UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

Análise de conformidade de processos de negócios em relação a LGPD

Trabalho de Graduação

Aluno: Eric Araújo da Costa Júnior
Orientadora: Jéssyka Flavyanne Ferreira Vilela
Área: Engenharia de Software

RECIFE
2020

Universidade Federal de Pernambuco

Centro de Informática

Eric Araújo da Costa Júnior

Análise de conformidade de processos de negócios em relação a LGPD

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientadora: *Jéssyka Flavyanne Ferreira Vilela*

Recife
2020

Este trabalho é dedicado aos meus Pais, Professores, e Amigos que sempre estiveram comigo e fizeram o melhor que podiam para me ajudar nos momentos em que mais precisei.

AGRADECIMENTOS

Agradeço aos meus pais, Maria e Eric, por todo amor e carinho que recebi durante todos esses anos, por sempre me apoiarem em toda e qualquer decisão que eu tomei na vida e por nunca duvidarem de minha capacidade. Essa não é uma conquista só minha, é uma conquista também de vocês. Se eu consegui chegar até aqui foi porque vocês me proporcionaram isso: colocaram um teto sob minha cabeça, comida sobre a mesa e sempre fizeram das tripas coração para garantir que eu sempre tivesse o necessário pra seguir em frente... Então, meus pais, parabéns pra nós. Nós conseguimos. Amo vocês do fundo do meu coração.

À minha amada, melhor amiga e mulher da minha vida, Rayanne Lúcia, por sempre conseguir fazer aflorar o melhor de mim e me transformar cada dia a mais em uma pessoa melhor. Obrigado por ser o meu porto seguro por todo carinho e amor incondicional que você me dá, por estar sempre presente na minha vida, por nunca ter desistido de mim e ter me ajudado a sair de minha pior fase. Também por todo apoio, disponibilidade e todas as dicas que você me deu para que este trabalho pudesse ser feito da melhor maneira possível.

Aos meus melhores amigos: Pedro Vinícius, que sempre esteve lá pra mim quando mais precisei, que sempre ouviu todas as minhas reclamações e me ensinou tudo o que eu sei, sem você meu amigo, nem metade disso teria sido possível. E Gustavo Lopes, por ser aquele que me deu um rumo e me ajudou a encontrar a área em que atuo hoje e me ajudado com os dilemas da área de tecnologia, sem você eu não teria conseguido o que tenho hoje. E principalmente pela amizade incrível e sincera de vocês, também por estarem presentes em todos os instantes, por me ajudarem em todos os momentos que tive dificuldades e sempre dispostos a me ensinar algo que eu não sabia. Obrigado por tudo.

À minha orientadora, Jéssyka, por ter me aceitado como orientando mesmo depois do período conturbado que tivemos durante a primeira cadeira na qual fui seu aluno, por toda a ajuda, todo o interesse, vontade e disponibilidade para fazer este trabalho acontecer. Sou extremamente grato à Senhora por tudo.

Although my heart may be weak, it's not alone. It's grown with each new experience. And it's found a home with all the friends I've made. I've become a part of their heart, just as they've become a part of mine. And if they think of me now and then, if they don't forget me, then our hearts will be one.

—SORA

RESUMO

Contexto: Notícias e relatórios sobre vazamentos de dados confidenciais e privados são reportados com frequência crescente. Nesse sentido, o cenário é tão crítico e preocupante que os governos têm tomado medidas para garantir que as empresas aumentem os investimentos e as ações relacionadas com a segurança dos dados dos usuários. Foram criadas leis, como a lei europeia General Data Protection Regulation (GDPR) e a Brasileira Lei Geral de Proteção de Dados Pessoais (LGPD), que definem os direitos de privacidade sobre os dados dos usuários e penalidades explícitas para empresas que não estejam em conformidade com a lei. Problema: Uma vez que a privacidade e a segurança dos dados pessoais se tornaram uma prioridade entre os problemas enfrentados por muitas empresas, os processos de negócios são de fundamental importância em um programa de cumprimento das leis e para equilibrar a transparência nos serviços prestados. No entanto, é necessário uma abordagem para ajudar a cumprir a LGPD nos processos de negócio. Objetivo: Este trabalho propõe uma solução para obter a conformidade dos processos de negócios em relação a LGPD. Método: Para atingir esse objetivo, foi realizada uma revisão da literatura, análise das leis de privacidades GDPR e LGPD e trabalhos relevantes na área. Resultados: Este trabalho propõe o método LGPD4BP (LGPD for Business Process) que é composto por um questionário de avaliação e um método de modelagem com um catálogo de padrões de modelagem. O método foi aplicado em um estudo de caso do colégio de aplicação da Universidade Federal de Pernambuco (UFPE) e validado por uma turma de pós-graduação que aplicou o método e respondeu um questionário sobre facilidade de uso e completude do método. Conclusões: Os resultados das avaliações dos alunos demonstraram que a parte mais difícil é a modelagem do processo de negócio e não os componentes do método proposto. O método proposto orienta os analistas a avaliar a conformidade dos processos de negócio com a LGPD e guia os analistas a modelarem processos de acordo com a LGPD.

Palavras-chave: Privacidade, LGPD, GDPR, Processos de Negócios, Proteção de Dados, Análise de Privacidade.

ABSTRACT

Context: News and reports about data leaks of private and confidential data are being reported with increasing frequency. The scenario is so critical and worrisome that governments have taken actions to ensure that companies raise their investments and the actions related to user's data security. Laws were created, like the European General Data Protection Regulation (GDPR) and the Brazilian law Lei Geral de Proteção de Dados Pessoais (LGPD), which define the privacy rights on user data and spell out penalties to the companies which do not comply with the law. Problem: Since data privacy and data security became a priority among the problems faced by many companies, business processes are of fundamental importance in a compliance program to these laws and to balance transparency on services provided. However, it is necessary an approach to help the compliance with LGPD on business processes. Objective: This work proposes a solution to obtain LGPD compliance on business processes. Method: To achieve this goal, this work carried out a literature review, an analysis of GDPR and LGPD privacy laws, and relevant works on the area. Results: This work proposes the LGPD4BP (LGPD for Business Process) method, which is composed by an evaluation questionnaire and a modelling method with a modelling patterns catalog. The method was applied on a case study of Colégio de Aplicação from Federal University of Pernambuco and validated by a postgraduate class which applied the method and answered a questionnaire about easiness and completeness of the method. Conclusions: The results from students evaluations showed that the most hard step is the business process modeling and not the components from the proposed method. The proposed method guides analysts to evaluate LGPD compliance of business processes and it guides analysts to model business processes to comply with LGPD.

Keywords: Privacy, LGPD, GDPR, Business Processes, Data Protection, Privacy Analysis.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. Introdução

1.1. Contexto

A privacidade tem sido o centro de várias discussões entre provedores de serviço que gostariam de utilizar os dados coletados automaticamente por sistemas e usuários que querem ter serviços que usem o mínimo de dados pessoais possíveis (AGOSTINELLI et al., 2019).

A Netflix, plataforma de stream de vídeos online, é um exemplo desse tipo de sistema. Ela coleta os dados de histórico de visualizações dentro de sua plataforma e mais tarde utiliza estes dados para gerar recomendações. A Netflix consegue vasculhar perfis com escolhas de filmes semelhantes para utilizá-los como novas recomendações (VERHALEN et al., 2019).

Tendo em vista a capacidade desses novos sistemas de coletar automaticamente dados dos usuários, a Lei Geral de Proteção de Dados (LGPD), cuja previsão de implantação no Brasil é em Agosto de 2020, tem como ponto focal a privacidade de dados de usuários (BRASIL, 2020). Esta lei mudará a forma com que as empresas lidam com processamento de dados, a regulamentação da Lei prevê que será necessário ter uma abordagem diferente da maneira em que processam dados no seu dia-a-dia.

No entanto, inúmeras empresas não estão preparadas para lidar com as novos procedimentos impostos pela lei, várias delas precisarão reformular seus processos para atingir a conformidade com a lei. Dessa forma, será necessário que as empresas que coletam e processam dados pessoais precisarão serem explícitas sobre o motivo para o armazenamento destes dados, quem tem acesso a eles, como, quando e quantas vezes tais dados serão utilizados (BRASIL, 2020).

A LGPD (Brasil, 2020) é inspirada na lei de privacidade de dados europeia, a GDPR (*General Data Protection Regulation)* de 2018 (UNIAO EUROPEIA, 2018). A GDPR implementou o conceito de *privacy-by-design* que tem como princípio evitar a prática comum de implementar contramedidas de segurança somente depois que as brechas de privacidade acontecem em um processo de negócio (AGOSTINELLI et al., 2019), o que significa dizer que a privacidade não é um complemento ao processo de negócio, mas sim uma parte integral dele (AGOSTINELLI et al., 2019), o processo deve obedecer às leis da GDPR desde o início projeto.

Processos de negócio é um dos três pilares da segurança da informação, desta forma, eles são de importância fundamental em um programa de conformidade com a lei. Partindo do princípio de que um processo de negócio compreende o conjunto de um ou mais procedimentos ou atividades relacionadas, as quais, coletivamente, realizam um objetivo de negócio no contexto de uma estrutura organizacional (WFMC, 2020) pode-se de dizer que é o processo de negócio que determina como o trabalho será executado na organização e toda a sequência lógica das atividades. Sendo assim, se o processo aborda questões de

privacidade e conformidade com a LGPD, dificilmente uma organização sofrerá com as sanções da lei.

1.2. Motivação e Justificativa

A governança da segurança da informação exige que três pilares sejam considerados: pessoas, tecnologia e processos (VEIGA, 2007). Considerando que os processos são o componente de segurança mais importante (ANDRESS, 2003), a GDPR especifica que um processo deve estar em conformidade com a Lei desde a sua fase de design (AGOSTINELLI et al., 2019). Portanto, em um programa de conformidade com as leis de privacidade, as empresas devem primeiro especificar seus processos de negócios.

Após a definição dos processos de uma organização, é possível identificar o uso de dados pessoais em cada uma das atividades destes processos, passando por vários departamentos e conduzindo o mapeamento dos dados que são manipulados pela organização. Além disso, a LGPD sugere que seja implementado um programa de governança em privacidade (BRASIL, 2020).

Adotar um programa de governança em privacidade que a LGPD significa dizer que uma organização estabeleceu políticas adequadas com base na sua avaliação sistemática de impactos e risco à privacidade e atua de forma transparente (BRASIL, 2020). Também é possível identificar as responsabilidades de cada envolvido no processamento de dados, além de tornar possível que uma organização consiga agir rapidamente em casos de vazamento de dados, solicitação de acesso, revisões de tomada de decisão automatizadas, entre outros.

A análise da privacidade de processos de negócio de organizações é essencial em virtude da necessidade de se equilibrar a transparência requerida nos serviços prestados e a conformidade com as leis de privacidade (UNIAO EUROPEIA, 2018). Portanto, o intuito da análise é a de melhoria de processos organizacionais bem como a otimização de seus recursos.

É imprescindível que as organizações sejam transparentes com os dados que processam uma vez que punições severas estão previstas na LGPD para aqueles que não cumprirem com suas demandas. As penalidades variam de simples advertências com prazo de adoção de medidas protetivas à multas que equivalem até 2% do faturamento total da empresa, podendo chegar a R$ 50.000.000,00 (cinquenta milhões de reais) por infração (BRASIL, 2020).

Além de multas em dinheiro, a organização também pode ser penalizada com uma suspensão parcial do funcionamento do banco de dados a que não estava em conformidade por um período máximo de seis meses podendo se estender até a regularização do banco (BRASIL, 2020) ou também tendo a proibição total ou parcial da execução de seus serviços e atividades relacionados ao tratamento de dados (BRASIL, 2020). Sendo assim, as empresas além de perderem dinheiro podem perder credibilidade no mercado, o que afetará o futuro da organização.

Apesar da LGPD estar em vigor desde Setembro de 2020, muitas organizações não estão preparadas para lidar com os novos procedimentos impostos por esta lei e a maioria das organizações ainda precisam reformular seus processos de negócio para alcançar a conformidade com a lei. Essa reformulação pode ser uma tarefa bastante árdua e custosa. Guiado por esta motivação, este trabalho investiga a conformidade de processos de negócio com a LGPD.

Nesse contexto, esse trabalho pretende responder às seguintes perguntas de pesquisa:

(1) Como avaliar a conformidade de um processo de negócio com a LGPD?

(2) Como modelar um processo de negócio em conformidade com a LGPD?

1.3. Objetivos

Este trabalho tem como objetivo propor uma solução para obter a conformidade dos processos de negócios de organizações em relação a LGPD. Para atingir esse objetivo geral, pretende-se alcançar os seguintes objetivos específicos:

(i) Investigar padrões de privacidade de modelagem BPMN (Business Process Modeling Notation) existentes na literatura;

(ii) Propor um questionário de análise da conformidade de processos de negócio em relação a LGPD;

(iii) Propor um método de modelagem de processos de negócio em conformidade com a LGPD;

(iv) Aplicar o método proposto em um estudo de caso;

(v) Remodelar o processo analisado para que atenda os requisitos de privacidade estabelecidos pela LGPD;

(vi) Avaliar a solução proposta em relação a facilidade de uso e completude.

Dessa forma, após a investigação da conformidade dos processos de negócio, será proposto um método de modelagem de processos, de forma que o processo atenda às exigências estabelecidas pela LGPD, utilizando a notação BPMN que é uma notação bastante reconhecida na modelagem de processos de negócios (LÜBKE e VAN LESSEN, 2016)

A notação BPMN tem a intenção de criar um padrão de linguagem visual que todos os modeladores de processos vão reconhecer e entender (OMG, 2009). Diante destes fatores, essa linguagem foi escolhida para adaptação dos processos de negócio, sendo ideal para fácil entendimento das soluções propostas nesse trabalho.

1.4. Trabalhos Relacionados

A privacidade de dados pessoais vem atraindo atenção ao longo dos anos e vem sendo investigada por muitas áreas da literatura como Privacidade na engenharia de requisitos (PEIXOTO et. al., 2018); Modelagem de requisitos de privacidade (PEIXOTO et al., 2020)(BARTOLINI et al., 2019)(DAMIANO et al., 2019); Avaliação de conformidade de processos de negócio (CAPODIECI; MAINETTI, 2019) (AGOSTINELLI et al., 2019) (TOM, 2018).

1.4.1. Privacidade na engenharia de requisitos

A necessidade de métodos de engenharia de requisitos para privacidade é discutida em Peixoto et al. (2018). No artigo apresentado, uma pesquisa é realizada com 13 desenvolvedores para entender como eles percebem os elementos de privacidade de um projeto e também são investigados os fatores pessoais que levam um desenvolvedor ao não entendimento dos requisitos de privacidade de um projeto. Após conduzirem entrevistas guiadas por um questionário, os autores transcreveram as mesmas e criaram categorias para agrupar as respostas similares, dessa forma, os autores conseguiram agrupar todas as respostas em nove categorias, identificando-as como as categorias de fatores pessoais, foram elas:

1. Conhecimento empírico sobre privacidade informacional;
2. Experiência em permitir que o usuário controle seus próprios dados armazenados pelo sistema;
3. A decisão de privacidade depende de cada projeto de desenvolvimento;
4. A privacidade é responsabilidade de todos, inclusive dos arquitetos de software;
5. Confusão entre as definições de segurança e privacidade;
6. Falta de importância para com os dados do usuário;
7. A proatividade do usuário está relacionada aos direitos de privacidade;
8. Falta de conhecimento formal sobre privacidade;
9. Foco apenas nos problemas de segurança.

A pesquisa ainda classificou os 4 primeiros fatores como tendo impacto positivo num projeto de desenvolvimento de software e os 5 últimos como tendo um impacto negativo dentro de um projeto.

Em outro trabalho, Peixoto et al. (2020) apresentam uma abordagem baseada em linguagem natural para especificação de requisitos de privacidade, chamada Privacy Criteria Method (PCM). O PCM tem o objetivo de, com o uso de sua ferramenta web, auxiliar os desenvolvedores a lidar com questões de privacidade quando se trata de um contexto de desenvolvimento ágil. O método proposto pode ser usado em conjunto com qualquer técnica de especificação de requisitos, como as user stories, que são um método popular para representar requerimentos usando um template simples (GARM et al. 2016).

1.4.2. Modelagem de requisitos de privacidade

Uma visão geral das linguagens de modelagem existentes que suportam conceitos de privacidade e um catálogo dos principais conceitos de privacidade encontrados nessas linguagens são apresentados em Peixoto et al. (2020). Em uma revisão sistemática literária, os autores encontraram cerca de 24 linguagens de modelagem que suportam conceitos de privacidade, dentre elas estão a iStar e a Tropos, como sendo as que mais trouxeram resultados dentro da revisão. x

Em seguida, conceitos relacionados à privacidade foram levantados durante a revisão sistemática e foram catalogados, criando um modelo conceitual que contribui para a formação de uma base para padronizar conceitos relacionados à privacidade que podem ser usados para avaliar o suporte à privacidade que determinada linguagem possui.

Damiano et al. (2019) tem o objetivo de apresentar um modelo UML (*Unified Modelling Language*) voltado para o design de métodos de automação para checagem de conformidade com a GDPR, para isso o trabalho apresenta 4 artefatos: um modelo conceitual com rastreabilidade completa para as classes do GDPR, um glossário que ajuda no entendimento do modelo, a descrição em linguagem simplificada de 35 regras de conformidade derivadas do GDPR junto com sua codificação em OCL (*Object Constraint Language*) e um conjunto de 20 pontos de variação derivado da GDPR para especializar o modelo genérico.

De forma simplificada, o trabalho apresenta o modelo GDPR genérico junto com regras de conformidade e pontos de variação para que o modelo possa ser aplicado em qualquer uma de suas variações, tornando-o adaptável à realidade de uma organização. A verificação de conformidade ocorre em 4 etapas: No passo 1 o modelo genérico da GDPR foi construído de forma manual, com a assessoria jurídica adequada para ajudar na interpretação da lei, o objetivo do passo é construir o modelo e todas as suas restrições usando diagramas UML e OCL.

No passo 2, o modelo GDPR foi processado junto com as suas restrições com o objetivo de adaptá-lo em um modelo especializado de restrições em OCL, para construir uma base acionável que implemente a GDPR de acordo com as Leis e outras restrições.

O passo 3 diz respeito ao desenvolvimento de uma ferramenta de geração de modelo-instância a fim de criar instâncias do modelo especializado obtido na etapa 2. Isso é feito via uma ferramenta de edição de modelos que permite que especialistas jurídicos criem representações de documentos jurídicos e técnicos na forma de uma instância do modelo especializado.

E por fim, no passo 4, a instância do modelo gerada no passo 3 é verificada com relação às restrições OCL especializadas criadas no passo 2. Os diagnósticos de conformidade resultantes do processo de verificação de restrição são entregues aos usuários finais.

1.4.3. Conformidade com leis de privacidade na engenharia de requisitos

Ayala-Rivera Pasquale (2018) propõem o método Guide-me que consiste em uma abordagem em seis etapas: *Data Audit, Gap Analysis, Planning and Preparation, Plan Review, Execution, Post-Implementation Review. O método* também oferece suporte à obtenção de requisitos de solução que vinculam as obrigações de proteção de dados do GDPR aos controles de privacidade. O método proposto é inspirado no *Business Analysis Body Of Knowledge* (BABOK) o que sugere obter requisitos progressivamente, passando de uma perspectiva de negócios para uma nível de solução. Considerando esse princípio, são propostos os 6 passos que vão desde a perspectiva de negócios (*Data Audit, Gap analysis*) até o nível da solução (*Execution, Post-Implementation*). Dessa forma, o Guide-Me tem o objetivo de preencher a lacuna entre as obrigações legais e os controles de privacidade.

1.4.4. Avaliação de conformidade de processos de negócio

Sugestões e recomendações sobre o gerenciamento de dados na GDPR para a execução de processos de negócios são propostos no trabalho de Bartolini et al. (2019). Um Framework foi desenvolvido no artigo, sendo composto por três principais componentes:

1. Um modelo estruturado dos termos legais da GDPR;
2. Um modelo conceitual descrevendo os termos legais utilizados na lei de proteção de dados;
3. Uma tradução das disposições normativas que seja “legível para máquinas”.

De forma geral, o framework pode ser utilizado para checar se o processo de negócio está em conformidade com a GDPR e pode automaticamente sugerir as atividades mandatórias para que um processo de negócio fique em conformidade. Ele também alerta quando alguma das tarefas específicas da GDPR não foi cumprida e pode dar uma visão completa do processo e os procedimentos adotados para a proteção de dados.

No trabalho de Tom (2018) são propostas duas técnicas baseadas em artefatos para avaliar a conformidade de um processo, bem como capturar os principais aspectos de privacidade contidos nele. O objetivo de Tom é criar fundamentos de análise de processos de negócio para gerenciamento de privacidade dentro de um contexto organizacional.

Tom (2018) divide o objetivo em dois: Avaliação e Melhoria. Na fase de avaliação Tom identifica os pontos de não conformidade de um processo de negócio com a GDPR gerando uma série de requerimentos para que a conformidade seja alcançada, após isso o processo de negócio é convertido em um diagrama de

classes para ser melhor examinado. Na fase de Melhoria são levantados todos os pontos analisados na fase de avaliação e catalogados entre pontos de melhoria tecnológica e pontos de melhoria do processo de negócios, enquanto melhorias de processo são simplesmente revisões dos processos de negócios existentes em BPMN, melhorias tecnológicas se referem à *Privacy Enhanced Technologies*.

Capodieci e Mainetti (2019) apresentam uma abordagem orientada a modelos baseada em negócios buscando a conscientização do processo para apoiar a conformidade com a GDPR. O objetivo do trabalho é o de apontar um método de identificar os pontos-chave de como ter um processo em conformidade com as exigências da GDPR. O artigo fala sobre o ciclo de vida de desenvolvimento de software e sobre como é fácil transferir informações entre sistemas, no entanto, dificilmente existem registros sobre como foi o ciclo de vida dos dados utilizados nos sistemas.

No trabalho de Raimundas (MATULEVIČIUS, 2020), o autor expõe um método para alcançar a conformidade com a GDPR juntamente com uma ferramenta de avaliação e extração de informações de um BPMN. O método consiste em extrair informações de um BPMN *as-is* e verificar quais pontos estão em conformidade com a lei, após apontar as falhas de conformidade, é dada uma explicação para cada ponto e, em seguida, é modelado um *to-be* atendendo os requisitos de privacidade da lei européia.

O método é executado em 4 partes: O primeiro consiste em checar o atual nível de conformidade que o processo de negócio tem extraindo as informações do *as-is* utilizando a ferramenta provida pelo artigo, na segunda parte as informações extraídas do BPMN são comparadas com as informações extraídas da GDPR, para que na terceira parte, seja gerada uma lista com todos os pontos em não conformidade, juntamente com as devidas explicações sobre os pontos e dependendo de quais sejam estes pontos pode ser tomada a decisão que julgará se o processo está em conformidade ou não.

Caso não esteja em conformidade, o processo seguirá para a parte quatro, onde são feitas alterações no BPMN para que os pontos em não conformidade sejam ajustados. Trata-se de um processo contínuo, então sempre que chega ao fim o processo é novamente revisado voltando à primeira parte, até que o processo esteja em conformidade, devido ao julgamento realizado na parte três.

Dessa forma, o BPMN é apontado como sendo o ideal no cenário de descrita de processos, pois ele foca em gerenciamento de dados e torna-se possível expressar os conceitos de *privacy by design* propostos pela lei européia. O artigo procura facilitar também o processo de auditoria e revisão de conformidade nos processos de negócio, através do uso do BPMN para ilustrar todo o processo.

1.4.5. Padrões de modelagem de processos de negócio em conformidade com leis de privacidade

No trabalho de Agostinelli et al. (2019), são apresentados 7 padrões de design de privacidade que agem em conformidade com a GDPR. Os padrões, que consistem diagramas em BPMN, foram modelados diretamente dos textos da lei e atendem as requisições de privacidade da lei européia. Os padrões modelados foram: *Data Breach, Consent to use, Right to access and rectify, Right of portability, Right to withdraw, Right to be forgotte*n.

Uma análise é feita junto com a proposta de cada um dos padrões, destacando os principais pontos de privacidade do padrão e apontando nos textos da lei onde ele se encaixa. O objetivo do artigo é entregar padrões de privacidade para que as empresas possam se basear para criar ou adaptar seus processos de negócio à lei, conseguindo assim ficar em conformidade com a mesma. Por meio dos padrões, Agostinelli et al. (2019) procuram enfatizar a conscientização e a preocupação com a privacidade de dados pessoais e defendem que privacidade deve ser uma prioridade de classe alta em um projeto, e deve ser introduzida desde a fase de design, através dos processos de negócio, da mesma forma que a lei europeia recomenda.

Nosso trabalho tem como foco a Lei Geral de Proteção de Dados e propõe o método chamado LGPD4BP (LGPD for Business Process). O método se baseia nos padrões de designs propostos por Agostinelli et al. (2019) para a GDPR e complementa a contribuição dos autores ao propor um questionário para avaliar a conformidade de processos de negócios com a LGPD e um método de modelagem contendo 16 passos para orientar o analista a modelar um processo de negócios em conformidade com a Lei Brasileira. Este trabalho é uma etapa inicial importante para a especificação de processos de negócios compatíveis com LGPD.

A Tabela 1 apresenta as principais semelhanças e diferenças entre este trabalho e os principais trabalhos relacionados.

Critério	**Agostinelli et al. (2019)**	**Capodieci e Mainetti (2019)**	**MATULEVIČIUS (2020)**	**TOM (2018)**	**Trabalho Proposto**
Lei de privacidade contemplada	GDPR	GDPR	GDPR	GDPR	LGPD
Tipo de contribuição	Padrões de design		Método para alcançar a conformidade com a GDPR juntamente com uma	Método para avaliar e melhorar a conformidade com a GDPR, utilizando	Questionário de avaliação, Padrões de modelagem e Método de modelagem

			ferramenta de avaliação e extração de informações de um BPMN.	*Privacy Enhanced Technologies.*	
Quantidade de padrões propostos	7	-	-	-	9
Padrões de modelagem propostos	Data Breach, Consent to use, Right to access and rectify, Right of portability, Right to withdraw, Right to be forgotten	-	-	-	Consentimento, Confirmação da existência de tratamento e direito de acesso, Portabilidade, Vazamento de Dados, Revisão de tomada de decisão automatizada, Revogação de consentimento, Retificação de dados, Direito de esquecimento ou eliminação de dados pessoais, Transferência internacional de dados
Validação da proposta	Ausente	Aplicação do método em um processo de negócio fictício de solicitação de férias.	Aplicação do método em um processo de negócio fictício.	Aplicação do método em processos de negócios do *RapidGather.*	Aplicação do método no processo de Matrícula de alunos do colégio de aplicação da UFPE

Tabela 1 – Comparação entre os trabalhos relacionados e o proposto.

