de como os requisitos são tratados entre as visões da abordagem para que seja possível colher os benefícios da proposta foi apresentado, trazendo os resultados de um ponto de vista do usuário e do sistema e, por fim, uma visão geral dos dados extraídos foi apresentada (figura 25).

Outro ponto, como definido na introdução, dado aos inúmeros regulamentos e serviços possíveis para atendê-los, a implementação teve como foco o regulamento LGPD e o artefato mapa dos dados. Desta forma, apesar da proposta de 4 etapas feita na seção 4.3, somente a etapa ”*Initial Data Analysis*” e ”*Regulations*” foram implementadas. Também, dentre os 5 serviços propostos na seção 4.4, somente os serviços ”*Requirement Manager Service*”, ”*Data Classification Service*” e *”Regulation Manager Service”* foram implementados.

Para finalizar, é importante destacar que este capítulo serviu como base para a publicação de um artigo completo intitulado “Framework for the development of computational solutions for the support of requirements engineering with a focus on

data protection” (DA SILVA *et al.*, 2022a), que foi apresentado no Simpósio Brasileiro de Engenharia de Software (SBES) com o objetivo de divulgar e obter feedbacks sobre o funcionamento e arquitetura da abordagem proposta.

6 AVALIAÇÃO

A avaliação da abordagem foi realizada de duas formas: (i) painel de especialistas visando avaliar a entrega de valor da abordagem e a capacidade de ser evoluída, adaptada e utilizada em diferentes cenários de desenvolvimento em prol da proteção de dados; e (ii) prova de conceito visando demonstrar a flexibilidade da abordagem através da integração da abordagem com uma ferramenta de mercado.

6.1 PAINEL DE ESPECIALISTAS

O Painel de Especialistas é uma técnica de pesquisa que reúne pessoas consideradas capazes para abordar questões relacionadas ao objetivo de pesquisa (PINHEIRO *et al.*, 2013). No planejamento e condução do Painel de Especialistas, optou-se por utilizar o *Goals, Questions and Metrics (GQM)* como guia para a definição da forma de medir os resultados em um estudo de caso.

Em resumo, a abordagem GQM inicia com a definição de metas claras (Planejamento), em seguida, formula perguntas para atingir essas metas (Execução) e, por fim, escolhe métricas para responder a essas perguntas e avaliar os resultados (Resultados)(BASILI *et al.*, 1994).

6.1.1 Planejamento

Para iniciar o processo de avaliação, primeiramente, foram estabelecidos os objetivos a serem alcançados, conforme indicado pela abordagem GQM: Entrega de Valor e Flexibilidade. Após isto, foram elaboradas perguntas destinadas a coletar impressões e percepções relacionadas à abordagem. Finalmente, definiram-se métricas para avaliar se os objetivos foram alcançados. O planejamento pode ser encontrado na Tabela 7.

Objetivo 1 (Goal): Entrega de Valor
Avaliar a eficácia da abordagem de suporte à LGPD e à proteção do usuário nos requisitos de software em termos de entrega de valor.
Perguntas 1(Questions)
Q1.1: A abordagem alerta quando dados pessoais são utilizados nos requisitos sem terem sido devidamente cadastrados? Q1.2: A abordagem utiliza a redação de requisitos para informar o usuário sobre o uso de dados pessoais? Q1.3: A abordagem utiliza a redação de requisitos para informar o usuário sobre o uso de dados pessoais sensíveis? Q1.4: A abordagem contribui para a elaboração do RIPD (Relatório de Impacto à Proteção de Dados)? Q1.5: A abordagem alerta sobre informações obrigatórias pela LGPD relacionadas a dados pessoais cadastrados nos requisitos? Q1.6: A abordagem sugere elementos relevantes da LGPD para o contexto dos requisitos? Q1.7: A abordagem apoia a proteção de dados com base nos requisitos?
Métricas (Metrics)
A métrica será a avaliação das respostas dos especialistas em uma escala que inclui "Concordo Totalmente", "Concordo", "Indiferente (ou Neutro)", "Discordo"e "Discordo Totalmente". Para determinar o sucesso dos objetivos foi estabelecido como critério para interpretação que pelo menos 70% das respostas sejam "Concordo Totalmente"ou "Concordo"em relação ao total de respostas.
Objetivo 2 (Goal): Flexibilidade
Avaliar a flexibilidade da abordagem em relação à sua capacidade de ser facilmente acoplada, implementada e utilizada em diferentes cenários de desenvolvimento de software.
Perguntas 2(Questions)
Q2.1: O sistema consegue interpretar corretamente diferentes formas de requisitos de software, como entradas para a abordagem (por exemplo, casos de uso, histórias de usuário e linguagem natural)? Q2.2: A visão de requisitos implementada na aplicação FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos) é desacoplada e flexível? Q2.3: A abordagem pode se adaptar facilmente para acomodar a integração de novos serviços de forma dinâmica? Q2.4: A abordagem permite a adição de novas etapas para a avaliação de um requisito sem dificuldades? Q2.5: Você acredita que a abordagem poderia ser utilizada com sucesso no contexto da sua empresa/organização?
Métricas (Metrics):
A métrica será a avaliação das respostas dos especialistas em uma escala que inclui "Concordo Totalmente", "Concordo", "Indiferente (ou Neutro)", "Discordo"e "Discordo Totalmente". Para determinar o sucesso dos objetivos foi estabelecido como critério para interpretação que pelo menos 70% das respostas sejam "Concordo Totalmente"ou "Concordo"em relação ao total de respostas.

Tabela 7 – GQM

Com os objetivos, perguntas e métricas definidos, a avaliação foi planejada em três fases distintas, ilustradas na Figura 22.

A fase 1 avalia a entrega de valor da abordagem (Objetivo 1) e, para tanto, foi desenvolvido um estudo de caso que contou com um cenário hipotético representando a necessidade de uma escola. O cenário ilustrou a necessidade da escola em gerenciar a entrada e saída de seus alunos por meio de um software. Requisitos de software foram elaborados e adicionados em uma ferramenta com objetivo de avaliar como a abordagem se comporta de um ponto de vista prático.

A fase 2 teve como foco analisar a flexibilidade da abordagem (Objetivo 2) e, para isto, foi disponibilizado um vídeo cujo conteúdo é uma visão geral sobre os componentes da arquitetura do software, como eles interagem entre si e as possibilidades de evolução e manutenção da abordagem.

Por fim, a fase 3 teve o objetivo de coletar o feedback dos especialistas por meio de um formulário de avaliação. É importante salientar que houveram discussões com o objetivo de esclarecer dúvidas e obter sugestões dos participantes nas duas primeiras fases realizadas, como mostra a Figura 22.

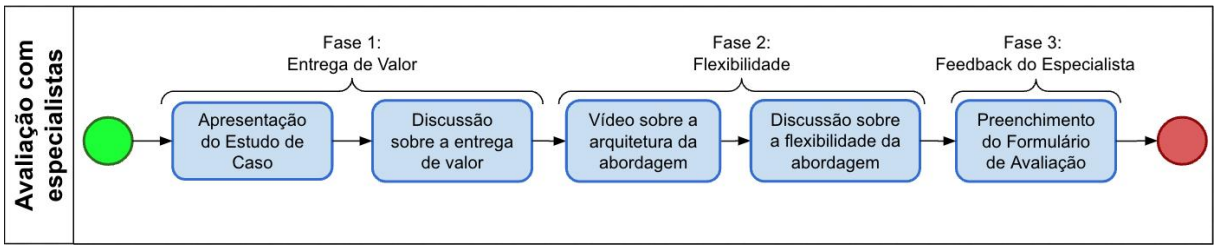


Figura 22 – Fases da Avaliação com Especialistas

6.1.1.1 Fase 1: Entrega de Valor

Na avaliação da entrega de valor, como já introduzido anteriormente, foi apresentado aos participantes da avaliação um cenário hipotético envolvendo uma escola. Os requisitos desenvolvidos também foram escritos em linguagem natural e sem se preocupar com e especificações já definidas em boas práticas ou normas, a ideia foi alcançar ambientes de desenvolvimento onde tais padrões não são considerados. Abaixo estão listados os requisitos e seus respectivos objetivos:

> *"A escola Alegra, tendo a necessidade de gerenciar a entrada e saída de seus estudantes, contratou uma empresa terceira para desenvolver um software para tal gerenciamento, a empresa então utilizou sua ferramenta de gerenciamento de requisitos interna chamada FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos) para criar os requisitos necessários para a primeira versão do software solicitado."*

1. **RF01:** É preciso que o sistema solicite credenciais para que os usuários possam acompanhar a entrada e saída dos alunos. **Objetivo**: Verificar a capacidade da abordagem de apontar informações faltantes sobre dado pessoal segundo a LGPD.

2. **RF02:** Como usuário do sistema preciso cadastrar o aluno para poder gerenciar sua entrada e saída nos portões. **Objetivo**: Verificar a capacidade da abordagem identificar e classificar dados comuns e realizar análise de dados infantis do ponto de vista da LGPD.

3. **RF03:** É preciso cadastrar os responsáveis pelos alunos, indicando nome, telefone, email e sexo. **Objetivo**: Verificar se a abordagem gera alerta quando um requisito cadastrado sem o apontamento de dados indica de maneira implícita o uso de dados pessoais.

4. **RF04:** O sistema deve possibilitar que uma das formas de autorização de entrada nas dependências seja por meio do reconhecimento facial do responsável. Para tanto, o sistema deve permitir que seja inserido a matrícula do aluno (para associar ao responsável), nome e email do responsável. **Objetivo**: Verificar a capacidade da abordagem gerar alertas para dados pessoais comuns e sensíveis. Além disso a análise de regulamentos deve apontar trechos relacionados ao uso de dados sensíveis segundo a LGPD.

5. **RF05:** O sistema precisa cadastrar os funcionários da escola. **Objetivo**: Verificar a capacidade da abordagem de apontar indicações da LGPD para compartilhamento de dados tratados.

6. **RF06:** O sistema deve permitir o envio dos dados dos responsáveis para a empresa parceira que faz o serviço de segurança da escola. **Objetivo**: Verificar a capacidade da abordagem de apontar indicações da LGPD para transferência de dados.

6.1.1.1.1 FHGR

Para viabilizar a execução da avaliação foi desenvolvida uma aplicação para simular um sistema aderente à abordagem proposta por este trabalho, chamada FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos). Originalmente, a ferramenta permite a criação, exclusão, edição e listagem de requisitos, onde um requisito é composto apenas por duas informações, Título e Descrição. Após o desenvolvimento da aplicação FHGR, foi implementado na mesma o modelo conceitual proposto, o que adicionou também outras capacidades como cadastro de dados para associar aos requisitos já gerenciados, a capacidade de interpretar os eventos recebidos da

Visão do Workflow e o envio de requisitos para análise. Para tanto, foram utilizadas as bibliotecas React e Javascript.

Estes requisitos foram adicionados na ferramenta FHGR e durante a apresentação cada um foi enviado para análise da abordagem, o objetivo foi demonstrar ao especialista de forma prática como a abordagem responde para cada um dos requisitos criados. A Figura 23 apresenta os requisitos dispostos na ferramenta.

