UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

DIEGO MENEGAZZI

Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução

Recife

2021

DIEGO MENEGAZZI

Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre Profissional em Ciência da Computação.

Área de Concentração: Sistemas de Informação

Orientador (a): Carla Taciana Lima Lourenco Silva Schuenemann

Recife

2021

Catalogação na fonte
Bibliotecário Cristiano Cosme S. dos Anjos, CRB4-2290

M541g Menegazzi, Diego
Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução / Diego Menegazzi. – 2021.
111 f.: il., fig., tab.

Orientadora: Carla Taciana Lima Lourenco Silva Schuenemann.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2021.
Inclui referências e apêndices.

1. Sistemas de Informação. 2. Engenharia de requisitos. 3. Engenharia de software. 4. Lei Geral de Proteção de Dados. I. Schuenemann, Carla Taciana Lima Lourenco Silva (orientadora). II. Título.

681.3 CDD (23. ed.) UFPE - CCEN 2021 – 91

Diego Menegazzi

“**Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução**”

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em 26 de fevereiro de 2021.

Aprovado em 26 de fevereiro de 2021.

BANCA EXAMINADORA

_____

Profa. Carina Frota Alves
Centro de Informática / UFPE

_____

Profa. Edna Dias Canedo
Universidade de Brasília

_____

Profa. Carla Taciana Lima Lourenço Silva Schuenemann
Centro de Informática / UFPE
(Orientadora)

Dedico este trabalho a minha família e a minha namorada que foram porto seguro perante as dificuldades durante este percurso.

AGRADECIMENTOS

Agradeço a minha família, principalmente minha mãe Clarisse, meu pai Ivo e meu irmão Felipe pelo incentivo que tive para chegar até aqui. Muitíssimo obrigado por tudo!.

Ao meu amor, Eduarda, pelo apoio, incentivo, pela compreensão e auxílio em todo momento que precisava. Obrigado do fundo do coração!

Aos meus professores do Centro de Informática da UFPE, por toda dedicação e entusiasmo no ensino. Agradecimento especial a minha professora orientadora, Carla Taciana Lima Lourenco Silva Schuenemann, pelos ensinamentos e por me mostrar uma área muito interessante que eu não havia pensado em explorar e que me trouxe grande conhecimento.

A todos os meus colegas e amigos conquistados durante o curso. Em especial, agradeço aos amigos da equipe Tabajara: Carlos, Gustavo, Lucas e Welington, que compartilharam angústias, alegrias, brigas, e também boas risadas durante esta convivência. Obrigado pela grande amizade construída.

Aos meus colegas de trabalho do Instituto Federal Catarinense e à própria instituição pela oportunidade de parceria com a Universidade.

A Universidade Federal de Pernambuco pela oportunidade.

RESUMO

Contexto: Em maio de 2018, entrou em vigor na União Europeia a lei chamada *General Data Protection Regulation* (GDPR), uma versão atualizada de outra lei de privacidade de dados chamada *Data Protection Directive*. A intenção é proteger a privacidade dos dados pessoais dos cidadãos europeus e evitar o vazamento de informações. No Brasil, em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020 e tem como base o GDPR. Segundo a legislação, as organizações públicas e privadas devem seguir regras para a coleta e o tratamento de informações pessoais, de modo que o não cumprimento dessas obrigações pode acarretar multas que chegam a R$ 50 milhões por infração. Motivação: O principal motivo de trabalhar este tema é a relevância, para organizações, da necessidade de conformidade com a lei federal, que, por ser legislação recente, ainda não conta com tantas abordagens teóricas. As organizações públicas e privadas vêm enfrentando dificuldades para conseguir alcançar essa conformidade. Esse problema pode estar associado à interpretação da Lei, muitas vezes ambígua, e pela falta de conhecimento jurídico dos analistas de sistemas. A extração de requisitos e a sua correta interpretação também são passíveis de erros. Esse problema é comum em pequenas e médias empresas que não possuem um setor ou apoio jurídico. Fornecer técnicas e ferramentas para profissionais de Tecnologia da Informação e Comunicação (TIC) que trabalham com privacidade de dados é fundamental para alcançar a conformidade com a LGPD. Objetivo: Diante dos desafios apresentados, propomos um guia de 6 etapas para apoiar os profissionais de TIC nas atividades de conformidade legal por meio de requisitos de negócio e de solução com foco no artigo 6º da LGPD. Método: Em relação aos procedimentos metodológicos, esse trabalho se baseou em um levantamento bibliográfico não exaustivo sobre o tema de conformidade com leis de proteção de dados na Engenharia de Requisitos. O estudo identificou uma lacuna de pesquisa e propôs um guia de conformidade legal de requisitos de negócio com a LGPD, além de avaliar referido guia com potenciais usuários por meio de um questionário distribuído nacionalmente. Resultados: Como resultado e com base na avaliação feita por meio do questionário, os 31 participantes da avaliação responderam que o guia é útil para alcançar a conformidade com a LGPD. Para os participantes, as etapas mais úteis do guia foram a Auditoria de Dados e a Análise de Lacunas. Dos componentes do guia, o mais útil foi o Exemplo de Ilustração de uso, enquanto o mais difícil foi o Catálogo de Controles de Privacidade. Com o guia proposto, espera-se auxiliar

instituições que desejam alcançar a conformidade com a LGPD para que elas não sofram nenhuma sanção da lei.

Palavras-chaves: Engenharia de Requisitos. Engenharia de Software. Lei Geral de Proteção de Dados. Proteção de Dados Pessoais.

ABSTRACT

Context: In May 2018, the General Data Protection Regulation (GDPR) came into force in the European Union, as an updated version of another data privacy law called the Data Protection Directive. The intention is to protect the privacy of European citizens' personal data and prevent information leakage. In Brazil, in August 2018, the General Data Protection Law (LGPD) was sanctioned, which came into force in September 2020 and is based on the GDPR. Public and private organizations must follow rules for the collection and treatment of personal information and failure to comply with these obligations can lead to fines of up to R$ 50 million per violation. Motivation: The main reason for working on this issue is the need to comply with a federal law, as it is a recent law created, there are not many approaches on the subject. Public and private organizations are struggling to achieve compliance with such law. This problem may be associated with the interpretation of the law, which is often ambiguous, and the lack of legal knowledge of systems analysts. The extraction of requirements and their correct interpretation can also be amenable to errors. This is a common problem in small and medium-sized companies that do not have a specialised department or legal support. Providing techniques and tools to Information and Comunication Technology (ICT) professionals who work with and privacy is essential to achieve compliance with LGPD. Objective: Facing these challenges, we propose a 6-step guide to support ICT professionals in legal compliance activities by means of business and solution requirements focused on the on Article 6 of LGPD. Method: Regarding the methodological procedures, this work was based on a non-exhaustive bibliographical search on the subject of compliance with data protection laws in Requirements Engineering. Then, we identified a research gap, proposed a guide for legal compliance of business requirements with LGPD and evaluated this guide with potential users by means of a nationally distributed questionnaire. Results: Based on the assessment made through the questionnaire, the survey included 31 respondents who said that the guide is useful for achieving LGPD compliance. The results were separated between the guide Steps and Components. The most useful steps for the participants were the Data Audit and Gap Analysis. Regarding the components, the most useful was the Illustrative Example and the most difficult was the Privacy Controls Catalog. The proposed guide is expected to assist institutions that need to achieve LGPD compliance so that they do not suffer any sanction from the law.

Keywords: Requirements Engineering. Software Engineering. LGPD. General Data Protection

Law. Protection of Personal Data.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BPMN	*Business Process Model and Notation*
GDPR	*General Data Protection Regulation*
IFC	Instituto Federal Catarinense
IFSC	Instituto Federal de Santa Catarina
LGPD	Lei Geral Proteção de Dados
SGD	Secretaria de Governo Digital
SRS	Especificação de Requisitos de *Software*
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTO

Atualmente, os avanços na tecnologia tornaram possível armazenar e processar praticamente qualquer informação que possa ser de interesse para uma organização, de modo que ela possa fornecer rapidamente seus serviços digitais e físicos para seus clientes (NAMBISAN, 2017). A transformação digital trouxe inúmeras mudanças na forma como a humanidade vive, pois hoje é possível fazer compras, realizar pagamento de contas, estudar, trabalhar, praticar atividades de lazer e muito mais de forma totalmente digital. AGOSTINELLI et al. (2019).

Segundo HARARI (2019), o futuro dos dados é, talvez, uma das mais importantes questões políticas atualmente, porque os dados estão se tornando o capital mais importante do mundo.

Diante dessa transformação digital, existem diversos dispositivos conectados que acompanham nossas rotinas, coletando, transmitindo, armazenando e compartilhando uma quantidade enorme de dados (CUNHA; SANTOS; CARVALHO, 2019). É o caso da socialização *online* por meio dos serviços prestados pela Rede Social Virtual, como *Facebook, Messenger, Instagram, WhatsApp, Google, Twitter, LinkedIn*, entre outros, que transformaram as tendências convencionais de amizade e comunicação.

Recentemente houve diversos casos de violação de privacidade de dados dos usuários em várias plataformas, mas o caso mais famoso aconteceu em 2018, relativo à empresa *Cambridge Analytica*, que expôs 87 milhões de dados pessoais de usuários do *Facebook* e os utilizou para fins políticos. Diante de situações como essa, diversos países tomaram medidas para evitar a violação de dados pessoais e, em maio de 2018, entrou em vigor na União Europeia a lei chamada *General Data Protection Regulation* (GDPR), uma versão atualizada de outra lei de privacidade de dados chamada *Data Protection Directive* [1]. A intenção é proteger a privacidade dos dados pessoais dos cidadãos europeus e evitar o vazamento de informações. No Brasil, em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020 e tem como base a *General Data Protection Regulation* GDPR (2018).

O objetivo da LGPD é regulamentar a manipulação de dados pessoais, trazendo maior segurança e privacidade para as pessoas, prevendo que esses dados possam ser tratados com autorização do proprietário ou se existir uma hipótese legal para o tratamento. O proprietário

[1] https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX%3A31995L0046

do dado tem a permissão de acessar seus dados a qualquer momento, conferir como eles estão sendo tratados, verificar em quais organizações foram compartilhados, solicitar a transferência de dados para outras organizações, solicitar a sua exclusão e até mesmo revogar o seu consentimento de uso. A Lei Geral Proteção de Dados (LGPD) é uma lei que impõe sanções variadas a quem infringir as regras. Inicialmente é dada uma advertência simples, que determina uma data para correção da irregularidade. Multas de até 2% do faturamento líquido da empresa também podem ser aplicadas, não chegando a mais de R$ 50 milhões, havendo a possibilidade também de aplicação de multa diária (BRASIL, 2018).

1.2 MOTIVAÇÃO E JUSTIFICATIVA

No Brasil muitas organizações não estão habituadas a cultura de privacidade de dados e o que a lei está propondo, em muitos casos, altera seus processos e até mesmo o seu modelo de negócio. Alcançar a conformidade com a LGPD tornou-se algo novo e essas organizações vêm enfrentando dificuldades para conseguir alcançar a conformidade.

Várias organizações ainda não iniciaram a sua conformidade com a LGPD e muitas não estão cientes ou não entendem as mudanças que a LGPD trará para seus negócios. Uma pesquisa foi realizada entre junho e julho de 2020 com 400 organizações com atuação no Brasil pela AKAMAI (2019), uma empresa americana de serviços e desempenho de tráfego global na internet. A pesquisa aponta que 64% das empresas não estão em conformidade com a LGPD, 24% estão se adaptando à legislação, 16% ainda não iniciaram o processo, mas sabem da necessidade, e 24% nem sequer sabem do que se trata a legislação. Esse problema está associado à interpretação de leis em geral - que é, muitas vezes, ambígua - e à falta de conhecimento jurídico dos profissionais de Tecnologia da Informação e Comunicação (TIC). Da mesma forma, o processo de entender os requisitos legais geralmente é demorado e complicado, atrasando, assim, sua operacionalização. A extração de requisitos e a sua correta interpretação também são passíveis de erros, um problema que é comum em pequenas e médias organizações que não possuem um setor ou apoio jurídico. Fornecer técnicas e ferramentas para profissionais de TIC que trabalham com privacidade de dados é fundamental para alcançar a conformidade com a LGPD. Por exemplo, a lei diz que as empresas devem utilizar medidas técnicas aptas a proteger os dados contra acessos não autorizados, de situações acidentais ou ilícitas, de destruição, perda, alteração, comunicação ou difusão, mas não deixa evidente como devem ser tomadas essas medidas (BRASIL, 2018).

Diante do exposto, existe a necessidade de ajudar as organizações a atingir a conformidade com a LGPD já que, por ser um tema recente, existem poucas abordagens sobre o assunto, sendo a maioria parte da literatura cinzenta (*Grey literature*). Portanto, esse trabalho pretende responder às seguintes perguntas de pesquisa:

(1) Como analistas de sistemas sem nenhum conhecimento jurídico podem realizar as adequações necessárias em sistemas de software para alcançar a conformidade com a LGPD?

(2) Quais medidas são necessárias para alcançar a conformidade com a LGPD?

1.3 OBJETIVO GERAL

Este trabalho visa definir uma guia para as organizações entenderem as obrigações da LGPD e identificar medidas para alcançar a conformidade dos sistemas de software com a LGPD.

1.3.1 Objetivos Específicos

Este trabalho apresenta os seguintes objetivos específicos:

1. Analisar na literatura possíveis trabalhos relacionados à Engenharia de Requisitos com o tema de conformidade com leis de proteção de dados;
2. Propor um guia para alcançar a conformidade de sistemas de software com a LGPD por meio de Requisitos de Negócio e Requisitos de Solução;
3. Propor um modelo de mapeamento de dados pessoais;
4. Criar um catálogo de controle de privacidade relacionando os princípios da LGPD;
5. Definir um questionário de análise da viabilidade do guia para profissionais de TIC;
6. Aplicar o método proposto para avaliação por parte de profissionais de TIC interessados na conformidade com a LGPD.

1.4 ESTRUTURA DA PESQUISA

Esta dissertação está organizada da seguinte mandeira:

- Capítulo 2 – Fundamentação Teórica: revê conceitos essenciais utilizados ao longo desta pesquisa.
- Capítulo 3 – Guia de Conformidade de Requisitos de Negócio com a LGPD: descrição e utilização do guia e seus componentes. Utilização do guia em um estudo de caso.
- Capítulo 4 - Avaliação do Guia de Conformidade da LGPD: Resultados do guia obtidos por meio do questionário.
- Capítulo 5 – Conclusões e Trabalhos futuros: descreve os resultados obtidos e os trabalhos em andamento.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta conceitos da Engenharia de Requisitos. Além disso, serão apresentados o *General Data Protection Regulation* (GDPR), a Lei Geral de Proteção de dados (LGPD) e conceitos sobre privacidade e proteção de dados.

2.1 ENGENHARIA DE REQUISITOS

O desenvolvimento de software é uma atividade vital para os negócios. Em muitos casos, o sucesso de uma empresa ou organização depende da utilização de softwares que conseguem promover mais eficiência para a empresa (NISTALA; NORI; REDDY, 2019). Entretanto, desenvolver software de qualidade é um grande desafio que as empresas de software enfrentam. O processo de identificar e documentar as funcionalidades que o software conterá exige entender o processo e as demandas da organização e dos usuários. É nessa etapa que entra a Engenharia de Requisitos, uma etapa muito importante da Engenharia de Software (PRESSMAN, 2016).

A Engenharia de Requisitos apareceu pela primeira vez na literatura em 1980. Neste ano, já havia a abordagem relacionada à verificação e à validação, cujo objetivo é assegurar que o software seja adequado e atenda às necessidades que motivaram a sua criação (KAMALRUDIN; SIDEK, 2015). A ausência da Engenharia de Requisitos está entre os principais fatores de falhas em projetos de softwares (LEHTINEN et al., 2014).

Conforme THAYER e DORFMAN (1997), a definição de requisitos se baseia em uma característica do software necessária para atender ou propor uma solução para um problema, visando alcançar o objetivo proposto. Essa característica deve ser realizada ou implementada por um sistema.

2.2 REQUISITOS

Os requisitos variam na intenção e nos tipos de propriedades. Eles podem ser funções, restrições ou outros elementos que devem estar presentes para atender às necessidades das partes interessadas. Os requisitos podem ser descritos como uma condição ou capacidade de que um cliente precisa para resolver um problema ou atingir um objetivo (JACKSON, 1997).

2.3 TIPOS DE REQUISITOS

2.3.1 Domínio do problema

Antes de iniciar o desenvolvimento ou buscar uma solução para um determinando problema de software, é preciso entender o motivo do problema. Na Engenharia de Requisitos, essa abordagem é chamada de entender o domínio do problema (VAZQUEZ; SIMÕES, 2016).

O domínio é uma área em análise. Ela corresponde às fronteiras de unidades organizacionais ou mesmo à organização como um todo; as partes interessadas chave e suas interações com os recursos compreendidos dentro das fronteiras (VAZQUEZ; SIMÕES, 2016).

O domínio do problema delimita o escopo inicial de uma solução em termos de áreas funcionais ou processos de negócio. É nele que estão as partes interessadas chave, que são o ponto de partida para toda a atividade da Engenharia de Requisitos (VAZQUEZ; SIMÕES, 2016).

2.3.2 Requisitos de negócio

Requisitos de negócio são declarações de nível superior de metas, objetivos ou necessidades da empresa. Eles descrevem os motivos pelos quais um projeto é iniciado, os objetivos que o projeto alcançará e as métricas que serão usadas para medir seu sucesso (VAZQUEZ; SIMÕES, 2016).

2.3.3 Requisitos de Usuário

Requisitos de usuário são declarações das necessidades de uma determinada parte interessada. Eles servem como uma ponte entre os Requisitos de Negócios e as várias classes de requisitos de solução (VAZQUEZ; SIMÕES, 2016).

Os requisitos de usuário descrevem os requisitos funcionais e não funcionais de forma compreensível pelos usuários do sistema que não têm conhecimentos técnicos detalhados. Devem especificar somente o comportamento externo do sistema, evitando o quanto for possível as características de projeto do sistema. Podem ser escritos em linguagem natural, como em formulários e diagramas simples e intuitivos. Entretanto, de acordo com SOMMERVILLE (2007), podem surgir alguns problemas quando os requisitos são escritos em linguagem natural:

- Falta de precisão: não é fácil utilizar a linguagem natural de forma precisa e sem ambiguidades sem acarretar em um documento de difícil leitura.
- Confusão de requisitos: os requisitos funcionais e não funcionais, os objetivos do sistema e informações do projeto podem estar descritos de forma obscura.
- Fusão de requisitos: vários requisitos distintos podem ser unificados em um único requisito.

Uma boa pratica é separar os requisitos de usuário dos requisitos de solução. Caso contrário, os leitores podem ser sobrecarregados por detalhes técnicos que não lhes são relevantes.