1.5. Estrutura do documento

Este documento está estruturado da seguinte forma: no Capítulo 2 são apresentados os principais conceitos envolvidos nesse trabalho; no Capítulo 3 é descrita a metodologia de pesquisa adotada neste trabalho; no Capítulo 4 é descrita

a solução proposta juntamente com a aplicação em um estudo de caso; no Capítulo 5 é apresentado um exemplo de aplicação do método LGPD4BP em um estudo de caso; no Capítulo 6 são discutidos os resultados iniciais da avaliação da proposta; e, finalmente, no Capítulo 7 são discutidas as conclusões e trabalhos futuros.

2. Revisão da Literatura

2.1. Processos de negócios

As organizações, sejam do setor público ou privado, executam tarefas diárias para que possam se manter no mercado de acordo com o tipo de negócio desempenhado. As atividades podem compreender atividades como entrar em contato com fornecedores, processar diversos tipos de dados ou até mesmo realizar a entrega de produtos na residência de um cliente.

Sendo assim, as organizações possuem processos de negócio que são definidos como um conjunto de atividades pré-estabelecidas pela empresa em uma determinada sequência que agrega valor a um cliente interno ou externo (KIRCHMER, 2017). Uma definição mais antiga como a de Weske (2007) define um processo de negócio como uma "*Coleção de atividades que recebe um ou mais tipos de entrada e cria uma saída que é de valor para o cliente*" .

A definição de Weske (2007) mantém a ideia de que existe um conjunto de atividades que precisam ser executadas de forma a agregar valor a um cliente, porém a definição deixa explícito que é necessário que o processo receba alguma entrada, que pode ser algo como por exemplo, um objetivo da empresa, uma solicitação de cliente, uma compra feita por meio de um site que sinalize o início do processo de envio do produto, para que seja possível gerar uma saída, que poderia ser classificada como o recebimento de um produto ou fornecimento de serviço por exemplo.

Portanto, o processo de negócio resulta em um produto ou serviço para um consumidor explicitando quais passos devem ser seguidos para alcançar aquele objetivo. Por fim, como complemento, um processo de negócios segundo o livro *The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM, Volume I* é: "*Um conjunto de atividades ou tarefas estruturadas com comportamentos lógicos que produzem um serviço ou produto específico*" (ROSING; SCHEEL; SCHEER, 2014).

2.2. Business Process Modeling Notation (BPMN)

A notação BPMN é uma das mais reconhecidas que tem como função desenhar o fluxo de um processo de negócio. De acordo com Pullomen et al. (2019), BPMN foi originalmente desenvolvida para prover uma notação que fosse facilmente entendida por todos os usuários de negócios, de analistas técnicos que

estão implementando um sistema de informação à analistas de negócios que vão gerenciar os processos.

BPMN é extremamente útil para descrever a lógica passo a passo de processos de negócios por meio de diagramas. Com esta modelagem, obtém-se uma visão gráfica que expressa de maneira simples e direta todo o processo de negócio. Sendo assim, é possível visualizar por completo todas as etapas de um processo e analisá-lo, se necessário for, fazendo também com que seja visível a responsabilidade de cada ator dentro do processo (BPM CBOK, 2013).

A notação foi desenvolvida por representantes dos principais fornecedores de modelagem de processos de negócios, sob os auspícios da BPMI (*Business Process Management Initiative*), o grupo de interesse de processos de negócios da OMG (*Object Management Group*), uma organização internacional de padrões (HARMON, 2010).BPMN estabelece um padrão pelos quais os fluxos possam ser representados graficamente, permitindo a criação de diagramas dos processos, junto com esse padrão foram criados um conjunto de regras e símbolos universais que permite que vários tipos de processos sejam modelados e entendidos por qualquer usuário de negócios/técnico de qualquer nacionalidade.

Dentro da notação BPMN existem vários símbolos utilizados para representar algo que se passa dentro do processo, ou até algo que ainda vai acontecer "*símbolos descrevem relacionamentos claramente definidos, tais como fluxo de atividades e ordem de precedência*" (BPM CBOK, 2013). Isto remete à definição de processo de negócio, citando que as atividades devem ter uma ordem pré definida para que o objetivo do produto final seja alcançado.

Tendo em vista os aspectos observados, BPMN necessita que os processos sejam modelados a partir de um ponto de vista completo da organização, para que seja possível transcrever quais departamentos se sobrepõem na hora de executar uma atividade e/ou quais esforços têm que ser tomado para que um valor seja agregado a um cliente ao final do processo.

2.3. Privacidade de dados

A privacidade, segundo Tom (2019), aborda a forma como informações confidenciais são obtidas e processadas. Em termos práticos: No primeiro momento de uma conversa com um desconhecido, a maioria das pessoas não vê problema de dizer seu nome para ele no processo de apresentação, no entanto, dificilmente uma pessoa vai passar seus dados bancários para alguém que acabou de conhecer. No entanto, ao contratar algum serviço, como o de telefonia por exemplo, é normal fornecer várias informações além do nome.

O artigo 5, inciso X da Constituição Federal Brasileira diz que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (Brasil, 2020). Em outras palavras, todo brasileiro têm direito à privacidade, seja em sua própria casa ou seja na internet. Tendo isso em vista, é possível concluir que a privacidade é de fato, algo de extrema importância, para os usuários de serviços on line como

exposto por Agostinelli et al. (2019): "*De fato, usuários se preocupam com qualquer dado que possa identificá-los*".

Por fim, privacidade de dados é exatamente isso: como lidar com os dados coletados para que não haja nenhuma brecha de segurança e esses dados venham a ser expostos e cair nas mãos de terceiros, são todas as técnicas de privacidade utilizadas em sistemas que garantam que essa privacidade não seja violada nunca, que jamais um dado possa ser ligado à uma pessoa.

2.3.1. Fair Information Practice Principles (FIPPs)

O conceito de Privacidade ainda é algo muito abstrato com relação à privacidade de dados, portanto, com o passar dos anos foram criados uma série de conceitos conhecidos como *Fair Information Practice Principles* (FIPPs) que tentam traduzir o abstrato conceito de privacidade em diretrizes mais concretas e viáveis (HADAR et al., 2018). Dessa forma, Hadar et al. (2018) define 8 princípios a serem seguidos:

1. Aviso prévio (*Notice*): o FIPPs demanda que o titular dos dados seja notificado sobre a coleta de seus dados;
2. Consentimento ou Escolha (*Consent or Choice*): O titular dos dados tem a opção de aceitar a coleta e processamento de seus dados;
3. Minimização de dados (*Data Minimization*): Os *data controllers* e/ou o grupo que coleta e processa os dados estão sujeitos a uma série de deveres para com os dados, que serão coletados somente o mínimo de dados necessários para a finalidade do negócio ou tecnologia;
4. Especificação de propósito (*Purpose Specification*): É necessário garantir que os dados não vão ser utilizados para outros propósitos para os quais o titular dos dados não deu consentimento;
5. Confidencialidade (*Confidentiality*): O *data controller* também tem o dever de manter o sigilo quanto aos dados, ou seja, de não divulgar ou entregar estes dados à terceiros;
6. Segurança dos dados (*Data Security*): É necessário que haja a prevenção do acesso dos dados por parte de terceiros;
7. Acesso (*Access*): O titular dos dados também tem direitos, bem como o direito de acessar os dados que um data controller tem sobre ele;
8. Retificação (*Rectification*): No caso dos dados não serem precisos, o titular dos dados pode requerer que tais dados sejam retificados.

2.4. Leis de Privacidade de Dados

2.4.1. General Data Protection Regulation (GDPR)

A *General Data Protection Regulation* (GDPR) é uma lei da união europeia criada em 2016 e que só entrou em operação em 28 de Abril de 2018. A GDPR se

preocupa com o processamento de dados pessoais e a livre movimentação desses dados. O objetivo principal da GDPR é salvaguardar a dignidade humana e os direitos fundamentais do titular dos dados (CAPODIECI e MAINETTI, 2019).

A lei define como as empresas e órgãos públicos da união europeia devem lidar com os dados e informações sensíveis de seus usuários, prezando pela total privacidade de tais informações. Para que tal objetivo seja cumprido, é necessário que seja identificado o motivo pelos quais esses dados serão guardados e processados, definir quem tem acesso a esses dados, quantas vezes esses dados poderão ser acessados e por quanto tempo ficarão armazenados (UNIAO EUROPEIA, 2016).

Dados pessoais somente poderão ser processados caso o titular dos dados forneça consentimento por meio de uma afirmação explícita e uma declaração escrita, indicando que seus dados podem ser processados por determinada empresa (UNIAO EUROPEIA, 2016). Após a introdução da Lei e das mudanças que ela trazia acerca de privacidade da informação e proteção de dados, houve repercussão para quem faz a modelagem de processos de negócios utilizando o BPMN, pois na época de desenvolvimento do BPMN a GDPR ainda não existia, portanto, em sua fase de análise o BPMN não incluía todas as informações necessárias que garantem que uma organização está em conformidade com o GDPR (CAPODIECI e MAINETTI, 2019).

Por isso, para identificar as atividades e os respectivos responsáveis em um modelo BPMN onde os dados pessoais são manipulados a GDPR define quatro entidades (AGOSTINELLI et al., 2019):

1. *Data Subject*: A pessoa titular dos dados;
2. *Data Controller:* Entidade que coleta e armazena os dados de uma pessoa e determina os propósitos de processá-los;
3. *Data Processor:* Entidade que processa os dados pessoais de um *Data subject* por solicitação do *Data Controller;*
4. *Data Protection Officer (DPO):* Entidade que faz monitoramento sistemático no *Data Controller* e no *Data Processor* para garantir que estejam em conformidade com a GDPR nos dados coletados do *Data Subject*. .

Além de definir os responsáveis pelas ações tomadas dentro de um BPMN que processa dados pessoais, a GDPR define que informação pessoal é qualquer tipo de informação que poderia ser atribuído à identificação de uma pessoa de forma direta ou indireta (UNIAO EUROPEIA, 2016). Ou seja, não existe um tamanho mínimo de informação que precise ser protegida, todas as informações pessoais, independente do quão mínima ela seja, devem estar protegidas, segundo a GDPR.

Dessa forma a Lei classifica dados pessoais em 3 tipos (AGOSTINELLI et al., 2019):

1. Dados pessoais (*Personal Data):* Qualquer tipo de informação que identifique uma pessoa;

2. *Dados sensíveis (Sensible Data):* É um tipo especial de dado pessoal e requer um nível mais alto de segurança, são informações como saúde, dados bancários, dados biométricos, etc;
3. *Dados criminais (Criminal Records):* É um tipo de dado sensível (*Sensible Data) que* contém informações que possam identificar crimes cometidos pelo *Data Subject*.

A GDPR também define uma lista de obrigações que devem ser cumpridas pelo *Data Controller* para que ele esteja em conformidade com a Lei. As obrigações são uma série de regras que devem ser seguidas em determinadas situações. A lei também prevê uma série de direitos ao titular dos dados, direitos estes que devem ser assegurados acima de tudo pelas empresas e órgãos públicos que utilizarem os dados pessoais do consumidor, são alguns deles (UNIAO EUROPEIA, 2016):

1. Informação, comunicação e modalidades transparentes para o exercício dos direitos dos dados pessoais do titular (*Transparent information, Communication and modalities for the exercise of the rights of the data subject*) - Artigo 12;
2. Informações de onde são coletados os dados pessoais do titular dos dados (*Information to be provided where personal data are collected from the data subject*) - Artigo 13;
3. Informações de onde não são coletados os dados pessoais do titular dos dados (*Information to be provided where personal data have not been obtained from the data subjec*t) - Artigo 14;
4. O direito de acessar seus dados (*Right of access by the data subject*) - Artigo 15;
5. O direito de retificar seus dados (*Right to rectification*) - Artigo 16;
6. O direito de ser “esquecido” (*Right to erasure ‘right to be forgotten’*) - Artigo 17;
7. O direito à restrição do processamento (*Right to restriction of processing*) - Artigo 18;
8. O direito à portabilidade de dados (*Right to data portability*) - Artigo 20;
9. O direito de se opor (*Right to object*) - Artigo 21.

A GDPR procura proteger os direitos dos titulares dos dados em relação a privacidade de forma que as empresas que descumprirem a Lei estarão sujeitas à receber desde uma simples notificação à uma multa de até 20 Milhões de Euros ou 4% do faturamento anual da empresa, o que for maior como disposto no artigo 83, cláusula 5 (UNIAO EUROPEIA, 2016). A GDPR não deve resolver todos os problemas com relação à privacidade, mas é um grande exemplo em prol da proteção de dados.

2.4.2. Lei Geral de Proteção de Dados (LGPD)

A Lei 13.709, Lei Geral de Proteção de Dados (LGPD) foi sancionada em 14 de Agosto de 2018 (BRASIL, 2020) e a expectativa é entrar em vigor em Agosto de 2020. Esta lei visa a proteção de dados pessoais de indivíduos, sejam eles utilizados em empresas do setor público ou privado.

A Lei abrange todo território Brasileiro, se fazendo válida em todo país, tendo como principal objetivo proteger todos os dados coletados, armazenados e processados por empresas públicas ou privadas, com isso, qualquer empresa em território Brasileiro que possuir uma base de dados com informações de seus clientes, por mais básicas que sejam essas, deverão seguir os procedimentos que estarão previstos na nova lei.

De forma bem semelhante à GDPR, a LGPD define como informação pessoal Informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2020). Ela também define 3 tipos de dados pessoais (BRASIL, 2020):

1. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
2. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, etc;
3. Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Há uma diferença entre os tipos de dados definidos pela LGPD e pela GDPR, enquanto a GDPR prevê dados criminais como um tipo de dados sensíveis e prevê um tipo de segurança ainda maior para ele, a LGPD adiciona um novo tipo de dado pessoal, o dado anonimizado. Trata-se de um tipo de dado que não pode ser ligado à um titular de formas convencionais, ou seja, não é possível identificar a quem pertence aquele dado durante seu processamento.

A LGPD também define seus atores de forma semelhante à LGPD (BRASIL, 2020):

- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Diferente de sua semelhante lei europeia, na Lei Brasileira o Encarregado é uma pessoa indicada tanto pelo Controlador quanto pelo Operador e serve de ponte de comunicação entre eles, o titular de dados e a Autoridade Nacional de Proteção de Dados *(*ANPD), ao invés de monitorar sistematicamente o Controlador e o Operador, como faz o *Data Protection Officer.*

Dentro da LGPD, o tratamento dos dados pessoais de um indivíduo apenas pode ser realizado a partir de uma declaração de consentimento do mesmo, sendo este consentimento definido como "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*" (BRASIL, 2020). Tal consentimento pode ser revogado a qualquer momento caso o Titular não deseje mais continuar com o processamento de seus dados.

Existe uma lista de direitos previstos para o titular dos dados no artigo 18 da lei que devem ser assegurados enquanto seus dados forem processados:

1. Direito de Confirmação da Existência de tratamento dos dados;
2. Direito de acesso aos dados;
3. Direito de correção de dados incompletos, inexatos ou desatualizados;
4. Direito de anonimização, bloqueio ou eliminação de dados desnecessários;
5. Direito de portabilidade;
6. Direito de Eliminação dos dados;
7. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

As punições previstas para as empresas que descumprirem as regras vão de uma simples multa à 2% do faturamento total da empresa. Pode-se dizer que de forma geral a LGPD tem várias semelhanças com a GDPR, porém a Lei Brasileira tem um nível de detalhamento menor do que a GDPR, no geral a Lei cobre tudo o que a GDPR aborda, as duas são quase iguais em termos de abrangência.

2.4.3. Leis de proteção de dados ao redor do mundo

Não apenas o Reino Unido com a GDPR e o Brasil com a LGPD criaram suas leis de privacidade, outros países ao redor do mundo avançaram no campo de leis de privacidade. Por exemplo, os Estados Unidos da América possuem várias leis de privacidade estaduais. Desde 2004, o estado da Califórnia já havia posto em prática a *California Online Privacy Protection Act* ou CalOPPA (ZACHARY et. al., 2014), o que fez com que a Califórnia se tornasse o primeiro estado americano a aprovar uma lei exclusiva de privacidade de dados.

A CalOPPA diz que o operador de um serviço online ou site comercial que coleta dados pessoais ou informações identificáveis através da internet de consumidores residentes no estado da Califórnia que usam ou visitam o serviço online devem postar explícitamente sua política de privacidade (CALIFORNIA, 2004). Vale ressaltar que este artigo em específico tem o intuito de deixar explícito os termos de privacidade de um site, além de fazê-lo acessível à população, pois é uma preocupação que a lei Californiana tem, a de ter políticas de privacidade em termos de fácil entendimento da população.

A lei Californiana define que qualquer informação pessoal que possa identificar uma pessoa é um *Personal Identifiable Information* (PII) porém, diferente das leis Européia e Brasileira, não é necessário que um PII tenha algum nível de segurança. A lei também implementa um sistema chamado de *Do Not Track* (DNT) *Requests* que trata-se de um mecanismo presente nos navegadores em que os usuários podem habilitar a opção para que suas atividades em um site não sejam registradas (CALIFORNIA, 2004)

Em resumo, a CalOPPA diz que os principais pontos que uma política de privacidade deve apresentar são:

1. Indicar a data de efetivação da política;
2. Listar os tipos de informações que são coletadas do usuário (e como eles podem cancelar esta coleta);
3. Explicar como os usuários podem requisitar a revisão (e exclusão) de seus PII;
4. Explicar como as mudanças e atualizações na política de privacidade serão informadas aos usuários;
5. Informar se seus dados serão compartilhados com terceiros;
6. Informar se uma DNT será honrada ou não.

O Canadá também conta com sua própria lei de privacidade, a *Personal Information Protection And Electronic Documents Act* (PIPEDA). A lei diz que os negócios que estejam usando dados com o propósito de atividades comerciais devem especificar os motivos do processamento dos dados aos seus respectivos donos, e obter seu consentimento para que possa continuar (CANADÁ, 2020).

A Lei Canadense define como atividade comercial como qualquer transação, ato ou conduta particular, ou qualquer curso regular de conduta que seja de caráter comercial, incluindo a venda, troca ou arrendamento de doadores, membros ou outras listas de arrecadação de fundos (CANADÁ, 2020). A PIPEDA também define dado pessoal como qualquer informação fatual ou subjetiva, gravada ou não, sobre um indivíduo identificável.

A PIPEDA define 10 *fair information principles* (FIP) para que se esteja em conformidade com a lei, os princípios são:

1. *Accountability*: A lei aconselha a criação de um programa de privacidade para a empresa, nomear um oficial de privacidade e conduzir uma avaliação do

impacto da privacidade e uma análise de ameaças das práticas de tratamento de informações pessoais da sua organização, incluindo atividades em andamento, novas iniciativas e novas tecnologias;

2. *Identifying Purposes:* Este FIP aconselha que seja feita a revisão do uso dos dados pessoais para garantir que são coletados para um propósito em específico e caso não sejam, obter um novo consentimento ao especificar o propósito, tanto verbalmente quanto por escrito;
3. *Consent*: Aqui existem algumas dicas sobre como deve ser o documento de consentimento que será entregue ao usuário, as instruções vão desde prover informações claras e legíveis ao usuário até sobre como obter o consentimento de crianças, que nesse caso, deve ser cedido por pais ou guardiões legais;
4. *Limiting Collection:* A PIPEDA pede que a organização identifique os tipos de dados que estão sendo colhidos e que limite a coleta para apenas os tipos de dados que serão necessários para o propósito já especificado, garantindo que seja possível explicar o porquê do uso daquele tipo de dado;
5. *Limiting Use, Disclosure, and Retention:* Neste FIP , é necessário documentar qualquer novo propósito para uso de dados pessoais, bem como limitar e monitorar quem tem acesso às informações dentro da organização e a eliminação de dados que já não são mais utilizados;
6. *Accuracy:* Neste passo é indicado manter as informações pessoais o mais precisas e atualizadas o possível, levando em consideração os interesses de um indivíduo e também criar uma política que indique quais tipos de informação devem ser atualizadas;
7. *Safeguards:* Este passo instrui a proteger todo e qualquer tipo de informação pessoal, independente de como ela é armazenada contra perda, roubo, acesso não autorizado, cópia, uso ou modificação. Para isto é aconselhado desenvolver e implementar uma política de segurança para proteger as informações pessoais. Além de usar a segurança apropriada para impedir o acesso físico e lógico às informações;
8. *Openness:* Este FIP diz que uma organização deve ser transparente com os seus consumidores e funcionários sobre como os dados pessoais são gerenciados, apresentando-os da forma mais fácil e sucinta possível;
9. *Individual Access:* Uma organização deve estar pronta para responder solicitações de acesso à dados pessoais por parte de seus usuários, este FIP diz que a organização deve ajudar na criação da solicitação e respondê-lo em até 30 dias depois do recebimento, caso não seja possível responder em até 30 dias, o solicitante deve ser alertado para que possa abrir uma queixa ao *Office of the Privacy Commissioner of Canada* se desejar. A organização deve garantir que a informação é entendível, explicando acrônimos e termos e abreviações;

10. *Challenging Compliance*: Um indivíduo deve ser capaz de desafiar a conformidade de sua organização com os FIP. Dessa forma, a organização deve registrar a data e o motivo pelo qual recebeu o desafio, atribuir o desafio à uma pessoa com as habilidades necessárias para que possa revisá-lo de maneira justa e imparcial e fornecer à essa pessoa acesso a todos os registros relevantes, funcionários ou outras pessoas que lidaram com as informações pessoais ou solicitação de acesso. Logo após isso é necessário notificar o resultado à todos os envolvidos e realizar as alterações nas políticas ou dados pessoais caso seja necessário.

Outras leis de privacidade são encontradas em outros países como a África do Sul, que possui a *Protection of Personal Information Act* (POPI) (SOUTH AFRICA, 2013) e a *Personal Data Protection Bill*, na Índia (INDIA, 2019).

Na próxima seção, é descrita a metodologia adotada na condução deste trabalho.

3. Metodologia

Este trabalho tem como objetivo responder às seguintes questões de pesquisa:

(1) Como avaliar a conformidade de um processo de negócio com a LGPD?

(2) Como modelar um processo de negócio em conformidade com a LGPD?

Para que tais questões sejam respondidas, foi seguida a metodologia apresentada na Figura 1, que consiste em 4 passos: Planejamento, Design e Construção, Validação e Avaliação do Método.

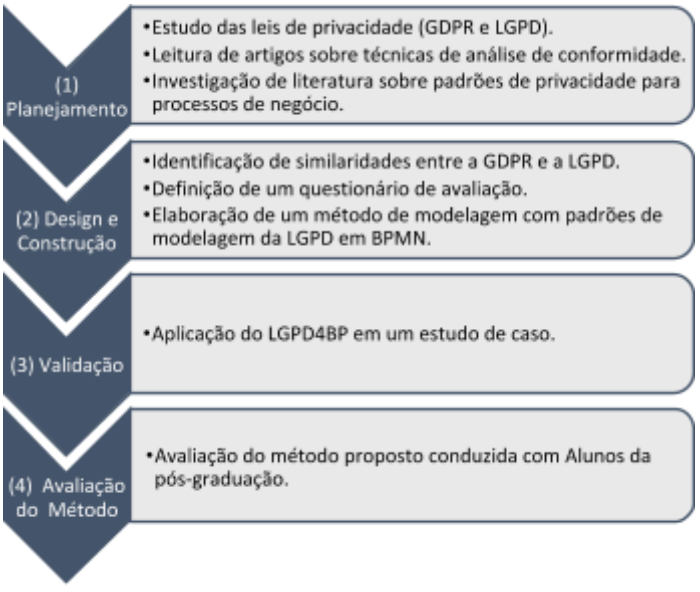


Figura 1. Metodologia de pesquisa seguida neste trabalho.

O passo de Planejamento consistiu no estudo das leis de privacidade, tanto a GDPR quanto a LGPD, no qual a leitura dos documentos oficiais das duas leis foi realizada juntamente com a interpretação de alguns autores sobre as respectivas leis. Após a leitura e estudo das duas leis, foi conduzida uma leitura de artigos sobre técnicas de análise de conformidade de processos bem como trabalhos mais específicos de análise de conformidade de processos com a GDPR como o trabalho de (TOM, 2018). Após levantar várias hipóteses de análise de conformidade, foram investigados padrões de privacidade para processos de negócios de (AGOSTINELLI et al., 2019) para que fosse possível elaborar um padrão que atendesse às perguntas de pesquisa deste trabalho.

O passo de Design e Construção foi realizado após a conclusão do passo de planejamento. Após o estudo da GDPR e LGPD, foi possível mapear suas semelhanças, tendo em vista que as leis possuem diversos pontos em comum. A partir desse mapeamento, foi elaborado uma tabela que aponta os artigos de cada lei que são semelhantes e os motivos conforme apresentado na Tabela 2. O foco dessa comparação é enfatizar as similaridades entre a LGPD e GDPR ressaltando os aspectos considerados relevantes para este trabalho.

Artigo GDPR	**Artigo LGPD**	**O que dizem as leis**
(26)	Art 5. I.	Definem o que é dado pessoal perante as leis.
(75)	Art 5. II. & III.	Definição de dados sensíveis, criminais e anonimizados, sendo este último pertencente apenas à LGPD.
(85), (86)	Art 48.	Definem o *Modus Operandi* em caso de um vazamento de dados.
Art 4, 11	Art 5. XII.	Definem o que é e como deve ser declarado o consentimento por parte do titular dos dados.
Art 8, 1	Art 14. I, III.	Definem as regras para tratamento de dados de menores de idade levando em consideração a maioridade penal de ambos os países.
Art 12, Art 13, Art 14, Art 15, Art 16, Art 17, Art, 18, Art 20, Art 21.	Art 18. I, II, III, IV, V, VI, VII, VIII, IX.	Definem os direitos do titular dos dados.
Art 28, 3.	Art 39.	Definem as regras para

		processamento dos dados.
Art. 44, Art. 45, Art. 46, Art. 48.	Art. 33, Art. 34.	Definem as regras para transferência internacional dos dados.
Art 83, 5. Portabilidade, revogação de consentimento, revisão de decisão automatizada, direito de se opor	Art 52, II. Procurar direitos implícitos da GDPR que estejam na LGPD	Definem as multas e sanções administrativas para os inadimplentes.

Tabela 2. Semelhanças entre a GDPR e a LGPD.

Para responder a pergunta de pesquisa 1 (*Como avaliar a conformidade de um processo de negócio com a LGPD?*) foi proposto um questionário para avaliar se um processo de negócio é compatível com LGPD. O questionário possui 18 perguntas elaboradas para avaliar aspectos da LGPD nos processos de negócio de uma organização. O intuito de cada pergunta no questionário é direcionar os passos que devem ser corrigidos em um processo de negócio para atingir a conformidade com a lei. O questionário é apresentado na Seção 4.1 do Capítulo 4.