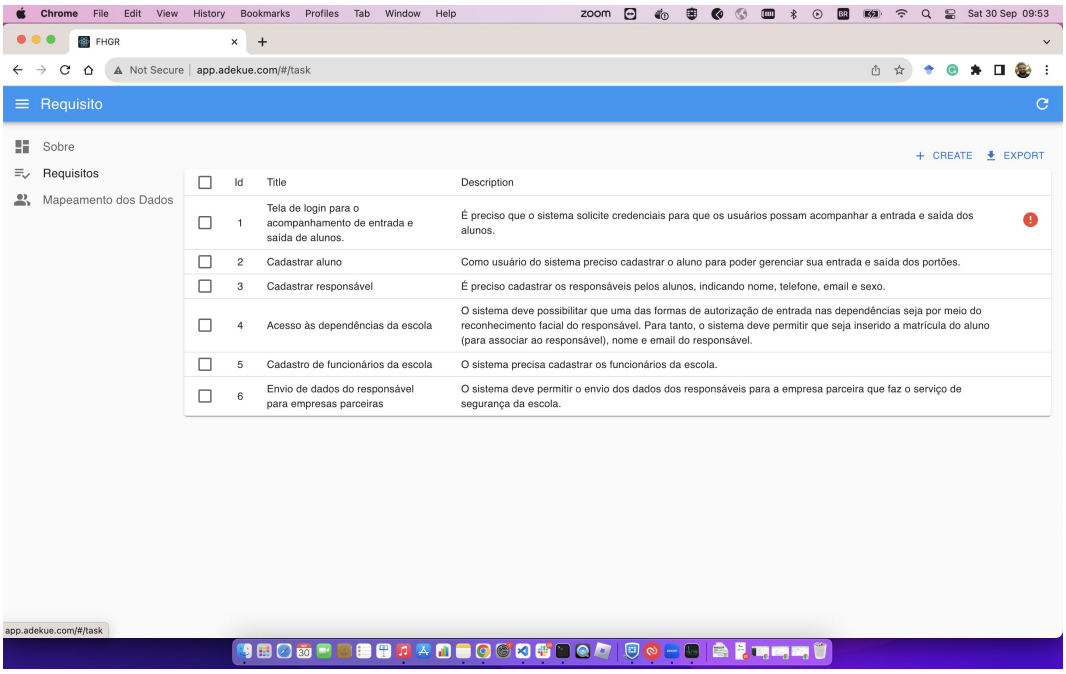


Figura 23 – FHGR - Requisitos Cadastrados

A Figura 24 demonstra a análise realizada pela abordagem após o envio do requisito RF02, neste caso em especial, a abordagem apontou que não havia pendência para o requisito enviado (marcação "A"). Contudo, a abordagem trouxe um alerta de que possíveis dados pessoais foram detectados no requisito (marcação "B") e, além disto, a abordagem sugere um trecho da LGPD para o tratamento de dados pessoais de crianças e adolescentes (marcação "C").

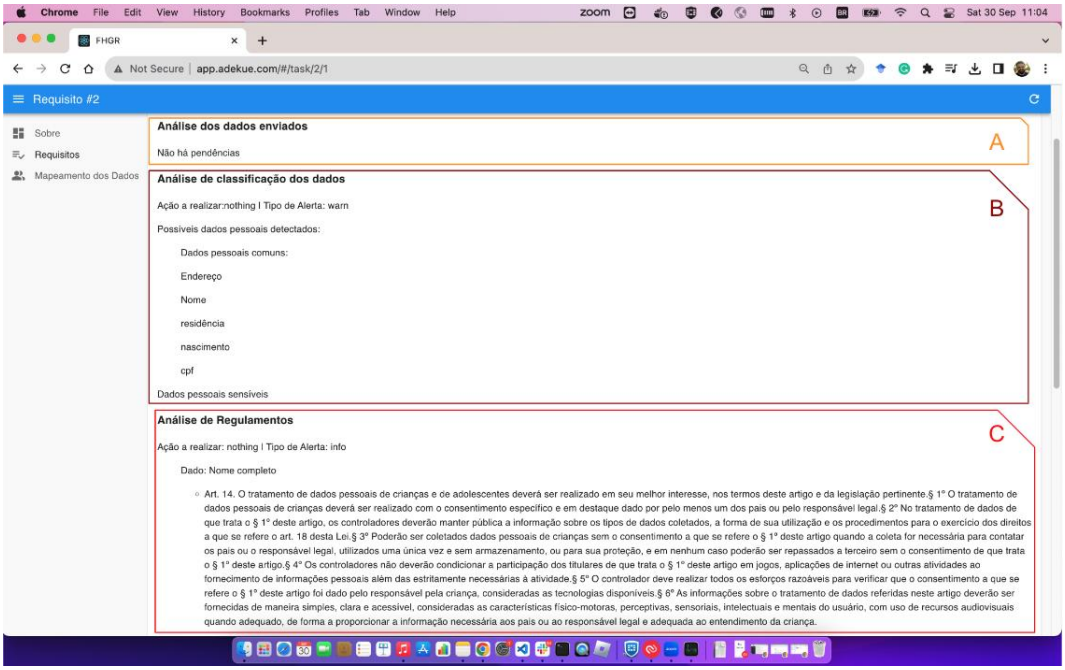


Figura 24 – FHGR - Requisito Analisado

Após passar por todos os requisitos, realizando a leitura, enviando para análise e apresentando os resultados gerados pela abordagem, foi então apresentado a cada especialista o mapa de dados gerado, onde foi possível visualizar o dado tratado associado a cada requisito de software analisado, como ilustra a Figura 25.

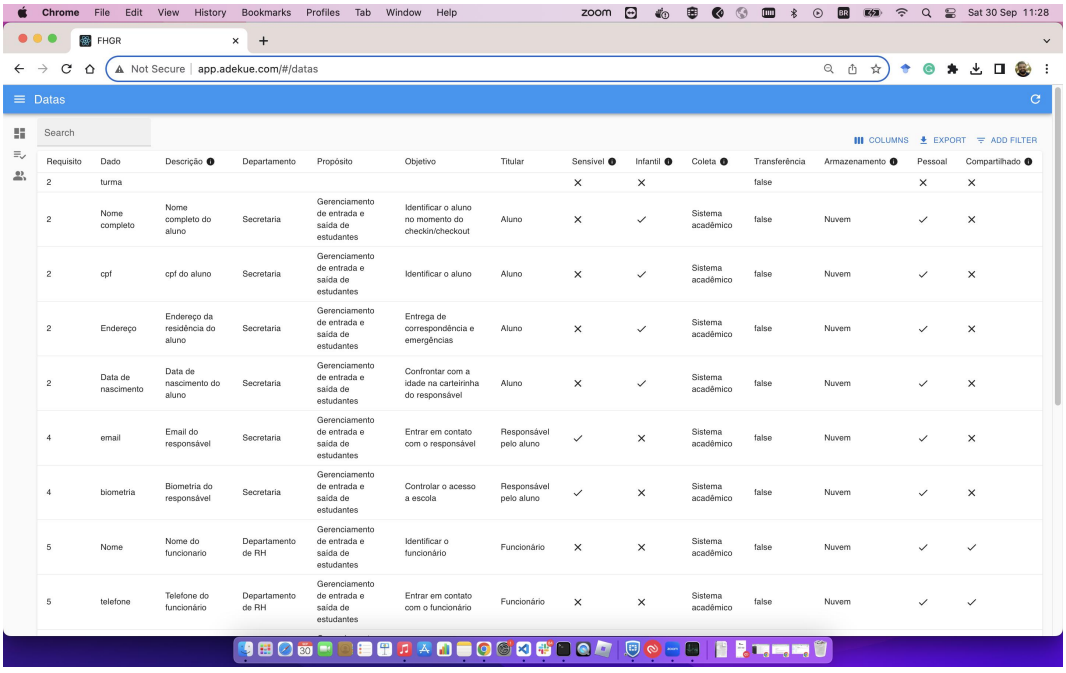


Figura 25 – FHGR - Mapeamento dos Dados

6.1.1.2 Fase 2: Flexibilidade

A segunda etapa consistiu em um vídeo com a duração de 15 minutos e 43 segundos com o objetivo de demonstrar a capacidade da abordagem ser evoluída, adaptada e utilizada em diferentes cenários de desenvolvimento em prol da proteção de dados. Para tanto, a apresentação foi segmentada considerando as visões da abordagem, apresentando no detalhe a arquitetura de cada visão e como os componentes interagem entre si.

O vídeo não se ateve apenas à apresentação, trouxe também exemplos práticos do envio do requisito para ser analisado na abordagem, bem como uma breve explicação no modelo de entidade e relacionamento, da mensageria e do código fonte desenvolvido para a aplicação FHGR juntamente com a sua implementação do modelo conceitual. O vídeo está disponível por meio da seguinte URL: `https://www.youtube.com/watch?v=qUUruEeDEgo`.

6.1.1.3 Fase 3: Feedback do Especialista

Para coletar o *feedback* dos especialistas, foi elaborado um formulário de avaliação com 4 seções: i) Termo de Consentimento; ii) Perfil do Especialista; iii) Entrega de Valor; e iv) Flexibilidade.

O Termo de consentimento buscou dar uma visão geral dos objetivos, procedimentos, riscos e benefícios, confidencialidade e privacidade do estudo em questão com objetivo de coletar do participante sua aceitação voluntária ao estudo.

A seção de Perfil do Especialista focou em trazer questões que apoiassem a posterior classificação dos voluntários com relação às suas especialidades.

Já a seção de Entrega de Valor trouxe um grupo de afirmações e questões com foco em responder as perguntas elaboradas no objetivo 1 definidas na Tabela 7, de forma geral nesta seção procurou-se coletar a opinião dos participantes sobre a capacidade da abordagem em interpretar requisitos de maneiras distintas, apoiar a conformidade do software com a LGPD e gerar alertas para que a equipe de desenvolvimento esteja atenta às questões de privacidade no software.

Assim como a seção anterior, a seção de Flexibilidade trouxe afirmações e questões com foco em responder as questões do objetivo 2 definidas na Tabela 7. Contudo, o foco foi extrair as opiniões dos participantes sobre a capacidade da arquitetura ser evoluída, adaptada e utilizada em diferentes cenários de desenvolvimento em prol da proteção de dados.

O formulário de avaliação na íntegra está disponibilizado no Apêndice C.

6.1.2 Execução

A avaliação contou com a participação de seis especialistas, selecionados pelos pesquisadores deste trabalho (amostragem por conveniência), com formação em Ciência da Computação e Sistemas de Informação, iniciando em 23 de agosto de 2023 e se estendeu até 19 de setembro de 2023, durando entre 1h (uma hora) e 1h30 (uma hora e meia), com uma das avaliações realizada presencialmente e as outras cinco conduzidas de forma remota. Todos os especialistas tem experiência em grupos ou comitês relacionados à proteção de dados. O perfil desses especialistas está detalhado na Tabela 8.

Sigla	Experiência Proteção de Dados (anos)	Nível em Proteção de Dados	Experiência LGPD (anos)	Nível em LGPD	Nível em Arquitetura de Software	Nível em Requisito de Software
E1-PLAR	Mais de 3	8 a 10	Mais de 3	8 a 10	8 a 10	8 a 10
E2-A	1 a 3	2 a 4	Mais de 3	2 a 4	6 a 8	4 a 6
E3-R	1 a 3	4 a 6	Entre 1 e 3	4 a 6	0 a 2	8 a 10
E4-PAR	Mais de 3	6 a 8	Entre 1 e 3	4 a 6	8 a 10	8 a 10
E5-PLR	Entre 1 e 3	8 e 10	Entre 1 e 3	8 a 10	4 a 6	6 a 8
E6-PLAR	Mais de 3	6 a 8	Mais de 3	6 a 8	6 a 8	8 a 10

Tabela 8 – Perfil dos Especialistas <> Legendas: P: Proteção de Dados, L: LGPD, A: Arquitetura de Software, R: Requisito de Software

Conforme evidenciado na tabela, os especialistas possuem experiências e conhecimentos que se distribuem nas seguintes áreas: Proteção de Dados e LGPD, Arquitetura de Software e Requisitos de Software. A existência de perfis distintos, mas ao mesmo tempo relacionados ao tema de Proteção de Dados e LGPD, decorre do próprio escopo deste trabalho e da consequente necessidade para avaliação realizada.

Além disto, a tabela apresenta uma coluna "sigla", que identifica as principais especialidades do especialista em questão. É considerado especialista nos critérios deste trabalho, o voluntário com nível igual ou superior a 6. É importante destacar que o voluntário pode ter mais de uma especialidade, desde que atenda os critérios. Além disto, as questões/definições associadas a cada nível dos temas estão disponíveis no formulário de avaliação, que pode ser encontrado no Apêndice C.