2.3.4 Requisitos de Solução

Essa categoria de requisitos se caracteriza por descrever as características do produto que atenderão às expectativas e às necessidades de negócio. Os requisitos da solução descrevem as características do sistema de forma a satisfazer os requisitos de negócio e os requisitos de usuário (VAZQUEZ; SIMÕES, 2016).

2.4 FASES DA ENGENHARIA DE REQUISITOS

THAYER e DORFMAN (1997) descrevem a divisão da Engenharia de Requisitos nas seguintes fases (Figura 1).

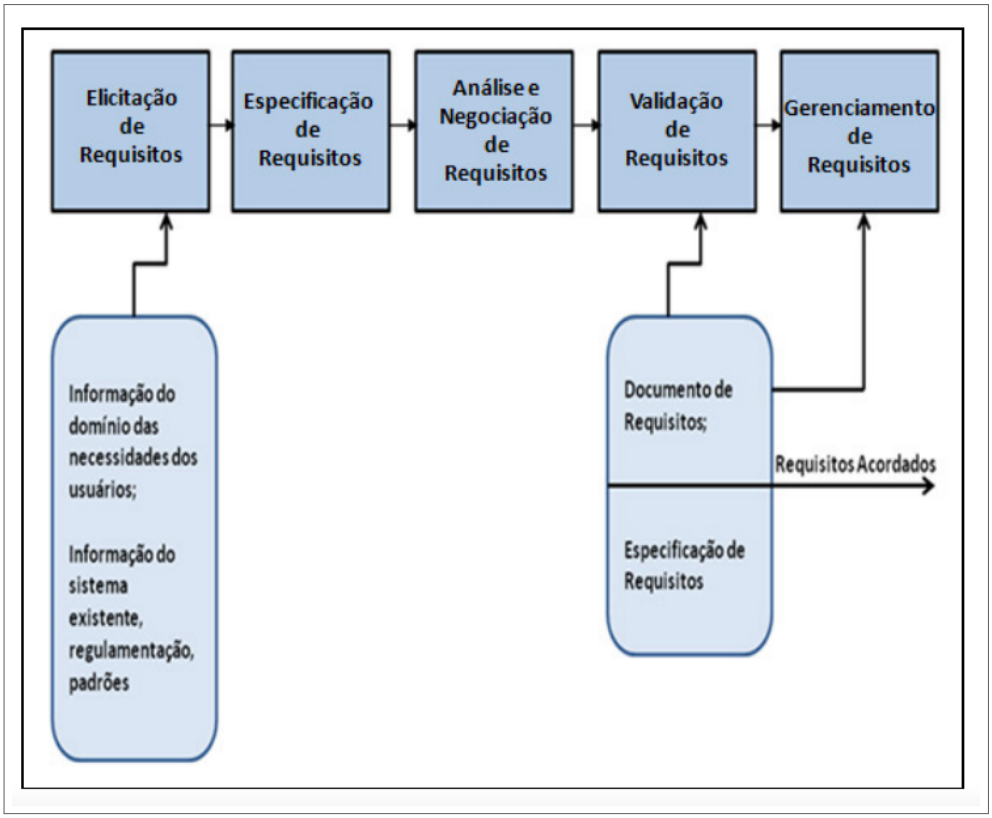
- Concepção: o objetivo é obter uma visão geral do negócio e do sistema. É importante conhecer as expectativas do cliente e das demais partes interessadas. Além disso, é imprescindível compreender qual problema está sendo resolvido com o desenvolvimento do software.
- Elicitação: a elicitação de requisitos tenta descobrir requisitos e identificar completamente as necessidades, os riscos e premissas do negócio associados ao projeto.
- Negociação: a análise de requisitos verifica os requisitos por necessidade, consistência, integridade e viabilidade. Os conflitos entre requisitos são resolvidos por meio de negociação com stakeholders. Resolvidos os conflitos, os requisitos são priorizados para identificar os requisitos críticos.

- Especificação: o objetivo da documentação de requisitos é comunicar requisitos entre as partes interessadas e os desenvolvedores. O documento de requisitos é a linha de base para avaliar produtos e processos subsequentes e para controle de mudanças. Um bom documento de requisitos é inequívoco, completo, correto, compreensível, consistente, conciso e viável. Dependendo da relação cliente-fornecedor, a especificação de requisitos pode fazer parte do contrato.

- Validação: nesta etapa, é realizada a validação do documento de requisitos de software com o usuário. Essa atividade é importante para evitar retrabalho com futuros custos relacionados ao desenvolvimento do software.

- Gerenciamento: permite gerenciar e acompanhar as mudanças que podem ocorrer com os requisitos durante todo o processo de desenvolvimento do software.

Figura 1 – Processo de Engenharia de Requisitos



Fonte: THAYER e DORFMAN (1997)

2.5 CONFORMIDADE LEGAL DE REQUISITOS

A palavra conformidade está ligada ao termo *compliance*, que possui o significado "de acordo com uma ordem, conjunto de regras ou solicitação". Lei é um conjunto de regras e normas que regulamentam determinadas ações dos indivíduos em uma determinada sociedade ou organização. Por sua vez, o termo "conformidade legal"implica em atender às leis estabelecidas por algum órgão, seja ele nacional ou internacional. De acordo com OTTO e ANTÓN (2007), extrair os requisitos legais geralmente é demorado e complicado, pois extrair requisitos de textos legais e interpretá-los adequadamente é um processo complexo e passível de erros.

Os sistemas de software estão cada vez mais sujeitos às leis e regulamentações. Para desenvolver um sistema em conformidade legal, os engenheiros de software precisam interpretar - normalmente em colaboração com especialistas jurídicos - os textos jurídicos relevantes e, a partir deles, extrair os requisitos legais que o sistema em desenvolvimento deve cumprir (AKHIGBE; AMYOT; RICHARDS, 2019).

A conformidade legal tem sido um tópico ativo em Engenharia de Software e Sistemas de Informação por muitos anos, porém, apenas recentemente, analistas de negócio começaram a explorar técnicas de Engenharia de Requisitos para alcançar a conformidade legal. Tais técnicas são baseadas em linguagem natural, como anotações semânticas, o uso de programação lógica ou o uso da Taxonomia (AKHIGBE; AMYOT; RICHARDS, 2019).

2.6 PRIVACIDADE

A privacidade é o direito de um cidadão ser deixado sozinho, ou livre de interferência ou intrusão (WARREN; BRANDEIS, 1890). Privacidade de dados é o direito de um cidadão ter controle sobre como suas informações pessoais são coletadas e usadas (GONÇALVES, 2012). A proteção de dados é um subconjunto da privacidade. Esses são direitos bastante relevantes porque proteger os dados pessoais e informações confidenciais é o primeiro passo para manter a privacidade dos dados do indivíduo (KALLONIATIS, 2017). Além disso, a privacidade de dados descreve práticas que garantem que os dados compartilhados por um indivíduo sejam usados apenas para os fins pretendidos. Em um mundo com montanhas cada vez maiores de dados coletados e manipulados, a privacidade é um tópico cada vez mais investigado (PEIXOTO; SILVA, 2018).

Como proteção de dados pessoais entende-se a possibilidade de cada cidadão determinar,

de forma autônoma, qual será a utilização de seus próprios dados, em conjunto com o estabelecimento de uma série de garantias para evitar que estes dados pessoais sejam utilizados de forma a causar discriminação ou danos de qualquer espécie ao cidadão ou à coletividade (PINHEIRO, 2019).

2.7 *GENERAL DATA PROTECTION REGULATION* (GDPR)

O Regulamento Geral de Proteção de Dados, conhecido também como GDPR (2018), é a nova Lei da União Europeia para a proteção de dados pessoais. A GDPR define dados pessoais como qualquer informação que identifique uma pessoa. Isso significa que o titular de dados é uma pessoa física natural cujos dados são gerenciados por um controlador de dados. O regulamento entrou em vigor em maio de 2018 e substitui a anterior diretiva relacionada à proteção de dados do ano de 1995. Os objetivos do novo regulamento são fortalecer os direitos dos cidadãos sobre seus próprios dados e tornar as organizações mais responsáveis. Além disso, a GDPR eliminará burocracias nos serviços prestados na União Europeia, a fim de melhorar oportunidades e negócios no meio digital. A referida legislação contribui, ainda, no aperfeiçoamento das leis anteriores sobre proteção de dados, garantindo igualdade dos direitos humanos sobre seus dados. A GDPR está dividida em duas partes: a primeira é composta por 173 considerações que explicam a motivação do regulamento e seus objetivos pretendidos, enquanto a segunda é composta por 99 artigos que representam normativas a serem seguidas. O regulamento é aplicado em ambientes automatizados ou não e define os seguintes princípios sobre o tratamento de dados:

- Legalidade, justiça e transparência: os dados devem ser processados de maneira justa, legal e transparente em relação ao titular dos dados;
- Limitação da finalidade: os dados devem ser coletados para fins específicos, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses fins;
- Minimização de dados: os dados processados devem ser adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados;
- Precisão: os dados processados devem ser precisos e, quando necessário, atualizados. Devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais

inexatos sejam apagados ou retificados, tendo em conta as finalidades para que são tratados;

- Limitação de armazenamento: os dados devem ser mantidos em uma forma que permita a identificação dos seus titulares por tempo não superior ao necessário para as finalidades do processamento desses dados pessoais;
- Integridade e confidencialidade: os dados podem ser processados de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, utilizando medidas técnicas ou organizacionais adequadas;
- Responsabilização: O responsável pelo tratamento deve ser diligente e capaz de comprovar o cumprimento do disposto no artigo 5º.

2.8 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Após anos de debate, com base na GDPR, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18) foi sancionada em agosto de 2018. A LGPD determina como os dados pessoais devem ser tratados e tem como objetivo garantir a transparência no uso de dados de pessoas físicas. O prazo de conformidade foi até agosto de 2020. A lei se aplica a qualquer pessoa física ou jurídica de direito privado ou público, que realize algum tipo de tratamento de dados pessoais, seja por meio digital ou físico. Podemos concluir, então, que a lei possui aplicação ampla e abrangente, uma vez que abarca grande parte dos projetos e atividades do cotidiano empresarial e público. Embora o Brasil não possua um histórico com grandes evoluções sobre proteção de dados, a LGPD é um marco importante para o país, pois ela se alinha às legislações internacionais de nível elevado referentes a países que possuem várias regulamentações sobre o assunto. A lei é importante para o Brasil porque gera maior segurança jurídica, atrai investimentos do exterior e promove mais segurança e privacidade aos cidadãos. É, portanto, crucial entender os conceitos relevantes desta nova norma para compreensão dos seus impactos na prática. BRASIL (2018)

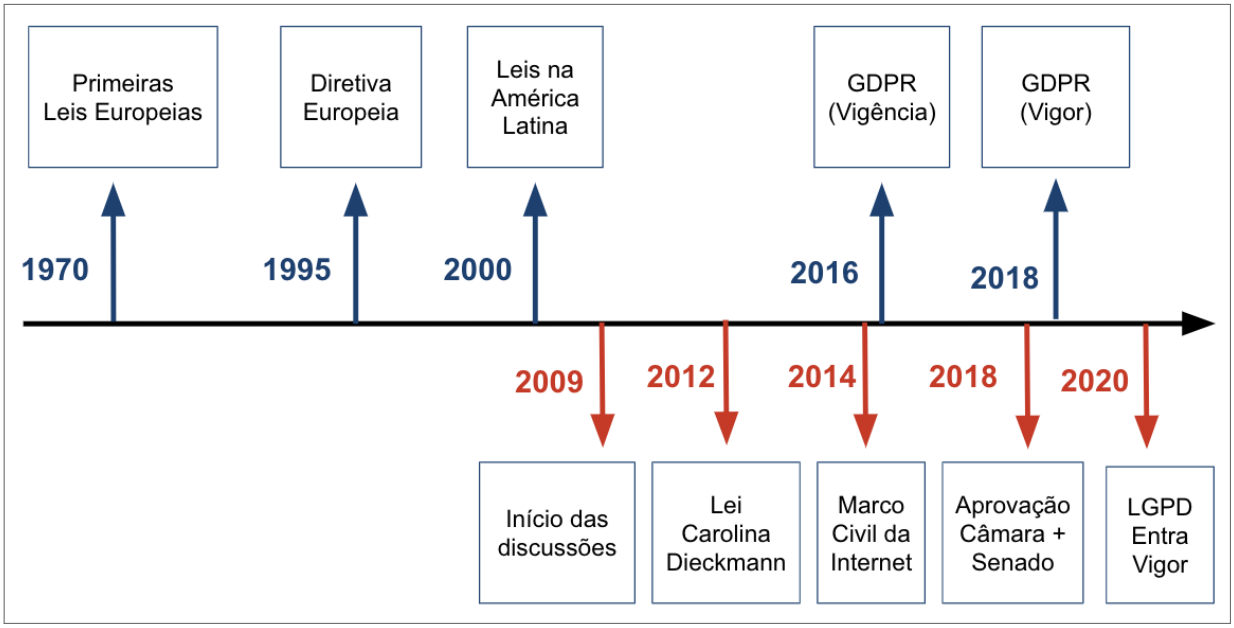
Os seguintes princípios devem ser observados na hora de tratar dados pessoais:

- I - Finalidade específica e informada explicitamente ao titular;
- II - Adequação à finalidade previamente acordada e divulgada;

- III - Necessidade de tratamento limitado de dados essenciais para alcançar a finalidade inicial;
- IV - Acesso livre, fácil e gratuito das pessoas à forma como seus dados são tratados;
- V - Qualidade dos dados, que devem ser precisos e atualizados de acordo com a real necessidade no tratamento;
- VI - Transparência ao titular, com informações claras e acessíveis sobre o tratamento dos seus dados e sobre os responsáveis pelo tratamento;
- VII - Segurança para coibir situações acidentais ou ilícitas como invasão, destruição, perda ou difusão;
- VIII - Prevenção contra danos ao titular e aos demais envolvidos;
- IX - Não discriminação ou seja, não permitir atos ilícitos ou abusivos;
- X - Responsabilização do agente, que fica obrigado a demonstrar a eficácia das medidas adotadas.

Abaixo, a Figura 2 retrata uma linha temporal relativa às leis de privacidade de dados no Brasil, na Europa e na América Latina. Pode-se observar que, em 1970, a Europa regulamenta suas primeiras leis de privacidade e, no ano de 1995, cria as diretivas. Em 2000, na América Latina, alguns países também criaram suas próprias leis relativas aos dados. Em 2016, foi aprovada a GDPR, que substituiu as diretivas de 1995 e entrou em vigor em 2018. As informações em vermelho se referem ao Brasil. Em 2009, já havia discussões sobre a criação de leis de privacidade e, em 2012, foi criada a Lei Carolina Dieckmann, que versava sobre crimes de invasão em dispositivos de informática. Dois anos depois, foi aprovado o Marco Civil da Internet, que fez referência à proteção de privacidade em um de seus artigos. No entanto, somente em 2018 foi aprovada, no Congresso Nacional, a criação da LGPD, que entrou em vigor em 2020.

Figura 2 – Linha do tempo



Fonte: Elaborada pelo Autor (2020).

2.9 TRABALHOS RELACIONADOS

Na época da entrada em vigor da lei, pouco havia sido tratado sobre como auxiliar as organizações a alcançar a conformidade legal. Diversos pesquisadores e profissionais, então, passaram a investigar diferentes soluções ou abordagens para que as organizações públicas ou privadas pudessem se adequar às leis de proteção de dados. Essas abordagens compreendem guias, roteiros, modelos de processos, *software* ou soluções de mapeamento de dados. Alguns desses trabalhos focados no entendimento do impacto da LGPD e no auxílio às organizações serviram de referência e inspiração para a proposta apresentada na presente pesquisa.

AYALA-RIVERA e PASQUALE (2018) propuseram o *GuideMe*, um guia contendo seis etapas que suporta a elicitação de requisitos de solução vinculados às obrigações da GDPR. O guia visa auxiliar as organizações a entender as obrigações da GDPR e identificar medidas para garantir a conformidade legal por meio da utilização de controles de privacidade que devem ser implementados nos sistemas de software da organização. O trabalho trata basicamente da legislação de proteção de dados da União Europeia, que, apesar de ser muito semelhante à LGPD do Brasil, possui algumas diferenças que precisam ser observadas. A presente dissertação propõe um guia de conformidade com a LGPD adaptado do *GuideMe*.

RINGMANN, Langweg e Waldvogel (2018) utilizaram um método chamado *KORA*, por meio do qual foi possível identificar 74 requisitos técnicos genéricos reutilizáveis para a GDPR.

Tais requisitos podem ser aplicados em softwares que utilizam dados pessoais. Porém, segundo os autores, como o escopo do artigo foi limitado, não foi aplicado o método utilizando dados pessoais de menores de idade e nem as categorias especiais da GDPR (dados sensíveis), como origem racial, orientação sexual, opiniões políticas, dados sobre a saúde, entre outros. Outra consideração feita pelos autores é referente ao fato de que não foram consultados especialistas da área, principalmente da área do Direito, para saber se os requisitos estavam de acordo com a GDPR.

HJERPPE, RUOHONEN e LEPPÄNEN (2019) apresentam um estudo de caso sobre a implementação de requisitos legais extraídos da GDPR em uma empresa de *software* de médio porte da Finlândia. O escopo do artigo é restrito à arquitetura de *software* em geral e às Arquiteturas Orientadas a Serviço. Este trabalho focou em descobrir as principais implicações da GDPR para o desenvolvimento de *software*, identificando novas restrições práticas fundamentadas em três categorias: negócios, infraestrutura e restrições de engenharia de software.

PIRAS et al. (2019) apresentam a plataforma *DEFeNDA* que visa guiar as organizações no cumprimento da conformidade com a *General Data Protection Regulation* (GDPR) por meio da *privacy by design* e no suporte ao gerenciamento de consentimento, à análise de privacidade, à avaliação de risco de segurança e ao gerenciamento de violação de dados. O referido trabalho apresentou, além da metodologia de engenharia de *software*, os passos seguidos para capturar as necessidades dos usuários e modelar os requisitos de *software* para o desenvolvimento da plataforma de conformidade com GDPR. Sua aplicação foi realizada no setor financeiro de uma organização.

FERNANDES et al. (2018) apresentam uma metodologia para elaborar um catálogo reutilizável de especificação de requisitos de dados pessoais. A abordagem consiste em uma análise de requisitos legais da GDPR para tratar padrões e estilos linguísticos na especificação de requisitos que são extraídos da lei. Este catálogo deve servir ao propósito de implementação em sistemas de informação que processam dados pessoais.

CANEDO et al. (2020) realizaram uma revisão sistemática da literatura para identificar trabalhos relacionados à privacidade de *software* e aos requisitos de privacidade, elencando as metodologias e técnicas usadas para especificá-los. Além disso, os autores realizaram pesquisas qualitativas com profissionais de Tecnologia da Informação e Comunicação (TIC) na indústria de desenvolvimento de *software* para identificar a percepção desses profissionais em relação à privacidade. Em seus resultados, os autores mostram que a maioria dos profissionais de TIC não tem conhecimento abrangente dos requisitos de privacidade e, ainda, declara não

deter conhecimento necessário para implementar os princípios de privacidade e as diretrizes da LGPD.