Para responder a pergunta de pesquisa 2 (*Como modelar um processo de negócio em conformidade com a LGPD*?) foi proposto um método de modelagem e um catálogo de padrões de modelagem em BPMN. O Método de modelagem é composto por 16 passos e têm o suporte de um catálogo de padrões de modelagem que contém 9 padrões. O objetivo de utilizar padrões de modelagem partiu dos princípios de padrões de projeto, que segundo Christopher (1979) é "*Cada padrão é uma regra de três partes que expressa uma relação entre um certo contexto, um problema e uma solução*". É possível então considerar que para entender a necessidade de um padrão, é necessário que primeiro se entendam suas três partes.

Desta forma, pode-se inferir que um padrão de projeto é uma solução periódica para um problema dentro de um contexto. Esse é exatamente o objetivo dos padrões de modelagem: apresentar as soluções em BPMN que devem ser usadas de forma recorrente, a fim de ilustrar como resolver questões de conformidade em processos de negócio. O catálogo de padrões de modelagem é apresentado na Seção 4.2 e o Método de modelagem explicado na Seção 4.3, ambos no Capítulo 4.

No passo de Validação, o método proposto, LGPD4BP, foi aplicado em um estudo de caso. O cenário escolhido para aplicação foi o processo de matrícula do Colégio de Aplicação (CAp) da Universidade Federal de Pernambuco. Esse processo foi escolhido por tratar dados pessoais de menores em uma instituição pública. Além disso, existe um plano de implantação dos processos do colégio nos

sistemas usados pela Universidade. . Viu-se então a oportunidade de aplicar o método ao processo de matrícula do CAp, com o intuito de encontrar, expor e sugerir correções de não-conformidades encontradas durante o processo. O processo de aplicação do método pode ser encontrado no Capítulo 5 deste trabalho.

Por fim, no passo de Avaliação, foi conduzido um estudo qualitativo, baseado nos trabalhos de Ferrari et al. (2019) e Bano et al. (2019), onde 18 alunos de pós-graduação, de uma disciplina abordou conceitos relacionados à *security*, ética, *safety,* privacidade e conformidade com leis, foram instruídos sobre como aplicar o LGPD4BP em processos de negócios.

Em seguida, foram solicitados à aplicar o método proposto no processo do colégio de aplicação para que pudessem responder perguntas sobre utilidade dos artefatos apresentados no método e as dificuldades encontradas na aplicação do método. Os participantes do estudo também responderam questões sobre a completude do método e foram encorajados à sugerir melhorias que pudessem ser incorporadas ao método proposto. A avaliação completa do perfil dos participantes e resultados do estudo podem ser encontradas na Seção 6.

O Capítulo seguinte descreve o Método LGPD4BP e seus componentes.

4. Método LGPD4BP

Guiado pelas perguntas de pesquisas e Objetivos descritos nas Seções 1.2 e 1.3 respectivamente, o método LGPD4BP (LGPD for Business Process) é proposto neste trabalho. Esse método é composto por um questionário de avaliação da conformidade dos processos em relação à LGPD (Seção 4.1), Catálogo de Padrões de Modelagem (Seção 4.2) e um Método de modelagem de processos em conformidade com a LGPD (Seção 4.3)

4.1. Questionário de avaliação de conformidade

Para responder a pergunta de pesquisa P1 deste trabalho (*Como avaliar a conformidade de um processo de negócio com a LGPD?*) foi proposto um questionário para avaliar se um processo de negócio está em conformidade com a LGPD.

As perguntas que compõem o questionário, presentes na Tabela 3, foram definidas com base nos direitos do titular e nos textos da lei Brasileira conforme explicitado na segunda coluna da tabela.

Pergunta	REFERÊNCIA LEGISLATIVA (LGPD)
1) O processo inclui as ações para obter consentimento? ( ) Sim. ( ) Não. ( ) Não se	Segundo o *Art. 7º da lei, "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*

aplica, o controlador de dados possui base legal para processamento. ( ) Não se aplica, a exigência de consentimento é dispensada porque os dados foram tornados públicos pelo titular dos dados.	*I - mediante o fornecimento de consentimento pelo titular;* Que de acordo com a especificação no *Art. 5° " Para os fins desta Lei, considera-se:* *XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;* Desta forma, faz-se necessário que o Controlador obtenha o consentimento do usuário para que possa iniciar o tratamento dos dados com ressalva para quando os dados foram tornados públicos pelo usuário, como fica registrado no *§ 4° "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei."*
2) O processo especifica as bases legais de processamento? ( ) Sim. ( ) Não. ( ) Não se aplica, o controlador possui consentimento do usuário.	De acordo com o *Art. 7º da lei, "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:* *I - mediante o fornecimento de consentimento pelo titular;* *II - para o cumprimento de obrigação legal ou regulatória pelo controlador; ….."* Sendo assim, o controlador poderá tratar dados pessoais (Artigo 7 - §II a §X) ou dados sensíveis (Artigo 11 - §II) mesmo sem ter consentimento do usuário desde que apresente base legal para o tratamento dos dados.
3) O processo inclui as ações para lidar com dados pessoais de crianças? ( ) Não. ( ) Sim, e foram modeladas com o consentimento dado por pelo menos um dos pais ou guardião legal ( ) Sim, mas não foram modeladas. ( ) Não se aplica.	Como citado no *Art.14, § 1°: "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.* *§ 1° O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal."* Portanto, como supracitado na lei, o controlador poderá tratar dados pessoais de crianças somente podem ser tratados com um consentimento específico que deve ser cedido por pelo menos um dos pais ou guardião legal do menor.

4) O processo contém informações sobre a possibilidade de não prover consentimento e as consequências da recusa? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Não se aplica.	Consta no *Art. 18: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:* *VII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;"* O controlador é obrigado a ceder ao titular dos dados as informações sobre a possibilidade de não fornecer o seu consentimento para tratamento de dados e bem como as consequências da negação.
5) O processo contém as ações para compartilhamento de dados com terceiros? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, e as ações não foram modeladas. ( ) Não se aplica, o processo não compartilha dados com terceiros.	O já supracitado Art. 7, diz no seu *§ 5º: "O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei."* Portanto, no caso de compartilhamento de dados com terceiros, o titular deve ficar ciente por meio do consentimento.
6) O processo inclui as ações para lidar com dados sensíveis? ( ) Não. ( ) Sim, e as ações foram modeladas.Sim, e as ações não foram modeladas. ( ) Não se aplica.	O Art. 11 diz que: "*Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:* *I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;"* Porém os dados sensíveis podem ser tratados em ocasiões específicas sem o consentimento de um titular, como diz a cláusula II: "*II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:* *a) cumprimento de obrigação legal ou regulatória pelo controlador;* *b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;"* Ainda existem várias outras ocasiões presentes no Art. 11, como mostrado de a) à g) e nos incisos §1 à §5.
7) O processo indica quem é o ator (Departamento/Posição) responsável pelo processamento de dados em cada atividade? ( ) Não. ( ) Sim, e foi modelado	O *Art. 42* diz que: *"O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."* Desta forma, faz-se necessário saber quem era

nas lanes do processo.	responsável pelo processamento de dados em cada etapa do processamento, para que em casos como os citados no Art.42 o responsável seja responsabilizado ou isentado de culpa, como diz o *Art. 43: "Os agentes de tratamento só não serão responsabilizados quando provarem:* *I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;* *II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou* *III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."*
8) O processo apresenta a finalidade de processamento dos dados no nome do modelo? ( ) Não. ( ) Sim.	De acordo com o *Art. 9: "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:* *I - finalidade específica do tratamento;"* Logo, um processo que possui sua finalidade logo no nome de seu modelo pode facilmente ser identificado pelo titular de forma clara e concisa de que seus dados estão sendo tratados para à finalidade descrita no documento de consentimento.
9) O processo apresenta o local em que os dados são armazenados e processados? ( ) Não. ( ) Sim.	As informações que constam no *Art. 19* são*: "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:* *§ 1o Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso."* Prover o local de armazenamento e processamento de dados facilita o atendimento da solicitação de acesso de dados.
10) O processo inclui as ações para realizar uma transferência internacional de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	Existem algumas restrições quanto à possibilidade de realizar uma transferência internacional de dados, portanto, o Art. 33 define algumas restrições, como diz na lei: "*A transferência internacional de dados pessoais somente é permitida nos seguintes casos:* *I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;"* Assim sendo, p controlador só pode realizar a transferência de dados em algum dos casos citados (em I a IX), e ainda no caso I, o Art 34 complementa que: "*O nível de proteção de dados do país estrangeiro*

	ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração: *I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;"* E mais outros requisitos que complementando o I vão de II a VI.
11) O processo inclui as ações para descarte de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	O Art.16 traz em seus textos legais o seguinte: "*Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:* *I - cumprimento de obrigação legal ou regulatória pelo controlador;* *II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;* *III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou* *IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."* Por conseguinte, os dados pessoais devem ser descartados ao término de seu processamento a menos que se enquadre em alguma das afirmativas presentes no artigo.
12) O processo inclui as ações para realizar portabilidade de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	O Art.18, em seu inciso V diz que: *"O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele* *tratados, a qualquer momento e mediante requisição:* *V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;"* Complementado pelo § 7°: *"A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador."* Portanto, algumas precauções devem ser tomadas com relação ao processo de portabilidade de dados, o mesmo só deve ser realizado mediante solicitação expressa do titular dos dados e apenas dados não anonimizados pelo controlador podem ser transferidos.
13) O processo inclui as ações para lidar com um vazamento de dados? ( ) Não. ( ) Sim, e as ações	O Art. 6° diz que: *"As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:* *VII - segurança: utilização de medidas técnicas e*

foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	*administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;* *VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;"* Complementando no Art. 46, que diz: *"Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."* Fechando com o Art. 48, que diz: *"Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares."* Além de ainda estabelecer as ações que devem ser tomadas durante um vazamento de dados e o tempo de comunicação à ANPD, incluindo na notificação os titulares que foram envolvidos no vazamento, a lista de dados vazados entre outros.
14) O processo inclui as ações para realizar decisões automatizadas? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	O Art 20 prevê que: *"O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade."* Complementado pelos seus incisos: *"§ 1° O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.* *§ 2° Em caso de não oferecimento de informações de que trata o § 1° deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais."* Desta forma, o controlador tem o dever de informar ao titular dos dados sobre as tomadas de decisão automatizadas baseadas no perfil que foi traçado para o titular dos dados.
15) O processo inclui as ações para o caso de haver revogação de consentimento?	Conforme descrito no § 5° do Art. 8: *"O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos*

( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	*realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei."* Sendo reiterado no § 6°: *"Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9o desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração."* Portanto, fica explícito que em caso de revogação de consentimento o tratamento de dados do titular deve ser imediatamente cessado, o que acarreta em alterações no processo.
16) O processo inclui as ações a serem tomadas o caso de haver uma retificação de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	O Art. 18 estipula que: *"Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:* *III - correção de dados incompletos, inexatos ou desatualizados;"* Logo, o titular pode retificar os dados a qualquer momento.
17) O processo inclui as ações a serem tomadas no caso de uma exclusão de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	Também no Art.18, é possível ver na sua cláusula VI que: "*VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art.16 desta Lei;"* Que possui algumas condições para que a solicitação seja cumprida, como descrito na pergunta 11.
18) O processo inclui as ações a serem tomadas no caso de uma solicitação de acesso de dados por parte do usuário? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.	Como previsto no Art. 9: *"O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:"* Tal solicitação deve ser cumprida com as seguintes características: *"I - finalidade específica do tratamento;* *II - forma e duração do tratamento, observados os segredos comercial e industrial;* *III - identificação do controlador;* *IV - informações de contato do controlador;* *V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;* *VI - responsabilidades dos agentes que realizarão o tratamento; e*

	VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei."

Tabela 3. Rastreamento entre as perguntas do questionário para avaliar a conformidade de um processo de negócio e a LGPD.

O intuito deste questionário também é avaliar o grau de conformidade dos processos de uma empresa. É possível perceber que todas as perguntas do questionário proposto foram elaboradas a partir de referências à lei Brasileira, de forma que existisse uma coesão entre o que o questionário almejava e o que a Lei determina.

Após responder as questões presentes no questionário de avaliação, para determinar se o processo de negócio está em conformidade com a LGPD, as respostas para todas as questões devem ser "Sim" quanto à modelagem das ações necessárias ou "Não aplicável". Portanto, como todas as ações são necessárias para atingir a conformidade, não existe um número mínimo de respostas "Sim"/"Não aplicável" para que um processo de negócio possa ser considerado compatível com a LGPD. Outro ponto importante é que não é possível que todas as perguntas sejam respondidas como "Não se aplica". Logo, não é possível estabelecer um valor limite (*threshold*) de avaliação.

4.2. Catálogo de Padrões de Modelagem

Para responder a pergunta Pergunta de Pesquisa P2 deste trabalho (*Como modelar um processo de negócio em conformidade com a LGPD?*) é proposto um catálogo de padrões de modelagem e um método de modelagem (Seção 4.3).

O catálogo foi construído considerando o formato comumente utilizado na engenharia de software para especificação de padrões arquiteturais. Segundo Buschmann (1996), um padrão de arquitetura consiste em um aglomerado de subsistemas já prontos que podem ser facilmente reutilizados quando necessários e que especificam suas próprias responsabilidades, incluindo seus próprios critérios e regras que organizam as relações entre eles (BUSCHMANN, 1996).

Sendo assim, Buschmann (1996) afirma que a forma mais comum de representar os padrões arquiteturais é pela apresentação das seguintes informações:

- Nome do padrão
- Contexto
- Problema:
    - Impõe a descrição de vários aspectos problemáticos que devem ser considerados
- Solução:
    - Fundamentos
    - Contexto resultante
    - Exemplos

O formato da apresentação dos padrões de modelagem adotado neste trabalho contém os seguintes campos: Nome, Diagrama, Propósito, Uso e Exemplo. Na Tabela 4 são descritos os nove padrões propostos assim como o propósito de cada um e uma referência de qual(is) pergunta (s) do questionário de avaliação

(Seção 4.1) são contempladas pelo uso do padrão.

Padrão de modelagem	Propósito do padrão	Perguntas atendidas
Consentimento	Permitir a modelagem de solicitações de consentimentos, ou quando é necessário solicitar o consentimento novamente ao titular dos dados, seja por uma mudança na política de privacidade ou por verificação de consentimento durante o processamento de dados.	Perguntas 1 a 5 do questionário.
Confirmação da existência de tratamento e direito de acesso	**Direito de acesso**: Determinar o processo de acesso a dados quando solicitado pelo titular dos dados, partindo do pressuposto de que os dados já foram armazenados de forma organizada facilitando tipo de solicitação. **Consentimento:** Permitir a modelagem de solicitações de consentimentos, ou quando é necessário solicitar o consentimento novamente ao titular dos dados, seja por uma mudança na política de privacidade ou por verificação de consentimento durante o processamento de dados.	Pergunta 5.
x	x	As perguntas 6 a 9 e 11 são contempladas diretamente no modelo BPMN.
Transferência Internacional de Dados	Exibir o *modus operandi* do controlador em cada uma das situações específicas para transferência internacional de dados	Pergunta 10.
Portabilidade	Registrar o processo de portabilidade de dados entre duas empresas.	Pergunta 12.
Vazamento de Dados	Estabelecer o comportamento esperado em caso de vazamento de dados.	Pergunta 13.

Revisão de tomada de decisão automatizada	Documentar o processo de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.	Pergunta 14.
Revogação de Consentimento	Definir os passos que devem ser seguidos pelo Controlador em caso de alteração na política de privacidade de processamento de dados.	Pergunta 15.
Retificação de Dados	Exibir os passos que devem ser seguidos para que seja feita a retificação de dados.	Pergunta 16.
Direito de Eliminação ou Esquecimento	Definir os passos do processo de exclusão de dados.	Pergunta 17.
Confirmação da existência de tratamento e direito de acesso.	Determinar o processo de acesso a dados quando solicitado pelo titular dos dados, partindo do pressuposto de que os dados já foram armazenados de forma organizada facilitando tipo de solicitação.	Pergunta 18.

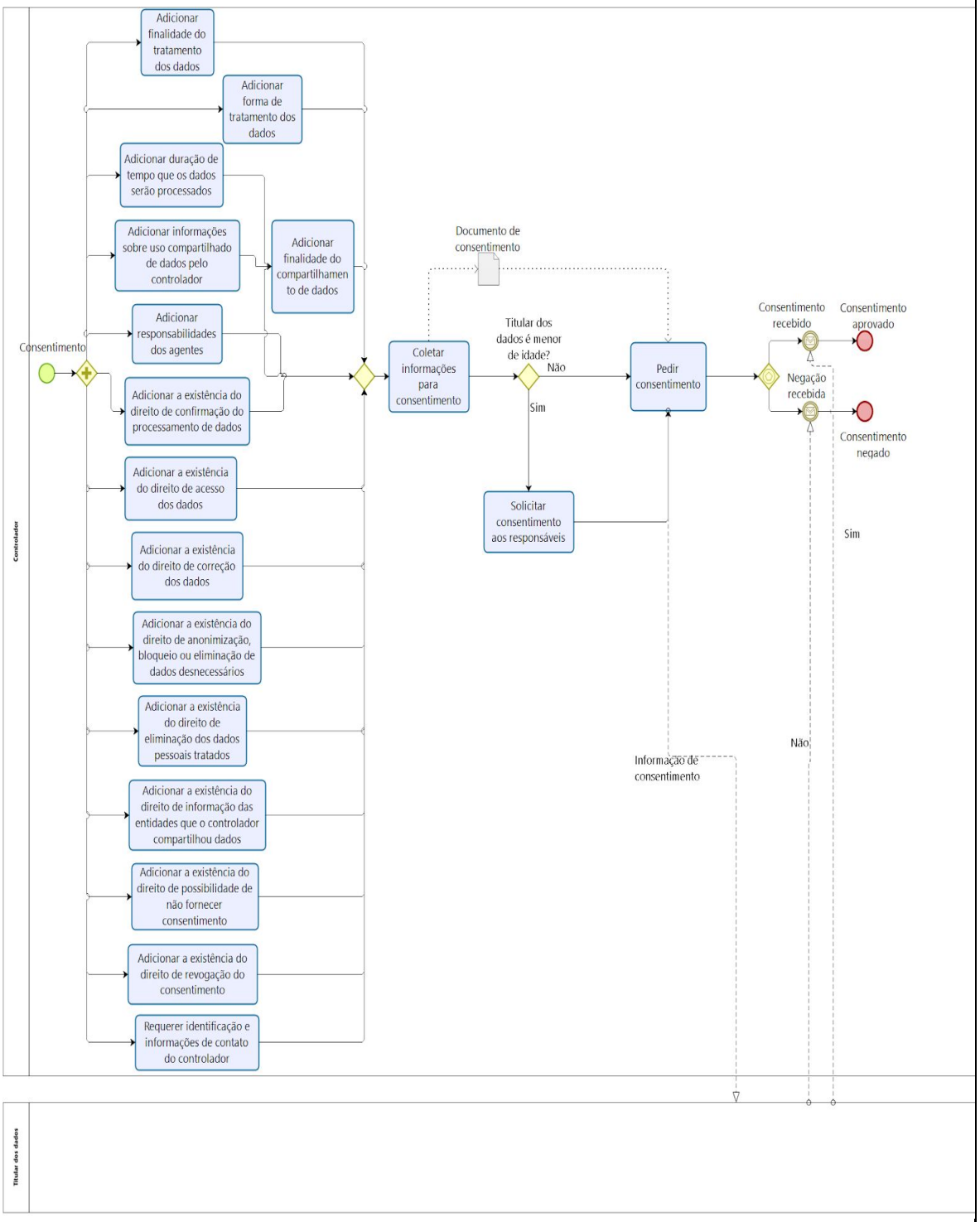
Tabela 4. Relação entre os padrões de modelagem e as perguntas do questionário de avaliação de conformidade de processos de negócio.

A descrição de cada padrão no formato adotado (Nome, Diagrama, Propósito, Uso e Exemplo) bem como os respectivos diagramas são apresentados nas Tabelas 5 a 13. O objetivo deste catálogo de padrões de modelagem de processos de negócio é consolidar os requisitos de LGPD, representando essas informações em modelos de processos de negócios expressos em BPMN.

O catálogo consiste em nove padrões: Consentimento, Direito de Acesso, Transferência internacional de dados, Portabilidade, Vazamento de Dados, Revisão de tomada de decisão automatizada, Retificação de Dados, Direito de Eliminação ou Esquecimento, Confirmação da existência de tratamento e direito de acesso. Esses padrões podem ser usados por analistas para modelar processos de negócio para atingir a conformidade LGPD.

Os padrões propostos também são apresentados na página do método:para melhor visualização: https://sites.google.com/view/lgpd4bp.

Nome do padrão: Consentimento



Propósito: Permitir a modelagem da solicitação de consentimento quando necessário requisitar novamente ao titular dos dados, seja por motivo de alteração de privacidade no contrato ou por verificação de consentimento em meio a operações de processamento de dados.

Usar quando:

● Necessário solicitar consentimento do titular dos dados; ● Necessário solicitar consentimento devido à alterações de privacidade no contrato; ● Verificar consentimento com titular de dados em meio a operações de processamento de dados.
Exemplo: Ao realizar uma operação de tratamento de dados sensíveis e constatar o compartilhamento de dados com terceiros, o controlador analisa o contrato de consentimento de uso de dados e percebe que a informação não está presente no documento. O Controlador então edita o contrato de consentimento e o envia ao titular dos dados, junto com a informação da alteração na política de privacidade presente no mesmo, de forma que o titular dos dados tenha que novamente, concordar com os termos de privacidade para que seus dados continuem sendo processados.

Tabela 5. Padrão de Consentimento.

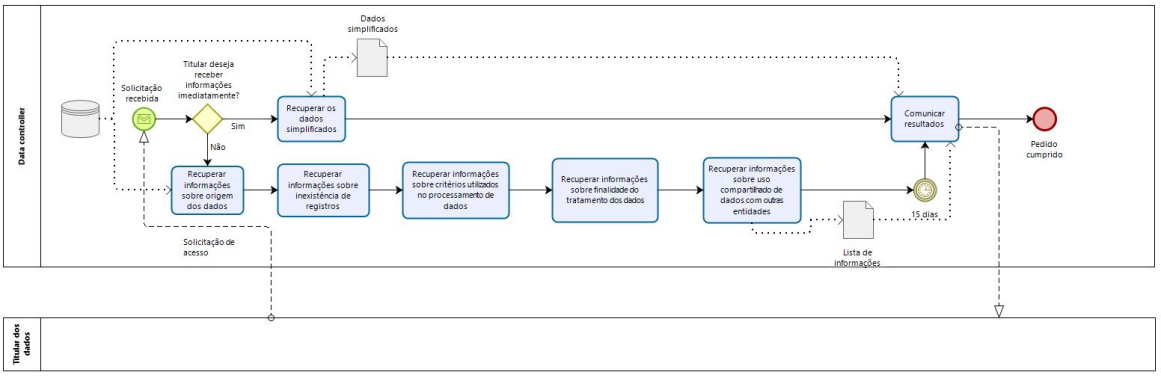
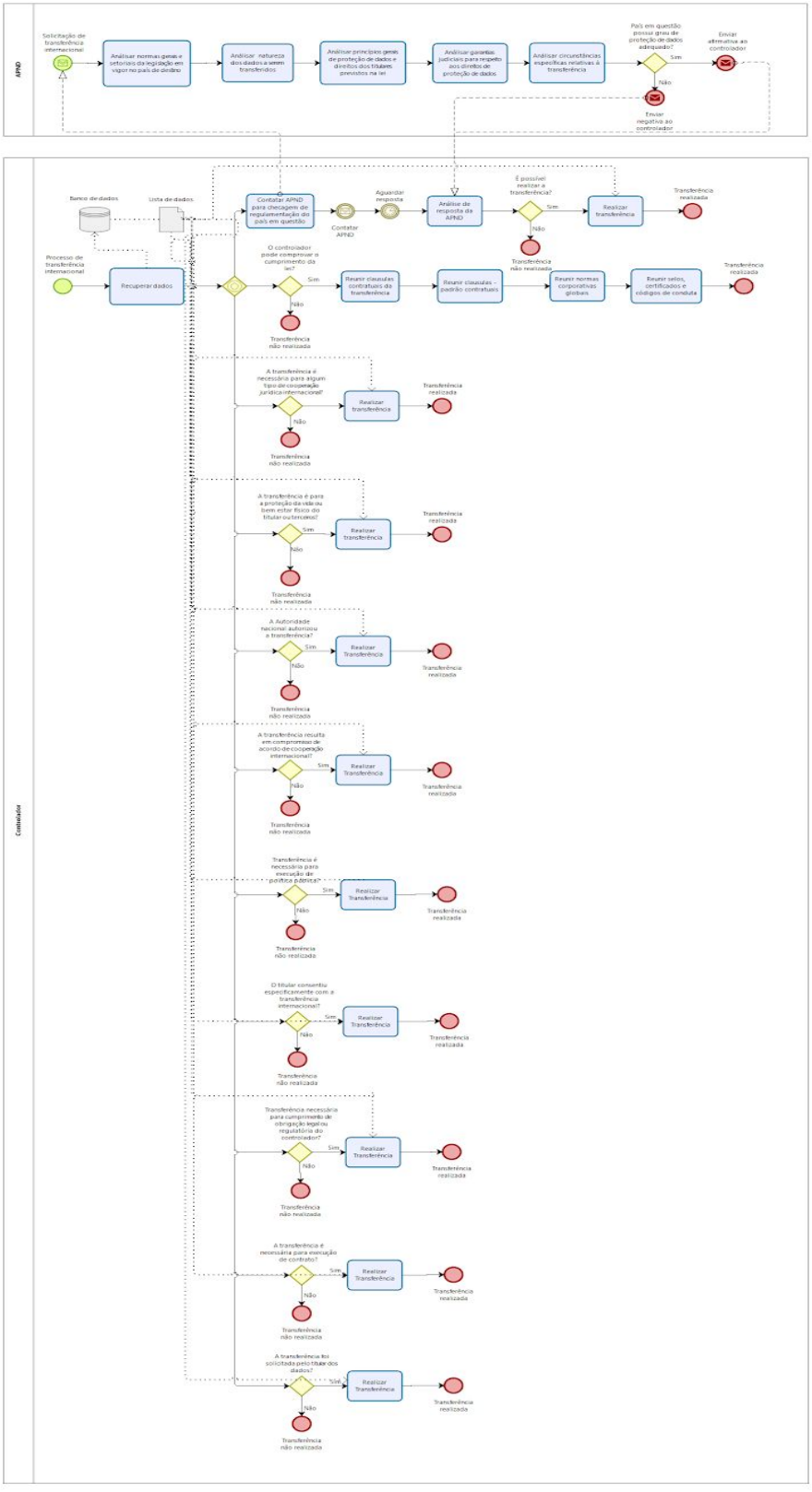
Nome do Padrão: Confirmação da existência de tratamento e direito de acesso

Propósito: Determinar o processo de acesso a dados quando solicitado pelo titular dos dados, partindo do pressuposto de que os dados já foram armazenados de forma organizada facilitando tipo de solicitação.
Usar quando: ● Titular dos dados solicitar acesso aos seus dados simplificados; ● Titular dos dados solicitar acesso aos seus dados completos; ● Titular dos dados solicitar informações sobre compartilhamento de dados com terceiros.
Exemplo: Titular solicita ao Controlador as informações armazenadas sobre ele.