Para melhor esclarecer as siglas dos perfis apresentados na Tabela 8, segue detalhado:

1. E1-PLAR: Especialista em Proteção de Dados, LGPD, Arquitetura de Software e Requisito de Software;

2. E2-A: Especialista em Arquitetura de Software;

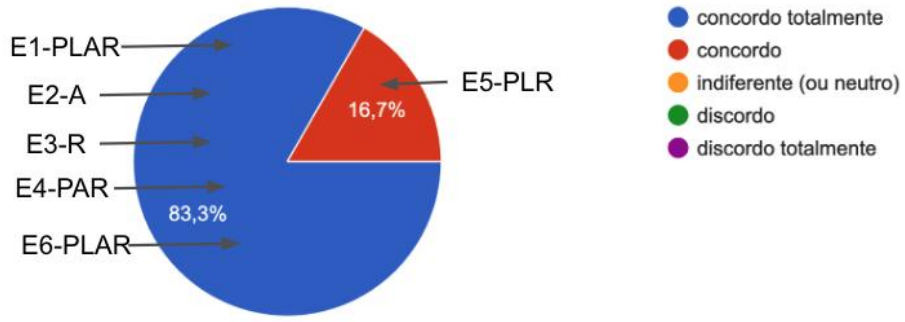
3. E3-R: Especialista em Requisito de Software;
4. E4-PAR: Especialista em Proteção de Dados, Arquitetura de Software e Requisito de Software;
5. E5-PLR: Especialista em Proteção de Dados, LGPD e Requisito de Software;
6. E6-PLAR: Especialista em Proteção de Dados, LGPD, Arquitetura de Software e Requisito de Software.

6.1.3 Resultados

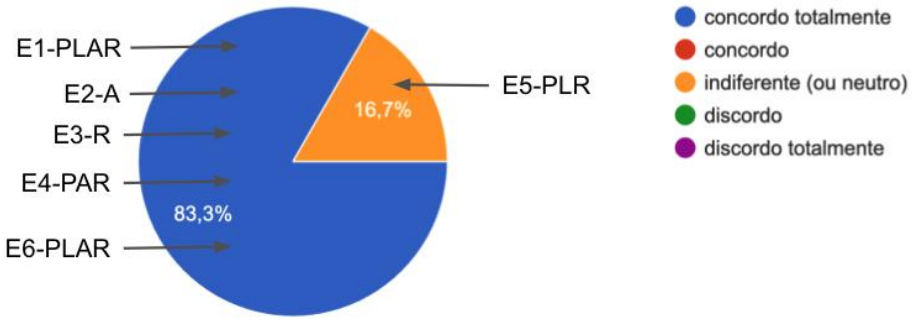
Aqui são apresentados os resultados obtidos via formulário de avaliação disponibilizado aos especialistas.

6.1.3.1 Entrega de Valor

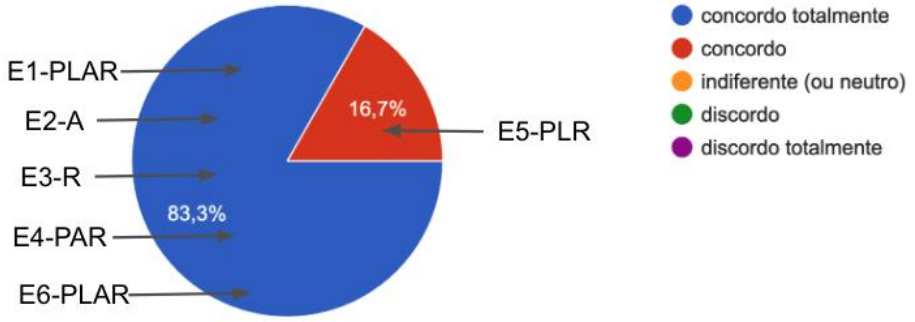
Q1: A abordagem alerta quanto ao possível uso de dados pessoais no requisito mesmo que o usuário não os tenha cadastrado



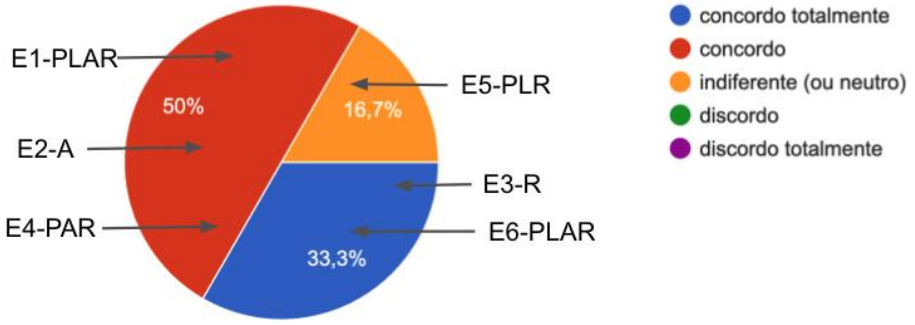
Q2: A abordagem colabora para a construção do RIPD (Relatório de Impacto a Proteção de Dados)



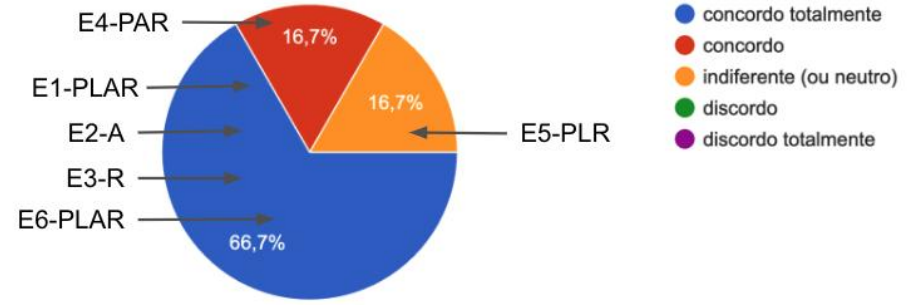
Q3: A abordagem alerta quanto a informações obrigatórias pela LGPD de dados pessoais cadastrados no requisito



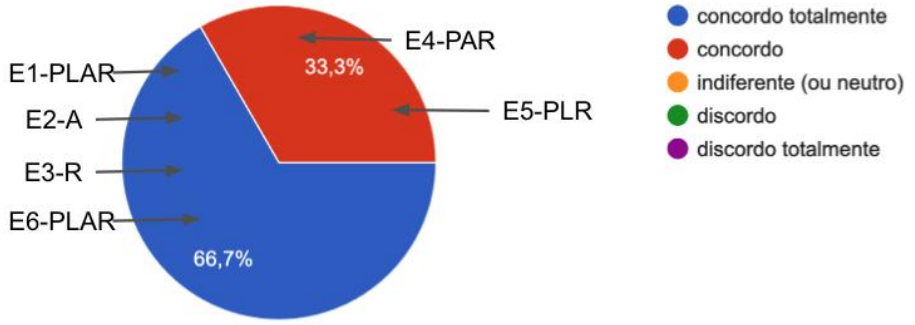
Q4: A abordagem sugere itens da LGPD relevantes para o contexto do requisito.



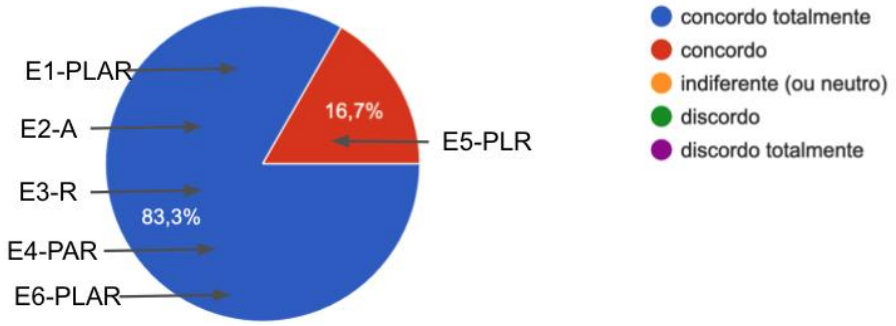
Q5: A abordagem utiliza a escrita de requisitos para alertar o usuário quanto ao uso de dados pessoais.



Q6: A abordagem utiliza a escrita de requisitos para alertar o usuário quanto ao uso de dados pessoais sensíveis.

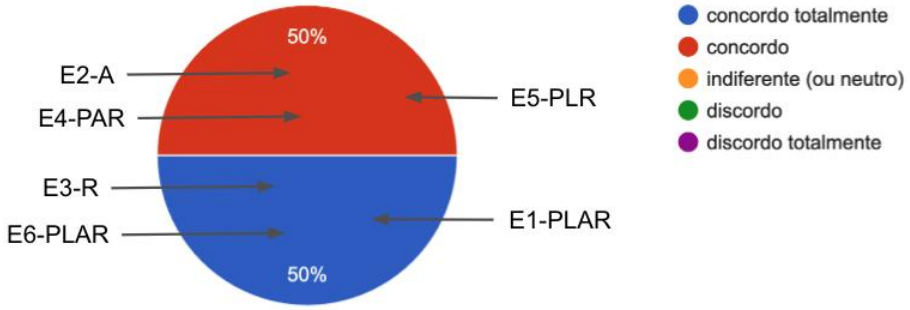


Q7: A abordagem apoia a proteção de dados com base nos requisitos.

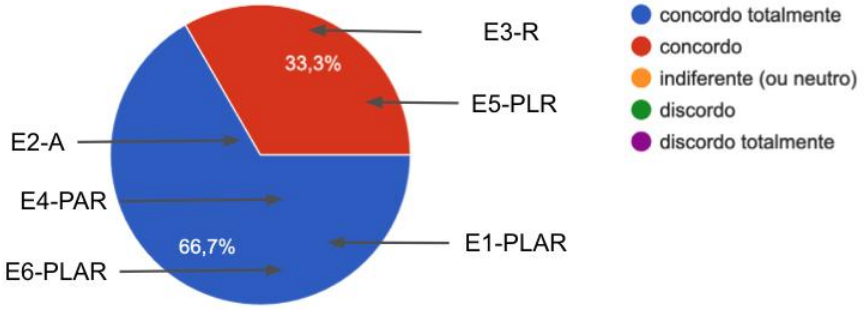


6.1.3.2 Flexibilidade

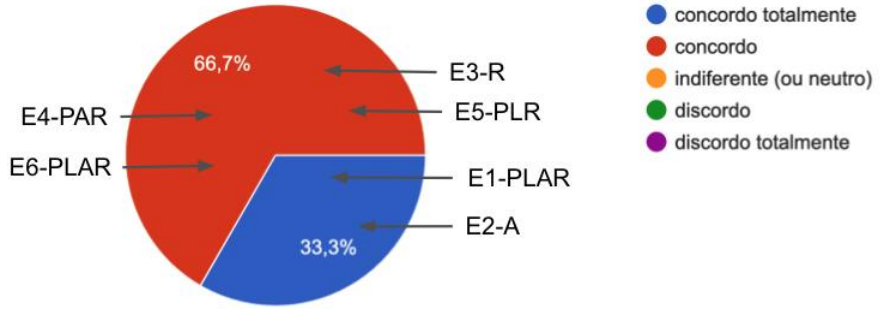
Q1: O sistema consegue interpretar corretamente escritas distintas de requisitos de software como input da abordagem. (ex: caso de uso, história de usuário e linguagem natural)



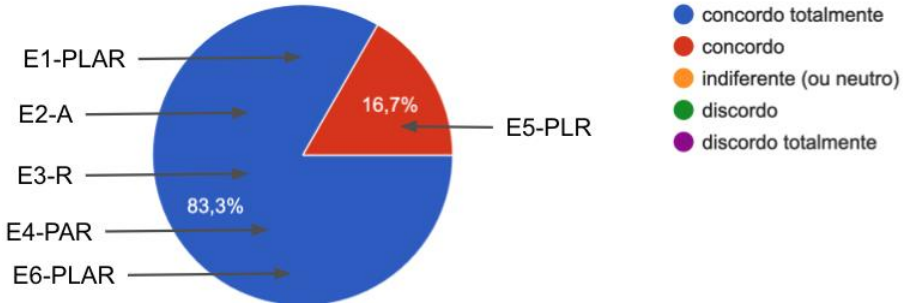
Q2:A visão de requisitos, implementada na aplicação FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos), é desacoplada .