ARAÚJO (2020) também propõe um método para obter a conformidade dos processos de negócio em relação à LGPD. Seu método consiste em um catálogo de padrões de modelagem. Para representar sua modelagem, foi utilizada a notação *Business Process Model and Notation* (BPMN). O estudo foi avaliado e validado por meio de um questionário respondido por uma turma de pós-graduação na Universidade Federal de Pernambuco (UFPE). O método, chamado de BPMN4LGPD orienta os analistas na avaliação da conformidade dos processos de negócio com a LGPD. Os resultados da avaliação demonstraram que a modelagem do processo de negócio é a etapa mais difícil.

RIBEIRO e CANEDO (2020) propõem utilizar o processo de Análise de Decisão de Múltiplos Critérios (MCDA) para selecionar as melhores alternativas de critérios de segurança de dados pessoais em conformidade com LGPD na Universidade de Brasília (UnB). Nos resultados, os autores mostram que o critério de riscos de privacidade de dados é prioritário na implementação da segurança de dados pessoais na UnB. Além disso, verificou-se que os princípios da LGPD com maior prioridade de implementação foram Segurança Prioritária (0,28), Necessidades Prioritárias (0,26) e Prevenção Prioritária (0,25).

ROJAS e MEDEIROS (2021), por sua vez, realizaram um estudo para identificar a aplicação da LGPD no Instituto Federal de Santa Catarina (IFSC). Na avaliação da conformidade da instituição, a pesquisa mostrou que o IFSC está no estágio inicial de adequação dos seus processos e sistemas. Para realizar a avaliação, foi elaborado um questionário e realizada uma entrevista com a equipe de Tecnologia da Informação (TI). Apesar de identificar que o processo de conformidade com a LGPD no IFSC está em fase inicial, as perguntas foram feitas apenas à equipe de TI, enquanto a LGPD envolve pessoas que trabalham com processos do dia a dia, além do próprio jurídico da instituição. Além disso, o trabalho não aponta quais medidas a instituição deve tomar para fazer as devidas adequações com a LGPD.

A Tabela 1 apresenta os principais trabalhos relacionados ao Regulamento Geral de Proteção de Dados (GDPR), enquanto a Tabela 2 apresenta os trabalhos relacionados à LGPD.

Tabela 1 – Principais trabalhos relacionados ao GDPR

Critérios	**Avaliação de Diagnóstico da Conformidade**	**Orientação para Alcançar a Conformidade**	**Orientação do Mapeamento de Dados Pessoais**	**Avaliação da Abordagem**
AYALA-RIVERA E PASQUALE (2018)	Aplicado um questionário	Não se aplica	Formulário + Entrevista	Questionário (Survey)
RINGMANN E WALDVOGEL (2018)	GuideMe	Não se aplica	Não se aplica	Não se aplica
HJERPPE E LEPPÄNEN (2019)	Não se aplica	Não se aplica	Não se aplica	Teoria Fundamentada
PIRAS et al. (2019)	Não se aplica	Não se aplica	Não se aplica	Não se aplica
FERNANDES et al. (2018)	Não se aplica	Catálogo de especificação de requisitos	Não se aplica	Não se aplica
TRABALHO PROPOSTO	Aplicado um questionário	Guia de 6 etapas	Formulário + Entrevista	Questionário (Survey)

Fonte: Elaborada pelo autor (2020)

Tabela 2 – Principais trabalhos relacionados à LGPD

Critérios	**Avaliação de Diagnóstico da Conformidade**	**Orientação para Alcançar a Conformidade**	**Orientação do Mapeamento de Dados Pessoais**	**Avaliação da Abordagem**
CANEDO et al. (2020)	Não se aplica	Não se aplica	Não se aplica	Pesquisa (Survey)

ARAÚJO (2020)	Questionário	LGPD4BP	BPMN	Questionário (Survey)
RIBEIRO e CANEDO (2020)	Não se aplica	Não se aplica	Não se aplica	Não se aplica
ROJAS e MEDEIROS (2021)	Entrevista	Não se aplica	Não se aplica	Questionário + Entrevista
TRABALHO PROPOSTO	Aplicado um questionário	Guia de 6 etapas	Formulário + Entrevista	Questionário (Survey)

Fonte: Elaborada pelo autor (2020)

2.9.1 Considerações finais do capítulo

Este capítulo apresentou a fundamentação teórica e os trabalhos relacionados. A maioria das organizações públicas e privadas vem encontrando dificuldades em alcançar a conformidade da LGPD e muitas não sabem como começar, como é o caso do Instituto Federal Catarinense, que está buscando orientações para iniciar o processo. Diante desse cenário, a presente dissertação propõe a criação de um passo a passo ou roteiro com orientações para as organizações. A partir das pesquisas na literatura disponível, foi identificado o trabalho de Ayala-Rivera e Pasquale (2018), referente à criação de um guia para alcançar a conformidade de requisitos de software ao Regulamento Geral de Proteção de Dados, a legislação europeia. Tomando este trabalho como referência, foi possível criar um guia de conformidade para a LGPD.

3 GUIA DE CONFORMIDADE DE REQUISITOS DE NEGÓCIO COM A LGPD

3.1 METODOLOGIA DE PESQUISA

Em relação aos procedimentos metodológicos, esse trabalho se baseou em um levantamento bibliográfico não exaustivo sobre o tema de conformidade com leis de proteção de dados na Engenharia de Requisitos. Identificada uma lacuna de pesquisa, o trabalho propôs um guia de conformidade legal de requisitos de negócio com a LGPD e avaliou este guia com potenciais usuários por meio de um questionário distribuído nacionalmente.

Uma vez definidas as questões de pesquisa, foi utilizada a metodologia proposta por GLASS (1995). Este método de pesquisa é dividido nas fases informativa, proposicional, analítica, avaliativa e de transferência de tecnologia. Ressalta-se que nem todas as fases são encontradas em cada estudo de pesquisa, e a última fase, em especial, é típica apenas de pesquisas construtivas, portanto não foi aplicada neste trabalho.

3.1.1 Fase Informativa

Essa fase pode ser usada para coletar informações sobre a caracterização de práticas, experiências e problemas atuais. Durante a revisão bibliográfica, foram encontradas poucas abordagens sobre o assunto da LGPD e a maioria fazia parte da literatura cinzenta (*Grey Literature*). Foi, ainda, realizado um levantamento de trabalhos que abordassem especificamente a conformidade com leis de proteção de dados na Engenharia de Requisitos, a partir do qual foi possível identificar uma lacuna de pesquisa que motivou a proposta de criação de um guia de conformidade legal de requisitos de negócio e de solução com foco no artigo 6º da LGPD.

3.1.2 Fase Analítica

Essa fase consiste em analisar os artefatos selecionados na fase informativa. A análise foi realizada em trabalhos relacionados ao alcance da conformidade com a GDPR ou com a LGPD. Com base nos trabalhos analisados, foi realizado um estudo aprofundado do *GuideMe* (AYALA-RIVERA; PASQUALE, 2018), um guia criado para alcançar a conformidade legal de requisitos de software com a GDPR.

3.1.3 Fase Proposicional

Essa fase consiste em propor modelos, teorias ou protótipos que possam ser submetidos à opinião de profissionais e potenciais usuários, objetivando a obtenção de feedback antecipado. Foi proposto, então, um guia de seis etapas adaptado do *GuideMe* (AYALA-RIVERA; PASQUALE, 2018). As etapas do guia proposto para alcançar a conformidade com a LGPD são:

1. Auditoria de dados: Essa etapa requer a realização de uma auditoria de informações para avaliar quais dados pessoais uma organização trata, onde se originam, como são obtidos, como são processados e sob quais bases legais, além de onde são armazenados e com quem os dados são compartilhados;

2. Análise de Lacunas: Essa etapa requer a realização de uma análise realizada na primeira etapa de auditoria de dados para identificar as áreas (por exemplo, fluxos, processos, sistemas) que precisam ser aprimoradas por meio de ações corretivas. Em outras palavras, essa atividade permite focar em quais princípios da LGPD o sistema não atende. Para avaliar a conformidade do sistema aos princípios, foram utilizados requisitos de negócios;

3. Planejamento e preparação: Com base nas lacunas identificadas, é necessário obter requisitos de solução que determinem quais controles de privacidade são necessários para satisfazer obrigações legais específicas. Também devem ser desenvolvidos planos para incorporar controles de privacidade nos sistemas de software da organização;

4. Revisão do Plano de Ação: Nessa etapa, todas as principais partes interessadas revisam o plano preparado para a conformidade com a LGPD, considerando quaisquer efeitos colaterais que as mudanças planejadas possam trazer para os processos de negócios;

5. Execução: Depois que os requisitos da solução são especificados e aprovados durante a análise de lacunas, os profissionais de TI (por exemplo, engenheiros de software) podem começar a implementar os controles de privacidade indicados nos requisitos da solução;

6. Revisão pós-implementação: Finalmente, a organização precisa garantir que todos os requisitos de solução presentes no guia sejam atendidos. Essa garantia pode ser alcançada por meio da avaliação, por especialistas em TI, Direito e conformidade, dos processos e procedimentos da organização. Além disso, auditorias regulares devem ser agendadas periodicamente para identificar os requisitos de solução que podem precisar de revisão.

Neste trabalho, foram definidas 6 etapas, com base no trabalho de Ayala-Rivera e Pasquale (2018), que possui a mesma quantidade de etapas. Para auxiliar o entendimento do guia, foi desenvolvido um website (MENEGAZZI, 2020) contendo uma seção com as etapas para a conformidade da LGPD e apresentando um exemplo ilustrativo da aplicação do guia em um sistema de processo seletivo de ingresso dos estudantes do Instituto Federal Catarinense (IFC). Além disso, o guia possui componentes necessários para a execução das etapas, os quais incluem o modelo de mapeamento de dados, os requisitos de negócio, os requisitos de solução e o catálogo de controles de privacidade. O guia contém, ainda, um vídeo explicativo sobre a execução das etapas e o uso dos componentes.

3.1.4 Fase Avaliativa

Para realizar a avaliação do guia, foi utilizado um questionário distribuído nacionalmente a ser respondido por meio eletrônico através de um formulário *Google Forms*. Após ler as etapas do website, o participante poderia começar a responder o questionário. O referido questionário pode ser consultado no Apêndice D.

- A etapa de auditoria é uma das fases fundamentais, pois é preciso saber quais dados pessoais a organização trata. Nesta etapa, foi desenvolvido um modelo inicial de mapeamento de dados, que consiste em avaliar quais dados pessoais uma organização está tratando, quais categorias de dados estão sendo coletadas, com quem os dados são compartilhados, como são armazenados e sob quais bases legais os dados são coletados e manipulados. Esse processo é realizado por meio de entrevista com a pessoa responsável pelo setor que manipula os dados.
- Na segunda etapa, foi produzido um formulário para ajudar o analista de sistema a identificar quais princípios o seu sistema não atendia. Foram realizados testes com alguns desenvolvedores no IFC para verificar se o formulário cumpria os requisitos necessários.

3.2 O GUIA

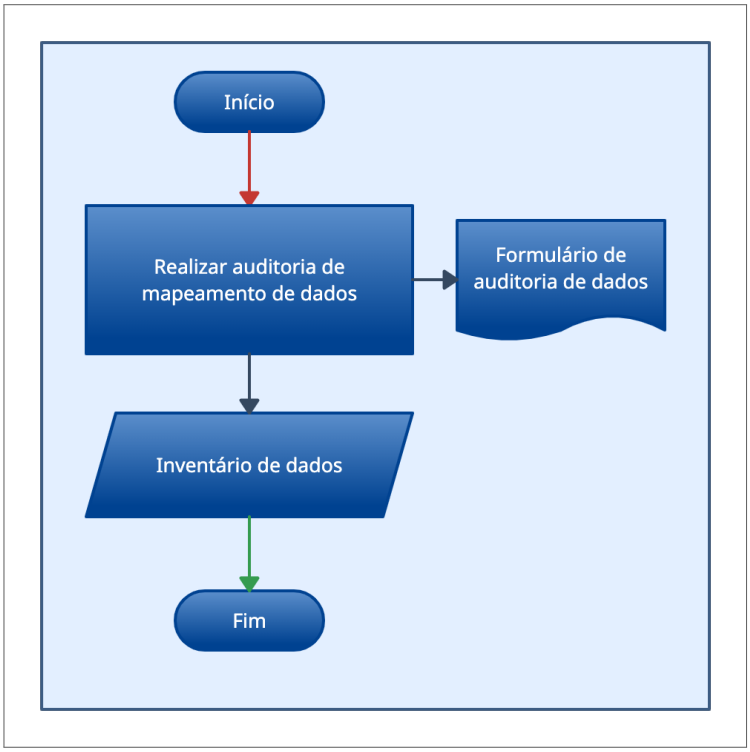
O guia proposto nesta pesquisa pode ser aplicado em sistemas que já estão em modo de produção - ou seja, que já estão sendo utilizados por seus usuários - ou para novos sistemas que precisam ser desenvolvidos. As etapas do guia são: Auditoria de Dados, Análise

de Lacunas, Planejamento e Preparação, Revisão do Plano de Ação, Execução e Revisão Pós-implementação. Para apoiar a execução das etapas, foram definidos alguns componentes: Modelo de Mapeamento de Dados, Requisitos de Negócio, Requisitos de Solução e Catálogo de Controles de Privacidade. A próxima seção explica o uso dos componentes em cada etapa e demonstra o exemplo de uso do guia no sistema de processo seletivo do Instituto Federal Catarinense.

3.2.1 1ª Etapa - Auditoria de Dados

Nesta etapa, é realizado o mapeamento de dados, que ocorreu por meio de entrevista com a pessoa responsável pelo setor que manipula os dados. Para auxiliar na coleta de informações, foi utilizado um modelo de mapeamento de dados (Apêndice C) construído a partir da experiência em entrevistas realizadas na instituição e do modelo disponibilizado pela Secretaria de Governo Digital (SGD). A Figura 3 apresenta o fluxo do processo de auditoria de dados, cuja primeira atividade é utilizar o modelo de mapeamento. Em seguida, é realizada a entrevista com os *stakeholders* e, como resultado, é obtido um inventário de dados que será utilizado na segunda etapa do guia.

Figura 3 – Fluxo da Etapa de Auditoria de dados

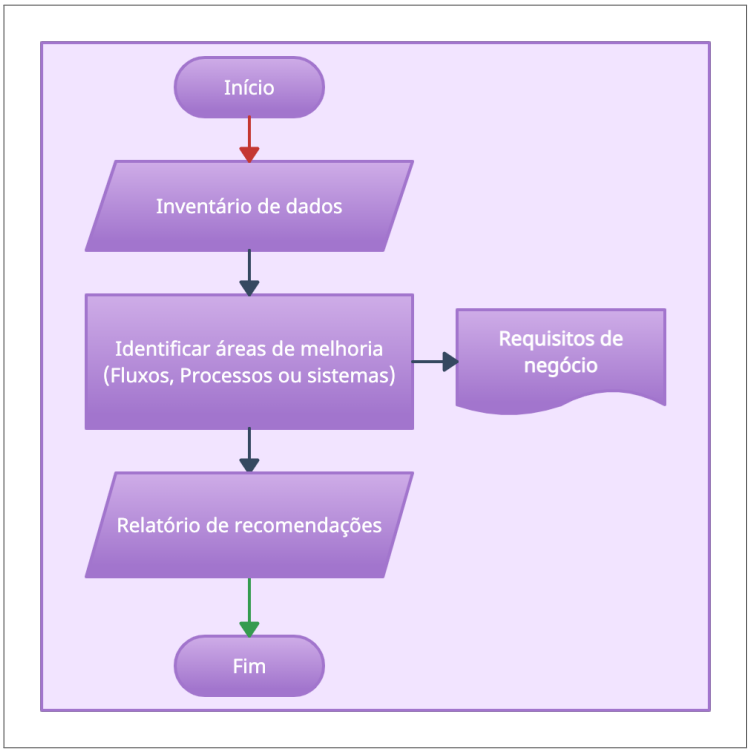


Fonte: Elaborada pelo Autor (2020).

3.2.2 2ª Etapa - Análise de Lacunas

Esta etapa requer a realização de uma análise do mapeamento de dados realizado na primeira etapa, objetivando identificar áreas (por exemplo, fluxos, processos, sistemas) que precisam ser aprimoradas por meio de ações corretivas ou preventivas. Em outras palavras, essa atividade permite focar nos princípios da LGPD com os quais o sistema não está em conformidade. Para ajudar nesse processo, o analista de sistemas deve usar os requisitos de negócio para identificar as lacunas. O profissional deve, ainda, responder o questionário (Apêndice E) e, assim, com base na sua experiência com o sistema, será possível identificar as violações dos princípios. Na Figura 4, é apresentado o fluxo do processo de Análise de Lacunas. Uma vez realizada a primeira etapa, o artefato de inventário de dados é analisado quanto ao cumprimento aos dez princípios da lei. Para apoiar esse processo, são utilizados os requisitos de negócio, componentes do guia. Após a identificação das melhorias necessárias ao sistema, elas serão comunicadas aos stakeholders e, como resultado dessa etapa, é gerado um relatório de recomendações de ajustes necessários para atender aos princípios da lei.

Figura 4 – Fluxo da Etapa de Análise de Lacunas

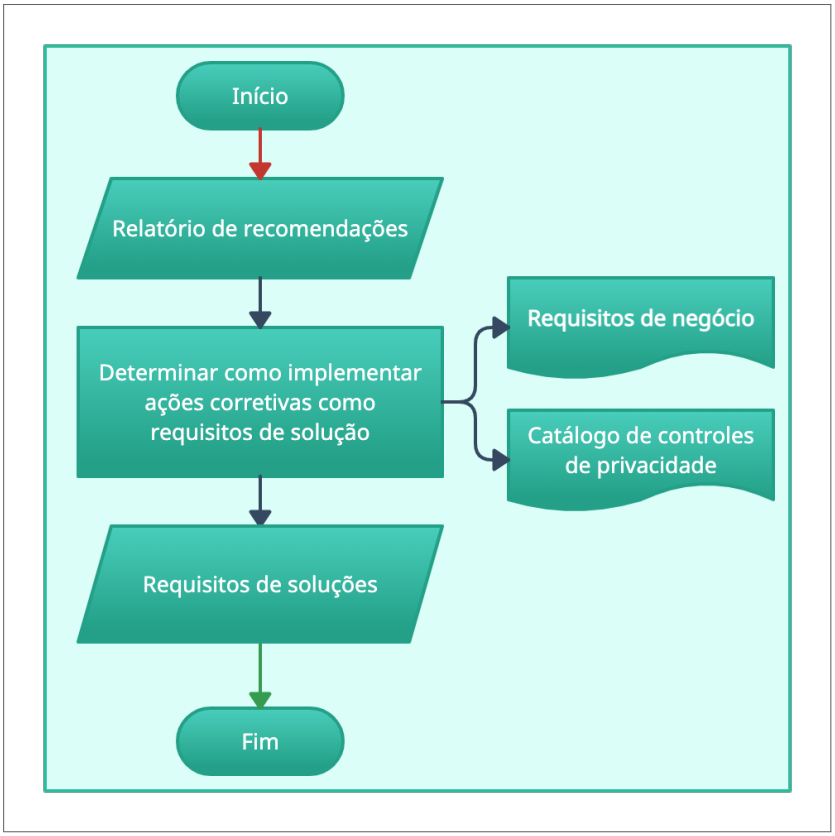


Fonte: Elaborada pelo Autor (2020).