Tabela 6. Padrão de Confirmação da existência de tratamento e direito de acesso.

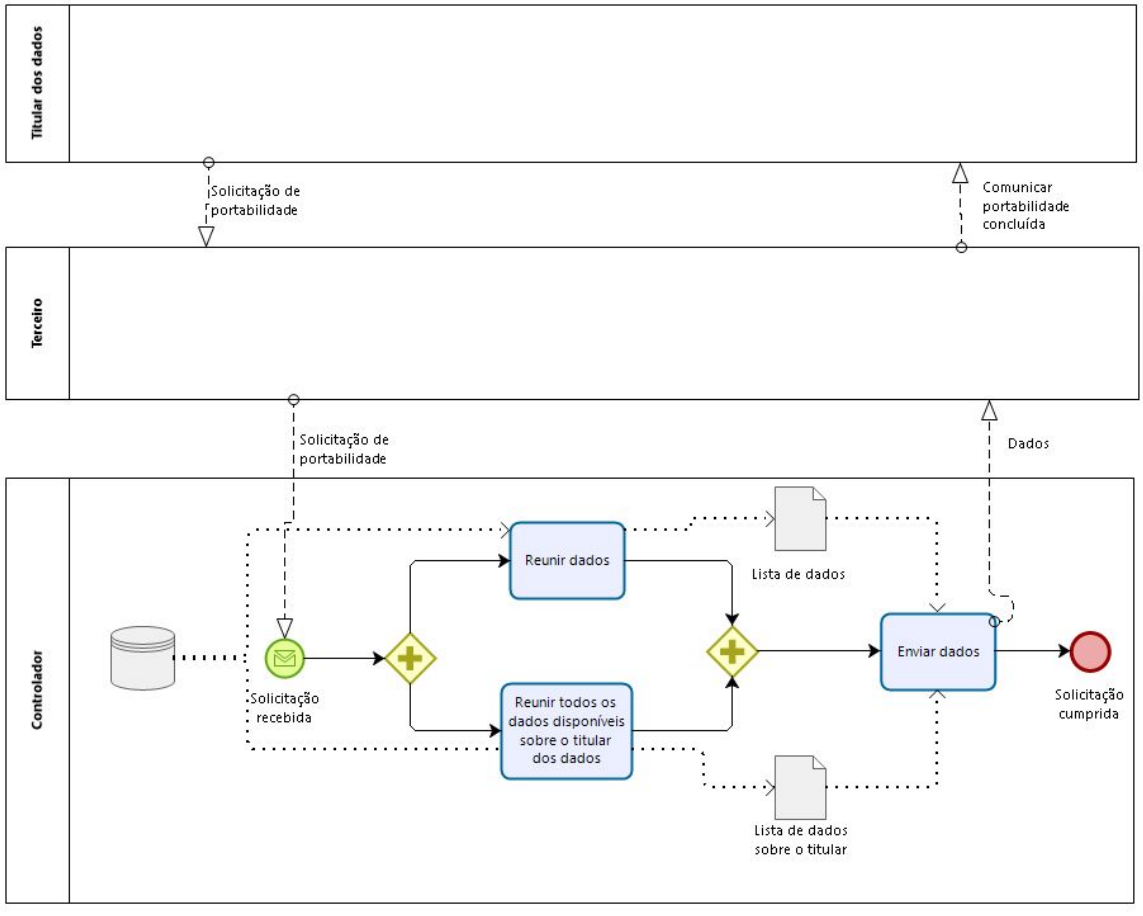
Nome do Padrão: Transferência internacional de dados



Propósito: Exibir o *modus operandi* do controlador em cada uma das situações específicas para transferência internacional de dados.
Quando usar: ● Titular solicita transferência de dados para outro país; ● Empresa solicita que dados sejam processados em outro país; ● Dados necessitam ser transferidos internacionalmente por questões jurídicas; ● Transferência tem finalidade de proteção da vida ou bem estar físico de titular ou terceiros; ● Transferência resulta em compromisso de acordo internacional; ● Transferência necessária para execução de políticas públicas; ● Transferência necessária para cumprimento de obrigação legal do controlador; ● Transferência necessária para execução de contrato.
Exemplo: O Controlador precisa transferir dados para empresa internacional devido à proteção da vida do titular que se encontra em outro país, como em casos de álibis ou ameaça à vida de terceiros relacionados ao titular.

Tabela 7. Padrão de Transferência Internacional de Dados.

Nome do Padrão: Portabilidade



Propósito: Registrar o processo de portabilidade de dados entre duas empresas
Usar quando: ● A portabilidade dos dados é solicitada ao operador de dados;
Exemplo: O titular dos dados deseja realizar a portabilidade de dados entre duas empresas. Sendo assim, o titular entra em contato com a empresa para qual seus dados devem ser portados e ela entra em contato com a empresa que mantém os atuais dados do titular. O ideal é que este padrão exista nas duas empresas.

Tabela 8. Padrão de Portabilidade.

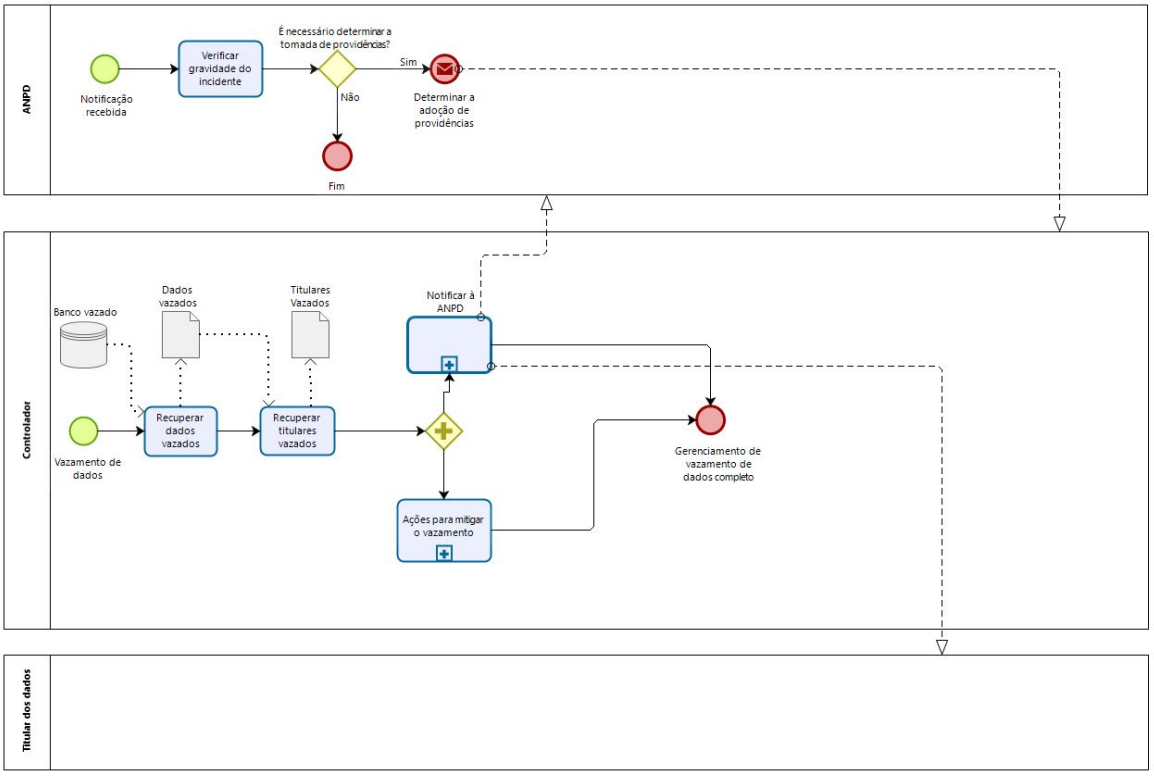
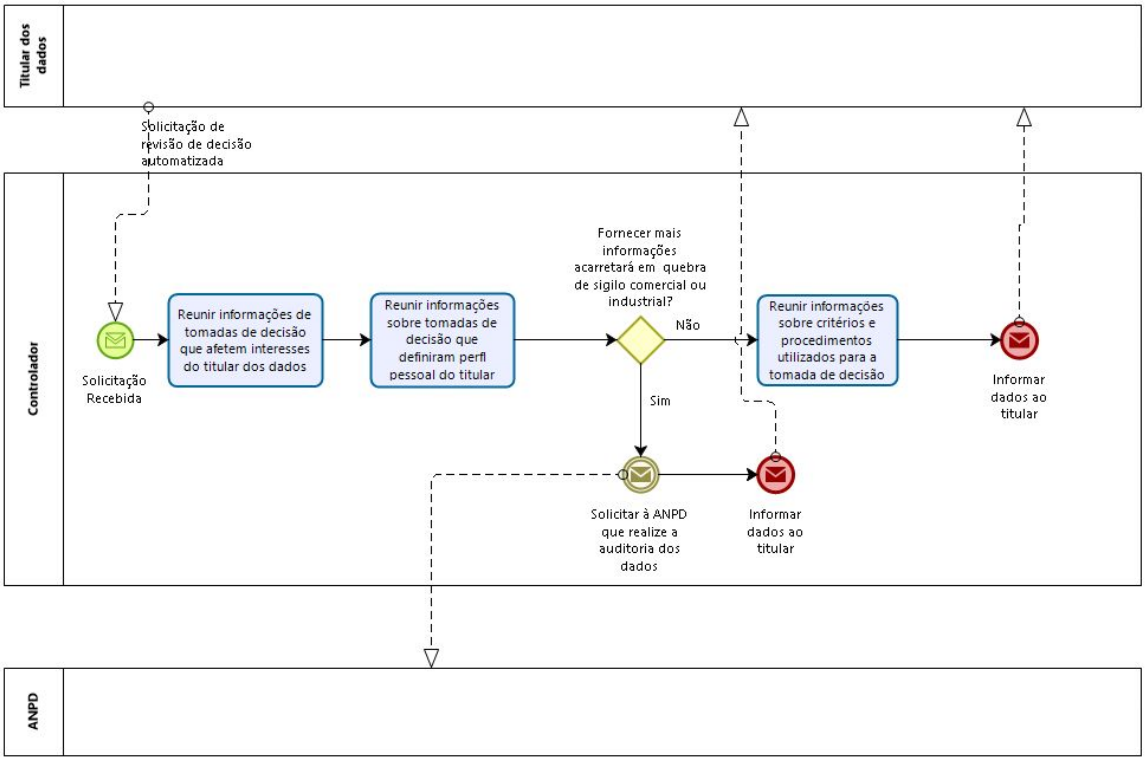
Nome do Padrão: Vazamento de dados

Propósito: Estabelecer o comportamento esperado em caso de vazamento de dados.
Usar quando: ● Ocorrer um vazamento de dados de qualquer tamanho; ● Ocorrer invasão de sistema; ● Ocorrer algum tipo de violação de privacidade de dados.
Exemplo: O controlador recebe uma notificação de vazamento de dados, seja por meio de um sistema previamente desenvolvido para indicar brechas e possíveis falhas de segurança ou por outra fonte de informação. A partir da notificação, é necessário desempenhar um conjunto de ações para minimizar este vazamento bem como informar à Autoridade Nacional e o titular dos dados sobre o vazamento.

Tabela 9. Padrão de Vazamento de Dados.

Nome do Padrão: Revisão de tomada de decisão automatizada



Propósito: Documentar o processo de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

Usar quando:

- Titular dos dados solicita que as decisões que utilizam seus dados e foram tomadas por um sistema automatizado sejam revisadas;
- Titular discordar de decisões que foram tomadas com base no perfil, seja pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade, que foi traçado através de seus dados.

Exemplo: O titular solicita que as decisões que foram tomadas, a partir de um perfil criado utilizando seus dados, sejam revisadas, independente dos motivos da solicitação.

Tabela 10. Padrão de Revisão de Tomada de Decisão Automatizada.

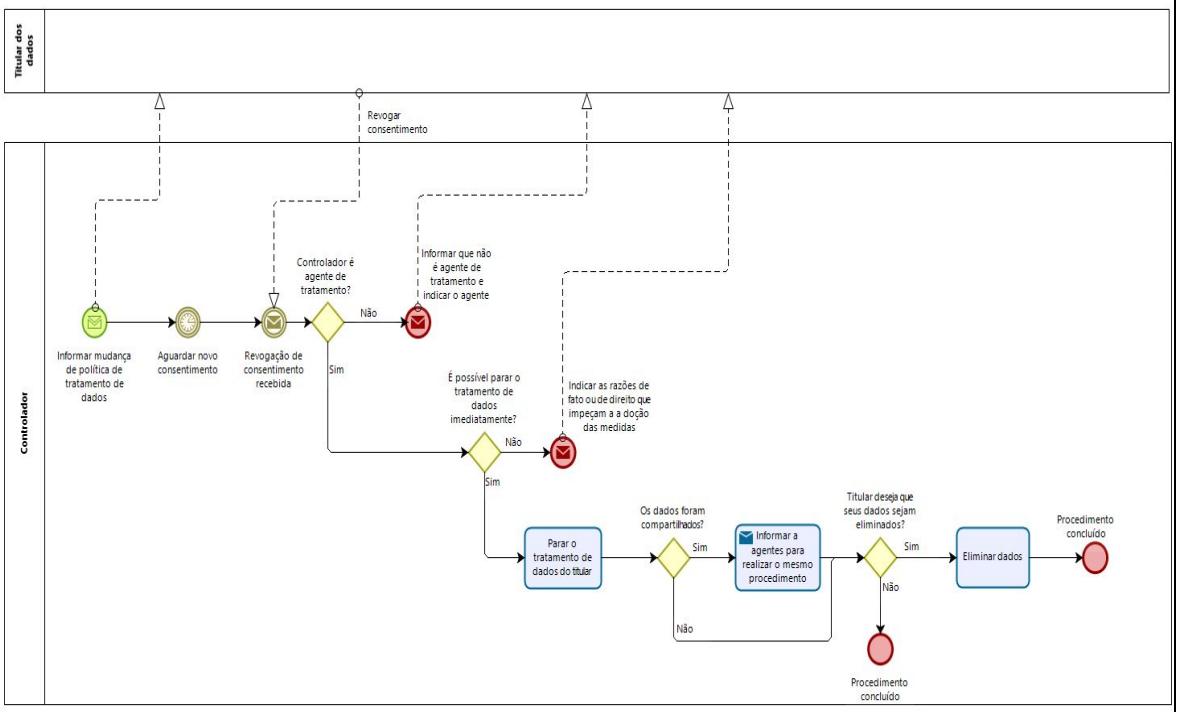
Nome do Padrão: Revogação de consentimento

Propósito: Definir os passos que devem ser seguidos pelo Controlador em caso de alteração na política de privacidade de processamento de dados.
Usar quando: ● Existir alguma modificação no contrato de privacidade; ● Titular dos dados revoga consentimento dado previamente.
Exemplo: Titular decide revogar consentimento prévio devido à alterações feitas no contrato de privacidade com as quais ele não concorda.

Tabela 11. Padrão de Revogação de Consentimento.

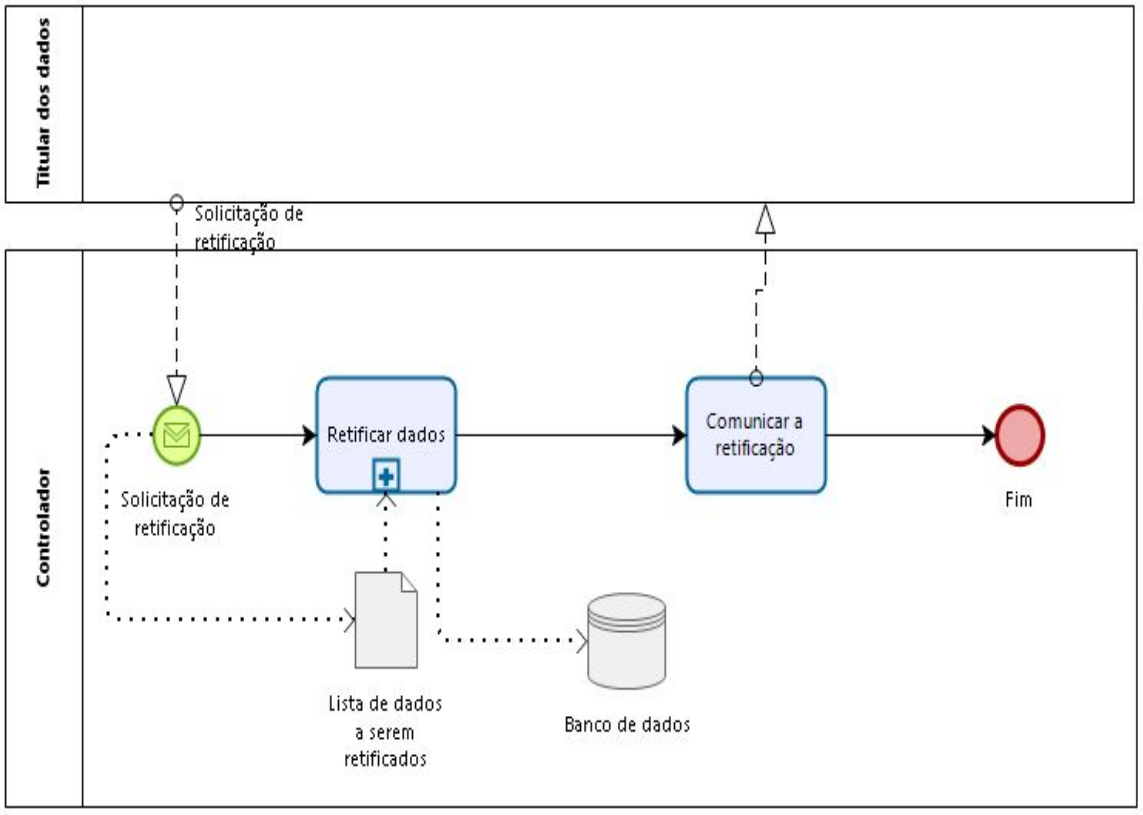
Nome do Padrão: Retificação de dados

Propósito: Exibir os passos que devem ser seguidos para que seja feita a retificação de dados.
Usar quando: ● Titular de dados deseja alterar seus dados cadastrais; ● Titular de dados deseja alterar dados com os quais não concorda.
Exemplo: Titular deseja fazer alterações de endereço em seus dados após fazer mudança.

Tabela 12. Padrão de Retificação de Dados.

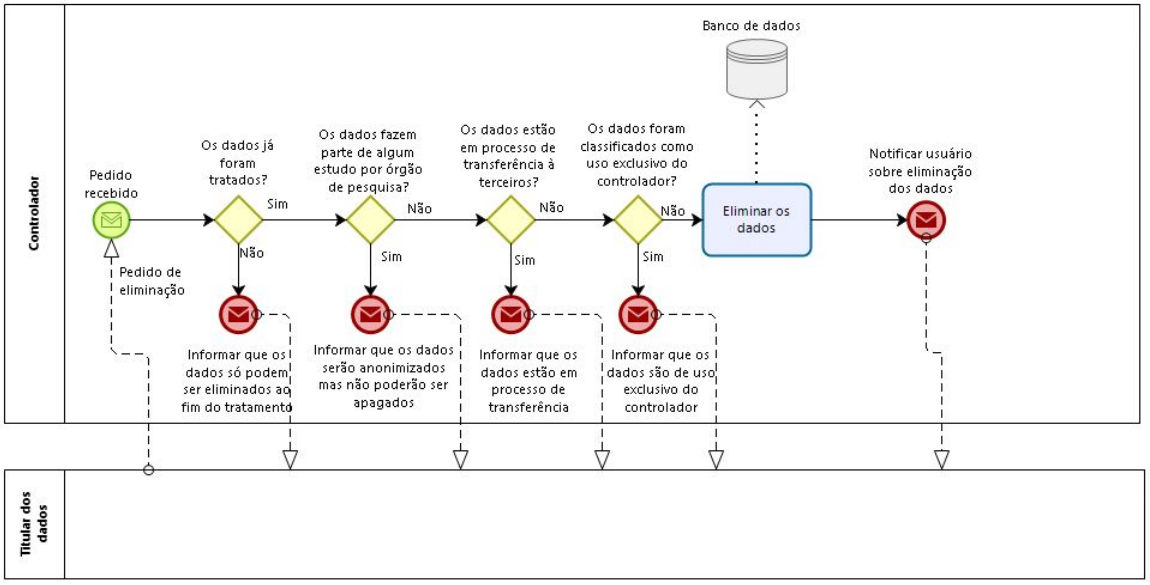
Nome do padrão: Direito de esquecimento ou eliminação de dados pessoais

Propósito: Definir os passos do processo de exclusão de dados.
Usar quando: ● Titular dos dados solicitar que seus dados sejam excluídos.
Exemplo: Titular dos dados não concorda com nova alteração no contrato de privacidade e revoga seu consentimento podendo solicitar também a exclusão de seus dados.

Tabela 13. Padrão de Eliminação de Dados ou Direito de Esquecimento.

4.3. Método de modelagem de processos de negócio em conformidade com a LGPD

Conforme discutido na Seção 4.2, para responder a Pergunta de Pesquisa P2 deste trabalho (*Como modelar um processo de negócio em conformidade com a LGPD?*) foi proposto um catálogo de padrões de modelagem (Seção 4.2) e um método de modelagem.

O método de modelagem é apresentado como um processo descrito em BPMN ilustrado na Figura 2. Ele consiste em 16 etapas nas quais os padrões de modelagem que foram apresentados (ver Seção 4.2) são representados como artefatos de entrada nas etapas relacionadas.

Este método orienta o analista para modelar um processo ou para corrigir algum modelo que foi avaliado como não compatível com a LGPD. Se o modelo já existe, o analista deve seguir o fluxo passando para a próxima etapa até encontrar

uma etapa que não esteja contemplada em seu modelo de forma que ao fim do processo, não hajam mais não-conformidades presentes no processo original. As ações do método, presentes na Figura 2, têm o seguinte intuito:

- **Mapear Dados (Passo 1)**: Antes de iniciar qualquer tipo de mudança é necessário que uma organização faça o mapeamento dos dados manipulados pelo processo de negócios, de forma que seja possível identificar como ocorre o fluxo de informação e processamento de dados atualmente na empresa. A ação de mapear dados tem o intuito de levantar informações sobre o fluxo de informações e como o processamento de dados ocorre atualmente no processo de negócio;
- **Ilustrar o termo de consentimento (Passo 2)**: Caso a resposta para a pergunta “O processo precisa de consentimento?” seja afirmativa, é necessário que o termo de consentimento seja exposto no processo para que seja possível ilustrar que o consentimento foi obtido pelo usuário. Esta ação recebe como entrada o padrão de modelagem do termo de consentimento que ilustra o processo de solicitação de consentimento e todas as suas cláusulas. Esta ação está intrinsecamente ligada às perguntas 1 a 4 do questionário (Seção 4.1).

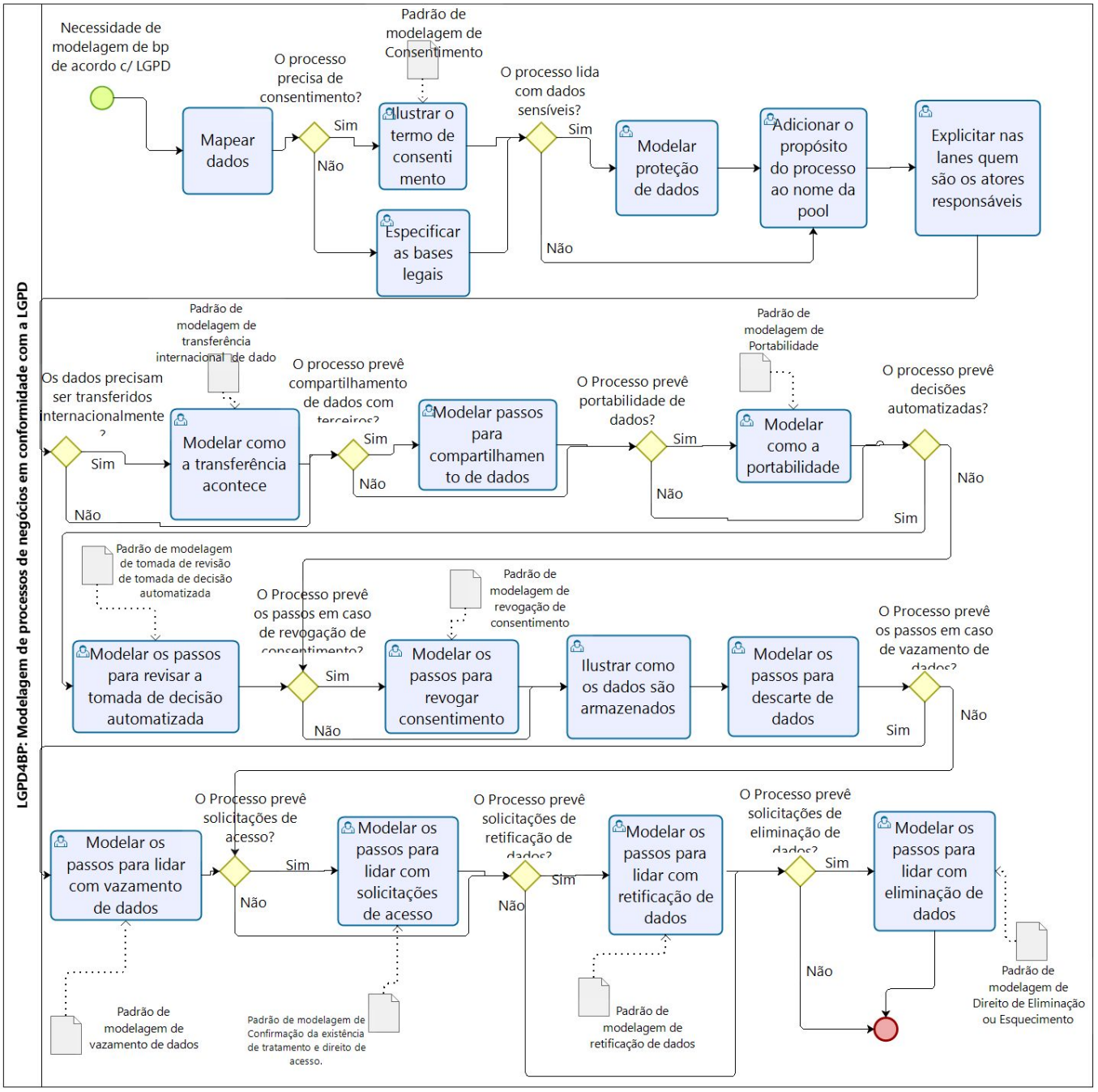


Figura 2. Etapas do método LGPD4BP para modelar um processo de negócio em conformidade com a LGPD.