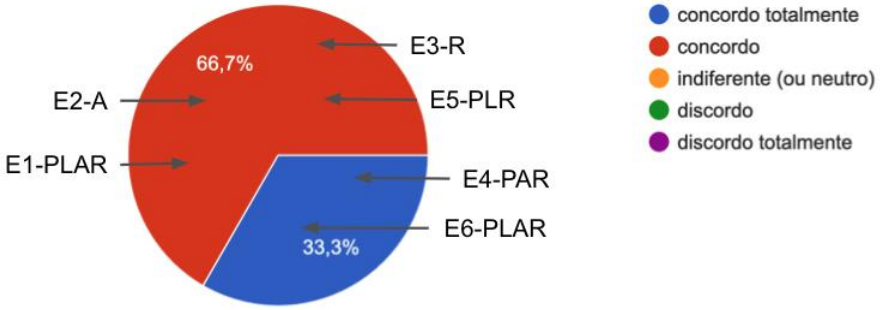
Q3: A abordagem consegue se adaptar para receber novos serviços de forma dinâmica.



Q4: A abordagem consegue adicionar novas etapas para avaliação de um requisito.



Q5: Você entende que a abordagem poderia ser utilizada no contexto da sua empresa/organização?



Com relação aos resultados da primeira fase, estes se mostraram bem consistentes no que tange o alcance dos objetivos, do ponto de vista da entrega de valor, como mostra a Figura 26. Os seis especialistas concordam com as afirmações apresentadas nas legendas (Q1, Q3, Q6, Q7) e, cinco dos seis especialistas concordam com todas as afirmações realizadas. O especialista E5-PLR, que se posiciona “indiferente” nas afirmações (Q2, Q4, Q5), registrou a justificativa que segue: “As questões que respondi como indiferente acredito que ainda precisam passar por um refinamento para conseguir atender plenamente.”.

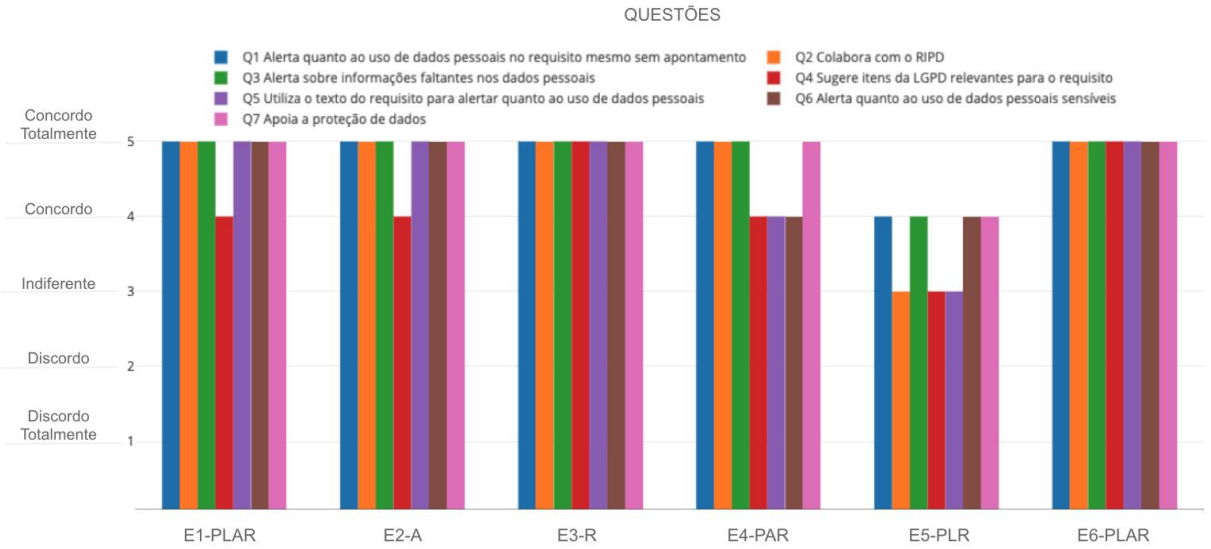


Figura 26 – Consolidado - Entrega de Valor

Com relação à flexibilidade da arquitetura, todos os participantes concordaram, em um nível ou outro, com relação à sua capacidade de ser facilmente acoplada, implementada e utilizada em diferentes cenários de desenvolvimento de software, como pode ser visto na Figura 27.

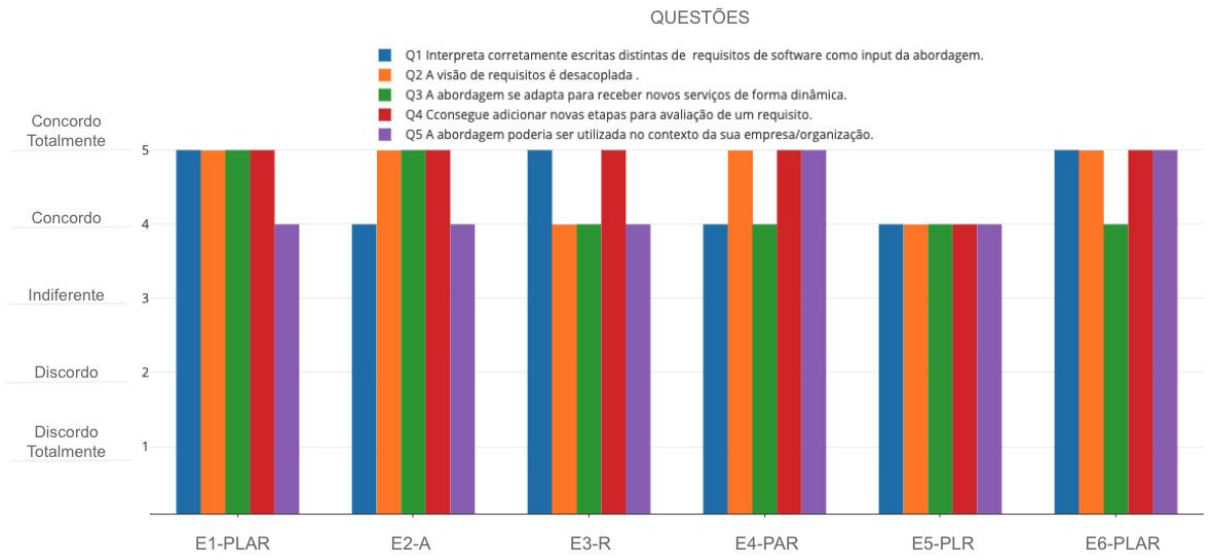


Figura 27 – Consolidado - Flexibilidade

Resumidamente, a média dos especialistas que concordaram ou concordaram totalmente com a Entrega de Valor da abordagem ficou em 90,47%, já a média dos especialistas que concordam ou concordam totalmente com a Flexibilidade da abordagem ficou em 100%. Desta forma, dado o critério de sucesso definido em 70%, pode-se afirmar que os objetivos definidos foram alcançados.

Durante as avaliações, especialistas trouxeram algumas sugestões. Uma dessas sugestões foi a incorporação da API Swagger UI para simplificar a renderização

da documentação da API *Orchestrator*, um componente da visão do Workflow.

Outra sugestão foi a implementação do modelo conceitual em forma de plugin, permitindo que desenvolvedores façam anotações ao lidar com dados pessoais no código. Isso possibilitaria a integração desse processo ao fluxo de integração contínua para alinhamento com a abordagem.

Além disso, foram fornecidas sugestões com foco na continuidade do trabalho, visando criar novos módulos de análise de risco e boas práticas para cobrir todo o processo de criação do RIPD.

6.2 PROVA DE CONCEITO

A Prova de Conceito consistiu em implementar o modelo conceitual em um plugin a ser instalado e configurado na ferramenta de monitoramento de tarefas e acompanhamento de projetos Jira. O plugin foi desenvolvido utilizando a plataforma de desenvolvimento Forge, disponibilizada pela Atlassian, empresa proprietária do Jira e encontra-se disponível na plataforma de versionamento disponibilizado pelo SETIC por meio da URL `https://codigos.ufsc.br/masters-degree/privacy_jira_plugin`

É importante destacar que, assim como a ferramenta FHGR foi desenvolvida para o estudo de caso desta avaliação, o plugin desenvolvido para o Jira também é uma implementação do modelo conceitual, ou seja, ambos tem o intuito de facilitar a integração com a abordagem, dando diretivas para estabelecer a comunicação com a Visão do Workflow. A Figura 28 mostra o board do Jira, onde foram cadastrados requisitos à serem analisados pela abordagem.

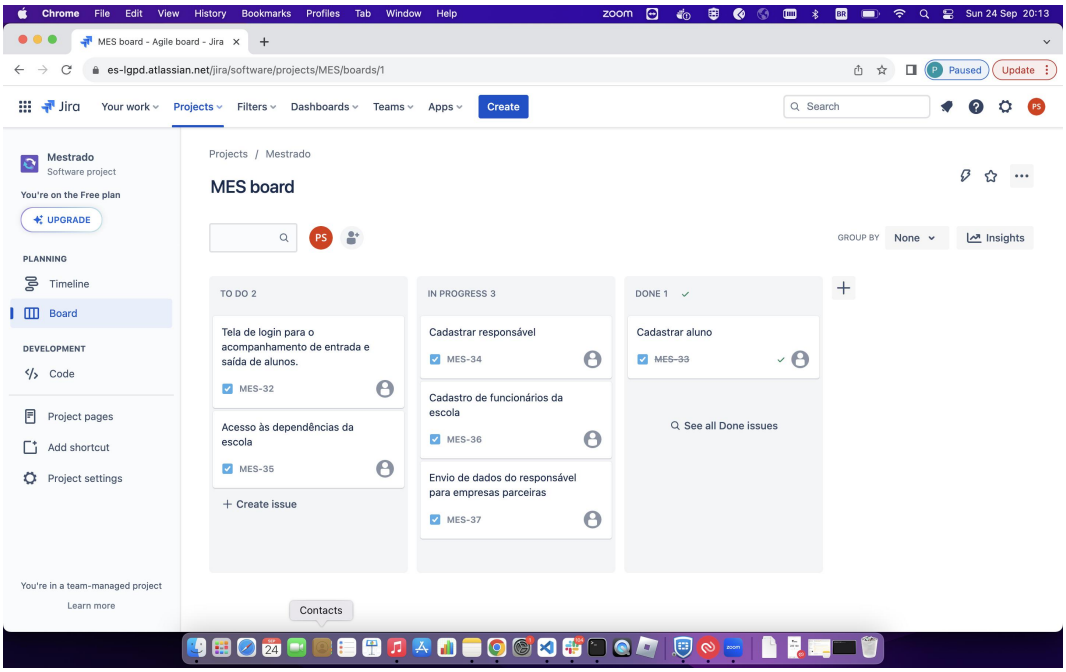


Figura 28 – Board Jira com tarefas

Ao clicar no card cadastrado no board do Jira, irá abrir uma janela que apresenta o plugin já instalado, identificado pelo triângulo azul na janela, como pode ser observado na Figura 29.

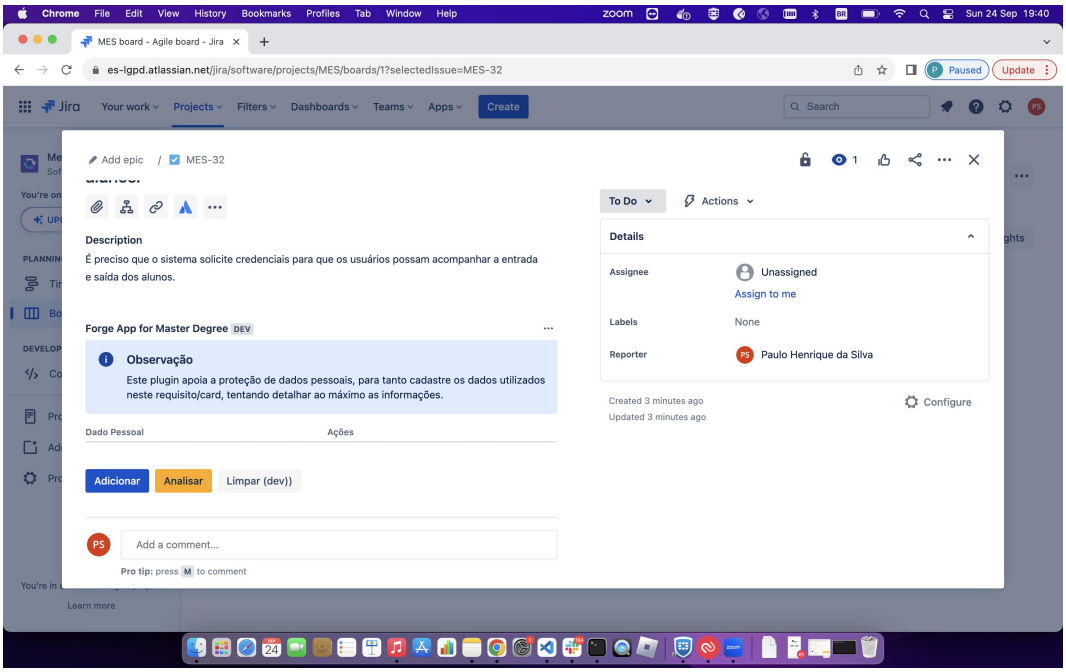


Figura 29 – Detalhe card Jira mostrando plugin

Ao clicar no botão adicionar, o plugin abre uma outra janela, permitindo que o usuário também cadastre dados pessoais, esta possibilidade de cadastro foi implementada pois é algo previsto pelo modelo conceitual para enriquecer o processo de análise da abordagem, a janela pode ser vista na Figura 30.