3.2.3 3ª Etapa - Planejamento e Preparação

Nesta etapa, será realizado o planejamento para solucionar os problemas identificados na segunda etapa. A Figura 5 apresenta o fluxo do processo de Planejamento e Preparação. Para resolver as violações dos princípios da LGPD, são observados os requisitos de negócio, as recomendações de alterações indicadas na segunda etapa e é utilizado o catálogo de controle de privacidade (Apêndice A), necessário para satisfazer obrigações legais específicas. Do processo resultam os requisitos de solução, que apoiarão a quarta etapa do guia.

Figura 5 – Fluxo da Etapa de Planejamento e Preparação



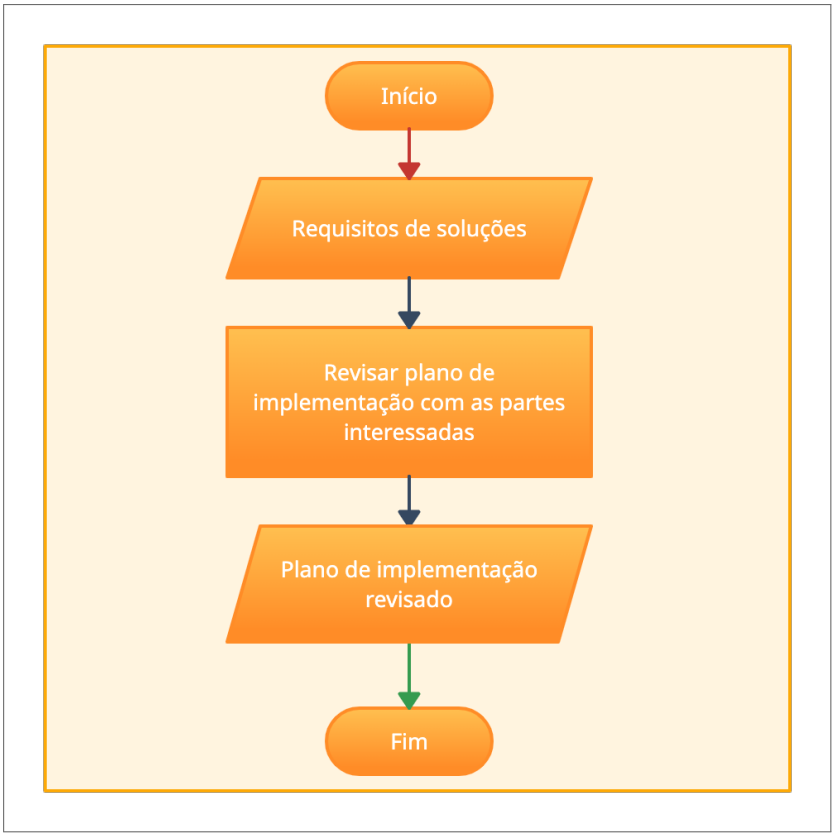
Fonte: Elaborada pelo Autor (2020).

3.2.4 4ª Etapa - Revisão do Plano de Ação

Nesta etapa, todos os *stakeholders* revisam o plano de ação elaborado na terceira etapa. A revisão antes da execução é necessária, pois é preciso avaliar se as mudanças afetarão o funcionamento do negócio ou do sistema. Embora os controles de privacidade listados no catálogo forneçam um conjunto de mecanismos que já se provaram úteis, conforme estudado na

literatura, eles não são a única maneira de satisfazer um requisito de privacidade. Portanto, as partes interessadas devem avaliar os prós e contras dos controles de privacidade sugeridos, de modo a selecionar um ou mais, dependendo sempre do cenário. Por exemplo, como sugestão para atender o princípio da responsabilização e prestação de contas, é recomendado que a organização implemente o registro de logs no sistema, porém, dependendo da situação, a organização não tem colaboradores suficientes para desenvolver ou implementar essa funcionalidade, de modo que é necessário que ela procure alternativas para cumprir o princípio. Na Figura 6, é apresentado o fluxo do processo de Revisão do Plano de Ação, cuja primeira atividade é utilizar os requisitos de solução. É preciso, então, revisar esses requisitos com os *stakeholders*, para que se tenha certeza de que as medidas não afetarão o desempenho ou as funcionalidades do sistema.

Figura 6 – Fluxo da Etapa de Revisão do Plano de Ação

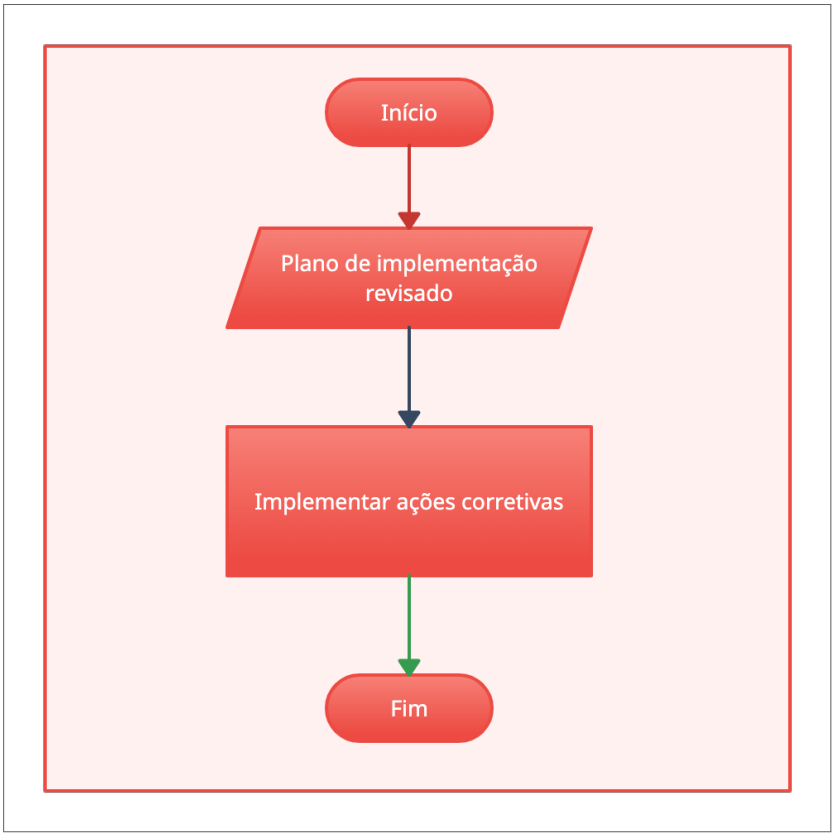


Fonte: Elaborada pelo Autor (2020).

3.2.5 5ª Etapa - Execução

Nesta etapa, após a análise feita pelos *stakeholders* e os requisitos de solução terem sido especificados e aprovados para o cenário em questão, a equipe de desenvolvimento de *software* deve realizar a implementação das soluções definidas. Nesta etapa, caso a organização possua profissionais de Direito e/ou Privacidade, é importante que eles façam o acompanhamento das implementações das soluções para contribuir no processo de validação dos controles de privacidade escolhidos. O processo pode ser acompanhado na Figura 7.

Figura 7 – Fluxo da Etapa de Execução



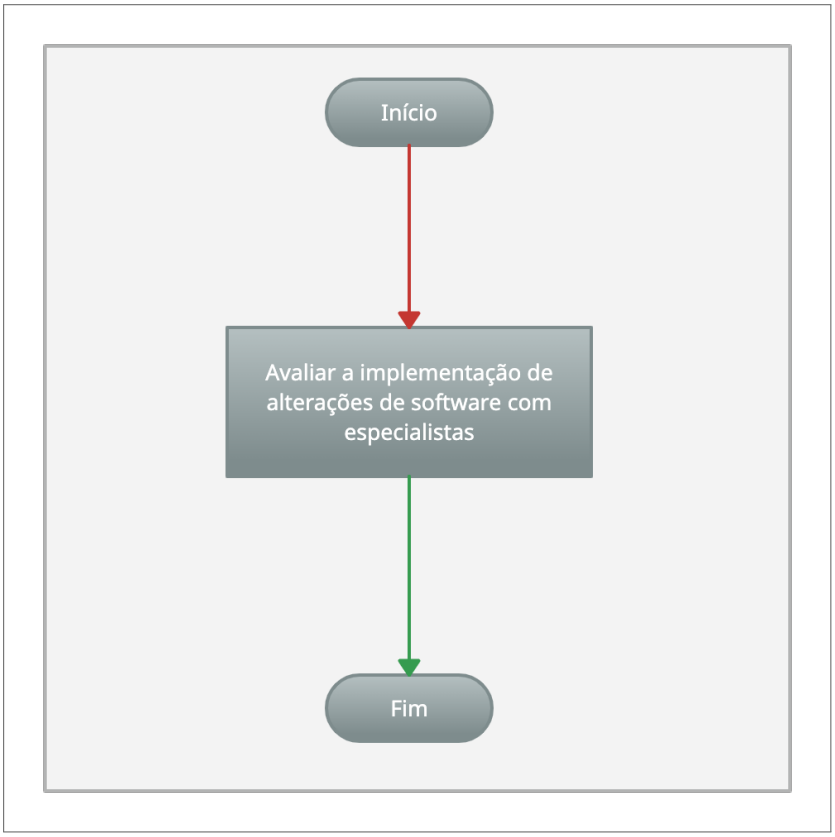
Fonte: Elaborada pelo Autor (2020).

3.2.6 6ª Etapa - Revisão Pós-implementação

Finalmente, as organizações precisam garantir que todos os requisitos da solução foram atendidos. Isso pode ser verificado por meio da avaliação de processos e procedimentos com especialistas em TI, Direito e conformidade. Além disso, auditorias regulares devem ser agendadas para identificar os requisitos de solução que podem precisar de revisão. Na Figura 8, é

apresentada a última etapa do guia.

Figura 8 – Fluxo da Etapa de Revisão Pós-implementação



Fonte: Elaborada pelo Autor (2020).

3.3 REQUISITOS DE NEGÓCIOS

Requisitos de Negócio - que podem ser chamados de Regras de Negócio - têm como função restringir algo e devem ser suficientemente claros para que a implementação das regras tenha sucesso nos resultados (SRIGANESH; RAMANATHAN, 2012). A LGPD possui diversas regras que a organização precisa seguir. Extrair essas regras ou esses requisitos de um texto legal e interpretá-los adequadamente é um processo complexo e passível de erros. A origem da maioria dos problemas está na natureza vaga, ambígua e detalhada da lei. Para tornar os princípios da LGPD mais compreensíveis para o público e com menos detalhes técnicos, eles podem ser expressados como requisitos de negócio. Mais precisamente, foi proposta a associação de cada princípio da LGPD a um requisito de negócio, usando um modelo de Especificação de Requisitos de *Software* (SRS). As Tabelas 3 até 12 estão relacionadas aos 10 princípios da LGPD, conforme seu artigo 6º. O modelo inclui um ID do requisito utilizado para realizar a

indexação com outro componente do guia, a declaração de exigência - que é o texto legal extraído da lei -, o autor responsável por obter as informações, o número de revisão que pode ser utilizado para rastrear as alterações do requisito, a data de lançamento, as palavras-chave associadas ao requisito e, por último, o atributo conformidade legal, que identifica o artigo e o inciso referenciados.

Tabela 3 – Requisito de negócio do Princípio da Finalidade

ID do requisito:	**BREQ-1**
Declaração de exigência:	A organização deve indicar pelo menos uma base legal, ou seja, uma hipótese para realizar o tratamento de dados pessoais. Antes de iniciar o processo de tratamento de dados pessoais, é importante realizar a documentação e indicar uma base legal para o princípio da finalidade. Se a finalidade mudar, a organização deve reavaliar a base legal ou pode manter a base legal original somente se a nova finalidade for compatível com a finalidade inicial.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Base Legal, Finalidade, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso I; Art. 7º.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 4 – Requisito de negócio do Princípio da Adequação

ID do requisito:	**BREQ-2**
Declaração de exigência:	A organização deve usar os dados de modo compatível com a finalidade informada ao titular, e de acordo com o contexto do tratamento dos dados. Ou seja, os dados não podem ser utilizados para outro fim.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Adequação, Finalidade, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso II.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 5 – Requisito de negócio do Princípio da Necessidade

ID do requisito:	**BREQ-3**
Declaração de exigência:	A organização deve realizar o tratamento de dados pessoais somente se for necessário e relevante para a realização da finalidade definida. Sempre que, possível, a coleta deve ser a mínima possível, coletando somente dados necessários para cumprir o propósito.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Minimização de dados, Necessidade, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso III.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 6 – Requisito de negócio do Princípio do Livre acesso

ID do requisito:	**BREQ-4**
Declaração de exigência:	A organização deve garantir aos titulares dos dados uma consulta de forma fácil e gratuita, sobre a forma como é realizado o tratamento de dados e a sua duração. Ou seja, não se deve manter os dados pessoais por mais tempo do que o necessário para atingir a finalidade específica, exceto nos casos em que tenha uma base legal ou legislação vigente para o cumprimento do armazenamento dos dados. Também deve-se tomar medidas técnicas para proteger a integridade dos dados pessoais.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Base Legal, Consulta, Livre acesso, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso IV.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 7 – Requisito de negócio do Princípio da Qualidade dos dados

ID do requisito:	**BREQ-5**
Declaração de exigência:	A organização deve implementar medidas para garantir aos titulares, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Confiabilidade, Integralidade, Princípio, Qualidade dos dados.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso V.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 8 – Requisito de negócio do Princípio da Transparência

ID do requisito:	**BREQ-6**
Declaração de exigência:	A organização deve atender ao princípio da transparência, garantindo aos titulares informações claras e precisa sobre o tratamento de dados pessoais. Caso a organização tenha o consentimento do titular, é necessário informar qual a finalidade, que deve ser de fácil compreensão. Sempre que houver uma mudança da finalidade, o usuário deve saber da mudança e realizar um novo consentimento para a nova finalidade. Também é necessário que a organização adote medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Confiabilidade, Princípio, Transparência.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso VI.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 9 – Requisito de negócio do Princípio da Segurança

ID do requisito:	**BREQ-7**
Declaração de exigência:	A organização deve garantir a existência de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, incluindo situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Deve também atuar junto ao princípio da prevenção, uma vez que se realiza a contratação de mecanismos de segurança exatamente para mitigar e prevenir eventuais incidentes.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Prevenção, Princípio, Segurança.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso VII.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 10 – Requisito de negócio do Princípio da Prevenção

ID do requisito:	**BREQ-8**
Declaração de exigência:	A organização deve garantir medidas técnicas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, ou seja, a organização deve agir antes dos problemas e não somente depois.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Prevenção, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso VIII.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 11 – Requisito de negócio do Princípio da Não Discriminação

ID do requisito:	**BREQ-9**
Declaração de exigência:	A organização, quando realizar um tratamento de dados, não poderá discriminar ou promover abusos contra os titulares dos dados. O princípio diz respeito, principalmente, ao tratamento de dados sensíveis. Em resumo, não é permitido utilizar os dados para fins que gerem discriminação.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Dados sensíveis, Não discriminação, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso IX.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

Tabela 12 – Requisito de negócio do Princípio da Responsabilização e Prestação de Contas

ID do requisito:	**BREQ-10**
Declaração de exigência:	A organização deve documentar as medidas usadas para tratamento de dados pessoais e ser capaz de demonstrar sua conformidade com a LGPD, sempre demonstrando sua boa-fé.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Documentação, Princípio, Responsabilização e Prestação de contas.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso X.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

3.4 REQUISITOS DE SOLUÇÃO

Os requisitos de solução vinculam as obrigações da LGPD e os requisitos de negócios relacionados aos controles de privacidade necessários para cumpri-los.

O modelo inclui espaços reservados que podem ser preenchidos com as informações que identificam os requisitos de negócio, o controle de privacidade escolhido e o cenário em que será aplicado. Quando todos os espaços reservados são preenchidos, o modelo de mapeamento se torna um requisito de solução (Tabela 13).

Tabela 13 – Requisito de negócio do Princípio da Finalidade

Modelo de Mapeamento
De acordo com a LGPD, o(a) **[organização]** é obrigado(a) a cumprir o princípio **[princípio_da_LGPD]** podendo sofrer as **[consequência_da_violação].**
Este princípio é expresso pelo requisito **[ID_requerimento]**, mapeado da **[referência_legal_de_conformidade]**. Este requisito especifica **[descrição_do_requisito]**.
Para ajudar a satisfazer **[ID_requerimento]**, no contexto do **[ID_cenário]**, o profissional implementará o controle **[nome_do_controle_de_privacidade]** (identificado pelo ID **[ID_da_entrada_do_catálogo]** do catálogo de controles de privacidade) para resolver o problema **[problema_de_controle_de_privacidade]**.
Esse controle de privacidade envolve **[descrição_dos_controles_de_privacidade]**. Como resultado, **[benefício_do_controle_de_privacidade]**.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018)

3.5 CATÁLOGO DE CONTROLE DE PRIVACIDADE

O catálogo de controles de privacidade foi traduzido do trabalho de Ayala-Rivera e Pasquale (2018), entretanto, os controles de privacidade descritos pelas autoras foram retirados da literatura, de modo que diversos autores contribuíram para a sua criação. Esses controles são baseados nas normas internacionais ISO/IEC da Família 27000 e 29100.

O catálogo apresenta os controles de privacidade que podem ser usados para atender os 10 princípios da LGPD. Ele serve para mapear a relação entre os controles de privacidade e os princípios da LGPD eles afetam. O catálogo pode ser consultado no Apêndice A.