- **Especificar as bases legais (alternativa do passo 2)**: No caso de a resposta para a pergunta “O processo precisa de consentimento?” ser negativa, significa dizer que o consentimento do usuário não é necessário, pois o controlador é capaz de especificar as bases legais pelas quais está processando os dados pessoais. As bases legais podem ser por exemplo, para cumprimento de obrigação legal ou regulatória por parte do controlador (BRASIL, 2020), ou para a realização de estudos por órgãos de pesquisa (BRASIL, 2020) ou até mesmo para a proteção da vida do titular ou terceiro

(BRASIL, 2020). O intuito desta ação é que fique explícito no processo o caso do Controlador de dados não precisar do consentimento do usuário. Esta ação está ligada à pergunta 2 do questionário.

- **Modelar a proteção de dados (Passo 3)**: A GDPR aconselha que dados sensíveis tenham um certo nível de segurança caso o processo esteja lidando com dados sensíveis, porém a Lei Brasileira não especifica o tipo de segurança deve ser utilizado. Porém, seguindo a linha do *Privacy-By-Design,* é aconselhável que a proteção de dados seja modelada de forma clara no processo de negócio, para que possa ser levada adiante. O método de modelagem não sugere nenhuma forma de segurança em específico, o que fica à critério do analista. Esta ação está ligada à pergunta 6 do questionário. É necessário lembrar que devem ser protegidos tanto dados armazenados eletronicamente quanto fisicamente.
- **Adicionar o propósito do processo ao nome da pool (Passo 4)**: Esta ação tem o intuito de facilitar o acesso aos dados no caso do titular dos dados solicitar acesso exercendo seu direito. No entanto, este não é seu único intuito, ao adicionar o propósito do processo ao nome da pool, é possível garantir que os dados de um cliente serão processados apenas para finalidade em que ele consentiu. Esta ação não possui padrão de modelagem atrelado à si pois é simples, pode ser feita utilizando os elementos da notação BPMN.
- **Explicitar nas lanes quem são os atores responsáveis (Passo 5)**: Ao explicitar os atores responsáveis pelo processamento de dados naquele momento torna-se possível identificar quem foi o responsável no caso de uma má conduta, uso indevido de dados ou danos patrimoniais. Os atores serão isentos de culpa quando provarem que o tratamento de dados não lhes foi atribuído (BRASIL, 2020). Assim, torna-se possível também utilizar esta ação para o caso de inocentar atores por sua conduta. Esta ação está diretamente ligada à pergunta 7 do questionário.
- **Modelar como a transferência acontece (Passo 6)**: A ação descrita deve ser modelada apenas caso a pergunta “Os dados precisam ser transferidos internacionalmente?” tenha uma resposta afirmativa. Nesse caso, as ações para realizar uma transferência internacional de dados devem ser modeladas. Como existem algumas restrições na LGPD para a transferência internacional de dados, o padrão de modelagem de transferência internacional de dados é recebido como entrada pela ação descrita no modelo, o que garante que as ações seguirão as restrições impostas pela lei. Esta ação está ligada à pergunta 10 do questionário.
- **Modelar passos para o compartilhamento de dados (Passo 7)**: No caso de existir o compartilhamento de dados entre terceiros, a ação de modelar os passos para que o compartilhamento ocorra deve ser utilizada, pois, é necessário que esteja explícito no termo de consentimento que os dados

precisarão ser compartilhados com terceiros e qual a finalidade deste compartilhamento. Sabendo como e o porquê do compartilhamento de dados com terceiros, deve-se modelar como este compartilhamento ocorre no processo de negócios. Esta ação está ligada à pergunta 5 do questionário.

- **Modelar como a portabilidade ocorre (Passo 8):** Se o processo prevê a portabilidade de dados, é necessário que seja explicitado no processo de negócio como esta portabilidade deve ocorrer. Para isto, as ações para a portabilidade devem ser modeladas. Esta ação recebe como entrada o padrão de modelagem de portabilidade e está diretamente ligada à pergunta 12.
- **Modelar os passos para revisar a tomada de decisão automatizada (Passo 9)**: Na hipótese de o processo utilizar de tomada de decisão automatizada baseada no perfil montado para um usuário, é necessário modelar as ações que executam esse processo. O titular tem o direito de solicitar a revisão da tomada de decisão automatizada baseada em seu perfil (BRASIL, 2020), portanto, para que esteja pronto para responder à solicitação, aconselha-se que estes passos já estejam modelados. Esta ação recebe o padrão de modelagem de revisão de tomada de decisão automatizada como entrada e está ligada à pergunta 14 do questionário.
- **Modelar os passos para revogar consentimento (Passo 10)**: O consentimento pode ser revogado a qualquer momento se o titular dos dados assim desejar (BRASIL, 2020). Portanto, os processos de negócio devem levar em consideração as ações que devem ser tomadas no caso do titular realizar esta solicitação. É possível fazê-lo em conformidade com a Lei, através do padrão de modelagem de revogação de consentimento, que é recebido como entrada da ação. Esta ação está ligada à pergunta 15 do questionário.
- **Ilustrar como os dados são armazenados (Passo 11)**: A qualquer momento, o titular dos dados pode solicitar a confirmação da existência de tratamento de dados (BRASIL, 2020). Ao ilustrar onde e como os dados são armazenados torna mais fácil o atendimento desta solicitação. Se estiver presente no processo de negócios, certamente será implementado ao projeto. Esta ação é implementada direto no processo de negócios e está ligada à pergunta 9 do questionário.
- **Modelar os passos para descarte de dados (Passo 12)**: Após o processamento dos dados, o Controlador tem o dever de descartá-los de forma segura e modelar os passos de descarte de dados proporciona uma direção de como e onde o controlador deve descartar os dados utilizados. Existem algumas ressalvas quanto ao descarte de dados como, por exemplo, no caso de os dados serem utilizados por órgãos de pesquisa (BRASIL, 2020), fora estas ressalvas, os dados devem ser descartados. Esta ação é

implementada direto no processo de negócios e está ligada à pergunta 11 do questionário.

- **Modelar os passos para lidar com vazamento de dados (Passo 13)**: Os agentes de tratamento devem adotar certas medidas de segurança para que possam processar os dados (BRASIL, 2020), sendo assim, em caso de um vazamento de dados, o Controlador deve avisar à autoridade nacional de proteção de dados (ANPD) e tomar as medidas cabíveis para lidar com o vazamento. A lei não especifica as ações que devem ser tomadas, por isso, fica à cargo do analista modelar estas ações em acordo com a organização, recebendo o padrão de modelagem de vazamento de dados. Esta ação está ligada diretamente à pergunta 13 do questionário.
- **Modelar os passos para lidar com solicitações de acesso (Passo 14)**: No caso de o processo prever solicitações de acesso, é necessário que as ações para lidar com estas requisições sejam modeladas, o titular tem direito de solicitar várias informações sobre seu tratamento de dados, que já foram facilitadas em outras ações como, por exemplo, as ações de armazenamento de dados, finalidade de processo no nome da *pool*, agentes de tratamentos, etc. O processo recebe como entrada o padrão de modelagem de solicitação de acesso e confirmação de tratamento de dados, e está ligada à pergunta 18 do questionário.
- **Modelar os passos para lidar com retificação de dados (Passo 15)**: O titular dos dados tem o direito de solicitar a qualquer momento a correção de dados errôneos ou que foram alterados (BRASIL, 2020) como, por exemplo, seu endereço, portanto, o processo deve modelar as ações que são tomadas quando um usuário solicita a retificação de seus dados, apontando o passo a passo na prática como ocorre essa retificação. O processo recebe como entrada o padrão de modelagem de retificação de dados e está ligado à pergunta 16 do questionário.
- **Modelar os passos para lidar com eliminação de dados (Passo 16)**: Existem algumas condições que devem ser cumpridas quando o titular dos dados solicita a eliminação dos dados, o intuito desta ação é modelar o passo a passo de como ocorre dentro da organização a eliminação destes dados. Diferente do descarte de dados, que ocorre ao final do processamento, a eliminação encerra o processo de dados imediatamente (caso seja possível). A ação recebe como entrada o padrão de modelagem de direito de eliminação ou esquecimento e está ligada à pergunta 17 do questionário.

A próxima seção demonstra na prática como o questionário, os padrões de modelagem e o método podem ser aplicados em um processo de negócio.

5. Exemplo de Aplicação do método LGPD4BP em um estudo de caso

5.1. Estudo de Caso: Colégio de Aplicação

O Colégio de Aplicação (CAp)[1] da Universidade Federal de Pernambuco (UFPE) foi fundado em março de 1958 para funcionar junto à Faculdade de Filosofia como um laboratório experimental, atendendo aos acadêmicos das diversas licenciaturas (UFPE, 2020).

Seu campo de atuação inclui a elaboração de novas técnicas pedagógicas e educacionais. Apresenta no seu projeto político-pedagógico os seguintes objetivos (UFPE, 2020):

- Promover a formação integral dos alunos do Ensino Fundamental e Médio;
- Servir de campo de experimentação na área do Ensino Fundamental e Médio;
- Servir de campo de estágio para as diversas licenciaturas da UFPE e de outras instituições;
- Ser um espaço privilegiado para formação continuada de professor da educação básica, realizada pela universidade, articulada com a participação institucional nos programas de apoio à formação de docentes .

O CAp desenvolve Regularmente (UFPE, 2020):

- Atividades de ensino do 6º ao 9º ano do Ensino Fundamental com um total de 8 turmas e da 1º a 3º série do Ensino Médio com um total de 6 turmas;
- Atendimento aos licenciandos da UFPE e de outras instituições no estágio de observação e regência de classe;
- Projetos de pesquisa relativos ao Ensino Fundamental e Médio;
- Atividades de extensão: programas, projetos, cursos, consultorias.

O colégio está desenvolvendo um Plano de Implantação do módulo de ensino fundamental e médio do SIGAA[2] para a matrícula de alunos do CAp UFPE. O SIGAA tem como objetivo cerne a integração, em uma única solução, em um único sistema, todos os processos e atividades acadêmicos da Universidade. Os módulos que foram focados para o estudo (Ensino Fundamental e Médio) são responsáveis por gerenciar todas as várias atividades administrativas de um colégio, como os contextos de matrícula, acompanhamento de notas, registros de planos de aula e outros.

O projeto surgiu com a exposição da necessidade que o Colégio de Aplicação da UFPE possui em gerenciar, do modo ágil, seus processos administrativos internos; bem como a preocupação levantada de gastos excessivos de recursos que provavelmente com outra solução de processo, seriam evitados. A ideia é que a implantação dos módulos já mencionados auxilie a atual e a futura equipe de servidores administrativos, professores, alunos e

[1] www.ufpe.br/cap/

[2] https://sigaa.ufpe.br/sigaa/public/home.jsf

responsáveis a ter acesso e,ou ter acesso de modo facilitado à informações necessárias e que o desenvolvimento do plano dessa implantação se torne um guia eficiente para essa ação ocorrer.

Os Objetivos Organizacionais do projeto são:

- Otimizar e melhorar os processos administrativos e gerenciais das matrículas dos alunos do Colégio de Aplicação da UFPE;
- Integrar os processos da biblioteca com a escolaridade do Colégio de Aplicação da UFPE dentro do SIGAA;
- Criar acesso online aos pais e responsáveis de alunos para que possam realizar a matrícula de seus filhos remotamente, sem a necessidade de ir para instituição para tal.

O processo do Módulo de Ensino Fundamental e Médio do SIGAA no Colégio de Aplicação da UFPE representado em BPMN é apresentado na Figura 3.

Para realizar a inscrição e participar do processo seletivo, é necessário informar no sistema (UNIVERSIDADE FEDERAL DE PERNAMBUCO, 2007):

- Nome do Candidato: com até 40 caracteres.
- Data de Nascimento: dia, mês e ano do nascimento do candidato.
- Número da carteira de identidade do candidato, órgão expedidor e sigla do Estado que a expediu.
- Nome da Mãe: com até 40 caracteres.
- Nome do Pai: com até 40 caracteres.
- Sexo: Selecione “Masculino” ou“ Feminino”.
- Telefone (residencial): código de área e o número do telefone.
- Telefone (celular): código de área e o número do telefone.
- CEP: ao digitar o CEP os campos Endereço, Bairro, Cidade e UF são preenchidos automaticamente.
- Número: Informar o número da residência.
- Complemento: Complementar, nesse campo, os dados do endereço (ex: Casa, Apto, Bloco, etc.).
- Nome do Responsável Legal pela Inscrição: com até 40 caracteres.
- CPF do Responsável Legal pela Inscrição: números sem utilizar ponto (.) e traço (-).
- Solicitação de isenção do pagamento da taxa de inscrição: O interessado deverá assinalar a quadrícula “Sim” deste campo e observar os critérios estabelecidos no item 6 deste Edital.
- Telefone de Contato com o Responsável Legal: código de área e o número do telefone.
- E-mail do Responsável Legal pela Inscrição.

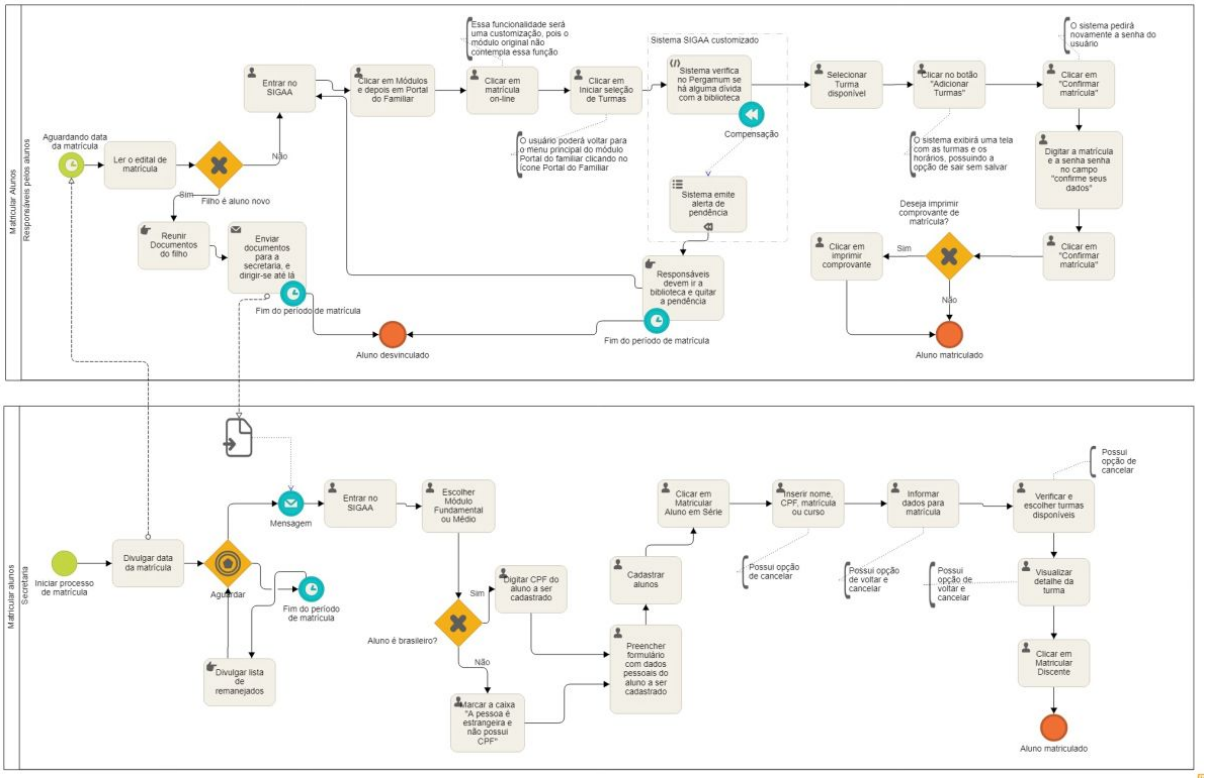


Figura 3. Processo do módulo de ensino fundamental e médio do SIGAA.
Fonte: https://drive.google.com/file/d/1khf1tTysUjnuCxRoJYUsimy2laeWc2DT/view

- Opção pelo sistema de reserva de vagas destinadas exclusivamente a alunos oriundos de Escolas Públicas.
    - o A comprovação se dará através de Histórico Escolar ou declaração da(s) escola(s) de origem de que tenha cursado do 1oao 5oano exclusivamente em escola pública, acompanhado do original da certidão de nascimento ou carteira de identidade do candidato e da declaração do responsável legal de que o candidato não cursou todo ou parte do Ensino Fundamental I em escola privada
- Questionário Socioeconômico: Nesse questionário, o Responsável Legal pelo candidato encontrará perguntas relativas tanto à trajetória educacional do candidato quanto à situação familiar.

Mais informações sobre o processo de seleção podem ser encontradas na página do CAp[3].

Caso o candidato seja aprovado no processo seletivo, no ato da matrícula, deverão ser entregues (UNIVERSIDADE FEDERAL DE PERNAMBUCO, 2007):

- Documento original da transferência definitiva ou transferência provisória;
- Cópia da Carteira de Identidade e do CPF do candidato;

[3] https://www.ufpe.br/documents/38970/2338189/EDITAL_CAp-Proacad-07-2019.pdf/bbd715d7-4716-4a0b-848b-d2710caa0d05

- Duas (2) fotos 3x4 recentes e iguais.

O processo prevê uma divulgação da lista de remanejados caso o total de vagas não seja preenchido. Um exemplo está disponível na página do CAp[4].

5.2. Aplicação do questionário de avaliação

Após o levantamento de dados na Seção 5.1, é possível aplicar o questionário de avaliação no processo atual do Colégio de aplicação e mapear os pontos de não-conformidade do processo e assim corrigí-los. Na Tabela 14 é apresentada as respostas para cada pergunta do questionário de avaliação de conformidade do processo de negócio (Seção 4.1) do método LGPD4BP para o processo do módulo de ensino fundamental e médio do SIGAA do CAp.

Avaliação BPMN - Colégio de Aplicação (CAp/UFPE)
1) O processo inclui as ações para obter consentimento? ( ) Sim. (**X**) Não. ( ) Não se aplica, o controlador de dados possui base legal para processamento. ( ) Não se aplica, a exigência de consentimento é dispensada porque os dados foram tornados públicos pelo titular dos dados.
2) O processo especifica as bases legais de processamento? ( ) Sim. (**X**) Não. ( ) Não se aplica, o controlador possui consentimento do usuário.
3) O processo inclui as ações para lidar com dados pessoais de crianças? (**X**) Não. ( ) Sim, e foram modeladas com o consentimento dado por pelo menos um dos pais ou guardião legal ( ) Sim, mas não foram modeladas. ( ) Não se aplica.
4) O processo contém informações sobre a possibilidade de não prover consentimento e as consequências da recusa? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Não se aplica.
5) O processo contém as ações para compartilhamento de dados com terceiros? ( ) Não. ( ) Sim, e as ações foram modeladas. (**X**) Sim, e as ações não foram modeladas. ( ) Não se aplica, o processo não compartilha dados com terceiros.
6) O processo inclui as ações para lidar com dados sensíveis? (**X**) Não. ( ) Sim, e as ações foram modeladas.Sim, e as ações não foram modeladas. ( ) Não se aplica.
7) O processo indica quem é o ator (Departamento/Posição) responsável pelo processamento de dados em cada atividade? ( ) Não. (**X**) Sim, e foi modelado nas lanes do processo.
8) O processo apresenta a finalidade de processamento dos dados no nome do modelo? ( ) Não. (**X**) Sim.
9) O processo apresenta o local em que os dados são armazenados e processados? (**X**) Não. ( ) Sim.

[4] https://selecaocap.com.br/6ano2020/anexo/noticias/140220_SEXTO_REMANEJAMENTO.pdf

10) O processo inclui as ações para realizar uma transferência internacional de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. (**X**) Não se aplica.
11) O processo inclui as ações para descarte de dados? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.
12) O processo inclui as ações para realizar portabilidade de dados? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. (**X**) Não se aplica.
13) O processo inclui as ações para lidar com um vazamento de dados? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.
14) O processo inclui as ações para realizar decisões automatizadas? ( ) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. (**X**) Não se aplica.
15) O processo inclui as ações para o caso de haver revogação de consentimento? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.
16) O processo inclui as ações a serem tomadas o caso de haver uma retificação de dados? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.
17) O processo inclui as ações a serem tomadas no caso de um apagamento de dados? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.
18) O processo inclui as ações a serem tomadas no caso de uma solicitação de acesso de dados por parte do usuário? (**X**) Não. ( ) Sim, e as ações foram modeladas. ( ) Sim, mas as ações não foram modeladas. ( ) Não se aplica.

Tabela 14. Questionário de avaliação aplicado no processo do Colégio de Aplicação.

Após a aplicação do questionário, ficam evidentes os pontos em não-conformidade, sendo eles as questões: 1 a 6, 9, 11, 13 e 15 a 18. O processo contém também pontos em que as perguntas não se aplicavam, sendo elas:10, 12 e 14. Apenas as perguntas 7 e 8 já estavam atendidas no processo. Na seção a seguir serão aplicadas as correções no modelo BPMN do processo.

5.3. Aplicação do método de modelagem

Com o levantamento dos pontos de não-conformidade no processo, agora é possível saber exatamente que alterações devem ser feitas para que o processo atinja a conformidade com a LGPD.

Esta seção apresenta a nova versão do processo (Figura 4) e destaca os pontos de alterações na cor laranja, para que seja possível compreender as mudanças. Para refinar o modelo e torná-lo em conformidade com a LGPD, foram

usados os padrões de Consentimento, Vazamento de Dados, Revogação de Consentimento, Retificação, Apagamento e Acesso de dados, adicionadas 15 novas ações que refletiam os padrões de modelagem.

O primeiro passo consistiu na realização do mapeamento dos dados manipulados pelo processo de negócio. A Tabela 15 apresenta esse mapeamento.

Função de Negócio	Propósito do processo	Categoria dos Indivíduos	Categoria dos dados pessoais	Dados de menores de idade	Existência de decisão automatizada	Localização dos dados pessoais
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Nativo	Documento original da transferência definitiva ou provisória	Sim	Não	Arquivo da Secretaria
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Nativo	Cópia da Carteira de Identidade	Sim	Não	Arquivo da Secretaria
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Nativo	Cópia CPF do candidato	Sim	Não	Arquivo da Secretaria
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Estrangeiro	Documento original da transferência definitiva ou provisória	Sim	Não	Arquivo da Secretaria
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Estrangeiro	Cópia da documento de Identidade	Sim	Não	Arquivo da Secretaria
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Nativo e Estrangeiro	Dados cadastrais pessoais	Sim	Não	Sistema SIGAA
Secretaria	Realizar Matrícula de Aluno Novo	Aluno Novato Nativo e Estrangeiro	Dados escolar (turma e disciplinas)	Sim	Não	Sistema SIGAA
Responsável Legal pelo Aluno	Realizar Matrícula de Aluno Veterano	Alunos Veterano Nativo e Estrangeiro	Dados escolar (turma e disciplinas)	Sim	Não	Sistema SIGAA

Tabela 15. Mapeamento de dados manipulados pelo processo.

Na Figura 4 estão destacados os pontos de melhoria no processo. Com o preenchimento do questionário foi possível notar que o processo não continha as ações necessárias para obter o consentimento do titular dos dados para

processamento de dados e nem as bases legais de processamento, bem como ações para lidar com dados pessoais de crianças, possibilidade de não prover consentimento e as consequências da recusa, ações para lidar com dados sensíveis, não apresentava o local em que os dados são armazenados e processados, não continha as ações para descarte de dados e nem ações para lidar com um vazamento de dados, nem estava preparado para lidar com solicitações de acesso, retificação ou apagamento de dados. A figura também pode ser encontrada no site do método para melhor visualização: https://sites.google.com/view/lgpd4bp.