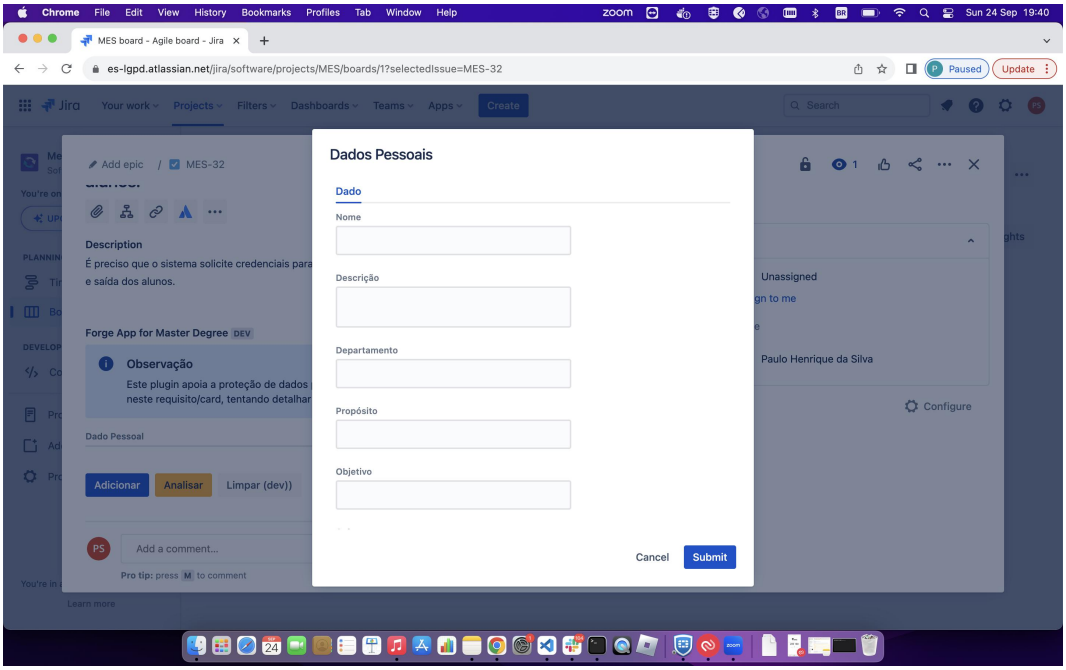


Figura 30 – Detalhe card Jira - modal dados pessoais

Ao clicar em salvar, o modal de cadastro dos dados pessoais é salvo, retornando à janela anterior, agora com os dados já cadastrados pelo usuário, sendo possível enviar o requisito para análise, ao clicar no botão Analisar, ver Figura 31.

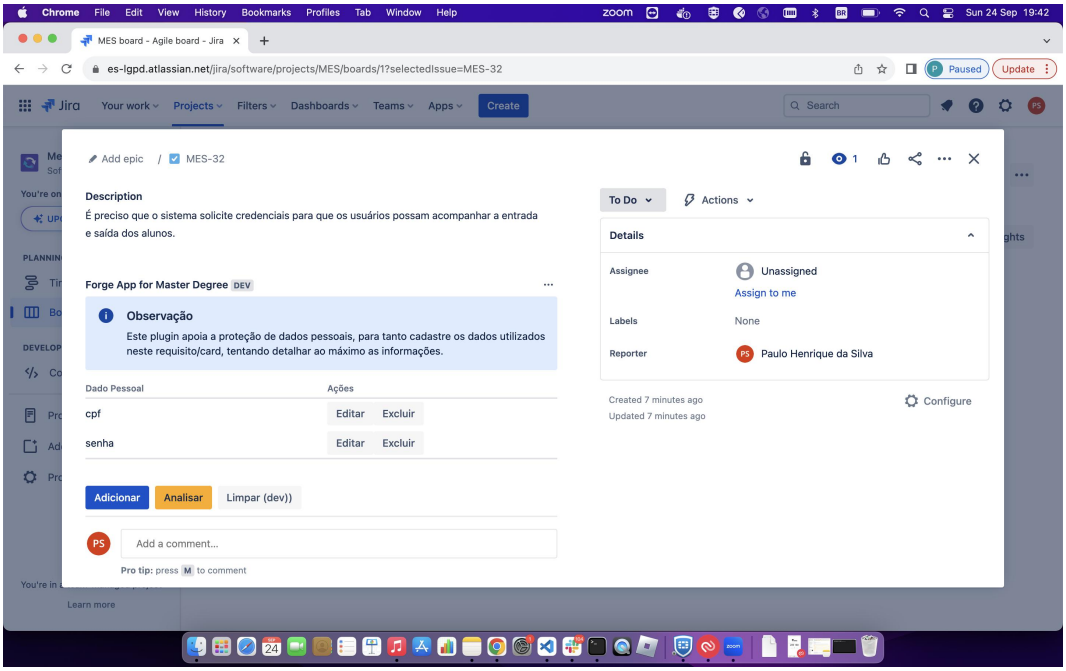


Figura 31 – Detalhe card Jira - dados pessoais cadastrados

Com a criação do plugin e a implementação do modelo conceitual proposto na seção 4.2, foi possível constatar viabilidade de estabelecer a comunicação de acordo com a abordagem proposta. No entanto, devido a restrições de tempo, não foi possível desenvolver uma interface visual para expor dados e análises dos requisitos, semelhante à ferramenta FHGR.

6.3 CONSIDERAÇÕES DO CAPÍTULO

Em conclusão, a avaliação da abordagem por meio do painel de especialistas apontou que os resultados foram alcançados conforme os critérios de sucesso definidos nas métricas do GQM, detalhada na Tabela 7. Além disso, a prova de conceito por si só é uma evidência da capacidade das soluções de mercado de se integrarem à abordagem por meio do modelo conceitual, corroborando assim com o posicionamento dos especialistas em relação à flexibilidade da abordagem.

Entretanto, é preciso ressaltar que não foram realizadas análises com relação a acurácia dos serviços de classificação de dados e o serviço de sugestão de trechos da LGPD. Outro ponto a se considerar, é que apesar do foco da prova de conceito ter objetivado apontar a viabilidade da abordagem se integrar à ferramentas de mercado, suas possibilidades não foram exauridas, deixando de fora a visualização contendo o mapa dos dados.

7 CONCLUSÕES

O objetivo deste trabalho foi apoiar a definição de requisitos de software atentos à proteção de dados por meio de uma abordagem que possa ser implementada por ferramentas de gerenciamento de requisitos. Para tanto, alguns objetivos específicos foram definidos e são recuperados nesta seção como forma de verificar seu alcance.

O primeiro objetivo específico foi definir um modelo conceitual para especificar aspectos essenciais para que ferramentas possam implementar a fim de definir requisitos de software com foco na proteção de dados pessoais. O modelo conceitual foi proposto na seção 4.2 e implementado na ferramenta FHGR, utilizada na avaliação deste trabalho, além disto o modelo também foi implementado no plugin utilizado na Prova de Conceito apresentada na seção 6.2.

O segundo objetivo específico, foi definir um Workflow que permita customizar etapas e acoplar serviços que processem requisitos de software em prol da proteção de dados. A proposta foi realizada na Seção 4.3 e implementada para o estudo de caso. Para este objetivo específico, duas afirmações foram direcionadas na avaliação do estudo de caso, as afirmações Q3 e Q4 do objetivo de Flexibilidade e, para ambas afirmações, todos os especialistas concordaram, com isto entende-se que este objetivo específico também foi alcançado.

O terceiro objetivo específico foi de propor um conjunto de serviços para apoiar a adesão aos regulamentos de proteção de dados pessoais. A Seção 4.4 especificou os serviços e três destes serviços foram implementados para a realização do estudo de caso, *i)requirement manager service*; *ii)data classification service*; e *e iii) regulation manager service*.

Sobre o quarto objetivo específico, ”Avaliar a viabilidade de uso da abordagem, sua capacidade de adaptação e entrega de valor”, é possível identificar sua viabilidade pela própria implementação da abordagem para avaliação deste trabalho, que incluiu tanto a implementação do modelo conceitual pela FHGR e pelo plugin Jira, quanto a implementação do Workflow e serviços.

Outro ponto, o posicionamento do painel de especialistas sobre a Entrega de Valor indica uma concordância de 90,47% no que tange a entrega de valor da abordagem, bem como o posicionamento em relação à flexibilidade da abordagem, onde o posicionamento dos especialistas foi unânime com relação à flexibilidade da abordagem, indicando forte capacidade de adaptação. Considerando as evidências expostas para o objetivo 4, é possível concluir que o objetivo foi alcançado.

Por fim, dado os resultados das avaliações e as evidências indicando o alcance dos objetivos específicos, conclui-se que a abordagem proposta por este trabalho apoia a definição de requisitos de software atentos à proteção de dados, por meio de uma abordagem que possa ser implementada por ferramentas de gerenciamento de

requisitos.

No âmbito dos trabalhos futuros, algumas direções se destacam como promissoras para o aprimoramento da pesquisa e sua aplicabilidade prática:

1. Implementação dos Serviços de Avaliação de Riscos e Boas Práticas para o RIPD: Uma das próximas etapas relevantes é a implementação efetiva dos serviços de análise de riscos e boas práticas para a entrega do RIPD. Isso ampliaria a capacidade da abordagem em auxiliar na conformidade com regulamentos de proteção de dados e no gerenciamento de riscos de privacidade.

2. Evolução dos Serviços com Aprendizado de Máquina: Uma abordagem interessante seria a evolução dos serviços desenvolvidos neste trabalho por meio da incorporação de técnicas de aprendizado de máquina. Isso poderia aprimorar a capacidade da classificação dos dados pessoais, sugerir trechos de regulamentos mais precisos, aprendizado baseado no feedback do usuário e para abordagem lidar com cenários complexos e em constante mudança relacionados à proteção de dados pessoais.

3. Desenvolvimento de Área Administrativa para a Visão do Workflow: Para facilitar a criação, edição e exclusão de etapas do Workflow, bem como adicionar as configurações de novos serviços ou alterar configurações existentes, sugere-se o desenvolvimento de uma interface específica para tal objetivo. Essa adição permitiria um controle mais eficiente, flexível e amigável, dando mais autonomia para os usuários.

4. Marketplace para plugins da Comunidade: A abordagem foi desenvolvida para permitir que novos serviços sejam acoplados a ela e de forma dinâmica, isto permite que serviços desenvolvidos por terceiros possam ficar disponíveis para quem tiver interesse de uma solução específica. Para tanto, é preciso disponibilizar documentação amigável para criação dos serviços e um ambiente que facilite a divulgação e adoção dos mesmos.

5. Integração de Plugin para Atualização de Dados Pessoais: Uma sugestão valiosa de um dos especialistas é a implementação de um plugin que possa se integrar à abordagem durante o desenvolvimento de software. Isso facilitaria a manutenção dos dados pessoais, mantendo-os sempre atualizados de forma eficaz. Essa melhoria reduziria as chances de falhas no mapeamento dos processos internos da empresa, permitindo maior conformidade com regulamentos de proteção de dados.