3.6 EXEMPLO DE ILUSTRAÇÃO DE USO NO CONTEXTO DE DESENVOLVIMENTO DE UM SISTEMA

O exemplo a seguir envolve uma Instituição de Ensino, o Instituto Federal Catarinense (IFC), que realiza o tratamento de dados pessoais de estudantes, servidores públicos e terceirizados. O foco foi o processo seletivo de ingresso dos estudantes, pois é nesse momento em que ocorre o primeiro contato com os estudantes e é realizado o tratamento de seus dados pessoais. Como o IFC realiza o tratamento de dados pessoais no Brasil, ele precisa estar em conformidade com a LGPD. Para entrar na instituição o aluno passa por um processo seletivo e, se for aprovado, é necessária a realização de matrícula para iniciar os estudos. É feita a publicação do edital, indicando os documentos necessários para que o estudante realize a

matrícula. Esses documentos são levados até a instituição, onde são feitas cópias deles. É importante enfatizar que, nesses documentos, constam dados pessoais dos estudantes. Algumas informações são registradas no sistema de gestão acadêmica, enquanto as cópias dos documentos físicos são armazenadas, no processo físico, dentro de um armário. Caso o estudante se inscreva por cotas, é necessário realizar uma entrevista para comprovação da informação fornecida e, neste momento, são coletados mais dados sensíveis. Caso os documentos estejam corretos, o aluno já pode iniciar as aulas conforme o calendário acadêmico.

1ª Etapa - Auditoria de dados: Nesta etapa, é realizado o mapeamento de dados, que consiste em avaliar quais dados pessoais uma organização está tratando, quais categorias de dados estão sendo coletados, com quem estão sendo compartilhados, como eles são armazenados e sob quais bases legais são coletados e manipulados. Esse processo é realizado por meio de entrevista com a pessoa responsável pelo setor que manipula os dados. Para auxiliar na coleta dessas informações, foi disponibilizado um modelo de mapeamento de dados (Apêndice C), construídos a partir da experiência em entrevistas realizadas na instituição e do modelo de mapeamento disponibilizado pela Secretaria de Governo Digital (SGD)[1].

2ª Etapa - Análise de Lacunas: Esta etapa requer a realização de uma análise do mapeamento de dados realizado na primeira etapa para identificar áreas (por exemplo, fluxos, processos, sistemas) que precisam ser aprimoradas por meio de ações corretivas ou preventivas. Em outras palavras, essa atividade permite focar nos princípios da LGPD com os quais o sistema não está em conformidade. Para ajudar nesse processo, o analista de sistemas deve usar os requisitos de negócio para identificar as lacunas. O profissional deve, ainda, responder o questionário conforme apresentado no Apêndice E e, assim, com base na sua experiência com o sistema, será possível identificar as violações dos princípios. No contexto do cenário 1, o Sistema de Processo Seletivo viola 5 princípios da LGPD e, para ajudar na identificação das possíveis violações, foi elaborado um passo a passo:

1º - Passo: O analista de sistema respondeu esse pequeno questionário (Apêndice E) com relação ao Sistema de Processo Seletivo.

2º - Passo: Caso alguma questão tenha sido respondida com **não**, o princípio não está em conformidade com a LGPD e precisa de correção. No exemplo em questão, tivemos algumas perguntas que foram respondidas negativamente e, portanto, referem-se à violação de alguns princípios. Abaixo, estão relacionados os princípios e as justificativas para a não conformidade:

[1] https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd

Primeira Violação: O Princípio da Finalidade é violado (expresso pelo requisito BREQ-1), pois não está documentada, no edital e no sistema, a finalidade da coleta dos dados pessoais. Também não foi informada qual é a base ou hipótese legal para o tratamento dos dados.

Segunda Violação: O Princípio da Necessidade é violado (expresso pelo requisito BREQ-3), pois o instituto está coletando dados pessoais mais do que o necessário para atender a finalidade do processo seletivo.

Terceira Violação: O Princípio do Livre acesso é violado (expresso pelo requisito BREQ-4), pois não é informado o tempo de armazenamento dos dados pessoais coletados para atingir a finalidade específica.

Quarta Violação: O Princípio da Transparência é violado (expresso pelo requisito BREQ-6), pois não é solicitado o consentimento do estudante e também não é informada a finalidade da coleta dos dados.

Quinta Violação: O Princípio da Responsabilização e Prestação de Contas é violado (expresso pelo requisito BREQ-10), pois é necessária a demonstração de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia dessas medidas.

3ª Etapa - Planejamento e Preparação: Nesta etapa, será realizado o planejamento para solucionar os problemas identificados na segunda etapa. Para resolver as violações dos princípios da LGPD, são observados os requisitos de negócio, as recomendações de alterações indicadas na segunda etapa e é utilizado o catálogo de controles de privacidade (Apêndice A), necessário para satisfazer obrigações legais específicas. Foram propostos apenas 5 requisitos de solução, conforme mostrado nas Tabelas 14 até 18, pois cada um deles equivale a um requisito de negócio não atendido pelo Sistema de Processo Seletivo. No exemplo, foi utilizado apenas um requisito de solução para resolver o problema das violações dos princípios, entretanto, podem ser utilizados mais de um controle de privacidade pelo analista de sistemas. Os requisitos de solução para cada princípio estão disponíveis no Apêndice B.

Tabela 14 – Solução da 1ª Violação - Finalidade

ID do requisito:	**SREQ-1**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense é obrigado a cumprir o princípio da **finalidade** que deve ser específica e informada explicitamente ao titular, sem possibilidade de tratamento de dados posterior de forma incompatível com essas finalidades, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-1, mapeado da Lei 13.709 - LGPD Art. 6º, inciso I. Esse requisito especifica que o Instituto Federal deve ter pelo menos uma base legal válida para processar dados pessoais. O Instituto deve determinar a base legal antes de iniciar o processamento e documentação de dados pessoais. A escolha da base jurídica dependerá da finalidade do processamento de dados. Se a finalidade for alterada, o Instituto deverá reavaliar a base ou poderá manter a base original somente se a nova finalidade for compatível com a finalidade inicial. Para ajudar a satisfazer a BREQ-1 no contexto do cenário 1, o profissional implementará o controle **consentimento informado** (identificado pelo ID **18** do catálogo de controles de privacidade) para resolver o problema de os usuários aceitarem os termos e condições de um serviço "com muita facilidade" sem terem lido ou entendido o que estavam aceitando. Esse controle de privacidade envolve que sempre que a coleta de dados precisar ser legitimada, forneça contratos de clique ("clique e aceite") para confirmar o entendimento ou consentimento do usuário "conforme necessário", usando ações de arrastar e soltar para consentir a divulgação de dados. Como resultado, a organização pode garantir que os titulares dos dados entendam totalmente e concordem com o processamento de seus dados pessoais.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020

Palavras-chave:	Consentimento informado, Finalidade, Princípio.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018).

Tabela 15 – Solução da 2ª Violação - Necessidade

ID do requisito:	**SREQ-3**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense é obrigado a cumprir o princípio da **necessidade** para evitar o acúmulo de dados redundantes ou desnecessários e minimizar os riscos de uma violação de dados, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-3, mapeado da Lei 13.709 - LGPD Art. 6º, inciso III. Esse requisito especifica que o Instituto Federal deve realizar o tratamento de dados pessoais somente se for necessário e relevante para a realização da finalidade definida. Sempre que possível, a coleta deve ser a mínima possível, coletando somente dados necessários para cumprir o propósito. Para ajudar a satisfazer a BREQ-3 no contexto do cenário 1, o profissional implementará o controle **minimização** (identificado pelo ID **3** do catálogo de controles de privacidade) para resolver o problema de coletar mais dados do que o necessário para a finalidade de uso. Esse controle de privacidade diz que, sempre que possível, quando houver coleta de dados pessoais com a finalidade apenas de estatísticas, os dados devem ser anonimizados, e a coleta deve ser a mínima possível, ou seja, evitando a coletar dados desnecessários. Como resultado, essa solução irá melhorar a proteção da privacidade e a minimização dos dados.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020

Palavras-chave:	Finalidade, Minimização de dados, Necessidade, Princípio.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018).

Tabela 16 – Solução da 3ª Violação - Livre acesso

ID do requisito:	**SREQ-4**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense é obrigado(a) a cumprir o princípio do **livre acesso** e garantir aos titulares dos dados uma consulta, de forma fácil e gratuita, sobre a forma como é realizado o tratamento de dados e sua duração, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-4, mapeado da Lei 13.709 - LGPD Art. 6º, inciso IV. Este requisito especifica que o Instituto Federal deve garantir aos titulares dos dados uma consulta de forma fácil e gratuita, sobre a forma como é realizado o tratamento de dados e sua duração. Ou seja, o Instituto Federal não deve manter os dados pessoais por mais tempo do que o necessário para atingir a finalidade específica, exceto nos casos em que tenha uma base legal, ou legislação vigente para justificar o armazenamento dos dados. O Instituto Federal também deve tomar medidas técnicas para proteger a integridade dos dados pessoais. Para ajudar a satisfazer a BREQ-4 no contexto do cenário 1, o profissional implementará o controle **painel de privacidade** (identificado pelo ID **28** do catálogo de controles de privacidade) para resolver o problema de os usuários esquecerem ou não perceberem quais dados um determinado serviço ou empresa coletou. Esse controle de privacidade diz que quando um serviço coleta ou processa dados pessoais de usuários, deve fornecer a eles resumos ou uma visão geral dos seus dados pessoais coletados em um painel de privacidade. Como resultado, os usuários podem ter uma visão geral dos seus dados pessoais coletados.
Autor:	Diego Menegazzi

Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Dados coletados, Livre acesso, Painel de privacidade, Princípio.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018).

Tabela 17 – Solução da 4ª Violação - Transparência

ID do requisito:	**SREQ-6**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense é obrigado a cumprir o princípio da **transparência**, garantindo aos titulares informações claras e precisas sobre o tratamento de seus dados pessoais, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-6, mapeado da Lei 13.709 - LGPD Art. 6º, inciso VI. Este requisito especifica que o Instituto Federal deve atender ao princípio da transparência, garantindo aos titulares informações claras e precisas sobre o tratamento de seus dados pessoais. Caso a organização tenha o consentimento do titular, é necessário informar qual a finalidade de uso dos seus dados e essa informação deve ser de fácil compreensão. Sempre que houver uma mudança da finalidade, o usuário deve ser informado da mudança e deve realizar um novo consentimento para a nova finalidade. Para ajudar a satisfazer o BREQ-6 no contexto do cenário 1, o profissional implementará o controle **painel de confiabilidade** (identificado pelo ID **9** do catálogo de controles de privacidade) para resolver o problema dos usuários superestimarem a quantidade de dados pessoais necessários para usar um serviço. Como resultado, isso facilita a seleção de credenciais adequadas para o usuário e aumenta a transparência sobre os dados pessoais que serão compartilhados.
Autor:	Diego Menegazzi

Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Confiabilidade, Princípio, Transparência.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018).

Tabela 18 – Solução da 5ª Violação - Responsabilização e Prestação de Contas

ID do requisito:	**SREQ-10**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense é obrigado a cumprir o princípio da **responsabilização e prestação de contas**, onde a organização deve documentar as medidas usadas para tratamento dos dados pessoais e ser capaz de demonstrar a sua conformidade com a LGPD, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-10, mapeado da Lei 13.709 - LGPD Art. 6º, inciso X. Este requisito especifica que o Instituto Federal deve documentar as medidas usadas para tratamento dos dados pessoais e ser capaz de demonstrar sua conformidade com a LGPD. Sempre demonstrando sua boa-fé. Para ajudar a satisfazer o BREQ-10 no contexto do cenário 1, o profissional implementará o controle **notificações de violação de dados** (identificado pelo ID **10** da entrada do catálogo de controles de privacidade) para resolver o problema de violação de dados. Esse controle de privacidade diz que sempre que ocorrer uma violação de dados, é mandatório notificar a autoridade supervisora e os usuários afetados imediatamente. Como resultado, isso irá mitigar danos e aumentar a transparência.
Autor:	Diego Menegazzi
Nº Revisão:	1.0

Data de Lançamento:	30/10/2020
Palavras-chave:	Documentação, Notificações, Princípio, Responsabilização e prestação de contas.

Fonte: Adaptado de Ayala-Rivera e Pasquale (2018).

4ª Etapa - Revisão do Plano de Ação Nesta etapa, todos os stakeholders revisam o plano de ação elaborado na terceira etapa. A revisão antes da execução é necessária, pois é preciso avaliar se as mudanças afetarão o funcionamento do negócio ou do sistema. Embora os controles de privacidade listados no catálogo forneçam um conjunto de mecanismos que já se provaram úteis, conforme estudado na literatura, eles não são a única maneira de satisfazer um requisito de privacidade. Portanto, as partes interessadas devem avaliar os prós e contras dos controles de privacidade sugeridos, de modo a selecionar um ou mais, dependendo sempre do cenário. Por exemplo, dependendo da situação, a organização não tem colaboradores suficientes para desenvolver ou implementar o controle de privacidade de logs no sistema, sendo necessário que ela procure outros modos para atender o princípio da responsabilização e prestação de contas.

5ª Etapa - Execução Nesta etapa, após a análise feita pelos stakeholders e os requisitos de solução terem sido especificados e aprovados para o cenário em questão (no caso do exemplo, o Sistema de Processo Seletivo), a equipe de desenvolvimento de software deve realizar a implementação das soluções definidas. Nesta etapa, caso a organização possua profissionais de Direito e/ou Privacidade, é importante que eles façam o acompanhamento das implementações das soluções para contribuir no processo de validação dos controles de privacidade escolhidos.

6ª Etapa - Revisão Pós-implementação

Finalmente, as organizações precisam garantir que todos os requisitos da solução foram atendidos. Isso pode ser verificado por meio da avaliação de processos e procedimentos com especialistas em TI, Direito e conformidade. Além disso, auditorias regulares devem ser agendadas para identificar os requisitos de solução que podem precisar de revisão.

4 AVALIAÇÃO DO GUIA DE CONFORMIDADE DA LGPD

Nesta seção, será apresentada a avaliação do guia de conformidade da LGPD do ponto de vista de profissionais que atuam nas áreas de Engenharia de Requisitos, Análise de Sistemas, Privacidade de Dados e conformidade legal. A pesquisa foi realizada entre dezembro de 2020 e janeiro de 2021, com 31 profissionais que aceitaram analisar o guia e responder o questionário de avaliação. O perfil ideal para avaliação do questionário são pessoas que trabalham diretamente ou estão relacionadas com a área de privacidade e, ainda, que tenham conhecimento sobre a LGPD. Infelizmente, pelo fato de a lei ser nova no Brasil, não conseguimos encontrar muitos profissionais que satisfizessem ambas as condições. A divulgação do formulário foi feita por meio de grupos nos serviços de mensagens instantâneas *Telegram* e *WhatsApp*, além da rede social de negócios *LinkedIn*. Foram enviados também e-mails para grupos focados em estudos de privacidade. As respostas obtidas no questionário são apresentadas nas seções subsequentes.

4.1 QUESTIONÁRIO DE AVALIAÇÃO

O questionário foi disponibilizado como um formulário no Google Forms. Um website (MENEGAZZI, 2020) foi desenvolvido para disponibilizar o guia para que os participantes pudessem analisar e reportar as suas impressões no questionário de avaliação. O website contém uma seção com as 6 etapas para alcançar a conformidade da LGPD, além de um exemplo ilustrado da aplicação do método. Ainda no website, há uma seção com os componentes do guia que são usados na execução das etapas: o modelo de mapeamento de dados, os requisitos de negócio, os requisitos de solução e o catálogo de controles de privacidade. Por fim, o website conta, ainda, com um vídeo de explicação de todos os componentes e as etapas do guia. O questionário de avaliação está no Apêndice D.

4.2 RESULTADOS

O questionário de avaliação está dividido em 5 conjuntos de perguntas. O primeiro conjunto trata do perfil dos participantes e suas experiências. O segundo conjunto trata do quão útil cada etapa do guia é para alcançar a conformidade legal. O terceiro conjunto trata do quão

útil cada componente do guia é para apoiar a execução das etapas. O quarto conjunto trata do quão difícil foi compreender os componentes do guia. O último conjunto inclui perguntas que podem auxiliar o autor a melhorar o guia proposto.

4.2.1 1º Conjunto - Perfil e Experiências

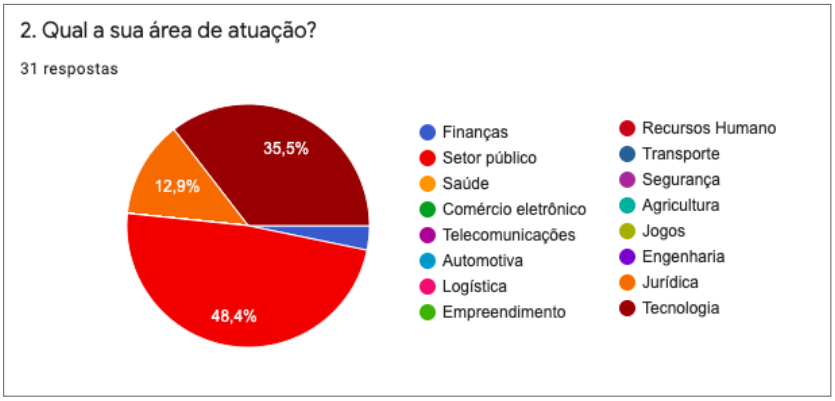
1: Qual é o seu papel atual na organização? Dentre os participantes, pode-se notar, na Figura 9, que a maioria é pessoa desenvolvedora de *software*. Segundo o levantamento, 15 são desenvolvedores, 3 são gerentes de projetos, 3 são líderes de negócio, 4 são analistas de negócio, 1 é coordenador de TI, 2 são técnicos de TI, 1 é analista de infraestrutura, 1 é analista de TI e 1 é analista de sistemas.

Figura 9 – Papel atual na organização

Fonte: Elaborada pelo Autor (2021).

2: Qual a sua área de atuação? Dentre os participantes, pode-se notar, na Figura 10, que a maioria faz parte do setor público (48,4%), 35,5% são da indústria de tecnologia, 12,9% são profissionais do setor jurídico e 3,2% fazem parte da área de finanças.

Figura 10 – Área de atuação dos participantes



Fonte: Elaborada pelo Autor (2021).

3: Quantos anos de experiência profissional você tem na área? Dentre os participantes, pode-se notar, na Figura 11, que a maioria possui experiência profissional entre 6 e 10 anos (38,7%). Nota-se, ainda, que 35,5% têm mais de 15 anos de experiência na área, 25,8% têm entre 11 e 15 anos e nenhum participante possui experiência entre 1 e 5 anos.

Figura 11 – Experiência profissional dos participantes na área

Fonte: Elaborada pelo Autor (2021).

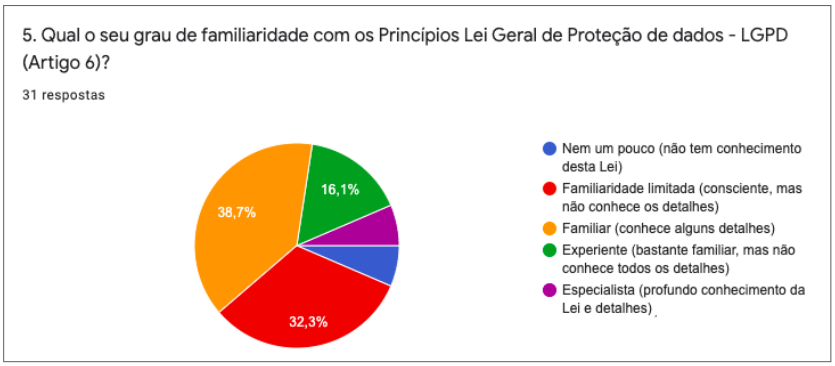
4: O seu setor de trabalho precisa estar em conformidade com a Lei 13.709 - Lei Geral de Proteção de Dados (LGPD)? De acordo com a Figura 12, observa-se que a maioria sabe que o seu setor precisa estar em conformidade com a LGPD. Assim, 90,3% responderam Sim, 3,2% responderam Não e 6,5% não souberam o que responder.