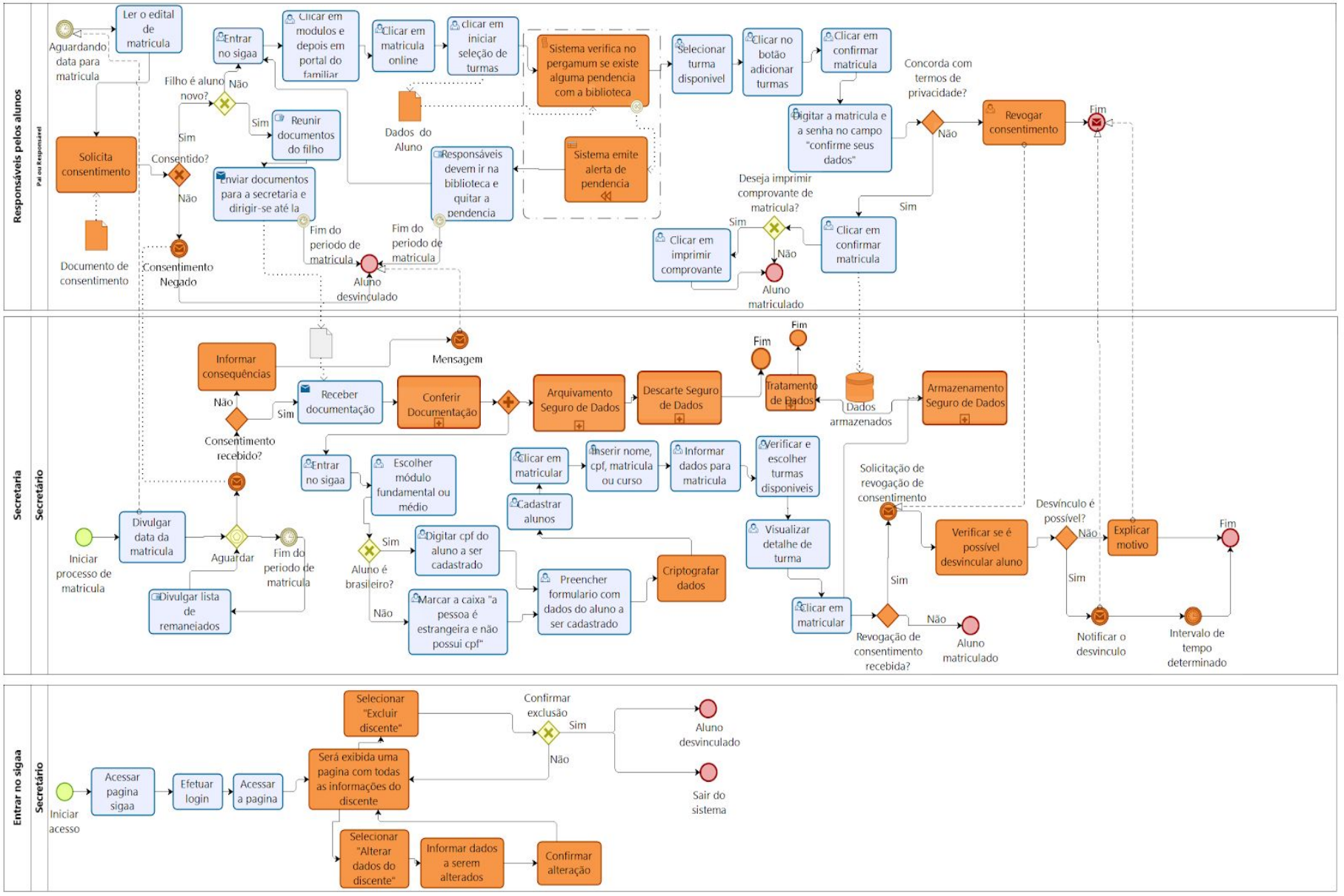

Responsáveis pelos alunos
Pai ou Responsável
Aguardando data para matricula
Ler o edital de matricula
Entrar no sigaa
Clicar em modulos e depois em portal do familiar
Clicar em matricula online
clicar em iniciar seleção de turmas
Sistema verifica no pergamum se existe alguma pendencia com a biblioteca
Selecionar turma disponivel
Clicar no botão adicionar turmas
Clicar em confirmar matricula
Concorda com termos de privacidade?
Revogar consentimento
Fim
Digitar a matricula e a senha no campo "confirme seus dados"
Não
Sim
Filho é aluno novo?
Não
Sim
Reunir documentos do filho
Solicita consentimento
Consentido?
Não
Sim
Enviar documentos para a secretaria e dirigir-se até la
Dados do Aluno
Responsáveis devem ir na biblioteca e quitar a pendencia
Sistema emite alerta de pendencia
Deseja imprimir comprovante de matricula?
Sim
Não
Clicar em imprimir comprovante
Clicar em confirmar matricula
Documento de consentimento
Consentimento Negado
Fim do periodo de matricula
Aluno desvinculado
Fim do periodo de matricula
Aluno matriculado
Secretaria
Secretário
Informar consequências
Mensagem
Fim
Fim
Não
Sim
Receber documentação
Conferir Documentação
Arquivamento Seguro de Dados
Descarte Seguro de Dados
Tratamento de Dados
Dados armazenados
Armazenamento Seguro de Dados
Consentimento recebido?
Entrar no sigaa
Escolher módulo fundamental ou médio
Clicar em matricular
Inserir nome, cpf, matricula ou curso
Informar dados para matricula
Verificar e escolher turmas disponiveis
Solicitação de revogação de consentimento
Desvínculo é possível?
Não
Sim
Explicar motivo
Fim
Cadastrar alunos
Visualizar detalhe de turma
Verificar se é possivel desvincular aluno
Iniciar processo de matricula
Divulgar data da matricula
Aguardar
Fim do periodo de matricula
Sim
Digitar cpf do aluno a ser cadastrado
Aluno é brasileiro?
Não
Marcar a caixa "a pessoa é estrangeira e não possui cpf"
Preencher formulario com dados do aluno a ser cadastrado
Criptografar dados
Clicar em matricular
Sim
Não
Revogação de consentimento recebida?
Aluno matriculado
Notificar o desvinculo
Intervalo de tempo determinado
Divulgar lista de remaneiados
Entrar no sigaa
Secretário
Selecionar "Excluir discente"
Confirmar exclusão
Sim
Não
Aluno desvinculado
Sair do sistema
Iniciar acesso
Acessar pagina sigaa
Efetuar login
Acessar a pagina
Será exibida uma pagina com todas as informações do discente
Selecionar "Alterar dados do discente"
Informar dados a serem alterados
Confirmar alteração

Figura 4. Processo do módulo de ensino fundamental e médio do SIGAA alterado pelo LGPD4BP.

Para responder a pergunta de número 1 (O processo inclui as ações para obter consentimento?) foram adicionadas as ações da Figura 5.

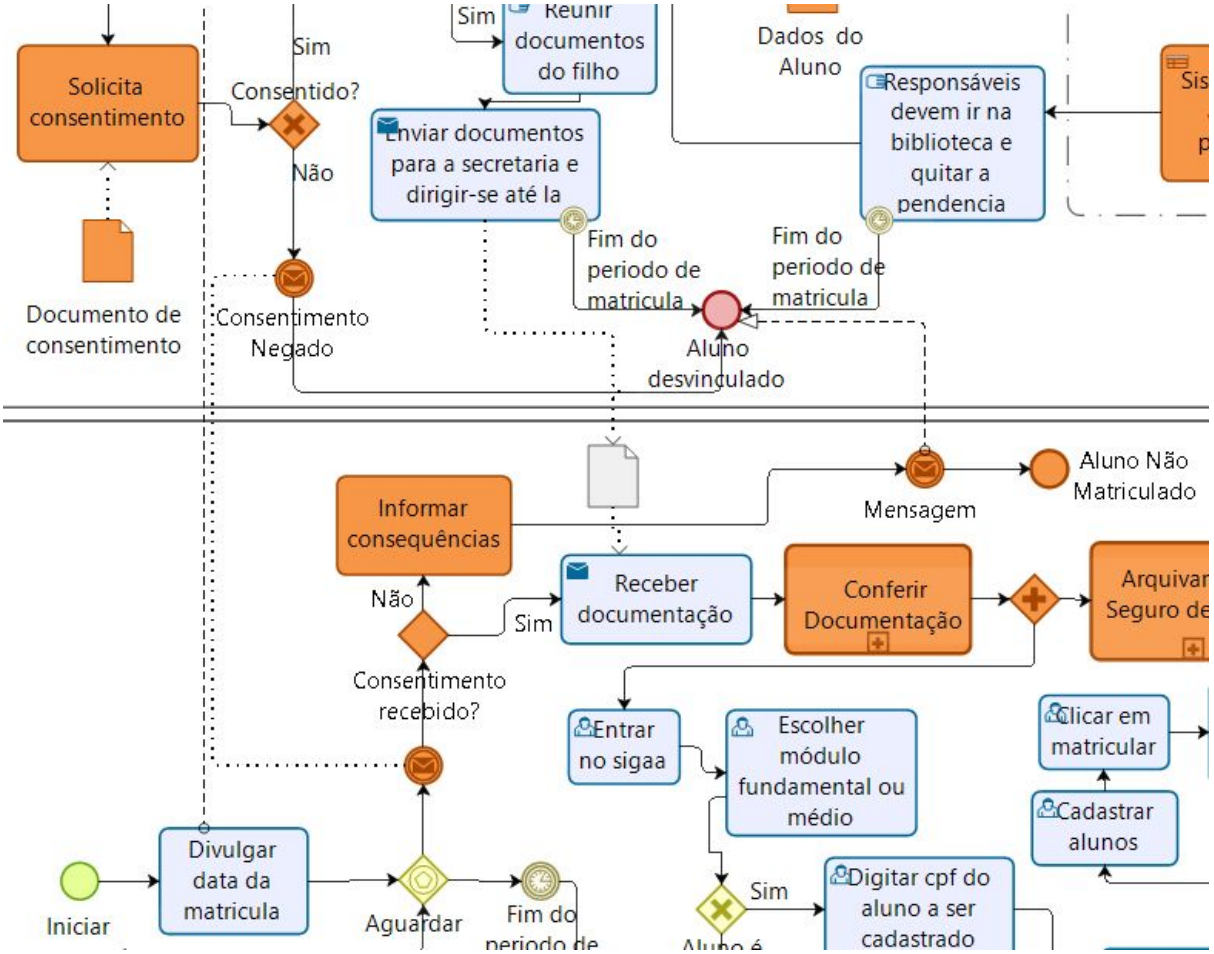


Figura 5. Ações para obter consentimento.

Foi utilizado o padrão de modelagem de consentimento e feitas as alterações acima, assim sendo, o processo consegue atender às exigências da pergunta 1, e dispensa a pergunta 2 (O processo especifica as bases legais de processamento?) pois, quando se tem o consentimento do titular dos dados, não é necessário que as bases legais sejam especificadas. Este trecho do processo também ajuda a responder a pergunta 3 (O processo inclui as ações para lidar com dados pessoais de crianças?) pois, segundo o padrão de modelagem de consentimento, existe uma cláusula específica de tratamento de dados de crianças que deve ser incluída ao termo de consentimento. Essa alteração também contempla a pergunta 4 (O processo contém informações sobre a possibilidade de não prover consentimento e

as consequências da recusa?) uma vez que essas informações estarão presentes no termo de consentimento.

Caso a resposta para a pergunta “Consentido?” seja negativa, irá ser enviada uma mensagem até à secretaria que possui outro gateway com a pergunta “Consentimento recebido?” que seguirá pelo caminho “Não” e informará as consequências da negativa ao responsável pelo aluno, encerrando o processo.

O Compartilhamento de dados com terceiros, como aborda a pergunta 5, já existia no processo, porém não era especificado como este compartilhamento acontecia. Sendo assim, na nova modelagem o compartilhamento de dados só ocorre caso o responsável pelo aluno tenha concordado com o termo de consentimento e os dados do aluno são utilizados para que o Pergamum (sistema terceiro) consiga investigar se existem pendências com a biblioteca ou não. É possível ver o fluxo da informação na Figura 6.

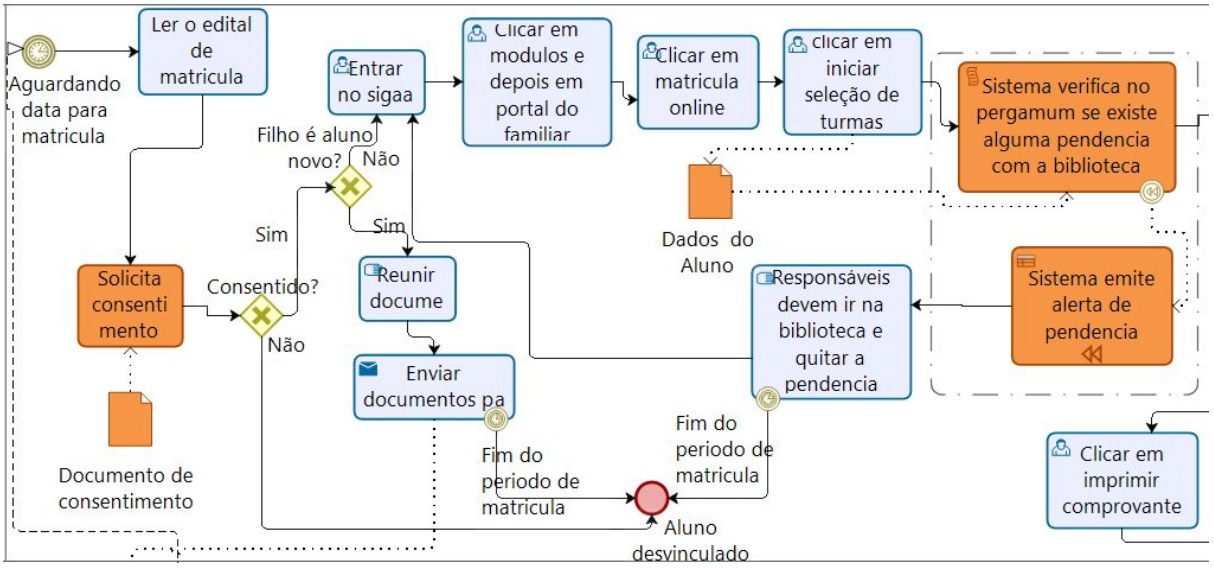


Figura 6. Ações para compartilhar dados com terceiros.

Para o próximo ponto de não-conformidade, a pergunta 6 (O processo inclui as ações para lidar com dados sensíveis?) não foi criado um padrão de modelagem pois, a própria LGPD não especifica que tipo de ações devem ser tomadas, como especificado na Tabela 3, fica à critério do analista como os dados vão ser protegidos. Tendo isso em vista, foi adicionado ao processo uma ação de criptografia de dados, que faz com o que os dados sensíveis sejam protegidos após o uso imediato. O tratamento de dados sensíveis não ocorre somente com os dados digitais, refere-se também aos documentos físicos que são recebidos pela secretaria: Os dados são arquivados e descartados de forma segura, de forma que não seja possível identificar um aluno que participou do processo de matrícula. Os dados que são armazenados no banco de dados também são armazenados de forma segura mesmo após passar pela ação de criptografia. É possível identificar todos estes pontos na Figura 7.

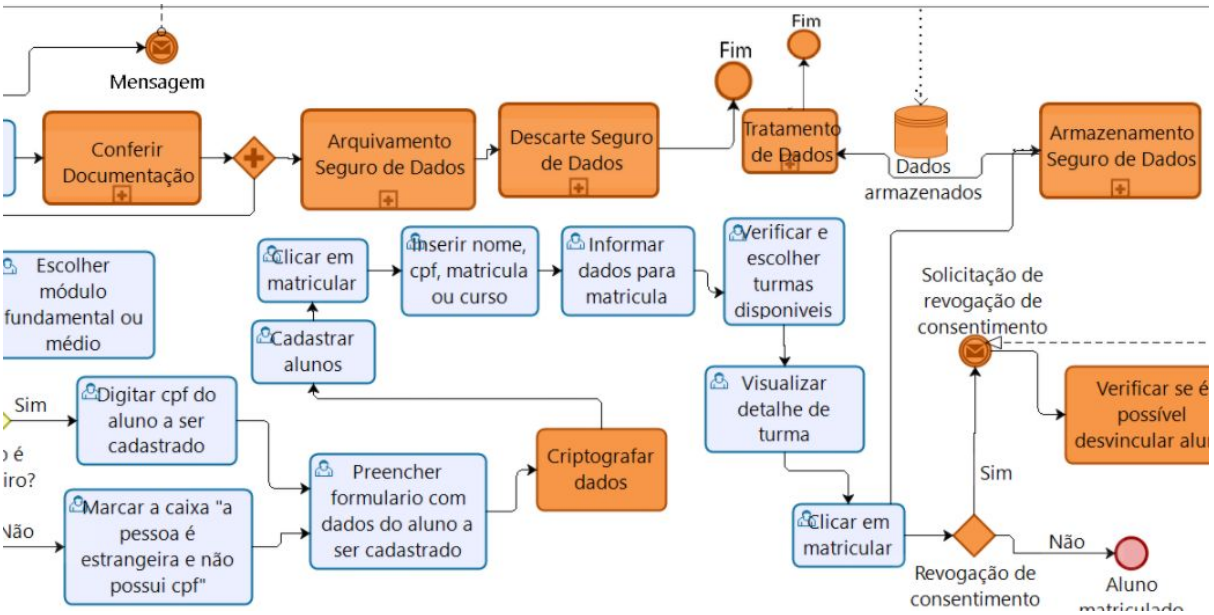


Figura 7. Ações para lidar com dados sensíveis.

Para cumprir as exigências impostas pela pergunta 9 (O processo apresenta o local em que os dados são armazenados e processados?) foi necessário fazer uma pequena alteração no processo, incluindo a notação BPMN para armazém de dados e um sub processo de tratamento de dados. Não foi criado um padrão de modelagem para este caso pois, é possível tratar esse ponto da lei diretamente no modelo BPMN, como apontado na Figura 8.

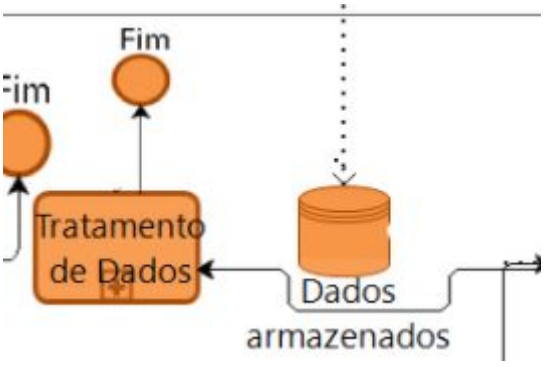


Figura 8. Local de armazenamento e processamento de dados.

Respondendo ao próximo ponto de não-conformidade, a pergunta 13 (O processo inclui as ações para lidar com um vazamento de dados?) Foi criado um processo auxiliar utilizando o padrão de modelagem de vazamento de dados, para que pudesse atender às restrições impostas pela lei (Figura 9).

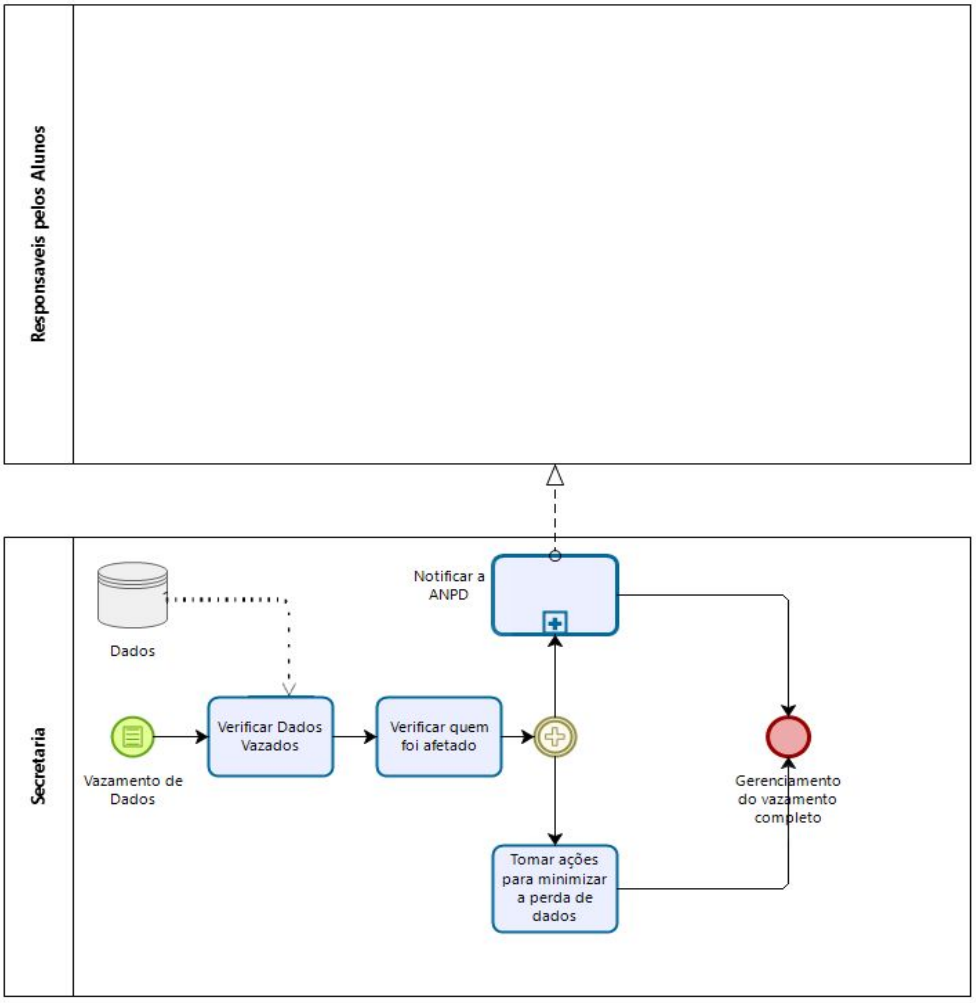


Figura 9. Ações para lidar com vazamento de dados.

Como descrito no padrão de modelagem, o processo reúne os dados vazados juntamente com os titulares de dados que foram afetados, e quem realiza esta ação é a Secretaria. Após reunir os dados, o processo, dentro de seu subprocesso notifica à Autoridade Nacional de Proteção de Dados (ANPD) e também todos os titulares que foram afetados pelo vazamento, ao mesmo tempo que toma as ações necessárias para mitigar o vazamento. Após isso o processo é finalizado.

Para responder a pergunta 15 do questionário (O processo inclui as ações para o caso de haver revogação de consentimento?) foram criados dois complementos do processo em duas *pools* diferentes: uma do lado do responsável pelo aluno (Figura 10) onde antes de confirmar a matrícula do aluno, o pai ou responsável será questionado se ele concorda com todos os termos de privacidade no termo de consentimento, caso a resposta seja positiva o aluno é matriculado e o processo acaba.

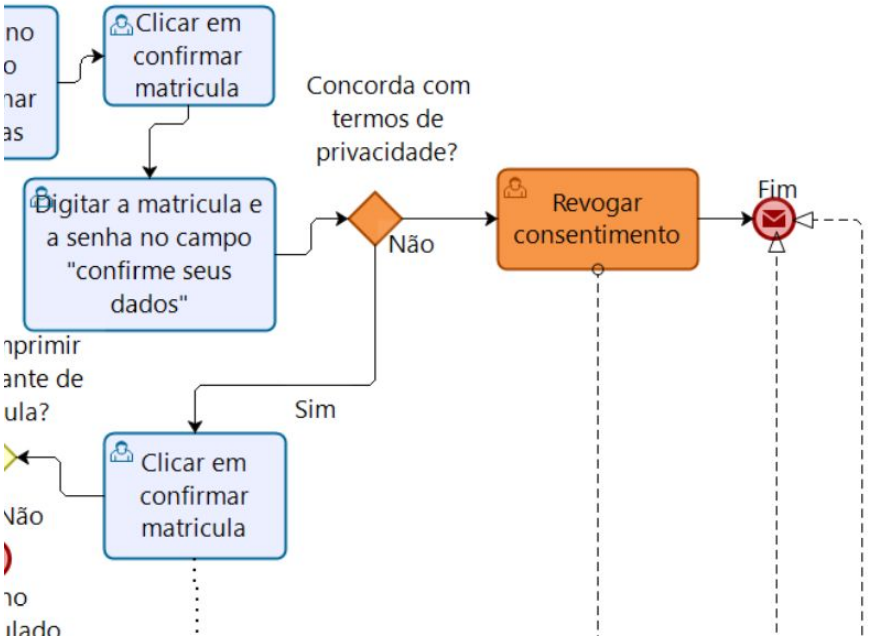


Figura 10. Inclusão de ações para revogação de consentimento na pool do responsável.

Caso seja negativa, será feita a revogação de consentimento, onde a solicitação da revogação é enviada para a secretaria, que verifica se houve ou não revogação após a matrícula do discente (Figura 11). Caso ocorra, a secretaria precisa checar se ainda é possível desvincular o aluno após a matrícula. Se não for possível, a secretaria deve explicar os motivos ao responsável e o processo finaliza, caso seja possível, deve ser notificado o desvínculo e aguardado um determinado tempo para que a ação seja concluída e após isso, o processo é finalizado.

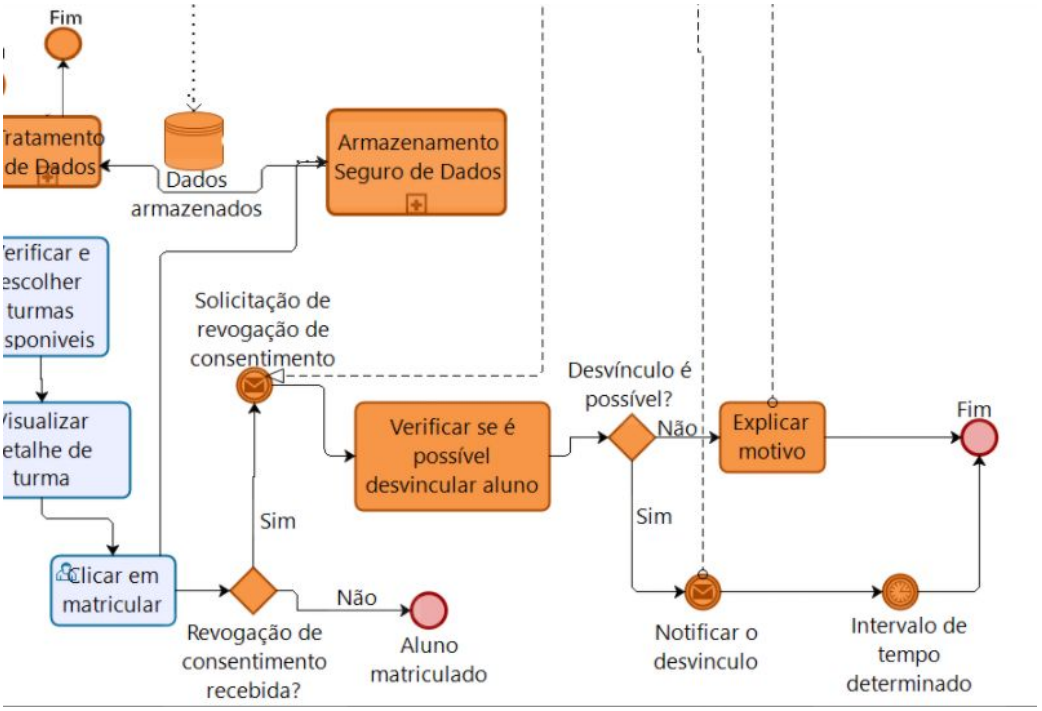


Figura 11. Inclusão de ações para revogação de consentimento na *pool* da secretaria.

Para responder as perguntas 16 (O processo inclui as ações a serem tomadas no caso de haver uma retificação de dados?), 17 (O processo inclui as ações a serem tomadas no caso de um apagamento de dados?) e 18 (O processo inclui as ações a serem tomadas no caso de uma solicitação de acesso de dados por parte do usuário?) do questionário foi criada uma nova *pool* chamada *Entrar no SIGAA*, que corresponde à ação executada pela secretaria em sua *pool*. Dentro da *pool* de acesso ao SIGAA estão as ações para executar uma retificação de dados, acesso e exclusão de dados, como apresentado na figura 12.

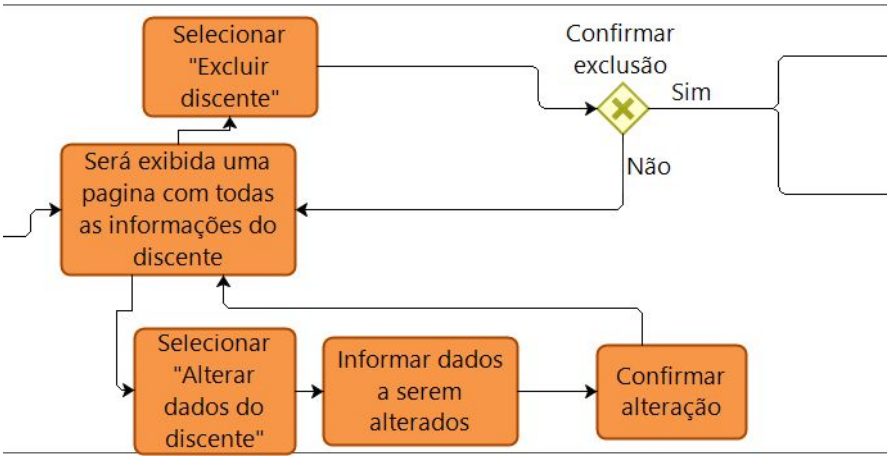


Figura 12. Ações para lidar com Retificação, Apagamento e Acesso de dados.