Essas perspectivas de desenvolvimento representam oportunidades significativas para aprimorar a abordagem proposta, tornando-a mais robusta e eficaz na gestão

de requisitos relacionados à proteção de dados e à privacidade. Ao explorar esses caminhos, é possível fortalecer a contribuição desta pesquisa para a área de segurança da informação e conformidade com regulamentos de privacidade.

REFERÊNCIAS

ABES SOFTWARE. **Mercado Brasileiro de Software: panorama e tendências**. [*S.l.*: *s.n.*], 2020. P. 24. ISBN 9788586700033.

ALSHAMMARI, Majed; SIMPSON, Andrew. A UML Profile for Privacy-Aware Data Lifecycle Models. *In*: COMPUTER Security. [*S.l.*: *s.n.*], 2018. P. 189–209.

ANSARI, Md Tarique Jamal; BAZ, Abdullah; ALHAKAMI, Hosam; ALHAKAMI, Wajdi; KUMAR, Rajeev; KHAN, Raees Ahmad. P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements. **Arabian Journal for Science and Engineering**, Springer Berlin Heidelberg, n. 0123456789, 2021. ISSN 21914281. DOI: 10.1007/s13369-021-05476-z. Disponível em: https://doi.org/10.1007/s13369-021-05476-z.

ANTIGNAC, Thibaud; LE MÉTAYER, Daniel. Trust Driven Strategies for Privacy by Design. *In*: DAMSGAARD JENSEN, Christian; MARSH, Stephen; DIMITRAKOS, Theo; MURAYAMA, Yuko (Ed.). **Trust Management IX**. Cham: Springer International Publishing, 2015. P. 60–75.

AYALA-RIVERA, Vanessa; PASQUALE, Liliana. The grace period has ended: An approach to operationalize GDPR requirements. **Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018**, IEEE, p. 136–146, 2018. DOI: 10.1109/RE.2018.00023.

BALDASSARRE, Maria Teresa; BARLETTA, Vita Santa; CAIVANO, Danilo; PICCINNO, Antonio. A Visual Tool for Supporting Decision-Making in Privacy Oriented Software Development. **ACM International Conference Proceeding Series**, 2020. DOI: 10.1145/3399715.3399818.

BARTOLINI, Cesare; CALABRÓ, Antonello; MARCHETTI, Eda. GDPR and Business Processes: An Effective Solution. *In*: PROCEEDINGS of the 2nd International Conference on Applications of Intelligent Systems. Las Palmas de Gran Canaria, Spain: Association for Computing Machinery, 2019. (APPIS '19). DOI: 10.1145/3309772.3309779. Disponível em: https://doi.org/10.1145/3309772.3309779.

BASILI, V.; CALDEIRA, G.; ROMBACH, H. D. The Goal Question Metric Approach. *In*: ENCYCLOPEDIA of Software Engineering. [*S.l.*]: John Wiley & Sons., 1994.

BEDNAR, Kathrin; SPIEKERMANN, Sarah; LANGHEINRICH, Marc. Engineering Privacy by Design: Are engineers ready to live up to the challenge? **Information Society**, Routledge, v. 35, n. 3, p. 122–142, mai. 2019. ISSN 10876537. DOI: 10.1080/01972243.2019.1583296.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **civilistica.com**, v. 9, n. 3, p. 2, 2020.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Editora Forense, n. 2, dez. 2019.

BOTELHO, Rafael Guimarães; CRUZ DE OLIVEIRA, Cristina da. **Literaturas branca e cinzenta: uma revisão conceitual White and grey literature: a conceptual revision**. v. 44. [*S.l.*], 2008. P. 501–513. Disponível em: http://lattes.cnpq.br/8870540362781423.

BRASIL. **Constituição da República Federativa do Brasil**. [*S.l.*: *s.n.*], 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** [*S.l.*: *s.n.*], 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BREAUX, Travis D.; ANTÓN, Annie I.; SPAFFORD, Eugene H. A distributed requirements management framework for legal compliance and accountability. **Computers and Security**, v. 28, n. 1-2, p. 8–17, 2009. ISSN 01674048. DOI: 10.1016/j.cose.2008.08.001.

C. TIKKINEN-PIRI, A. Rohunen; MARKKULA, J. Eu general data pro- tection regulation: Changes and implications for personal data collecting companies. **International Conference on Web Engineering. Springer**, 2017.

CAMACHO, Cristina Rosa; MARCZAK, Sabrina; CRUZES, Daniela S. Agile team members perceptions on non-functional testing influencing factors from an empirical Study. **Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016**, IEEE, p. 582–589, 2016. DOI: 10.1109/ARES.2016.98.

CANEDO, Edna Dias; CALAZANS, Angélica Toffano Seidel;
MASSON, Eloisa Toffano Seidel; COSTA, Pedro Henrique Teixeira; LIMA, Fernanda. Perceptions of ICT Practitioners Regarding Software Privacy. **Entropy**, v. 22, n. 4, p. 429, 2020. DOI: 10.3390/e22040429.

CAVOUKIAN, Ann. Privacy by Design. **Identity in the Information Society**, v. 3, n. 2, p. 1–12, 2010. ISSN 1876-0678.

CAVOUKIAN, Ann. Privacy by design [leading edge]. **IEEE Technology and Society Magazine**, IEEE, v. 31, n. 4, p. 18–19, 2012. ISSN 02780097. DOI: 10.1109/MTS.2012.2225459.

CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices**. Ontario, Canada, 2011.

CENTER FOR INTERNET SECURITY (CIS). **CIS Controls Version 8**. [*S.l.*: *s.n.*], 2021. Disponível em: https://www.cisecurity.org/controls/.

CNPD, Conselho Nacional de Proteção de Dados. **Como Proteger seus Dados Pessoais**. 21 de outubro de 2023. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-como-proteger-seus-dados-pessoais.pdf.

CUNHA, B. E. de M.; AL., et. As Dificuldades da Implementação da LGPD no Brasil. **Revista Projetos Extensionistas**, v. 1, n. 2, p. 39–47, 2021.

DA SILVA, Paulo Henrique; BENITTI, Fabiane; WANGHAM, Michelle. Framework for the Development of Computational Solutions for the Support of Requirements Engineering with a Focus on Data Protection. *In*: PROCEEDINGS of the XXXVI Brazilian Symposium on Software Engineering. Virtual Event, Brazil: Association for Computing Machinery, 2022a. (SBES '22), p. 419–424. DOI: 10.1145/3555228.3555262. Disponível em: https://doi.org/10.1145/3555228.3555262.

DA SILVA, Paulo Henrique; BENITTI, Fabiane B. Vavassori;
WANGHAM, Michelle Silva. How Has Requirements Engineering Supported Data Protection? *In*: 2022 XVLIII Latin American Computer Conference (CLEI). [*S.l.*: *s.n.*], 2022b. P. 1–8. DOI: 10.1109/CLEI56649.2022.9959962.

DIAMANTOPOULOU, Vasiliki; TSOHOU, Aggeliki; KARYDA, Maria. From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. *In*: KATSIKAS, Sokratis *et al.* (Ed.). **Computer Security**. Cham: Springer International Publishing, 2020. P. 238–257.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). **Official Journal of the European Union**, v. L119, p. 1–88, 2016.

FEDERAL, Governo. **RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**. [*S.l.*: *s.n.*], 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx.

FERREYRA, Nicolás E.Díaz; TESSIER, Patrick; PEDROZA, Gabriel; HEISEL, Maritta. PDP-ReqLite: A Lightweight Approach for the Elicitation of Privacy and Data Protection Requirements. **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**, 12484 LNCS, September, p. 161–177, 2020. ISSN 16113349. DOI: 10.1007/978-3-030-66172-4_10.

FURIAN, Nikolaus; O'SULLIVAN, Michael; WALKER, Cameron; VOESSNER, Siegfried; NEUBACHER, Dietmar. A conceptual modeling framework for discrete event simulation using hierarchical control structures. **Simulation Modelling Practice and Theory**, v. 53, mai. 2015. DOI: 10.1016/j.simpat.2015.04.004.

GUERRIERO, Michele; TAMBURRI, Damian A; RIDENE, Youssef; MARCONI, Francesco; BERSANI, Marcello M; ARTAC˘XLAB, Matej. **Towards DevOps for Privacy-by-Design in Data-Intensive Applications: A Research Roadmap**. [*S.l.*: *s.n.*]. ISBN 9781450344043. Disponível em: www.bluage.com/company/netfective-technology-group.

HADAR, Irit; HASSON, Tomer; AYALON, Oshrat; TOCH, Eran; BIRNHACK, Michael; SHERMAN, Sofia; BALISSA, Arod. Privacy by designers: software developers' privacy mindset. **Empirical Software Engineering**, Empirical Software Engineering, v. 23, n. 1, p. 259–289, 2018. ISSN 15737616. DOI: 10.1007/s10664-017-9517-1.

IBM. **Cost of Data Breach Report 2023**. Acessado em 21 de outubro de 2023. 2023. Disponível em: https://www.ibm.com/downloads/cas/E3G5JMBP.

IBM. **Estudo da IBM aponta que 96% dos brasileiros acreditam que as empresas não protegem seus dados pessoais**. [*S.l.*: *s.n.*], 2019. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-da-ibm-aponta-que-96-dos-brasileiros-acreditam-que-as-empresas-nao-protegem-seus-dados-pessoaisestudo-da-ibm-aponta-que-96-dos-brasileiros-acreditam-que-as-empresas-nao-protegem-seus-dados-pess/.

ICO. **Data Protection Act 2018**. [*S.l.*: *s.n.*], 2023. Disponível em: https://ico.org.uk/for-organisations/data-protection-act-2018/. Acesso em: 15 de junho de 2023.

ICO. **Data Protection Impact Assessment (DPIA) Guidance**. [*S.l.*: *s.n.*], 2022. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/. Acesso em: 02 de julho de 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **ISO/IEC 27002:2022 - Information technology — Security techniques — Code of practice for information security controls (3rd edition)**. [*S.l.*]: International Organization for Standardization (ISO), mar. 2022. P. 152.

JUTLA, Dawn N.; BODORIK, Peter; ALI, Sohail. Engineering Privacy for Big Data Apps with the Unified Modeling Language. *In*: 2013 IEEE International Congress on Big Data. [*S.l.*: *s.n.*], 2013. P. 38–45. DOI: 10.1109/BigData.Congress.2013.15.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature Reviews in Software Engineering, 2007. ISSN 00010782. DOI: 10.1145/1134285.1134500. arXiv: 1304.1186.

KNEUPER, Ralf. Translating data protection into software requirements. **ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy**, p. 257–264, December 2019 2020. DOI: 10.5220/0008873902570264.

KPMG. **Global Customer Experience Excellence report**. [*S.l.*: *s.n.*], 2020. Disponível em: https://home.kpmg/xx/en/home/insights/2020/01/home.html.

LANGHEINRICH, Marc. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. *In*: ABOWD, Gregory D.; BRUMITT, Barry; SHAFER, Steven (Ed.). **Ubicomp 2001: Ubiquitous Computing**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. P. 273–291.

LI, Tianshi; AGARWAL, Yuvraj; HONG, Jason. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. **Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies**, v. 2, n. 4, p. 1–35, 2018. ISSN 2474-9567. DOI: 10.1145/3287056.

LOPES, Isabel Maria; GUARDA, Teresa; OLIVEIRA, Pedro. How ISO 27001 Can Help Achieve GDPR Compliance. **Iberian Conference on Information Systems and Technologies, CISTI**, 2019-June, June, p. 19–22, 2019. ISSN 21660735. DOI: 10.23919/CISTI.2019.8760937.

MANNA, Asmita; SENGUPTA, Anirban; MAZUMDAR, Chandan. EDPRL: A Language for Specifying Data Privacy Requirements of Enterprises. *In*: 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP). [*S.l.*: *s.n.*], 2019. P. 1–6. DOI: 10.1109/ICACCP.2019.8882883. Disponível em: https://doi.org/10.1109/ICACCP.2019.8882883.