Figura 12 – Setor de trabalho em conformidade com a LGPD

Fonte: Elaborada pelo Autor (2021).

5: Qual o seu grau de familiaridade com os Princípios Lei Geral de Proteção de dados - LGPD (Artigo 6)? Na Figura 13, é possível perceber que a maioria respondeu possuir familiaridade (conhece alguns detalhes) com os princípios da LGPD, correspondendo a 38,7%. Ainda, 32,3% responderam que possuem familiaridade limitada (consciente, mas não conhece os detalhes da LGPD), 16,1% possuem experiência com a lei (bastante familiar, mas não conhece todos os detalhes), 6,5% responderam que são especialistas (possuem um profundo conhecimento da lei e seus detalhes) e 6,5% não possuem conhecimento da lei.

Figura 13 – Familiaridade com os princípios da LGPD



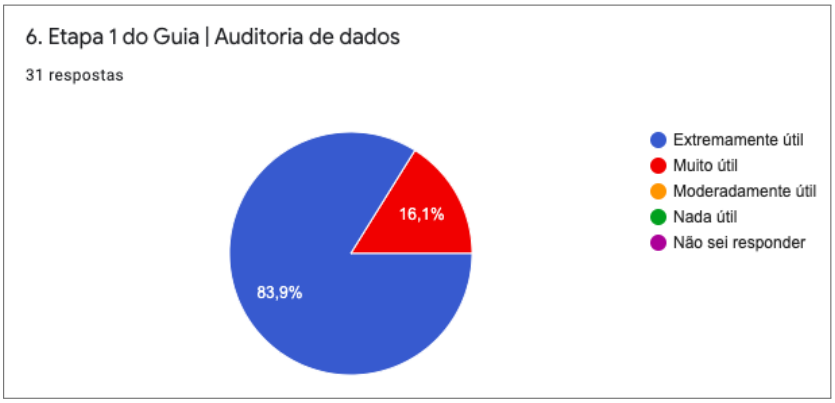
Fonte: Elaborada pelo Autor (2021).

4.2.2 2º Conjunto - Quão ÚTIL você classifica as diferentes etapas do guia?

O 2º conjunto de questões trata do quão útil os participantes classificam cada uma das diferentes etapas do guia. As opções de cada questão são: Extremamente útil, Muito útil, Moderadamente útil, Nada útil e Não sei responder.

6: Etapa 1 do Guia | Auditoria de dados. A primeira etapa diz respeito à auditoria de dados, na qual é realizado o mapeamento dos dados pessoais. Dentre os participantes, a Figura 14 indica que 83,9% consideraram essa etapa do guia extremamente útil e 16,1%, muito útil. As demais opções não foram respondidas por nenhum participante.

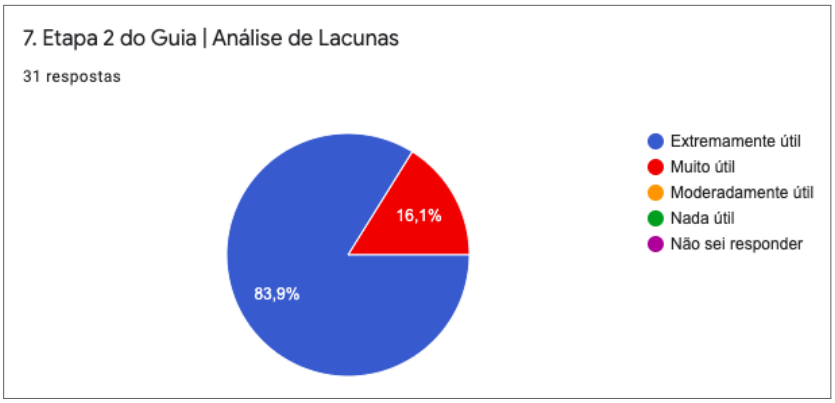
Figura 14 – Quão útil é a 1º Etapa - Auditoria de dados



Fonte: Elaborada pelo Autor (2021).

7: Etapa 2 do Guia | Análise de Lacunas. A segunda etapa diz respeito à análise de lacunas, na qual são identificadas as partes que precisam ser adequadas aos princípios da lei. Dentre os participantes, a Figura 15 mostra que 83,9% consideraram essa etapa do guia extremamente útil e 16,1%, muito útil. As demais opções não foram respondidas por nenhum participante.

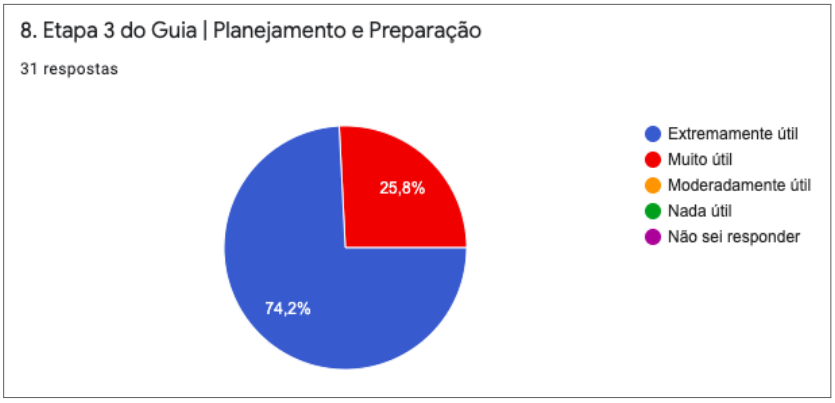
Figura 15 – Quão útil é a 2º Etapa - Análise de Lacunas



Fonte: Elaborada pelo Autor (2021).

8: Etapa 3 do Guia | Planejamento e Preparação. A terceira etapa visa verificar quais controles de privacidades são necessários para satisfazer os princípios da LGPD. Dentre os participantes, a Figura 16 mostra que 74,2% consideraram essa etapa do guia extremamente útil e 25,8%, muito útil. As demais opções não foram respondidas por nenhum participante.

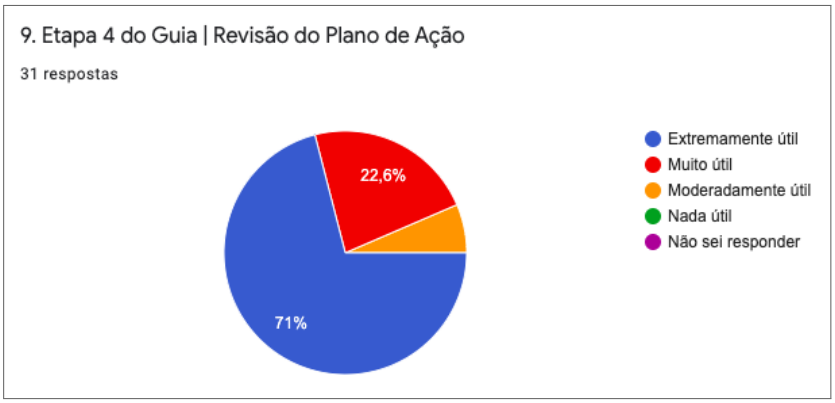
Figura 16 – Quão útil é a 3º Etapa - Planejamento e Preparação



Fonte: Elaborada pelo Autor (2021).

9: Etapa 4 do Guia | Revisão do Plano de Ação. A quarta etapa diz respeito à revisão do plano de ação, quando é verificado se as alterações necessárias para alcançar a conformidade não irão impactar no desempenho do *software* antes de serem executadas. Dentre os participantes, a Figura 17 mostra que 71% consideraram essa etapa do guia extremamente útil, 22,6% consideraram muito útil e 6,5% consideraram moderadamente útil. As demais opções não foram respondidas por nenhum participante.

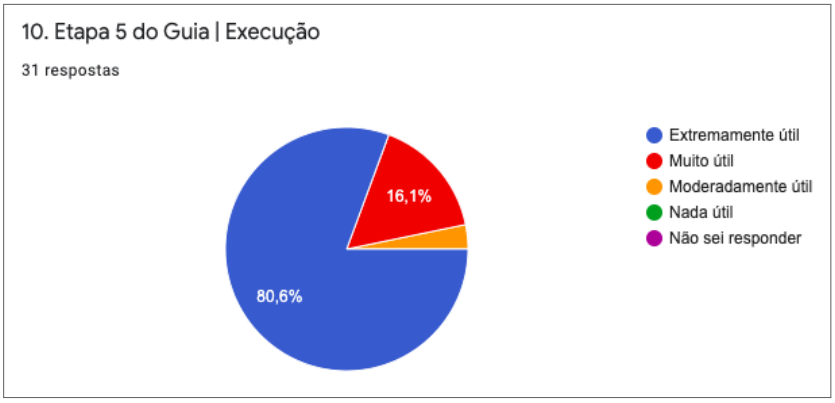
Figura 17 – Quão útil é a 4º Etapa - Revisão do Plano de Ação



Fonte: Elaborada pelo Autor (2021).

10: Etapa 5 do Guia | Execução. A quinta etapa diz respeito à execução, quando profissionais de TI implementam os controles de privacidade definidos na terceira etapa. A Figura 18 aponta que 80,6% dos participantes consideraram essa etapa do guia extremamente útil, 16,1% consideraram muito útil e 3,2% consideraram moderadamente útil. As demais opções não foram respondidas por nenhum participante.

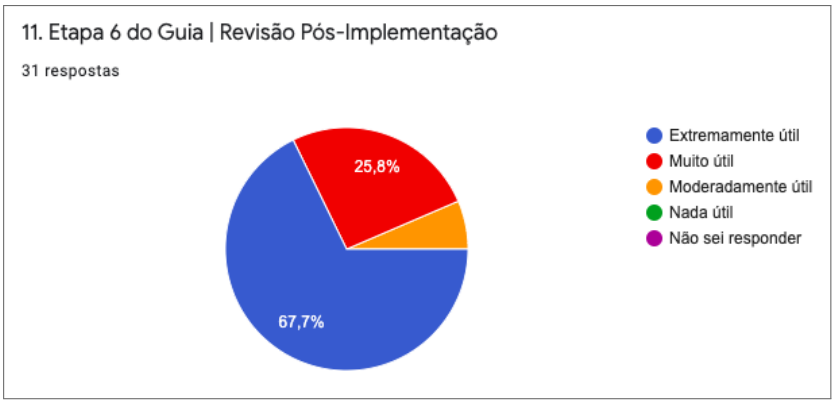
Figura 18 – Quão útil é a 5º Etapa - Execução



Fonte: Elaborada pelo Autor (2021).

11: Etapa 6 do Guia | Revisão Pós-Implementação. A sexta etapa diz respeito à revisão pós-implementação, na qual uma auditoria é realizada para verificar se os requisitos estão em conformidade e se não precisam de ajustes. A Figura 19 demonstra que 67,7% dos participantes consideraram essa etapa do guia extremamente útil, 25,8% consideraram muito útil e 6,5%, moderadamente útil. As demais opções não foram respondidas por nenhum participante.

Figura 19 – Quão útil é a 6º Etapa - Revisão Pós-Implementação



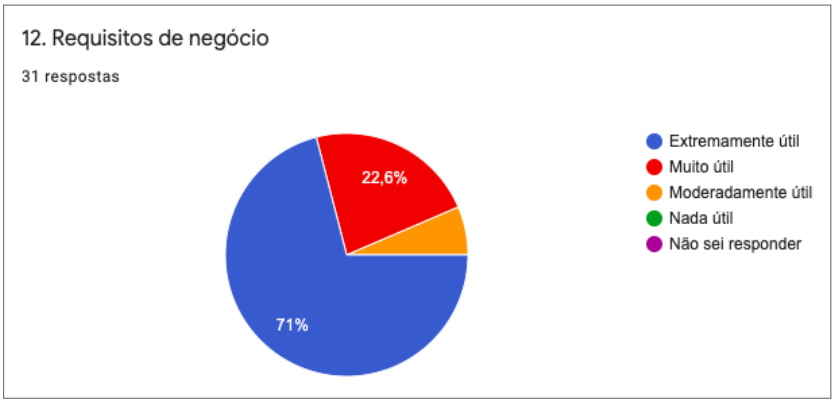
Fonte: Elaborada pelo Autor (2021).

4.2.3 3º Conjunto - Quão ÚTIL você classifica os diferentes componentes do guia?

O 3º conjunto de questões trata do quão útil os participantes classificam cada um dos diferentes componentes do guia. Os componentes são: requisitos de negócio, requisitos de solução, catálogo de controles de privacidade, exemplo de ilustração de uso do Guia e vídeo de explicação de uso do Guia. As opções de respostas para cada pergunta são: Extremamente útil, Muito útil, Moderadamente útil, Nada útil e Não sei responder.

12. Requisitos de negócio. Esse componente captura os princípios da LGPD como requisitos de negócio. A Figura 20 mostra que, dentre os participantes, 71% consideraram essa etapa do guia extremamente útil, 22,6% consideraram muito útil e 6,5%, moderadamente útil. As demais opções não foram respondidas por nenhum participante.

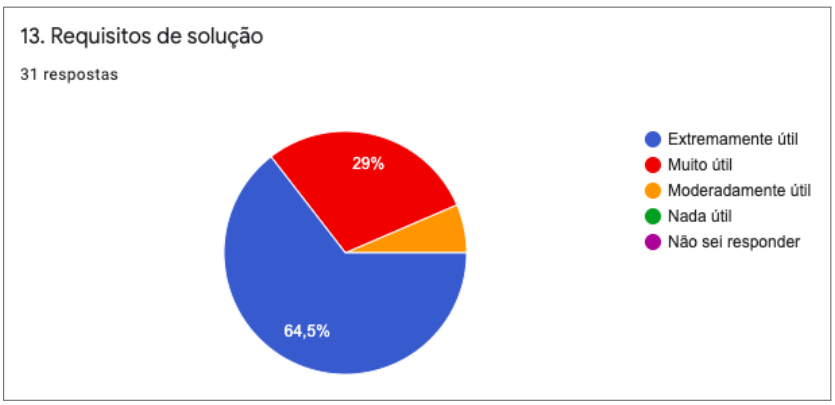
Figura 20 – Quão útil é o componente Requisitos de negócio



Fonte: Elaborada pelo Autor (2021).

13. Requisitos de solução. Esse componente vincula as obrigações da LGPD, representadas nos requisitos de negócio, aos controles de privacidade necessários para cumpri-las. A Figura 21 aponta que 64,5% dos participantes consideraram essa etapa do guia extremamente útil, 29% consideraram muito útil e 6,5%, moderadamente útil. As demais opções não foram respondidas por nenhum participante.

Figura 21 – Quão útil é o componente Requisitos de solução

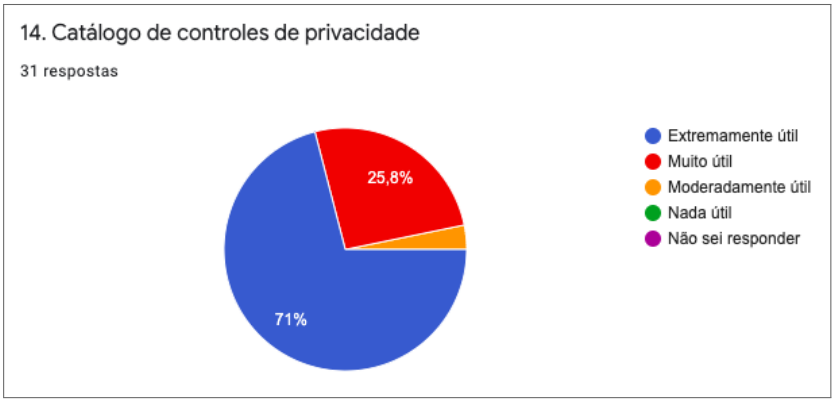


Fonte: Elaborada pelo Autor (2021).

14. Catálogo de controles de privacidade. Esse componente corresponde aos controles de privacidade que servem como soluções em potencial para atender os requisitos de negócio de forma total ou parcial. Dentre os participantes, a Figura 22 mostra que 71% consideraram essa

etapa do guia extremamente útil, 25,8% consideraram muito útil e 3,2%, moderadamente útil. As outras opções não foram respondidas por nenhum participante.

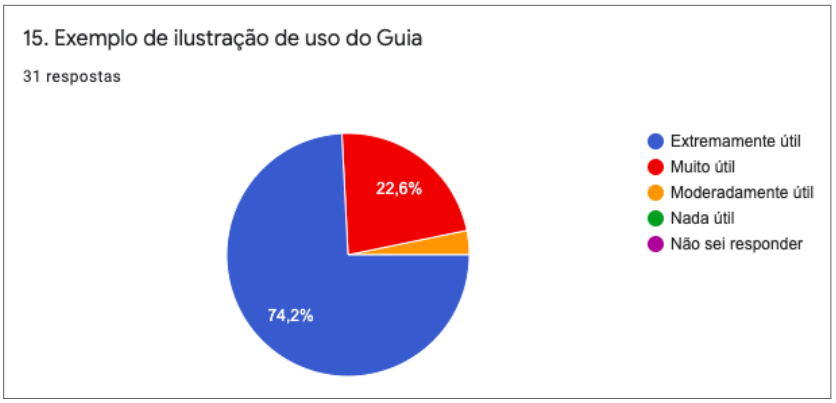
Figura 22 – Quão útil é o componente Catálogo de Controles de Privacidade



Fonte: Elaborada pelo Autor (2021).

15. Exemplo de ilustração de uso do Guia. Esse componente corresponde a um exemplo de ilustração do Guia, que foi aplicado no Instituto Federal Catarinense no Sistema de Processo Seletivo para o ingresso de estudantes na instituição. Observa-se na Figura 23 que, para 74,2% dos participantes, essa etapa do guia é extremamente útil, para 22,6%, é muito útil e, para 3,2%, é moderadamente útil. As demais opções não foram respondidas por nenhum participante.

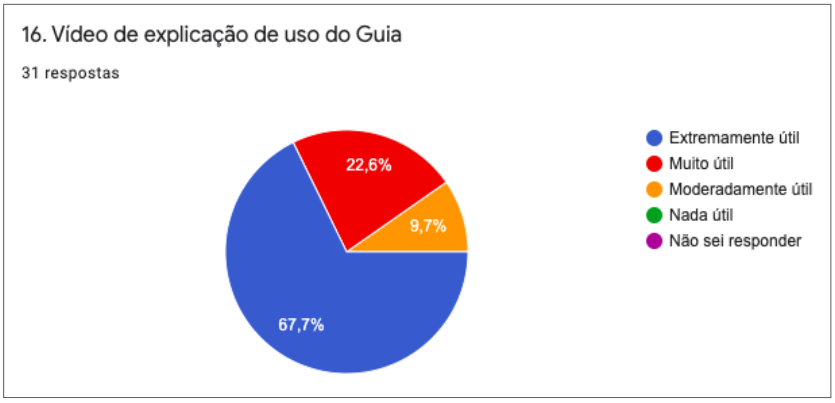
Figura 23 – Quão útil é o componente Exemplo de ilustração de uso do Guia



Fonte: Elaborada pelo Autor (2021).