Dentro do sistema SIGAA Secretaria pode responder à solicitações de acesso na ação "*Página com todas as informações do discente*", como também pode responder à retificações de dados na ação "*Alterar Dados do Discente*" e "*Informar dados a serem alterados*". Após confirmar a alteração dos dados, a secretaria volta para a tela de informações já com todas as alterações presentes. Também é possível lidar com apagamento de dados na opção "*Selecionar excluir discente*" que é completada por uma confirmação de exclusão, que se obtiver uma resposta positiva para a pergunta, excluirá os dados do discente e finalizará o processo.

Com a aplicação destas alterações, mesmo que o questionário seja novamente aplicado sobre o novo processo, não haverão melhorias ou pontos de conformidade que não foram atendidos. Sendo assim, pode-se considerar o processo como um processo em conformidade com a Lei Geral de Proteção de Dados.

Na próxima seção são apresentados os resultados da avaliação do método proposto em uma turma de alunos de graduação e pós-graduação com conhecimento sobre privacidade, LGPD e que aplicaram o método proposto.

6. Avaliação do LGPD4BP

Um estudo exploratório baseado na opinião de alunos de pós-graduação foi realizado com o intuito de realizar uma avaliação do método LGPD4BP e receber feedback sobre sua utilidade e facilidade de aplicação. A condução dessa avaliação foi baseada nos trabalhos de Ferrari et al. (2019) e Bano et al. (2019) que avaliam uma técnica proposta para ensinar entrevistas em cursos de engenharia de requisitos usando critérios utilidade e facilidade de uso. A seguir são ressaltadas as perguntas de pesquisa, o contexto e o procedimento adotado no experimento.

6.1. Perguntas da avaliação

O objetivo dessa avaliação foi entender se os participantes consideram úteis e fáceis de aplicar, os diferentes passos contidos no método proposto. Portanto, foram levantadas as seguintes perguntas para essa avaliação (PA):

PA1: Os passos do LGPD4BP são considerados úteis? Essa pergunta avalia a opinião dos participantes no termo de utilidade de cada passo da abordagem proposta.

PA2: Os passos do LGPD4BP são considerados fáceis? A pergunta almeja entender se os participantes consideram fáceis os passos e qual deles foi o mais desafiador.

6.2. Contexto do estudo

O estudo foi conduzido em Setembro de 2020 com 18 participantes matriculados em uma disciplina de pós-graduação que abordou conceitos relacionados à *security*, ética, *safety,* privacidade e conformidade com leis. Um levantamento sobre o perfil dos participantes foi realizado. Observa-se um perfil heterogêneo entre os alunos conforme dados apresentados nas Figuras 13 a 18.

Figura 13. Experiência profissional dos participantes.

Mais da metade dos participantes possuíam experiência profissional na área de TI no momento em que o estudo foi conduzido.

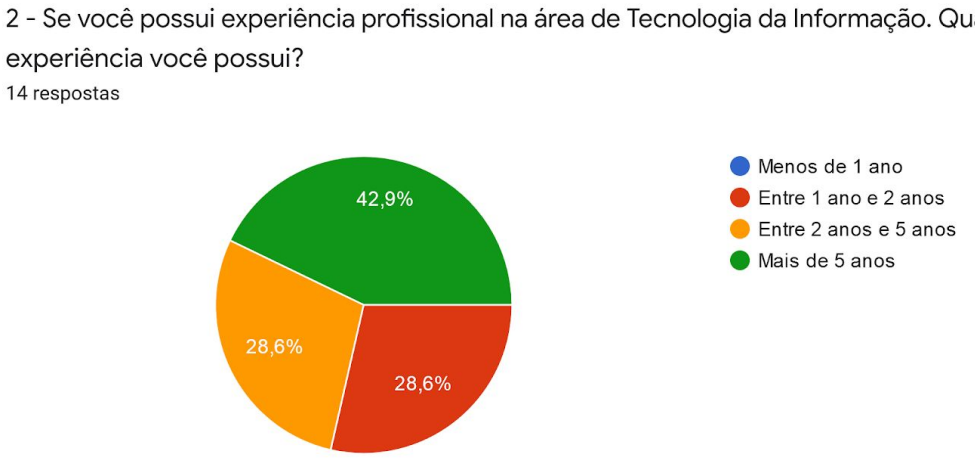


Figura 14. Tempo de experiência profissional dos participantes.

Na Figura 14 é possível perceber como se dividem os 77% dos participantes que têm experiência profissional na área de TI, quase metade deles possuem mais de 5 anos de experiência na área e nenhum deles possui menos de 1 ano de experiência.

Figura 15. Experiência em Privacidade dos participantes.

Apesar do grupo possuir profissionais com experiência na área, a Figura 15 mostra que menos da metade dos participantes possuem experiência profissional na área de Privacidade Informacional.

Figura 16. Tempo de experiência em Privacidade dos participantes.

Dentre os 16% que possuíam experiência profissional na área de Privacidade Informacional no momento em que o estudo foi conduzido, existiam alguns participantes que eram mais experientes que outros, metade deles tinha entre 1 e 2 anos de experiência na área e a outra metade se dividia entre os dois extremos opostos: possuir menos de 1 ano de experiência e possuir mais de 5 anos de experiência.

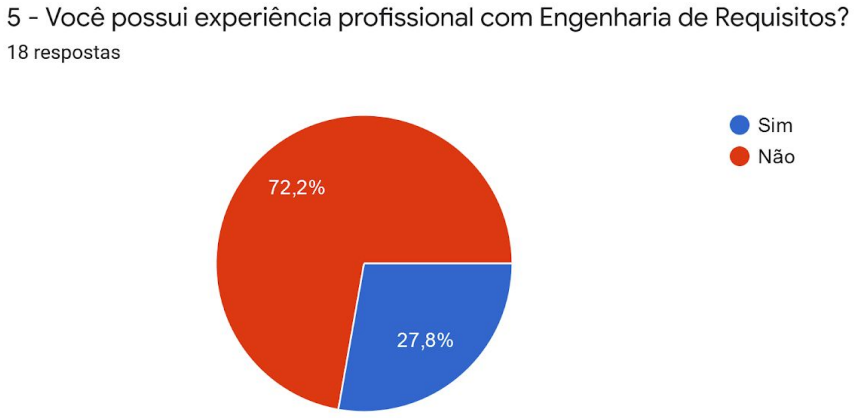


Figura 17. Experiência em Engenharia de Requisitos dos participantes.

Mais da metade dos participantes da pesquisa não possuía nenhum tipo de experiência profissional na área de Engenharia de Requisitos no momento em que o estudo foi conduzido.

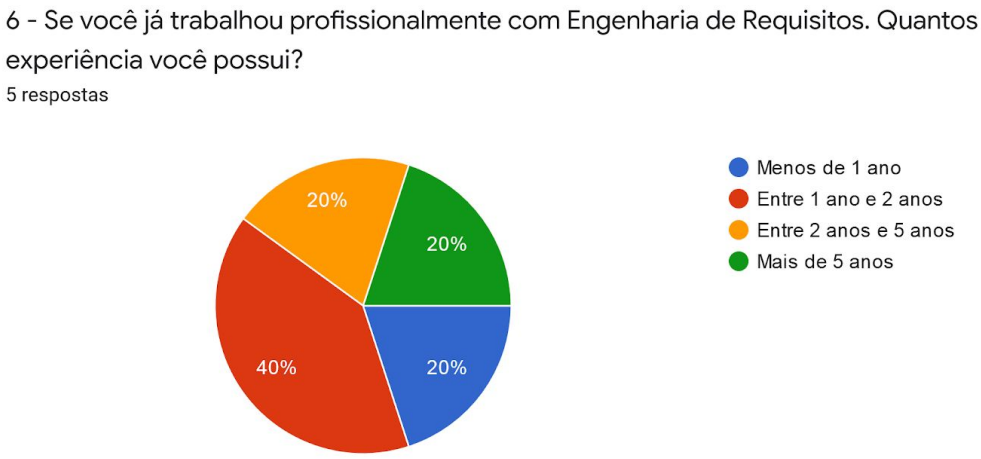


Figura 18. Experiência em Engenharia de Requisitos dos participantes.

Os 27% de Participantes que possuíam experiência profissional na área de engenharia de requisitos se dividem de forma bastante heterogênea, apesar de quase metade deles ter entre 1 e 2 anos de experiência na área, também existiam participantes com mais experiência na área.

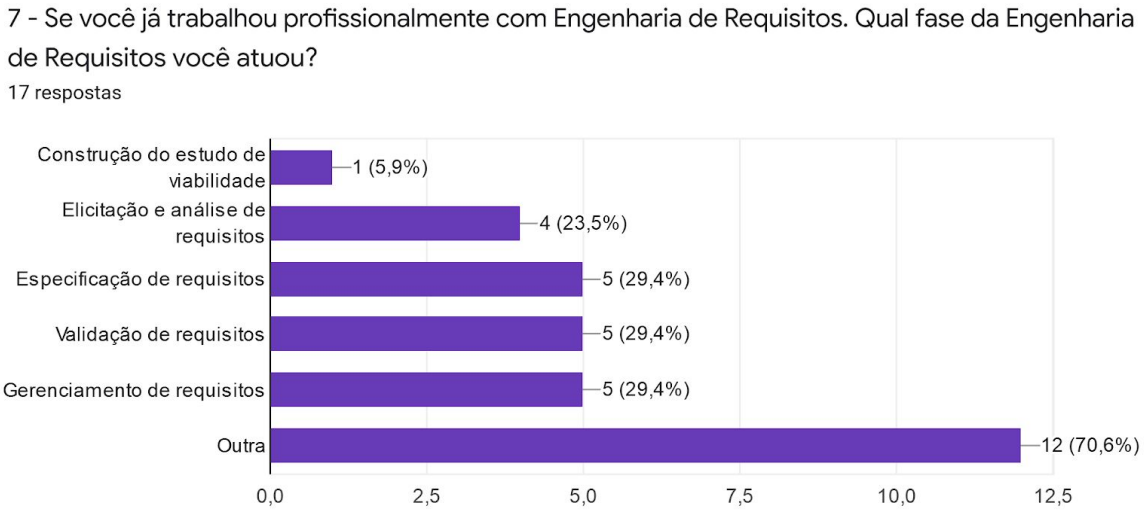


Figura 19. Área de atuação em Engenharia de Requisitos por parte dos participantes.

A Figura 19 mostra as áreas da engenharia de requisitos que os participantes já atuaram, é possível ver que existe bastante diversificação entre as áreas em que já passaram.

6.3. Coleta e Análise de dados

A pesquisa é exploratória e de natureza interpretativa e, portanto, foi utilizado uma abordagem qualitativa na coleta e análise de dados. Os alunos assistiram um vídeo de treinamento sobre o método proposto e foram solicitados a aplicar o método no estudo de caso do contexto do colégio de aplicação discutido na Seção 5. Após realizar o exercício, foi solicitado que eles respondessem um questionário de feedback sobre o método descrito na Tabela 16.

Questionário de feedback do método LGPD4BP
1) Quão ÚTIL você classifica as diferentes tarefas do método LGPD4BP? **Questionário de avaliação da conformidade do processo de negócio** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil. **Catálogo de padrões de modelagem** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil. **Método de 16 passos para modelagem de processo de negócio em conformidade** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil.
2) Qual foi a tarefa mais ÚTIL do método LGPD4BP e por quê?
3) Quão DIFÍCIL você classifica as diferentes tarefas do método LGPD4BP? **Questionário de avaliação da conformidade do processo de negócio** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil. **Catálogo de padrões de modelagem** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil. **Método de 16 passos para modelagem de processo de negócio em conformidade** ( ) Extremamente Útil. ( ) Muito Útil. ( ) Moderadamente útil. ( ) Ligeiramente útil. ( ) Nada útil.
4) Qual foi a tarefa mais DIFÍCIL do método LGPD4BP e por quê?
5) Alguma pergunta do questionário pode ser considerada desnecessária para avaliação da conformidade de um processo de negócio em relação a LGPD?
6) Alguma pergunta deveria ser adicionada ao processo de modelagem? Qual?
7) Algum padrão de modelagem presente no catálogo pode ser considerado desnecessário para modelagem de um processo de negócio em conformidade com a LGPD?
8) Algum padrão de modelagem deve ser adicionada ao catálogo do método LGPD4BP? Com que propósito?
9) Alguma atividade do processo de modelagem de 16 passos pode ser considerada desnecessária para modelagem de um processo de negócio em conformidade com a LGPD?
10)Alguma atividade deve ser adicionada ao processo de modelagem de 16 passos? Com que propósito?

11) Que dificuldades (se houve) você teve ao lidar com o método LGPD4BP?
12) Por favor, escreva recomendações para melhoria do método LGPD4BP (Opcional).

Tabela 16. Questionário de Feedback do Método LGPD4BP.

Em seguida, foi realizada uma análise temática dos dados e sintetizada a opinião dos participantes conforme análise realizada no trabalho de Ferrari et al. (2020).

6.4. Resultados

6.4.1. PA1: Utilidade

O questionário solicitava que os estudantes classificassem o grau de utilidade de cada uma das três tarefas que compõem o método proposto, sendo possível classificá-los como: Extremamente útil, Muito útil, Moderadamente útil, Ligeiramente útil e Nada útil. Com a ajuda da ferramenta de pesquisas Google Forms, foi possível coletar as respostas e gerar os gráficos (Figura 20) que indicavam o grau de utilidade de cada tarefa. Observa-se que todos os componentes do método LGPD4BP foram considerados úteis em algum grau para os participantes. Isso demonstra a importância dos componentes do método em algum momento da sua aplicação.

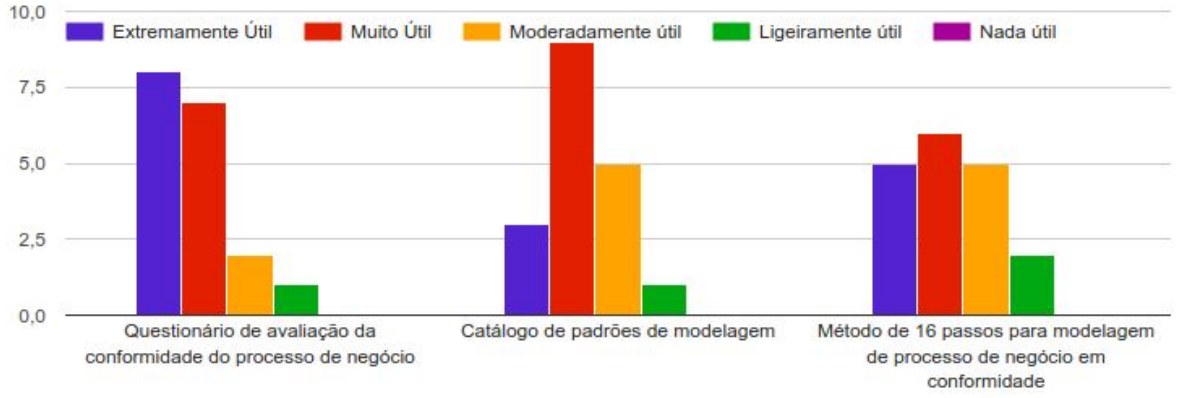


Figura 20. Grau de utilidade das tarefas do método LGPD4BP.

É possível perceber que o questionário de avaliação obteve uma resposta mais positiva quanto à sua usabilidade uma vez que 83,33% dos participantes da pesquisa o classificaram como Extremamente útil ou Muito útil. É possível observar também o baixo número de respostas que o consideram como Moderadamente útil ou Ligeiramente útil.

Já o catálogo de padrões de modelagem foi considerado como Muito útil por 50% dos participantes. Dentro dos outros 50% restantes, alguns participantes acreditam que o catálogo é Extremamente útil, enquanto outros acreditam que o catálogo de padrões é Moderadamente útil ou Ligeiramente útil.

O método de 16 passos teve opiniões bastante divididas acerca de sua utilidade, 33% dos participantes acreditam que ele é Muito útil, enquanto 55% se dividem entre considerá-lo Extremamente útil ou Moderadamente útil.

Em seguida, o questionário continha a pergunta: "*Qual foi a tarefa ÚTIL do LGPD4BP e por quê?*" por se tratar de uma pergunta aberta, as respostas foram analisadas e separadas para que fosse possível obter a porcentagem de cada uma delas. A partir dos dados, foi possível gerar um gráfico que expressa a tarefa considerada mais útil, é possível ver estes dados na Figura 21.

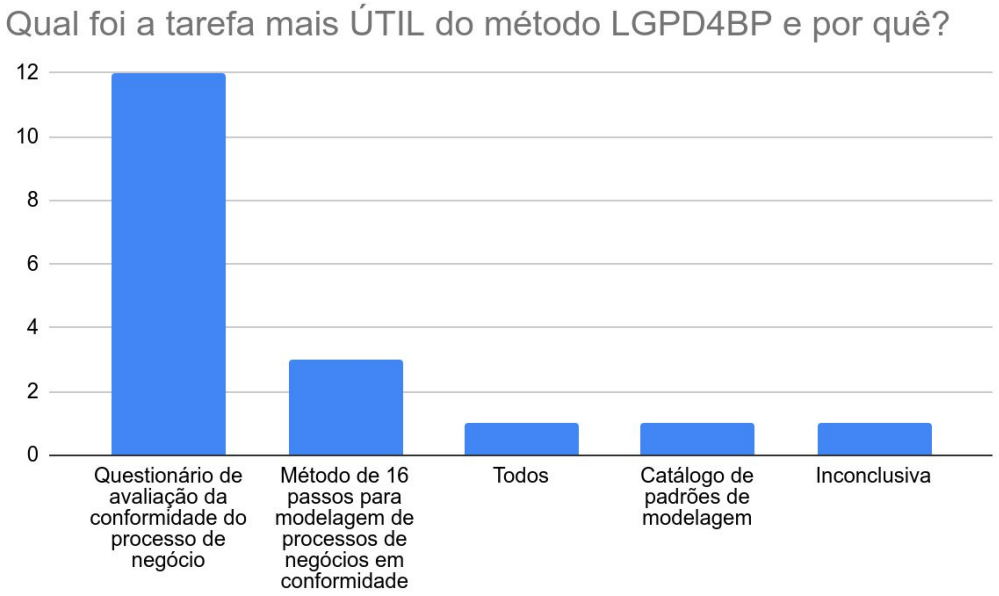


Figura 21. Feedback sobre qual a tarefa considerada mais útil do LGPD4BP.

A partir da Figura 21 é possível inferir que a tarefa considerada mais útil do método é o Questionário de avaliação da conformidade do processo de negócio, que obteve 61,11% dos votos dos participantes, alguns comentários explicam o motivo como: *"O questionário que vai nos guiar e garantir que não estamos esquecendo de nenhum ponto em relação a LGPD. Os outros facilitam o trabalho, mas podem ser testados empiricamente, consumindo mais tempo, porém se o questionário não estivesse bem definido, os outros se tornaríam um tanto quanto vazios, pois não saberíamos muito bem quando e como aplicá-los"* .

Logo em seguida vêm o Método de 16 passos para modelagem de processos de negócios em conformidade, que obteve 16,67% dos votos. Os comentários sobre ele afirmam que o uso dele auxiliou tanto no entendimento quanto no processo de modelagem dos processos.

Cerca de 5,55% dos participantes acreditam que todos os passos são úteis, segundo comentários: *"Os três, pois achei que é uma atividade que precisa do alinhamento das três tarefas."* acreditando que é necessário que os 3 passos se complementam.

Outros 5,55% dos participantes acreditam que o catálogo de padrões de modelagem é o passo mais útil, pois eles acreditam que ele é responsável por apresentar como obter a conformidade em pontos chave do processo. O restante dos participantes, cerca de 5,55%, forneceram respostas inconclusivas sobre o processo, não sendo possível compreender a qual dos 3 passos a resposta se referia.

6.4.2. PA2: Facilidade

Assim como a Utilidade dos passos do método proposto, os participantes foram questionados também sobre o nível de facilidade na aplicação dos passos, podendo classificá-los como: Muito fácil, Moderadamente Fácil, Nem fácil nem difícil, Moderadamente difícil e Muito difícil. É possível ver na Figura 22 os gráficos que representam as respostas sobre o nível de dificuldades dos passos do método proposto.

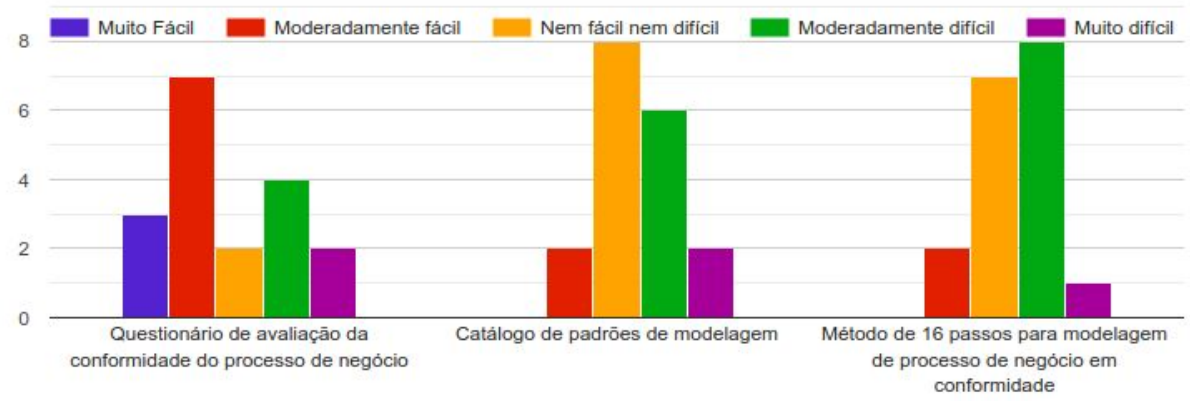


Figura 22. Grau de dificuldade em aplicar as tarefas do método LGPD4BP.

As opiniões acerca da facilidade de aplicação do questionário foram bastante diversificadas, no entanto, 38% dos participantes consideraram como Moderadamente Fácil a aplicação do questionário. Outros 16% acreditam que foi Muito fácil aplicar o questionário para encontrar os pontos de não conformidade de um processo. 22% ficaram divididos entre considerá-lo nem fácil nem difícil ou Muito difícil de aplicar, enquanto o restante dos participantes consideraram que o questionário era Moderadamente difícil de ser aplicado.

O Catálogo de padrões de modelagem foi majoritariamente considerado como Nem fácil nem difícil pelos participantes da pesquisa, enquanto o restante dos participantes, cerca de 33%, considerou-o como Moderadamente difícil, 22% dividiram-se entre considerá-lo Moderadamente fácil ou Muito difícil. Algumas pessoas o consideraram como Muito difícil devido à dificuldade de entender "*onde modelar*" os padrões apresentados. Dessa forma, observa-se que alguns participantes, por não terem experiência com engenharia de software, desconhecem

a forma de aplicação e uso de padrões de projeto e, logo, dos padrões de modelagem propostos neste trabalho.

44% dos participantes consideraram que o Método de 16 passos era Moderadamente difícil de ser aplicado. Ao analisar os comentários dos participantes, deve-se à alguns fatores como o cuidado ao modelar os padrões, conhecimento sobre os mesmos e a interferência que eles podem causar na maneira própria de modelar que um indivíduo possui. 38% consideraram que o método não é Nem fácil nem difícil, enquanto o restante considerou-o como Moderadamente fácil ou Muito difícil.

Logo após a avaliação do nível de dificuldade de cada uma das tarefas, o questionário continha a seguinte pergunta: "*Qual foi a tarefa mais DIFÍCIL do método LGPD4BP e por quê?*" realizando o mesmo processo adotado na Seção 6.4.1 foi possível a criação do gráfico presente na Figura 23.

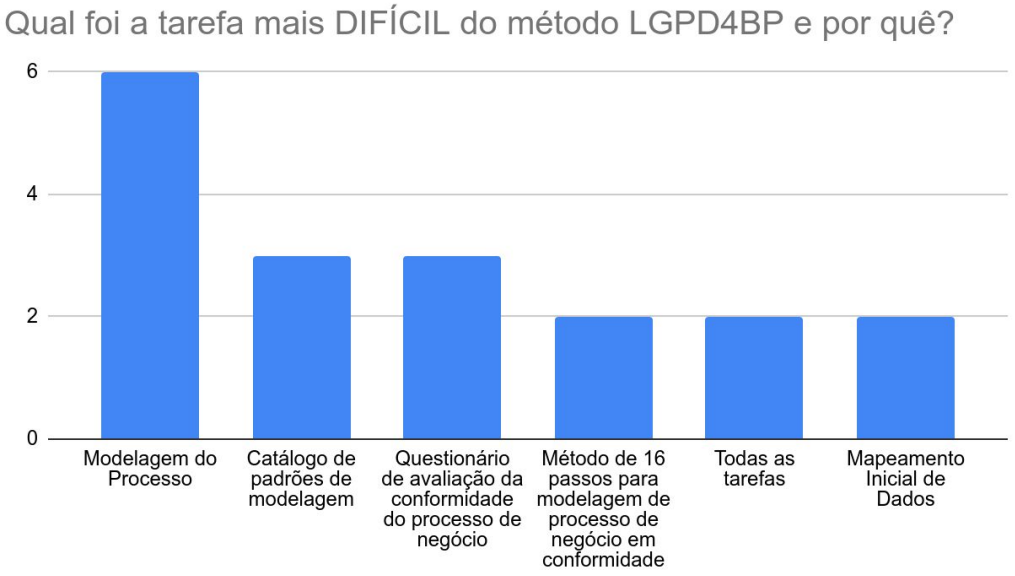


Figura 23. Feedback sobre qual a tarefa mais difícil do LGPD4BP.

Após a análise das respostas entregues pelos participantes, é possível perceber que a tarefa mais difícil não é nenhuma das 3 presentes no método LGPD4BP. Surpreendentemente os participantes acreditam que a Modelagem do processo que vem após a aplicação dos 3 passos é a tarefa mais difícil, alguns comentários como:

"Modelar os processos, uma vez que surgiam muitos questionamentos do que seria mais apropriado e de quem seria a responsabilidade de cada processo"

"A modelagem, pois são muitas etapas que precisam de cuidado, pois cada uma delas pode ser representada de maneiras diferentes, em locais diferentes etc e é

preciso atenção para que ela esteja bem representada e que nada esteja fora do lugar para evitar possíveis quebras de conformidade."

Essas observações dos participantes ressaltam que a percepção da dificuldade no método proposto não consiste no método em si, mas na ação subsequente à aplicação. Este resultado pode ser uma possível indicação que os participantes não têm muita prática com a notação BPMN. Esse resultado já era de certa forma esperado em virtude do perfil heterogêneo da turma com participantes experientes em engenharia de requisitos e outros em LGPD e outras áreas.