MASSENO, Manuel David. A (re) personalização de dados anonimizados entre o RGPD europeu e a LGPD brasileira. **Revista do CEJUR/TJSC: Prestação Jurisdicional**, v. 8, n. 1, p. 1–14, 2019. Disponível em: https://doi.org/10.21902/rctjsc.v8i1.346.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, Programa de Privacidade e Segurança da Informação (PPSI). **Guia de Elaboração de Inventário de Dados Pessoais**. Versão 2.0. Brasília: [*s.n.*], mar. 2023. Acesso em 10/09/2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf/view.

MORAIS, E. A. M.; AMBRÓSIO, A. P. L. **Mineração de Textos**. Goiânia, 2007. P. 30. Acesso em: 14 dez. 2023. Disponível em: http://www.inf.ufg.br/sites/default/files/uploads/relatorios-tecnicos/RT-INF_005-07.pdf.

MORALES-TRUJILLO, Miguel Ehecatl; GARCÍA-MIRELES, Gabriel Alberto; MATLA-CRUZ, Erick Orlando; PIATTINI, Mario. A Systematic Mapping Study on Privacy by Design in Software Engineering. **CLEI Electronic Journal**, v. 22, n. 1, p. 29, 2019. ISSN 0717-5000. DOI: 10.19153/cleiej.22.1.4.

NASCIMENTO, Luciano. **Governo publica MP que cria órgão para proteção de dados**. Acesso em 29 jun. 2021. dezembro 28 2018.

NASCIMENTO, Rafael; ARANHA, Eduardo; KULESZA, Uirá; LUCENA, Marcia. Requirements Smells como indicadores de má qualidade na especificação de requisitos: Um Mapeamento Sistemático da Literatura. *In*: ANAIS do WER 2018 - Workshop em Engenharia de Requisitos. [*S.l.*: *s.n.*], 2018. DOI: 10.17771/pucrio.wer.inf2018-40.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST Cybersecurity Framework Version 1.1**. [*S.l.*: *s.n.*], 2018. Disponível em: https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework.

NEWMAN, Sam. **Building microservices: designing fine-grained systems.** [*S.l.*: *s.n.*], 2015.

OFFERMANN, Philipp; LEVINA, Olga; SCHÖNHERR, Marten; BUB, Udo. Outline of a Design Science Research Process. *In*. DOI: 10.1145/1555619.1555629. Disponível em: https://doi.org/10.1145/1555619.1555629.

ONU. **Artigo 12: Direito á privacidade**. [*S.l.*: *s.n.*], 2018. Disponível em: https://brasil.un.org/pt-br/81736-artigo-12-direito-privacidade.

PETERSEN, Kai; VAKKALANKA, Sairam; KUZNIARZ, Ludwik. Guidelines for conducting systematic mapping studies in software engineering: An update. **Information and Software Technology**, v. 64, p. 1–18, 2015. ISSN 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2015.03.007. Disponível em: https://www.sciencedirect.com/science/article/pii/S0950584915000646.

PINHEIRO, José de Queiroz; FARIAS, Tadeu Mattos; ABE-LIME, July Yukie. Painel de Especialistas e Estratégia Multimétodos: Reflexões, Exemplos, Perspectivas. **PSICO**, Natal, RN, Brasil, v. 44, n. 2, p. 184–192, abr./jun. 2013.

PONCELET, Pascal; MASSEGLIA, Florent; TEISSEIRE, Maguelonne. Hershey, PA: Information Science Reference, 2008.

PRESSMAN, Roger S. **Software Engineering: A Practitioner's Approach**. 7th. New York, NY: McGraw-Hill, 2009. ISBN 978-0073375977.

PROTEÇÃO DE DADOS (ANPD), Autoridade Nacional de. **Relatório de Impacto à Proteção de Dados (RIPD)**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

QAISER, Shahzad; ALI, Ramsha. Text Mining: Use of TF-IDF to Examine the Relevance of Words to Documents. **International Journal of Computer Applications**, v. 181, n. 1, July, 2018 2018.

RADFORD, A.; NARASIMHAN, K.; SALIMANS, T.; SUTSKEVER, I. Improving Language Understanding by Generative Pre-training. **arXiv preprint arXiv:1801.10198**, 2018.

RAMADAN, Qusai; STRÜBER, Daniel; SALNITRI, Mattia; RIEDIGER, Volker; JÜRJENS, Jan. Detecting Conflicts Between Data-Minimization and Security Requirements in Business Process Models. *In*: PIERANTONIO, Alfonso; TRUJILLO, Salvador (Ed.). **Modelling Foundations and Applications**. Cham: Springer International Publishing, 2018. P. 179–198.

ROWAN, Mark; DEHLINGER, Josh. Encouraging Privacy by Design Concepts with Privacy Policy Auto-Generation in Eclipse (PAGE). DOI: 10.1145/2688130.2688134. Disponível em: http://dx.doi.org/10.1145/2688130.2688134.

SACHDEVA, Vaibhav; CHUNG, Lawrence. Handling non-functional requirements for big data and IOT projects in Scrum. **Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering**, IEEE, p. 216–221, 2017. DOI: 10.1109/CONFLUENCE.2017.7943152.

SCHÖN, Eva-Maria; THOMASCHEWSKI, Jörg; ESCALONA, María José. Agile Requirements Engineering: A systematic literature review. **Computer Standards Interfaces**, v. 49, p. 79–91, 2017. ISSN 0920-5489. DOI: https://doi.org/10.1016/j.csi.2016.08.011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0920548916300708.

SCHRAMM, Julie Katlyn A. A era biotecnológica: apontamento sobre os dados genéticos na LGPD (Lei Geral de Proteção de Dados). *In*: UNIBRASIL, 1. ANAIS do Evento de Iniciação Científica (EVINCI). Curitiba: [*s.n.*], 2019. (Caderno de Resumos, 1). Acesso em: 29 jun. 2021. Disponível em: `https://portaldeperiodicos.unibrasil.com.br/index.php/anaisevinci/article/view/5098/3865`.

SENADO, Agência. **Senado inclui proteção de dados pessoais como direito fundamental na Constituição**. [*S.l.*: *s.n.*], 2021. Disponível em: `https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao`.

SILVA, Deógenes P.; SOUZA, Patricia Cristiane de;
JESUS GONÇALVES, Thaıres A. de. Early Privacy: Approximating Mental Models in the Definition of Privacy Requirements in Systems Design. *In*: PROCEEDINGS of the 17th Brazilian Symposium on Human Factors in Computing Systems. Belém, Brazil: Association for Computing Machinery, 2018. (IHC 2018). DOI: `10.1145/3274192.3274211`. Disponível em: `https://doi.org/10.1145/3274192.3274211`.

SILVA JUNIOR, Deógenes P. da; SOUZA, Patricia Cristiane De; MACIEL, Cristiano. Method for privacy requirements elicitation in ubiquitous computing. **ACM International Conference Proceeding Series**, p. 178–183, 2018. DOI: `10.1145/3266237.3266239`.

SOLKA, Jeffrey L. Text Data Mining: Theory and Methods. **Naval Surface Warfare Center Dahlgren Division Statistics Surveys**, v. 2, p. 94–112, 2008.

SOLOVE, Daniel J; WASHINGTON, George. Understanding Privacy (Chapter One) Understanding Privacy daniel j . solove, 2008.

SOMMERVILLE, Ian. **Engenharia de Software**. [*S.l.*: *s.n.*], 2011. ISBN 8579361087.

STACH, Christoph; STEIMLE, Frank. Recommender-based privacy requirements elicitation - EPICUREAN. **Proceedings of the ACM Symposium on Applied Computing**, Part F1477, p. 1500–1507, 2019. DOI: `10.1145/3297280.3297432`.

SYPE, Van Der; SHIN, Yung; MAALEJ, Walid. On lawful disclosure of personal user data: What should app developers do? *In*: 2014 IEEE 7th International Workshop on

Requirements Engineering and Law, RELAW 2014 - Proceedings. [*S.l.*: *s.n.*], 2014. DOI: 10.1109/RELAW.2014.6893479.

TSE; ANPD. **Guia Orientativo da Lei Geral de Proteção de Dados por Agentes de Tratamento no Contexto Eleitoral**. Acessado em 21 de outubro de 2023. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf.

VERIZON. **Data Breach Investigations Report 2023**. Acessado em 21 de novembro de 2023. 2023. Disponível em: https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/.

WOHLIN, Claes; RUNESON, Per. Guiding the selection of research methodology in industry–academia collaboration in software engineering. **Information and Software Technology**, v. 140, p. 106678, 2021. ISSN 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2021.106678. Disponível em: https://www.sciencedirect.com/science/article/pii/S0950584921001361.

YANG, Y. Research and realization of internet public opinion analysis based on improved tf-idf algorithm. *In*: 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES). [*S.l.*: *s.n.*], 2017. P. 80–83.

YONGGUO, Jiang; QIANG, Liu; CHANGSHUAI, Qin; JIAN, Su; QIANQIAN, Liu. Message-oriented Middleware: A Review. *In*: 2019 5th International Conference on Big Data Computing and Communications (BIGCOM). [*S.l.*: *s.n.*], 2019. P. 88–97. DOI: 10.1109/BIGCOM.2019.00023.

ZINSMAIER, Sandra; LANGWEG, Hanno; WALDVOGEL, Marcel. A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria. *In*: FURNELL, Steven; MORI, Paolo; WEIPPL, Edgar (Ed.). **Proceedings of the 6th International Conference on Information Systems Security and Privacy**. Setúbal, Portugal: SCITEPRESS, 2020. P. 473–480. DOI: 10.5220/0008960604730480.

Apêndices

APÊNDICE A – STRING DE BUSCA POR FONTE

Scopus: *String SCOPUS: TITLE-ABS-KEY (("software requirements"OR "engineering requirements"OR "functional requirements"OR "privacy requirements"OR "non-functional requirements") AND ("LGPD"OR "GDPR"OR "data privacy"OR "27701"OR "privacy protection"OR "data protection"OR "privacy by design")) AND (LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018))*

IEEE *String IEEE: ("software requirements"OR "engineering requirements"OR "functional requirements"OR "privacy requirements"OR "non-functional requirements") AND ("LGPD"OR "GDPR"OR "data privacy"OR "27701"OR "privacy protection"OR "data protection"OR "privacy by design")*

ACM *String ACM: [[All: "software requirements"] OR [All: "engineering requirements"] OR [All: "functional requirements"] OR [All: "privacy requirements"] OR [All: "non-functional requirements"]] AND [[All: "lgpd"] OR [All: "gdpr"] OR [All: "data privacy"] OR [All: "27701"] OR [All: "privacy protection"] OR [All: "data protection"] OR [All: "privacy by design"]] AND [Publication Date: (01/01/2018 TO 12/31/2021)]*

APÊNDICE B – ESTUDOS SELECIONADOS

[1] Calabrò, A., Marchetti, E., Moroni, D., Pieri, G. (2019). GDPR and Business Processes: an effective solution Cesare. ACM International Conference Proceeding Series. https://doi.org/10.1145/3309772.3309796

[2] Baldassarre, M. T., Barletta, V. S., Caivano, D., Piccinno, A. (2020). A Visual Tool for Supporting Decision-Making in Privacy Oriented Software Development. ACM International Conference Proceeding Series. https://doi.org/10.1145/3399715.3399818

[3]Li, T., Agarwal, Y., Hong, J. (2018). Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(4), 1–35. https://doi.org/10.1145/3287056

[4]Ansari, M. T. J., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., Khan, R. A. (2021). P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements. Arabian Journal for Science and Engineering, 0123456789. https://doi.org/10.1007/s13369-021-05476-z

[5]Ferreyra, N. E. D., Tessier, P., Pedroza, G., Heisel, M. (2020). PDP-ReqLite: A Lightweight Approach for the Elicitation of Privacy and Data Protection Requirements. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12484 LNCS(September), 161–177. https://doi.org/10.1007/978-3-030-66172-4$_1$0

[6] Zinsmaier, S. D., Langweg, H., Waldvogel, M. (2020). A practical approach to stakeholder-driven determination of security requirements based on the GDPR and common criteria. ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy, 473–480. https://doi.org/10.5220/0008960604730480

[7] Stach, C., Steimle, F. (2019). Recommender-based privacy requirements elicitation - EPICUREAN. Proceedings of the ACM Symposium on Applied Computing, Part F1477, 1500–1507. https://doi.org/10.1145/3297280.3297432

[8]Ayala-Rivera, V., Pasquale, L. (2018). The grace period has ended: An approach to operationalize GDPR requirements. Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018, 136–146. https://doi.org/10.1109/RE.2018.00023

[9]Silva, D. P., de Souza, P. C., de Jesus Gonçalves, T. A. (2018). Early privacy: Approximating mental models in the definition of privacy requirements in systems design. ACM International Conference Proceeding Series, October. https://doi.org/10.1145/3274192.3

[10]Manna, A., Sengupta, A., Mazumdar, C. (2019). EDPRL: A language for specifying data privacy requirements of enterprises. 2019 2nd International Conference on Advanced Computational and Communication Paradigms, ICACCP 2019. https://doi.org/10.1109/ICACCP.2019.8882883

[11]Kneuper, R. (2020). Translating data protection into software requirements. ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems

Security and Privacy, December 2019, 257–264. https://doi.org/10.5220/0008873902570264

[12]Da Silva Junior, D. P., De Souza, P. C., Maciel, C. (2018). Method for privacy requirements elicitation in ubiquitous computing. ACM International Conference Proceeding Series, 178–183. https://doi.org/10.1145/3266237.3266239

APÊNDICE C – FORMULÁRIO DE AVALIAÇÃO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (T.C.L.E.)