16. Vídeo de explicação de uso do Guia. Esse componente demonstra como utilizar o guia descrito no website. Dentre os participantes, a Figura 24, mostra que 67,7% consideraram essa etapa do guia extremamente útil, 22,6% consideraram muito útil e 9,7%, moderadamente útil. As demais opções não foram respondidas por nenhum participante.

Figura 24 – Quão útil é o componente Vídeo de Explicação de uso do Guia



Fonte: Elaborada pelo Autor (2021).

17. Qual foi o componente mais ÚTIL do Guia e por quê? A Tabela 19 mostra os componentes escolhidos e as justificativas de escolha dos participantes. Na análise realizada, o componente mais útil é o Exemplo de ilustração de uso do Guia, com 10 votos. Em seguida, encontra-se o componente Vídeo de Explicação de Uso do Guia, com 5 votos. Depois, os Requisitos de Solução, com 6 votos; o Catálogo de Controles de Privacidade, com 5 votos; e os Requisitos de Negócio, com apenas 2 votos.

Tabela 19 – Componentes mais úteis do Guia

Respostas
"Requisitos de Solução."
"O exemplo de ilustração de uso do Guia exemplifica o uso e a forma de aplicar o guia e é muito importante em um ambiente prático, se tornando o componente mais importante do guia."
"Exemplo de ilustração, pois mostra como seria a garantia da LGPD na prática."
"Guia ilustrado"
"O exemplo de ilustração, pois levanta as etapas do guia detalhadamente com um caso real, com dados de candidatos que devem ser protegidos segundo a LGPD. Muito interessante o relacionamento dos requisitos legais com exemplos de violações no sistema analisado."
"Catálogo de Controles de Privacidade"
"Vídeo, pois explana o conteúdo de forma sucinta."

"Video, pois ajuda o entendimento do guia"
"A ilustração de uso do Guia, porque fica mais fácil para que qualquer pessoa que não seja familiarizada com implementações e adequações consiga entender"
"Controles de privacidade, pois são os balizadores para uma gestão de riscos."
"Auditoria"
Catálogo de controles de privacidade
"Exemplo de ilustração, pois assim temos uma ideia de como aplicar o guia."
"Requisitos de solução"
"Vídeo de explicação de uso do Guia"
"Todos os componentes são úteis. Um complementa o outro, mas o mais útil é o de requisitos de negócio, pois pelo que entendi, extrai os requisitos dos princípios da Lei em um quadro que para o desenvolvedor é importante. "
"Exemplo de ilustração de uso do Guia, pois é possível ver na prática um exemplo de utilização do guia."
"Requisitos de solução, pois nesse texto já está escrito o que o programador deve fazer no sistema para atender ao princípio da LGPD."

Fonte: Elaborada pelo Autor (2021).

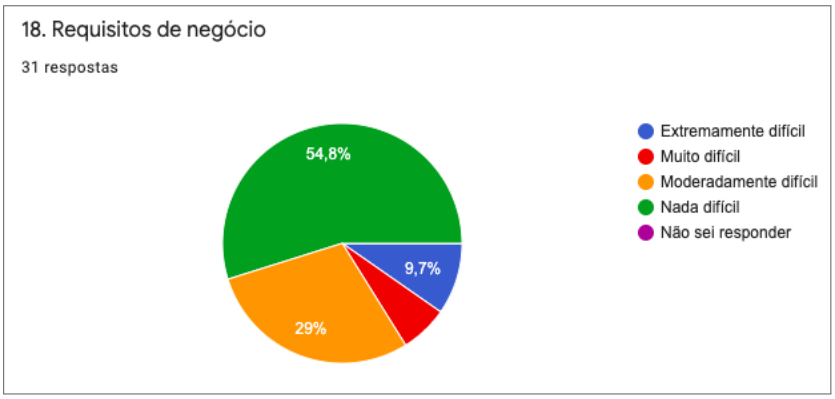
4.2.4 4º Conjunto - Quão DIFÍCIL de compreender você classifica os componentes do Guia?

O 4º conjunto de questões trata do quão difícil os participantes acharam a compreensão dos componentes do guia. Os componentes são: Requisitos de Negócio, Requisitos de Solução, Catálogo de controles de privacidade, Exemplo de ilustração de uso do Guia e Vídeo de explicação de uso do Guia. As opções de respostas para cada pergunta são: Extremamente difícil, Muito difícil, Moderadamente difícil, Nada difícil e Não sei responder.

18. Requisitos de negócio. Dentre os participantes, a Figura 25 mostra que 54,8% consideram essa etapa do guia nada difícil, 29% consideraram moderadamente difícil, 9,7% consideraram muito difícil e 6,5%, extremamente difícil. As demais opções não foram respondidas

por nenhum participante.

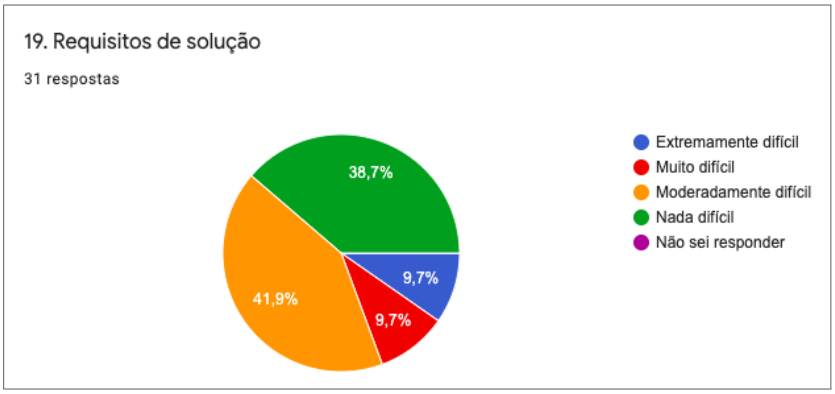
Figura 25 – Quão difícil é o componente Requisitos de negócio



Fonte: Elaborada pelo Autor (2021).

19. Requisitos de solução. Dentre os participantes, a Figura 26 aponta que 38,7% consideraram essa etapa do guia nada difícil, 41,9% moderadamente difícil, 9,7% muito difícil e 9,7% extremamente difícil. As outras opções não foram respondidas por nenhum participante. É possível perceber que mais de 60% dos participantes consideraram o componente difícil, o que pode ser atribuído ao fato de que o requisito de solução é muito extenso, o que o torna difícil de compreender e aplicar. Inclusive, alguns dos participantes sugeriram a redução do texto dos requisitos de solução por ser muito extenso para ler. No entanto, não foi reduzida a quantidade de texto dos requisitos, pois considera-se que as informações apresentadas são essenciais para o entendimento por parte dos profissionais de TIC. Para trabalhos futuros, porém, será considerada a redução do texto.

Figura 26 – Quão difícil é o componente Requisitos de solução

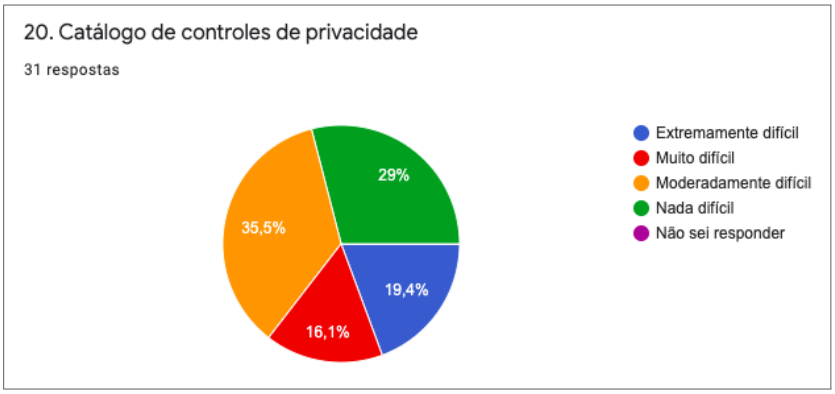


Fonte: Elaborada pelo Autor (2021).

20. Catálogo de controles de privacidade. Dentre os participantes, a Figura 27 mostra que 29% consideraram essa etapa do guia nada difícil, 35,5% moderadamente difícil, 16,1% muito

difícil e 19,4%, extremamente difícil. As demais opções não foram respondidas por nenhum participante. Pode-se notar que mais de 70% dos participantes consideraram o componente difícil, o que pode ser atribuído ao fato de que o catálogo de controle de privacidade é um artefato muito extenso, contando com 40 controles de privacidade, mas sua utilização é essencial para trabalhar com conformidade dos sistemas de software.

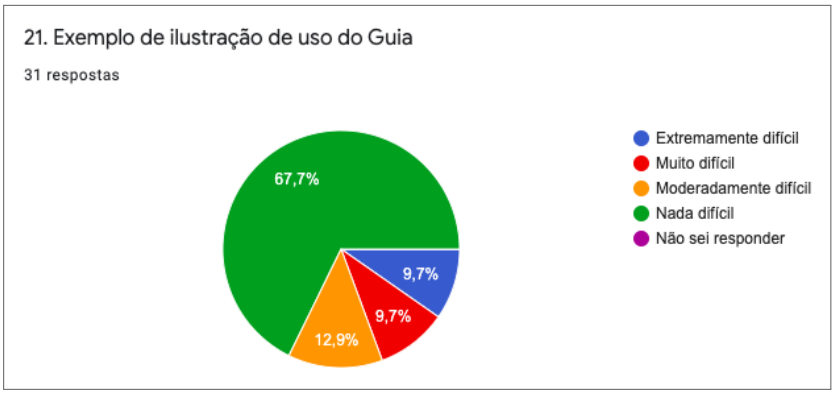
Figura 27 – Quão difícil é o componente Catálogo de Controles de Privacidade



Fonte: Elaborada pelo Autor (2021).

21. Exemplo de ilustração de uso do Guia. Dentre os participantes, a Figura 28 aponta que 67,7% consideraram essa etapa do guia nada difícil, 12,9% consideraram moderadamente difícil, 9,7% consideraram muito difícil e 9,7%, extremamente difícil. As demais opções não foram respondidas por nenhum participante.

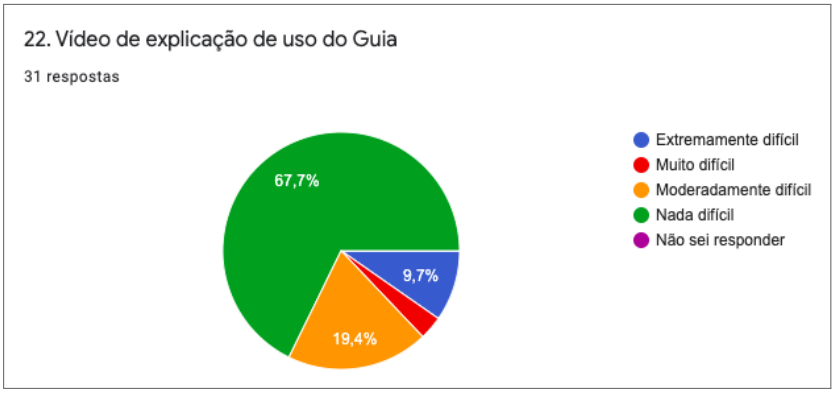
Figura 28 – Quão difícil é o componente Exemplo de Ilustração de uso do Guia



Fonte: Elaborada pelo Autor (2021).

22. Vídeo de explicação de uso do Guia. Dentre os participantes, a Figura 29 mostra que 67,7% consideraram essa etapa do guia nada difícil, 19,4% consideraram moderadamente difícil, 3,2% consideraram muito difícil e 9,7%, extremamente difícil. As demais opções não foram respondidas por nenhum participante.

Figura 29 – Quão difícil é o componente Vídeo de Explicação de uso do Guia



Fonte: Elaborada pelo Autor (2021).

23. Qual foi o componente mais difícil do Guia e por quê? A Tabela 20 apresenta os componentes escolhidos e as justificativas das escolhas dos participantes. O componente mais difícil é o Catálogo de Controles de Privacidade, com 8 votos, seguido de Requisitos de Solução, com 6 votos, Requisitos de negócio, com 4 votos, Exemplo de ilustração de uso do Guia, com apenas 2 votos, e Vídeo de explicação de uso do Guia, com apenas 1 voto.

Tabela 20 – Componentes mais difíceis do Guia

Respostas
"Requisitos de Solução. Exige estudo mais aplicados."
"Requisitos de negócio. Apresenta uma curva de aprendizado mais acentuada por se tratar de um assunto um pouco mais complexo."
"Planejamento e preparação."
"Requisitos de solução. Talvez pelo tamanho do texto."
"Catálogo de privacidade. Por [eu] ter pouco conhecimento sobre a LGPD e seus princípios."
"Catálogo de controles de privacidade."
"O Catálogo de controles de privacidade. Devido a grande quantidade de Controles de Privacidade que podem ser utilizados."
"Requisitos de Negócio. Para mim é a parte mais subjetiva e requer muito conhecimento da área de negócio para interpretar corretamente os requisitos."
"Análise de lacunas. Exige profundo conhecimento prévio da lei em questão."

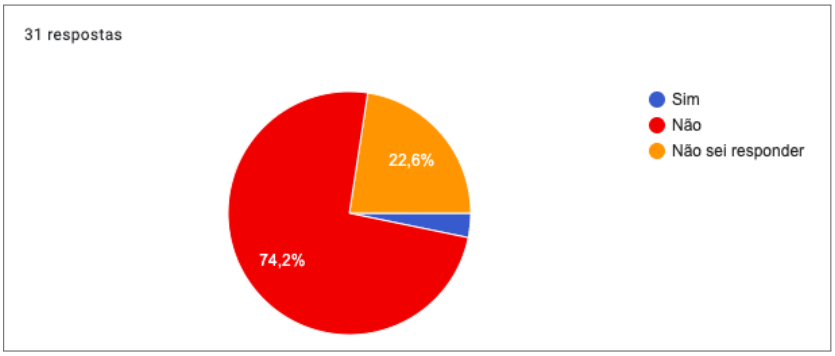
"Controles de Privacidade . Por que nem todos entendem sobre privacidade de dadosque é um segmento bem específico."
"O mais difícil foi o Catálogo de controles de privacidade, pois é um catalogo extenso e a primeira impressão que tenho é que será complexo implementar todos eles."
"Requisitos de solução. Ele poderia ter o texto menor, pois acredito que ficou muito extenso e isso pode confundir a interpretação da Lei."
"Catálogo de controles de privacidade, pois ele é extenso e precisa-se de um tempo para entender [os controles]."

Fonte: Elaborada pelo Autor (2021).

4.2.5 5º Conjunto - Informações Adicionais

24. Algum componente do Guia pode ser considerado desnecessário para apoiar o alcance da conformidade com a LGPD? Dentre os participantes, a Figura 30 mostra que 74,2% responderam Não, 22,6% não souberam responder, 3,2% responderam Sim, e a resposta para este caso foi: *"vídeo de explicação de uso."*

Figura 30 – Componente desnecessário

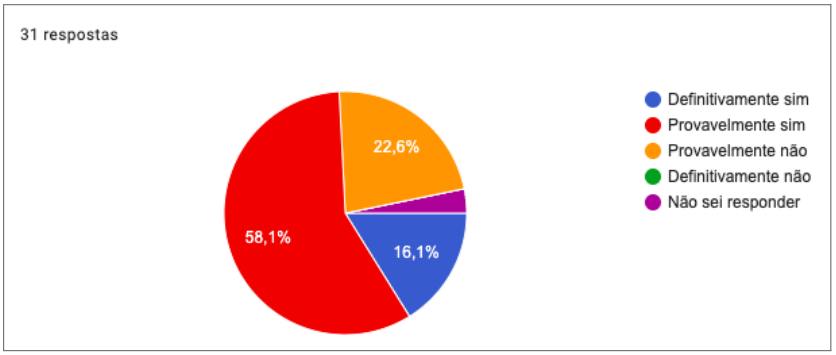


Fonte: Elaborada pelo Autor (2021).

25. Você acha que precisaria de treinamento para executar as etapas deste Guia? (As etapas do Guia são: Auditoria de dados, Análise de Lacunas, Planejamento e Preparação, Revisão do Plano de Ação, Execução e Revisão Pós-Implementação) Dentre os participantes, a Figura 31 mostra que 58,1% responderam provavelmente sim, 22,6% responderam provavelmente não,

16,1% responderam definitivamente sim e 3,2% responderam que não sabiam.

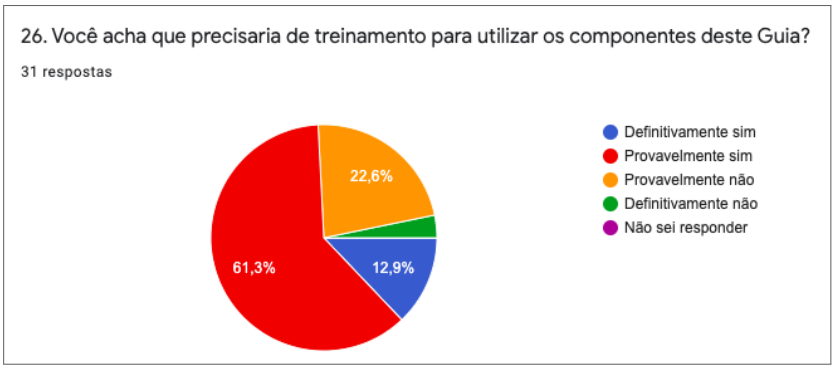
Figura 31 – Treinamento para as etapas do Guia



Fonte: Elaborada pelo Autor (2021).

26. Você acha que precisaria de treinamento para utilizar os componentes deste Guia? Dentre os participantes, a Figura 32 mostra que 61,3% responderam provavelmente sim, 22,6% responderam provavelmente não, 12,9% responderam definitivamente sim e 3,2% responderam definitivamente não.

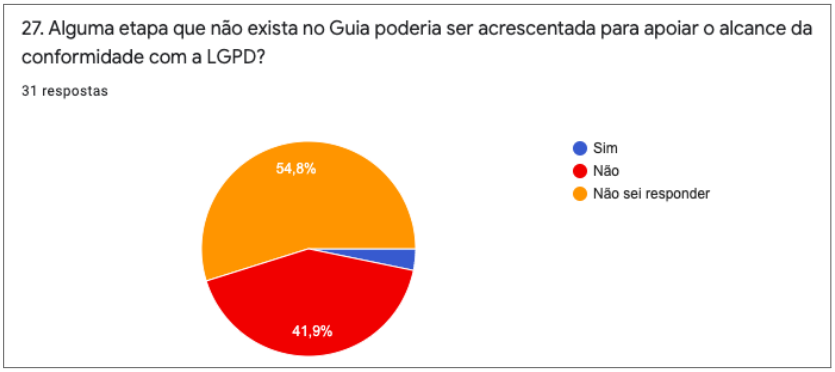
Figura 32 – Treinamento para utilizar os componentes



Fonte: Elaborada pelo Autor (2021).