Se a análise for feita sendo restringida apenas às 3 tarefas, é possível observar que tanto o Catálogo de padrões de modelagem quanto o Questionário de avaliação, que havia sido considerado como a tarefa mais útil do LGPD4BP, ficariam empatados. Ao analisar com mais rigor as respostas dos participantes, os motivos segundo o Catálogo dizem que *"É difícil entender onde modelar os padrões presente no catálogo."* e que *"É preciso entender da linguagem BPMN"*. Pode-se concluir que as questões voltadas mais para o lado técnico da notação BPMN ou mesmo do conhecimento sobre o que é um Padrão de projeto eram um fator que alguns participantes precisam de mais tempo para praticar por não terem formação em computação.

Quanto ao questionário de avaliação, alguns participantes disseram que o questionário era confuso quanto ao seu preenchimento, outros afirmaram que a tarefa se tornava difícil devido ao entendimento da LGPD. O restante dos participantes se dividiu entre classificar como mais difícil o Método de 16 passos, Todas as 3 tarefas e outro item que não estava disponível para votação: Mapeamento inicial de dados.

Sobre o método de 16 passos não existiram comentários significativos sobre o motivo da escolha. Quanto ao Mapeamento de dados, o comentário de um dos participantes que votou nesta alternativa dizia que *"O mapeamento dos dados, pois exige referências externas específicas de acordo com cada tipo de dado."* Isto reforça que para a aplicação do LGPD4BP, é necessária a participação dos analistas das organizações, que entendem do processo de negócio da empresa em que atuam.

Por fim, conclui-se com base nos resultados e comentários, a tarefa mais difícil do LGPD4BP não faz parte dela, e sim é uma ação que ocorre logo após a aplicação do método: A Modelagem do processo.

6.4.3. Análise temática das opiniões dos participantes

Com os resultados adquiridos por meio do do questionário, foi possível realizar uma análise temática dos dados (Ferrari et al., 2020) e as respostas foram agrupadas em 4 categorias: Dificuldades, Completude, Dispensável e Melhorias. A Figura 24 apresenta os resultados dessa análise.

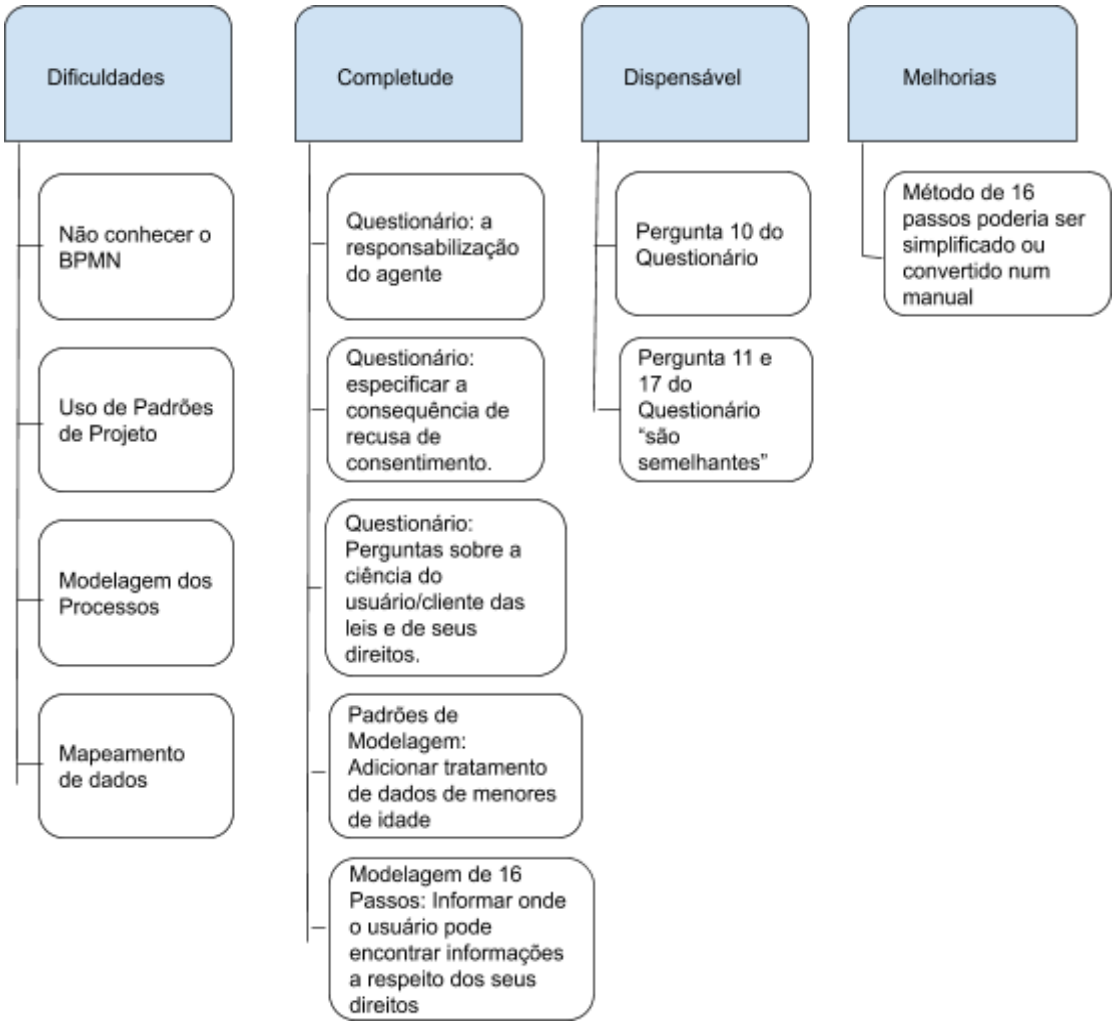


Figura 24. Mapeamento e Categorização de Respostas.

A categoria de Dificuldades tem o intuito de de agrupar as os desafios que os participantes tiveram durante a aplicação do método proposto. As respostas que foram obtidas foram bastante semelhantes, o que permitiu este agrupamento. Alguns participantes fizeram comentários como: *"não tenho habilidades com BPMN"* e *"Precisamos entender da linguagem BPMN"* . Por se tratar de uma turma heterogênea, existiam participantes que não tinham experiência com a Notação BPMN.

A maioria dos participantes fez comentários sobre a modelagem de processos, o que também está relacionado à dificuldade com o BPMN, porém outros foram bastante diretos ao dizer que teve dificuldades com a modelagem: *"Pois o método não é muito objetivo. É um pouco subjetivo."*

Existiram também aqueles que simplesmente não estavam acostumados a modelar processos, então responderam que a modelagem era bastante difícil: *"Pois são muitas etapas que precisam de cuidado, pois cada uma delas pode ser representada de maneiras diferentes, em locais diferentes etc e é preciso atenção*

para que ela esteja bem representada e que nada esteja fora do lugar para evitar possíveis quebras de conformidade."

Outros participantes não sabiam como utilizar os padrões de projeto dispostos no método, e ficaram bastante confusos com eles, enquanto outros acharam complicado realizar o mapeamento inicial dos dados para que se pudesse checar a conformidade do processo existente.

A Categoria de completude têm o objetivo de agrupar as respostas que sugeriam que algo deveria ser adicionado ao método, alguns participantes forneceram algumas ideias que serão brevemente discutidas a partir daqui.

O primeiro ponto da categoria vêm da sugestão de um dos participantes que dizia: *"Faltou focar na responsabilização do agente, na questão da demonstração da segurança dos dados."* Primeiramente, por se tratar de uma lei muito nova e ainda em processo de construção, a LGPD não especifica nenhum tipo de responsabilização específica ao agente, desta forma, não é possível que o processo de modelagem possa focar, um ponto que já existe no questionário e que supre esta falta é a pergunta 7 (O processo indica quem é o ator (Departamento/Posição) responsável pelo processamento de dados em cada atividade?). Desta forma, é possível representar no processo o responsável pelas atividades para que seja possível arcar com as consequências de um futuro problema.

O segundo ponto da categoria foi originado do comentário: *"A (pergunta) de se é especificada a consequência de recusa de consentimento."* A pergunta sugerida no comentário já existe no questionário do LGPD4BP, que é a pergunta 4 (O processo contém informações sobre a possibilidade de não prover consentimento e as consequências da recusa?). Não é possível focar apenas nas consequências de recusa de consentimento tendo em vista que cada organização terá consequências diferentes devido aos diferentes serviços prestados, portanto, a questão precisava ser um pouco mais abstrata para que pudesse ser atendida a nível de processo de negócio.

O terceiro ponto vem do seguinte comentário: *"Perguntas sobre a ciência do usuário/cliente das leis e de seus direitos."* Este ponto está inserido implicitamente dentro da questão 1 (O processo inclui as ações para obter consentimento?), pois o termo de consentimento deve possuir todas as informações sobre direitos do titular dos dados, finalidade de processamento, etc. Além disso, o tratamento só pode ser iniciado quando o titular concorda com todos os termos.

O quarto ponto partiu do comentário que dizia: *"Talvez tratamento de dados de menores de idade?"* quando perguntado se "*Algum padrão de modelagem deve ser adicionado ao catálogo do método LGPD4BP?"*. É importante ressaltar que o tratamento de dados de menores de idade ocorre da mesma forma que o tratamento dados de maiores de idade. A diferença é que para que o tratamento seja iniciado, o consentimento deve ser dado pelos pais ou responsáveis pelo menor. Esta condicional já está presente no padrão de modelagem de consentimento, portanto é desnecessário adicionar um padrão de modelagem apenas para esta questão.

O quinto e último ponto originou-se do comentário *"Informar onde o usuário pode encontrar informações a respeito dos seus direitos e quais tipos de tratamento específicos os dados terão. Onde encontrar não apenas a lei, mas também guias e comentários oficiais, como aquelas usados na elaboração do mapeamento de dados."* quando perguntado: "*Alguma atividade deve ser adicionada ao processo de modelagem de 16 passos*?". Novamente, assim como no terceiro ponto, as informações sugeridas já estão presentes no termo de consentimento, não sendo necessário criar um passo a mais no método para este intuito. Além disso o objetivo do método é guiar o analista a modelar o processo de negócio. Portanto, está fora do escopo do LGPD4BP fornecer informações adicionais sobre a lei, guias ou comentários oficiais.

Além destas questões de completude, outros participantes julgaram que o método está bem fechado, e não adicionariam mais nada. Foram obtidas respostas como: *"Acho que o questionário está bem completo."* e *"Acho que está tudo bem completo. Não tem necessidade de adição de algo além do que já existe."* e também *"Não vejo nenhum ponto para ser adicionado."* são alguns exemplos de respostas que afirmaram que o método já está completo para o fim a que se propõe.

A categoria Dispensável foi criada com as respostas dos participantes que julgaram que alguns dos pontos do método não eram necessários na sua aplicação, porém, neste quesito os participantes responderam que apenas o questionário continha pontos desnecessários, sendo um deles a pergunta 10 (O processo inclui as ações necessárias para a transferência internacional de dados?). Infelizmente o participante não explicou seus motivos, porém, é importante ressaltar que a questão 10 pode não ser aplicável em muitas das organizações que não são multinacionais, mas ainda assim é necessário que esteja presente para as ocasiões em que a organização seja. Não são todos os processos que terão transferência internacional de dados, porém o objetivo do questionário é ser o mais assertivo possível quanto aos pontos chaves da LGPD, e a transferência internacional de dados é um deles.

Outro ponto citado foi o de as questões 11 e 17 serem semelhantes, houveram casos em que os participantes perguntaram se não poderiam ser uma pergunta só: *"Eu achei as questões 11 e 17 com sentido semelhante. Elas não poderiam se tornar uma única pergunta?"* e o motivo de isto não ser possível é que existe uma diferença entre o descarte e o apagamento de dados. O primeiro se refere à quando os dados do titular já foram tratados e não existe mais sentido em continuar com eles, pois o propósito do tratamento com aqueles dados já foi cumprido, então a organização deve descartar os dados de forma segura para que não haja risco de roubo destes dados, o segundo refere-se ao caso de o titular dos dados solicitar que seus dados sejam excluídos dos sistemas, quer estes dados já tenham sido tratados ou não, e sendo assim o controlador deve atender ao pedido do mesmo. Logo, por se tratar de duas situações distintas é necessário que hajam duas perguntas diferentes no questionário.

No geral, todas as outras respostas julgavam que todos os passos do método eram necessárias devido à forma em que eles estão interligados, Como em alguns comentários: *“Acredito que todas as 18 perguntas são bem focadas na manipulação dos dados que a empresa ou usuario podem e devem ter. Seria difícil excluir alguma delas, portanto, não considero viável a exclusão de nenhuma.”*

e também:

“Não. Todas (as perguntas) são adequadas e possuem correlação com deveres e obrigações impostas pela LGPD.”

e em:

“Vejo que todos (os padrões) estão em conformidade e no mesmo direcionamento das 18 perguntas do questionário, acredito que nao tenha nenhum desnecessário.”

A categoria de melhorias agrupou as respostas em que os participantes sugeriram alguma melhoria ao método proposto, no entanto, foi obtida apenas uma resposta para esta categoria: *“Método de 16 passos para modelagem de processo de negócio em conformidade, poderia ser simplificado ou convertido num manual.”* O que pode levar à uma possível melhora para o método em trabalhos futuros.

7. Conclusões e Trabalhos Futuros

A LGPD descreve as obrigações que os controladores de dados e os agentes de processamento que são importantes para alcançar a conformidade com a lei de privacidade. A privacidade e a conformidade com a LGPD deve ser especificada no início de um projeto, para que a conformidade seja alcançada dentro de uma organização.

Considerando que processos de negócios é um dos pilares da segurança (ANDRESS, 2003), a modelagem de processo é o primeiro passo de um programa de conformidade.Portanto, este trabalho teve como objetivo responder às seguintes perguntas de pesquisa:

P1: Como avaliar a conformidade de um processo de negócio com a LGPD?

Este trabalho propôs o método LGPD4BP, que consiste em um questionário de avaliação, um método de modelagem e um catálogo de padrões de modelagem. Para que fosse possível responder a P1, o questionário de avaliação de conformidade foi proposto como parte do método.

O questionário foi elaborado a partir da análise da LGPD e possui correspondência direta entre as perguntas e artigos da lei. Com ele é possível realizar um diagnóstico da situação de um processo de negócios por meio de pontos-chave do processo, sendo possível encontrar até 18 pontos de não-conformidade em um processo.

P2: Como modelar um processo de negócio em conformidade com a LGPD?

O método proposto, LGPD4BP, é composto também por um método de modelagem de 16 passos e um catálogo de padrões de modelagem. O método de modelagem foi criado de forma que ficasse diretamente ligado ao questionário, ao ponto que é possível saber exatamente qual passo deve ser seguido de acordo com as respostas dadas ao questionário.

O catálogo de padrões de modelagem é composto por 9 padrões que ajudam no entendimento de como cada quesito de conformidade deve ser modelado, sendo usado também como consulta para cada passo do método de modelagem. Assim sendo, guiando-se pelas respostas obtidas do questionário e seguindo os passos correspondentes no método de modelagem, que recebem os padrões de modelagem como entrada, é possível garantir a modelagem de processos de negócio em conformidade com a lei.

7.1. Conclusões

- **O método foi utilizado para avaliar um processo de negócio real de uma instituição pública.** O método foi aplicado em um processo do Colégio de Aplicação (CAp) que ilustrava o procedimento de matrícula de alunos novos e antigos. Ao todo foram encontrados 12 pontos de não conformidade, entre eles, o processo não continha ações que indicassem a obtenção do consentimento por parte do usuário, também não especificava as bases legais de processamento, ou seja, segundo a LGPD não poderia processar dados pessoais de forma alguma. Também não haviam ações para processar os dados pessoais de crianças, o que era crítico pois tratando-se de um processo de matrícula de um colégio, certamente teria que processar dados de crianças. Também não continha ações para lidar com dados sensíveis, não apresentava o local em que os dados eram armazenados e processados, não incluía ações para o descarte de dados, nem ações para lidar com um possível vazamento de dados. O processo não contava com ações em caso de uma revogação de consentimento, ou as ações a serem tomadas no caso de uma solicitação de acesso, retificação ou apagamento de dados.Todos os pontos em não conformidade foram corrigidos utilizando tanto os padrões de modelagem como referência quanto o método de modelagem de 16 passos, de forma que informações sobre obtenção de consentimento, local de armazenamento e processamento de dados, Compartilhamento de dados com terceiros, ações para lidar com dados sensíveis, ações para lidar com uma revogação de consentimento e com vazamento de dados, solicitação de acesso, retificação e apagamento de dados também foram adicionados ao processo. Para refinar o modelo e torná-lo em conformidade com a LGPD,

foram usados os padrões de Consentimento, Vazamento de Dados, Revogação de Consentimento, Retificação, Apagamento e Acesso de dados e adicionadas 15 novas ações que refletiam os padrões de modelagem. Ao final das adições, o questionário pôde ser aplicado novamente e nenhum ponto de conformidade foi encontrado.

- **Necessário conhecimento do domínio para aplicar o método e avaliar a conformidade com a lei.** Após a aplicação do método no processo de negócio do colégio de aplicação, observou-se que o avaliador do processo deve possuir conhecimento do domínio para que a avaliação seja completa. No Cap, além do conhecimento do domínio, era necessário conhecer as leis que regem a educação, lei de acesso à informação entre outras normas aplicáveis.
- **O passo do LGPD4BP considerado mais útil é o Questionário de Avaliação de Conformidade.** Após o levantamento das respostas do estudo conduzido com 18 participantes, 61% deles consideraram o Questionário de Avaliação de Conformidade como sendo a tarefa mais útil do LGDP4BP. Segundo os mesmos isso se deve à capacidade de encontrar as não-conformidades diretamente nos pontos-chave de um processo.
- **A atividade considerada mais difícil é a modelagem do processo.** Surpreendentemente, o passo considerado mais difícil não é nenhum dos componentes do método LGPD4BP, após a análise das respostas do estudo, foi possível observar que os participantes indicaram que o passo mais difícil da LGPD4BP na verdade não pertence ao método, mas que é um passo subsequente à aplicação: a modelagem do processo de acordo com as leis de conformidade. Isso reforça que o analista deve ter um bom conhecimento do BPMN para que possa aplicar as melhorias no processo.

7.2. Contribuições da Pesquisa

É possível prever alguns benefícios de utilizar o método proposto:

- **Os *Stakeholders* podem realizar uma análise de conformidade de seus modelos de processos de negócios em relação ao LGPD.** Conseqüentemente, o LGPD4BP ajudará os profissionais a serem confrontados com os requisitos LGPD no início do processo de conformidade;
- **LGPD4BP pode ser usado como uma referência para modelar processos de negócios em conformidade com LGPD.** O método fornece uma compreensão e alinhamento compartilhados, comuns e consistentes dos requisitos da LGPD nos modelos de processos de negócios. Conseqüentemente, ele orienta analistas de negócios e engenheiros de requisitos na modelagem dos requisitos da LGPD em

qualquer domínio por meio da definição explícita de padrões de modelagem. Essa orientação pode contribuir para reduzir o tempo gasto no programa de conformidade e melhorar a qualidade dos processos de negócios. Portanto, o LGPD4BP pode fornecer artefatos para futuras responsabilidades de conformidade. Além disso, o método de modelagem e os padrões podem ser usados em qualquer ferramenta de modelagem BPMN.

7.3. Limitações da pesquisa

Como o LGPD4BP é uma abordagem em evolução, é plausível que existam algumas limitações:

- Ressalta-se que o LGPD4BP é baseado na versão da LGPD publicada em 2018. Considerando que a lei pode mudar ao longo dos anos, a proposta pode precisar ser atualizada;
- A proposta de avaliar a conformidade LGPD dos processos de negócios é uma atividade manual e sua eficácia depende do conhecimento que o analista tem do processo em análise;
- Embora a proposta tenha sido construída com uma base teórica sólida e seguindo um método de pesquisa bem definido, ainda é necessário validar a integralidade do LGPD4BP com especialistas em privacidade.

7.4. Trabalhos Futuros

Os próximos passos da agenda de pesquisa incluem:

- Conduzir entrevistas com especialistas em privacidade para avaliar a completude tanto do catálogo de padrões de modelagem quanto do método de modelagem;
- Aplicar o método proposto em diferentes domínios e tamanhos de processos de negócios para avaliar a efetividade mais a fundo;
- Desenvolver uma ferramenta para dar suporte ao método proposto e conduzir a checagem automática de conformidade com a LGPD.

REFERÊNCIAS

1. Workflow Management Coalition. (2020). Disponível em: <https://www.businessprocessglossary.com/12936/business-process>. Último acesso em Jul. 2020.
2. VERHALEN, Aline et al. O controle por detrás da tela: a Inteligência Artificial da NetFlix sob a ótica dos usuários. In: **Anais Estendidos do XVIII Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais**. SBC, 2019. p. 37-38.
3. AGOSTINELLI, Simone et al. Achieving GDPR compliance of BPMN process models. In: **International Conference on Advanced Information Systems Engineering**. Springer, Cham, 2019. p. 10-22.
4. ANDRESS, Amanda. Surviving security: how to integrate people, process, and technology. CRC press, 2003.
5. VEIGA, A. Da; ELOFF, Jan HP. **An information security governance framework. Information systems management**, v. 24, n. 4, p. 361-372, 2007.
6. OMG, Object Management Group. **Business Process Model and Notation (BPMN) Specification 2.0**, 2009.
7. TOM, Jake. **Assessing and Improving Compliance to Privacy Regulations in Business Processes**. Proceedings of the Doctoral Consortium Papers Presented at the 30th International Conference on Advanced Information Systems Engineering (CAiSE), 2018)
8. ALEXANDER, Christopher. **The timeless way of building**. New York: Oxford University Press, 1979.
9. PEIXOTO, Mariana Maia. **Privacy Requirements Engineering in Agile Software Development: a Specification Method**. In: REFSQ Workshops. 2020.
10. LUCASSEN, Garm et al. The use and effectiveness of user stories in practice. In: **International working conference on requirements engineering: Foundation for software quality**. Springer, Cham, 2016. p. 205-222.
11. PEIXOTO, Mariana et al. **On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview**. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. Springer, Cham, 2020. p. 116-123.
12. PEIXOTO, Mariana Maia et al. **Towards a Catalog of Privacy Related Concepts**. In: REFSQ Workshops. 2020.
13. TORRE, Damiano et al. Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR. **arXiv preprint arXiv:2007.12046**, 2020.

14. AYALA-RIVERA, Vanessa; PASQUALE, Liliana. **The grace period has ended: An approach to operationalize GDPR requirements**. In: 2018 IEEE 26th International Requirements Engineering Conference (RE). IEEE, 2018. p. 136-146.
15. 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. 2019. p. 1-5.
16. LÜBKE, Daniel; VAN LESSEN, Tammo. **Modeling test cases in BPMN for behavior-driven development.** IEEE software, v. 33, n. 5, p. 15-21, 2016.
17. BRASIL. DECRETO N° 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais**, Brasília, DF, ago 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 12 mar. 2020.
18. KIRCHMER, Mathias et al. **High performance through business process management.** West Chester: Springer, 2017.
19. WESKE, M. Business Process Management–Concepts, Languages, Architectures, Verlag. Berlin, 2007.
20. ROSING, Mark von; SCHEEL, Henrik von; SCHEER, August-Wilhelm. **The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM, Volume I**. Morgan Kaufmann Publishers Inc., 2014.
21. PULLONEN, Pille et al. Privacy-enhanced BPMN: Enabling data privacy analysis in business processes models. **Software and Systems Modeling**, v. 18, n. 6, p. 3235-3264, 2019.
22. HARMON, Paul; TRENDS, Business Process. **Business process change: A guide for business managers and BPM and Six Sigma professionals**. Elsevier, 2010.
23. DE NEGÓCIO, **Gerenciamento de Processos**. BPM CBOK. 2013.
24. DO BRASIL, Constituição Federal. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 25 mar. 2020
25. ZACHARY, Heather; TRZOP, Allison. **Online Consumer Privacy: Airlines Under Scrutiny. Air & Space Law**., v. 27, p. 1, 20, 2014.
26. LAW, California. **California Legislative Information.** Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC>. Acesso em 22 ago. 2020
27. CANADA, Office of the Privacy Comissioner of. **PIPEDA in brief.** Disponível em: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>. Acesso em 22 ago. 2020

28. SOUTH AFRICA, **Protection of Personal Information Act 4 of 2013.** Disponível em: <https://www.gov.za/documents/protection-personal-information-act>. Acesso em 31 ago. 2020
29. INDIA, **The Personal Data Protection Bill.** Disponível em: <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019> . Acesso em 31 ago. 2020
30. HADAR, Irit et al. Privacy by designers: software developers' privacy mindset. **Empirical Software Engineering**, v. 23, n. 1, p. 259-289, 2018.
31. MATULEVIČIUS, Raimundas et al. A **Method for Managing GDPR Compliance in Business Processes**. In: International Conference on Advanced Information Systems Engineering. Springer, Cham, 2020. p. 100-112.
32. CAPODIECI, Antonio; MAINETTI, Luca. Business process awareness to support GDPR compliance. In: **Proceedings of the 9th International Conference on Information Systems and Technologies**. 2019. p. 1-6.
33. REGULATION, Protection. Regulation (EU) 2016/679 of the European Parliament and of the Council. **REGULATION (EU)**, v. 679, p. 2016, 2016.
34. Frank Buschmann, Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stahl 1996. **Pattern-Oriented Software Architecture-A System of Patterns**, Nova York, NY: John Wiley e Sons, Inc.
35. UFPE, **Sobre o CAp**. Disponível em: <https://www.ufpe.br/cap/sobre> Acesso em 23 set. 2020.
36. UNIVERSIDADE FEDERAL DE PERNAMBUCO. PROACAD/UFPE. Resolução n° 24/2017, de 02 de setembro de 2019. **PROCESSO SELETIVO PARA INGRESSO NO 6º ANO DO ENSINO FUNDAMENTAL PARA 2020 - COLÉGIO DE APLICAÇÃO DO CENTRO DE EDUCAÇÃO DA UFPE - RECIFE - PE.**, Pernambuco, 2007. Disponível em: https://www.ufpe.br/documents/38970/2338189/EDITAL_CAp-Proacad-07-2019.pdf/bbd715d7-4716-4a0b-848b-d2710caa0d05. Acesso em: 17 set. 2020.
37. FERRARI, Alessio et al. Learning requirements elicitation interviews with role-playing, self-assessment and peer-review. In: **2019 IEEE 27th International Requirements Engineering Conference (RE)**. IEEE, 2019. p. 28-39.
38. BANO, Muneera et al. Teaching requirements elicitation interviews: an empirical study of learning from mistakes. **Requirements Engineering**, v. 24, n. 3, p. 259-289, 2019.
39. FERRARI, Alessio et al. SaPeer and ReverseSaPeer: teaching requirements elicitation interviews with role-playing and role reversal. **Requirements Engineering**, p. 1-22, 2020.