UNIVERSIDADE FEDERAL DE SANTA CATARINA CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Estudo de Avaliação da Abordagem de Suporte à LGPD e Análise de Flexibilidade

Caro(a) participante,

Você está sendo convidado(a) a participar de um estudo que tem como objetivo avaliar a **abordagem para o desenvolvimento de soluções computacionais de apoio a engenharia de requisitos com foco na proteção de dados**, tanto de um ponto de vista de entrega de valor quanto com relação a sua flexibilidade. Antes de prosseguir, pedimos que leia atentamente as informações a seguir:

Objetivos do Estudo:

1. Avaliar a entrega de valor da abordagem para apoiar a LGPD e a proteção do usuário nos requisitos de software.
2. Avaliar a flexibilidade da abordagem em relação à sua capacidade de ser facilmente acoplada, implementada e utilizada em diferentes cenários de desenvolvimento de software.

Procedimentos do Estudo:

- Você será convidado(a) a responder a um questionário com perguntas relacionadas aos objetivos do estudo.
- Suas respostas e dados pessoais serão tratados de forma confidencial e usados apenas para fins de pesquisa.

Riscos e Benefícios:

- Não há riscos físicos associados à sua participação neste estudo.
- Sua participação contribuirá para o aprimoramento da abordagem, beneficiando futuros usuários do software.

Confidencialidade e Privacidade:

- Todas as informações fornecidas serão tratadas de forma confidencial e armazenadas em ambiente seguro.
- Seu nome ou quaisquer informações pessoais não serão divulgados em nenhuma publicação ou resultado do estudo.

Participação Voluntária:

- Sua participação é voluntária, e você tem o direito de desistir a qualquer momento, sem qualquer penalidade.

Contato:

- Em caso de dúvidas ou esclarecimentos adicionais sobre o estudo, você pode entrar em contato com Paulo Henrique da Silva por meio do e-mail phs.paulohenriquesilva@gmail.com ou pelo telefone 48 996912206.

Ao selecionar "Sim" e continuar com o questionário, você estará indicando que leu e compreendeu as informações apresentadas neste Termo de Consentimento Livre e Esclarecido e concorda em participar deste estudo de forma voluntária.

2. Você aceita participar deste estudo de forma voluntária? *

Marcar apenas uma oval.

- ◯ Sim *Pular para a pergunta 3*
- ◯ Não

Informações pessoais

Antes de iniciar a avaliação por favor insira algumas infromações pessoais relevantes para esta avaliação

3. Nome completo *

_____

4. Email

_____

5. Empresa ou instituição em que trabalha

_____

6. Cargo ou profissão *

_____

7. Você possui formação superior completa? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Em andamento
- ◯ Outro: _____

8. Qual curso você fez ou está fazendo?

_____

9. Quanto tempo você tem ou teve de experiência com o tema "Proteção de Dados"? *

Marcar apenas uma oval.

- ◯ Menos de 1 ano
- ◯ Entre 1 e 3 anos
- ◯ Mais de 3 anos

10. Qual seu nível de conhecimento com relação a Proteção de Dados? *

Marcar apenas uma oval.

- ◯ Nível 0 a 2: Pouco ou nenhum conhecimento.
- ◯ Nível 2 a 4: Tem clareza sobre o objetivo e possui conhecimento dos fundamentos básicos.
- ◯ Nível 4 a 6: Possui conhecimento e já participou de projetos ou implementações relacionadas ao tema.
- ◯ Nível 6 a 8: Possui conhecimento e complementou sua compreensão através de curso de graduação e/ou treinamentos específicos.
- ◯ Nível 8 a 10: Possui conhecimentos avançados e atuou diretamente liderando ou orientando projetos voltados para o tema. Tem uma compreensão profunda e é capaz de fornecer orientações estratégicas.

11. Quanto tempo você tem ou teve de experiência com o tema "LGPD"? *

Marcar apenas uma oval.

- ◯ Menos de 1 ano
- ◯ Entre 1 e 3 anos
- ◯ Mais de 3 anos

12. Qual seu nível de conhecimento com relação a LGPD (Lei Geral de Proteção de Dados)? *

Marcar apenas uma oval.

- ◯ Nível 0 a 2: Pouco ou nenhum conhecimento na LGPD. Não está familiarizado com os conceitos fundamentais da LGPD.
- ◯ Nível 2 a 4: Tem clareza sobre o objetivo e possui conhecimento dos fundamentos básicos da LGPD. Pode entender os princípios gerais.
- ◯ Nível 4 a 6: Possui conhecimento sobre a LGPD e já participou de projetos ou implementações relacionadas à adequação.
- ◯ Nível 6 a 8: Possui conhecimento sólido sobre a LGPD e complementou sua compreensão através de curso de graduação e treinamentos específicos relacionados à lei.
- ◯ Nível 8 a 10: Possui conhecimentos avançados e atuou diretamente liderando ou orientando projetos voltados para a LGPD. Tem uma compreensão profunda e é capaz de fornecer orientações estratégicas.

13. A empresa ou instituição que você trabalha está adequada à LGPD? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Em andamento
- ◯ Não

14. Você participou ou participa de algum grupo/comitê volltado para a proteção de dados *

Marcar apenas uma oval.

- Sim
- Não

15. Qual seu nível de conhecimento com relação a arquitetura de software? *

Marcar apenas uma oval.

- Nível 0 a 2: Constrói/Reconhece componentes básicos de um sistema, pode identificar camadas simples em uma arquitetura e tem uma noção inicial de como os módulos interagem.
- Nível 2 a 4: Mantém componente de sensibilidade mais acentuada, como integrações com outros sistemas, e faz pequenas manutenções evolutivas com a supervisão de níveis mais sêniores.
- Nível 4 a 6: Constrói/mantém componentes de sensibilidade mais acentuada, como integrações com outros sistemas, com a supervisão de níveis mais sêniores.
- Nível 6 a 8: Constrói/mantém componentes mais complexos e Identifica oportunidades de melhoria relacionadas à performance e eficiência da arquitetura.
- Nível 8 a 10: Define a arquitetura de sistemas, constrói aplicações que sejam escaláveis, resilientes, performáticas, ponderando custos e o objetivo de negócio

16. Qual seu nível de conhecimento com relação a requisitos de software? *

Marcar apenas uma oval.

- ◯ Nível 0 a 2 : Pouco ou nenhum conhecimento sobre requisitos de software. Não compreende os conceitos fundamentais relacionados a especificações de software.
- ◯ Nível 2 a 4: Tem clareza sobre o objetivo dos requisitos de software e possui um entendimento básico das especificações e funcionalidades necessárias.
- ◯ Nível 4 a 6: Possui conhecimento sobre requisitos de software e já participou de projetos nos quais esteve envolvido na definição, análise ou validação de requisitos.
- ◯ Nível 6 a 8 : Possui um conhecimento sólido sobre requisitos de software e completou cursos de graduação ou treinamentos voltados para a área, aprimorando sua compreensão.
- ◯ Nível 8 a 10: Possui conhecimentos avançados sobre requisitos de software e já atuou como líder em projetos focados nessa área. É capaz de interpretar requisitos complexos e fornecer orientações estratégicas para sua elaboração e gerenciamento.

Entrega de valor

Avaliar a entrega de valor da abordagem para apoiar a LGPD e a proteção do usuário nos requisitos de software

17. A abordagem alerta quanto ao possível uso de dados pessoais no requisito mesmo que o usuário não os tenha cadastrado *

Marcar apenas uma oval.

- ◯ concordo totalmente
- ◯ concordo
- ◯ indiferente (ou neutro)
- ◯ discordo
- ◯ discordo totalmente

18. A abordagem colabora para a construção do RIPD (Relatório de Impacto a Proteção de Dados) *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

19. A abordagem alerta quanto a informações obrigatórias pela LGPD de dados pessoais cadastrados no requisito *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

20. A abordagem sugere itens da LGPD relevantes para o contexto do requisito. *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

21. A abordagem utiliza a escrita de requisitos para alertar o usuário quanto ao uso de dados pessoais. *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

22. A abordagem utiliza a escrita de requisitos para alertar o usuário quanto ao uso de dados pessoais sensíveis. *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

23. A abordagem apoia a proteção de dados com base nos requisitos. *

Marcar apenas uma oval.

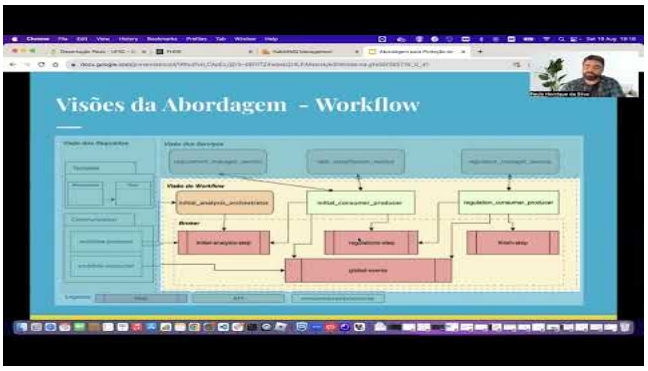
- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

24. Você tem alguma sugestão?

Flexibilidade

Avaliar a flexibilidade da abordagem em relação à sua capacidade de ser facilmente acoplada, implementada e utilizada em diferentes cenários de desenvolvimento de software.

Por favor, assista ao video abaixo no qual explico sobre a arquitetura da abordagem. Essa explicação é fundamental para viabilizar a avaliação da flexibilidade da abordagem proposta.



http://youtube.com/watch?v=qUUruEeDEgo

25. O sistema consegue interpretar corretamente escritas distintas de requisitos de software como input da abordagem. (ex: caso de uso, história de usuário e linguagem natural) *

Marcar apenas uma oval.

- ◯ concordo totalmente
- ◯ concordo
- ◯ indiferente (ou neutro)
- ◯ discordo
- ◯ discordo totalmente

26. A visão de requisitos, implementada na aplicação FHGR (Ferramenta Hipotética de Gerenciamento de Requisitos), é desacoplada . *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

27. A abordagem consegue se adaptar para receber novos serviços de forma dinâmica. *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

28. A abordagem consegue adicionar novas etapas para avaliação de um requisito. *

Marcar apenas uma oval.

- concordo totalmente
- concordo
- indiferente (ou neutro)
- discordo
- discordo totalmente

29. Você entende que a abordagem poderia ser utilizada no contexto da sua empresa/organização? *

Marcar apenas uma oval.

- ◯ concordo totalmente
- ◯ concordo
- ◯ indiferente (ou neutro)
- ◯ discordo
- ◯ discordo totalmente

30. Por favor, nos informe como sua empresa especifica os requisitos (ex: caso de uso, histórias de usuário, linguagem natual) e qual(is) ferramenta(s) são utilizadas para documentar os requisitos. *