27. Alguma etapa que não exista no Guia poderia ser acrescentada para apoiar o alcance da conformidade com a LGPD? Dentre os participantes, a Figura 33 mostra que 54,8% não souberam responder, 41,9% responderam Não, 3,2% responderam Sim, e a resposta para este caso foi: *"Poderia colocar uma etapa de avaliação e conscientização."*

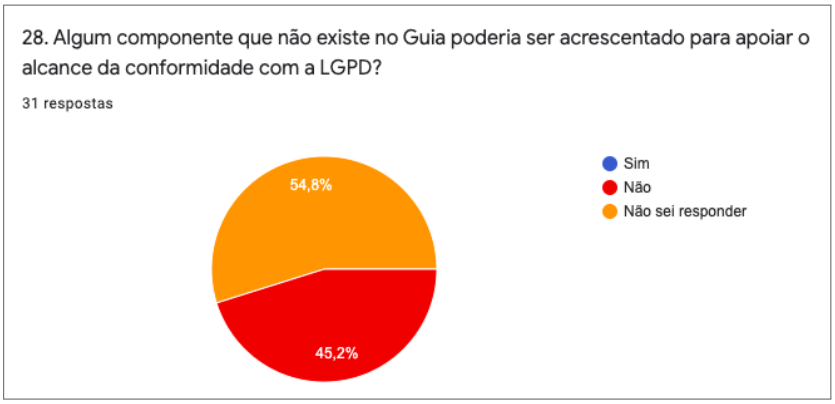
Figura 33 – Etapa do guia que pode ser acrescentada



Fonte: Elaborada pelo Autor (2021).

28. Algum componente que não existe no Guia poderia ser acrescentado para apoiar o alcance da conformidade com a LGPD? Dentre os participantes, a Figura 34 mostra que 54,8% não souberam responder e 45,2% responderam Não.

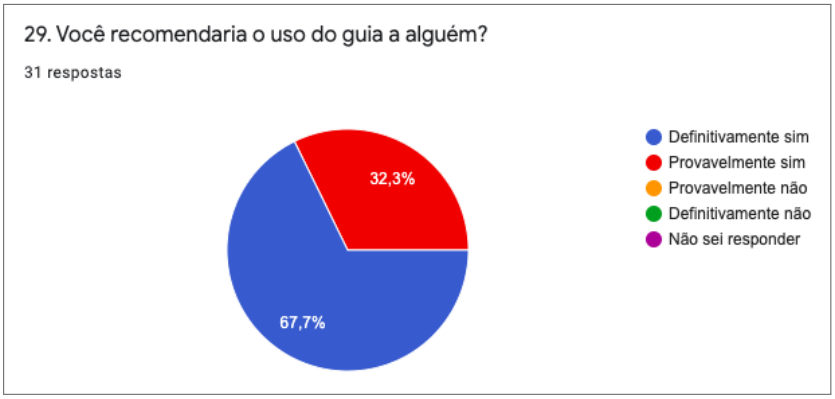
Figura 34 – Componente que pode ser acrescentada



Fonte: Elaborada pelo Autor (2021).

29. Você recomendaria o uso do guia a alguém? Dentre os participantes, a Figura 35 mostra que 67,7% responderam definitivamente sim e 32,3% responderam provavelmente sim.

Figura 35 – Recomendação do uso do Guia



Fonte: Elaborada pelo Autor (2021).

30. Qual recomendação você gostaria de deixar para o autor do Guia? A Tabela 23 apresenta as sugestões e as justificativas dadas pelos participantes.

Tabela 21 – Tabela de respostas do item 17

"Uma sugestão: antes de solicitar a resposta desse formulário, ressaltar a importância para ver o vídeo e depois ler os componentes do guia e, somente depois disso, partir para as respostas. Seria bom listar as ações feitas para resolver as violações identificadas no exemplo (mostrar o antes e o depois)."
"Seja simples, seja direto e claro."
"Algumas tabelas ficaram cortadas na apresentação do guia, se possível ajeitar o layout para facilitar a visualização. No mais a apresentação do guia está ótima, com sistemas de cores agradável e uma linguagem clara, tanto no vídeo quanto no texto."
"Que entre com o pedido de patente e divulgue largamente."
"Sabemos o quanto é complexo implantar a LGPD, talvez implementar esse guia em um software, para ajudar a alcançar a conformidade da Lei. Por exemplo a parte de auditoria de dados."
"Catálogo de controles de privacidade. Pelo fato do detalhamento."
"Persista na pesquisa."
"Como sugestão eu acredito que as atividades descritas nas Etapas seriam melhor representadas e ficariam mais claras se fossem adicionados diagramas do tipo BPMN."

"Condensar o texto nas partes introdutórias. Utilizar fontes maiores."
"Deixar bem didática e clara cada etapa de adequação no guia e colocar bem a sequencia das etapas, e se alguma pode ser feita em concorrência com outra(s)"
"Construção de um curso de realização da implantação da LGPD de forma completa."
"Parabéns pelo trabalho, estou na comissão de implantação da LGPD e já vimos que não será um trabalho simples de fazer. Os passos são úteis, não somente para os desenvolvedores mas para outras áreas. Recomendo fazer esses passos em um software para que possa ajudar as pessoas e tentar ser o mais simples possível."
"Excelente trabalho, continue trabalhando no método para melhorar e aperfeiçoar."
"O guia é excelente, apesar de não trabalhar no meio acadêmico, não encontrei nenhum artigo científico nesta área."

Fonte: Elaborada pelo Autor (2021).

Nesta pergunta, é possível observar diversas opiniões dos participantes da pesquisa. Algumas delas já eram esperadas, como a questão dos textos extensos e as sugestões de diminuir a quantidade de informações nos requisitos de soluções. Havia também a expectativa de que o guia seria útil para as organizações, porém foi bastante satisfatório perceber o apoio dos participantes para a continuidade do trabalho apresentado, com as devidas melhorias sugeridas. Devido à falta de tempo, não foi possível realizar as sugestões de melhorias no trabalho, mas elas representam grande contribuição e foram incluídas no capítulo de trabalhos futuros. Com base no resultado da pesquisa, algumas etapas foram difíceis para o entendimento dos participantes, mas são melhorias que serão feitas no futuro. Em geral, as respostas dos participantes foram satisfatórias para a conclusão deste trabalho.

4.3 CONSIDERAÇÕES FINAIS

Após a realização da pesquisa com os 31 participantes, foi possível obter resultados positivos e todos os participantes recomendariam o uso do guia. Os participantes fazem parte de diversas áreas, mas, em sua maioria, são desenvolvedores de software no setor público. Também foi questionado se o setor onde o participante trabalhava precisava se adequar à LGPD e mais de 90% responderam que sim, o que significa que a maioria conhece ou já ouviu falar

da lei.

De acordo com a avaliação dos participantes, as etapas mais úteis do guia foram Auditoria de Dados e Análise de Lacunas e, de fato, são as mais importantes. Na auditoria, é necessário saber quais dados pessoais a organização está tratando, enquanto a análise de lacunas é importante para avaliar se a organização precisa realmente coletar esses dados, se existe uma hipótese ou base legal para o tratamento desses dados e o que precisa ser feito para que a organização atenda os princípios da lei.

Em relação aos componentes, o mais útil foi o Exemplo de Ilustração de Uso do Guia e o mais difícil foi o Catálogo de Controles de Privacidade. A razão para o catálogo ter sido considerado o mais difícil tem a ver com a extensão do conteúdo do componente, que prevê 40 controles de privacidade. Apesar do desconforto da leitura extensa, o componente é essencial para trabalhar com conformidade dos sistemas de software. Como os próprios participantes apontaram, a escolha do controle ideal para o sistema poderia ser automatizada, mas a implementação dessa melhoria foi registrada para os trabalhos futuros.

Uma pergunta aberta mais geral sobre o guia foi realizada: Qual recomendação você gostaria de deixar para o autor do Guia? As respostas foram incluídas na Tabela 23. Algo que chamou a atenção nas respostas foi a grande aceitação do trabalho proposto e o incentivo para que a pesquisa tenha continuidade, com a melhoria do guia e a criação de um software de apoio para diminuir o esforço da sua aplicação.

5 CONCLUSÃO

A conformidade com a LGPD já é um desafio enorme para as organizações e pode se tornar um processo complexo por envolver diversos fatores. O guia proposto pelo trabalho foi definido com foco nas obrigações estabelecidas no artigo 6º da lei, que prevê 10 princípios fundamentais, eles direcionam tudo o que deve ser feito quanto ao tratamento de dados pessoais, sem saber o conceito dos princípios, é muito difícil colocar em prática as demais medidas da LGPD. Cumprir a lei parcialmente não é o suficiente, devendo as organizações atenderem integralmente as exigências legais para alcançar a conformidade total. A lei exige, por exemplo, que seja indicado um encarregado dos dados e que essa informação esteja prevista, preferencialmente, no site da organização.

Este trabalho propõe um guia com etapas que auxiliam os profissionais de TIC no alcance da conformidade com a LGPD, porém nem todas são obrigatórias. Sugere-se que as etapas fundamentais são a primeira e a segunda, enquanto as demais são apenas complementos.

5.1 CONTRIBUIÇÕES

Este trabalho teve como base a pesquisa realizada por Ayala-Rivera e Pasquale (2018), a partir da qual algumas etapas foram replicadas. Os dois trabalhos tratam de um guia com etapas para a conformidade de uma lei de privacidade vigente, com a diferença de que a presente dissertação trata sobre a LGPD e não sobre a GDPR. Apesar de serem leis parecidas, existem algumas diferenças e contribuições. Uma delas é o modelo de mapeamento de dados, cujo propósito é ajudar a organização a realizar a coleta das informações para cumprir a primeira etapa do guia. Outro artefato é o questionário com perguntas direcionadas aos analistas de sistemas que ajudam a compreender se o sistema atende os princípios legais. Além disso, há os controles de privacidade traduzidos do trabalho de base e definidos a partir dos princípios que os contemplam. Ainda, foi desenvolvido um website com orientações quanto aos passos do guia.

Com o guia proposto, espera-se auxiliar instituições que desejam alcançar a conformidade com a LGPD para que elas não sofram nenhuma sanção da lei. Além do objetivo de contribuir para que profissionais de TIC alcancem a conformidade com a LGPD, espera-se que o trabalho possa ajudar a alavancar outras pesquisas na área. Ainda, espera-se que as etapas do guia

possam ser utilizadas por outros setores de uma organização, além do setor de TIC, pois o guia pode servir como meio de compreensão da LGPD. Portanto, a principal contribuição deste trabalho é ajudar as organizações a entender as obrigações da LGPD e identificar medidas para garantir a conformidade.

Primeiramente foi realizado um levantamento bibliográfico não exaustivo sobre o tema de conformidade com leis de proteção de dados na Engenharia de Requisitos. Em seguida foi proposto um guia de 6 etapas adaptado do GuideMe (AYALA-RIVERA; PASQUALE, 2018). As etapas incluem Auditoria de Dados, Análise de Lacunas, Planejamento e Preparação, Revisão do Plano de Ação, Execução e Revisão Pós-implementação. Para tornar os princípios da LGPD mais compreensíveis para o público e com menos detalhes técnicos, eles foram expressados como requisitos de negócio. Os requisitos de solução vinculam as obrigações da LGPD representadas nos requisitos de negócio aos controles de privacidade necessários para cumpri-las. O guia inclui, também, um modelo de mapeamento de dados que foi criado a partir da experiência do autor com as entrevistas realizadas no IFC - instituição onde trabalha como analista de TI - e com base no modelo de mapeamento disponibilizado pela Secretaria de Governo Digital. Além do modelo de mapeamento, o guia conta com um exemplo de ilustração demonstrando a aplicação das suas etapas no sistema do processo seletivo do IFC. Por fim, a avaliação do guia se deu por meio de um questionário distribuído nacionalmente entre dezembro de 2020 e janeiro de 2021, que recebeu respostas de 31 profissionais.

5.2 LIMITAÇÕES

Este trabalho apresenta algumas limitações, listadas a seguir:

- O processo de utilização do guia ainda é manual;
- O fato de o guia ser extenso pode ter influenciado no número reduzido de participantes que aceitaram avaliá-lo;
- O guia deveria ser validado por especialistas em privacidade. Entretanto, por ser uma lei nova, não foi possível encontrar profissionais especialistas que estivessem disponíveis para participar de uma sessão de validação por meio de um grupo focal.
- Necessidade de treinamento para utilizar alguns componentes e etapas do guia. Uma solução para essa limitação é criar pequenos vídeos que orientem a prática das etapas

do guia.

5.3 SUGESTÕES DE TRABALHOS FUTUROS

Com base nas respostas dos participantes da avaliação do guia, foi possível identificar alguns trabalhos ou projetos para o futuro. Dentre eles, estão os seguintes:

1. Diante do número reduzido de profissionais que participaram da avaliação do guia, é necessário realizar uma nova avaliação visando aumentar a amostra, inclusive para confirmar os resultados iniciais;
2. É preciso avaliar o guia com profissionais especialistas em conformidade legal, utilizando o método grupo focal;
3. Também pretende-se avaliar o guia com profissionais que não sejam da área de TIC, objetivando avaliar se o guia pode beneficiar outros setores da organização além do setor de TI;
4. Modelar as etapas do guia utilizando notação BPMN;
5. Para reduzir o esforço na aplicação do guia, é necessário que exista uma ferramenta para automatizar algumas etapas, como o mapeamento de dados pessoais;
6. Apesar de todas as etapas do guia serem importantes para alcançar a conformidade com a LGPD, alguns participantes propuseram a diminuição no número de etapas, a simplicação do texto de requisitos de negócio e requisitos de solução, e melhorar os controles de privacidade para tornar a sua seleção mais fácil;
7. O guia foca no artigo 6º da LGPD, que trata sobre os 10 princípios, mas poderia ser ampliado para abranger outros artigos da referida legislação.

REFERÊNCIAS

AGOSTINELLI, S.; MAGGI, M. F.; MARRELLA, A.; SAPIO, F. **Achieving GDPR compliance of BPMN process models**. In: International Conference on Advanced Information Systems Engineering, p. 10–22, 2019.

AKAMAI, T. Pesquisa lgpd. In: . [s.n.], 2019. Disponível em: <https://bit.ly/384L4s>.

AKHIGBE, O.; AMYOT, D.; RICHARDS, G. A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. *Requirements Engineering*, v. 24, 12 2019.

ARAÚJO, E. **Análise de conformidade de processos de negócios em relação a LGPD**. TCC (Graduação em Sistemas de Informação) - Centro de Informática, Universidade Federal de Pernambuco. Recife, p. 90, 2020.

AYALA-RIVERA, V.; PASQUALE, L. **The grace period has ended: An approach to operationalize gdpr requirements**. *IEEE*, In: International Conference on Advanced Information Systems Engineering, p. 136–146, 2018.

BRASIL. Decreto n° 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

CANEDO, E. D.; CALAZANS, A. T. S.; MASSON, E. T. S.; COSTA, P. H. T.; LIMA, F. Perceptions of ict practitioners regarding software privacy. *Entropy*, v. 22, n. 4, 2020. ISSN 1099-4300. Disponível em: <https://www.mdpi.com/1099-4300/22/4/429>.

CUNHA, Y. L. d. O.; SANTOS, T. R. R.; CARVALHO, M. E. ***Impactos da transformação digital no modelo de negócios***. [S.l.: s.n.], 2019.

FERNANDES, M.; RODRIGUES, A. S.; GONÇALVES, A.; D. **Specification of Personal Data Protection Requirements - Analysis of Legal Requirements from the GDPR Regulation**. In Proceedings of the 20th International Conference on Enterprise Information Systems, v. 2, p. 398–405, 2018. Disponível em: <https://doi.org/10.5220/0006810603980405>.

GDPR. **General data protection regulation**. 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv\%3AOJ.L_.2016.119.01.0001.01.POR&toc=OJ\%3AL\%3A2016\%3A119\%3AFULL>.

GLASS, R. L. **A structure-based critique of contemporary computing research. Journal of Systems and Software**. Journal of Systems and Software, v. 28, n. 1, p. 3–7, 1995.

GONÇALVES, C. R. ireito civil brasileiro. *Ed. São Paulo: Saraiva*, v. 1, 2012.

HJERPPE, K.; RUOHONEN, J.; LEPPÄNEN, V. The general data protection regulation: Requirements, architectures, and constraints. In: *2019 IEEE 27th International Requirements Engineering Conference (RE)*. [S.l.: s.n.], 2019. p. 265–275.

JACKSON, M. ***The meaning of requirements***. [S.l.]: Brasport Rio de Janeiro, 1997. 5–21 p.

KALLONIATIS, C. Incorporando privacidade no projeto de sistemas baseados em nuvem: um metamodelo conceitual. *Information e Computer Security, 25 (5)*, v. 24, p. 614–633, 2017.

KAMALRUDIN, M.; SIDEK, S. A review on software requirements validation and consistency management. *International Journal of Software Engineering and Its Applications*, v. 9, p. 39–58, 10 2015.

LEHTINEN, T. O.; MäNTYLä, M. V.; VANHANEN, J.; ITKONEN, J.; LASSENIUS, C. Perceived causes of software project failures – an analysis of their relationships. *Information and Software Technology*, v. 56, n. 6, p. 623 – 643, 2014. ISSN 0950-5849. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0950584914000263>.

MENEGAZZI, D. Um guia para alcançar a conformidade da lgpd por meio de requisitos de gegócio e requisitos de solução. In: . [s.n.], 2020. Disponível em: <https://cin.ufpe.br/~dm5/guia-lgpd/>.

NAMBISAN, S. Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. *Entrepreneurship Theory and Practice*, v. 41, n. 6, p. 1029–1055, 2017. Disponível em: <https://doi.org/10.1111/etap.12254>.

NISTALA, P.; NORI, K. V.; REDDY, R. Software quality models: A systematic mapping study. In: *2019 IEEE/ACM International Conference on Software and System Processes (ICSSP)*. [S.l.: s.n.], 2019. p. 125–134.

OTTO, P. N.; ANTÓN, A. I. **Addressing legal requirements in Requirements Engineering.** In: 15th IEEE International Requirements Engineering Conference (RE 2007, Delhi), p. 5–14, 2007.

PEIXOTO, C.; SILVA, C. Especificando requisitos de privacidade com linguagens de modelagem orientadas a objetivos. *No XXXII Simpósio Brasileiro de Engenharia de Software (SBES)*, v. 24, p. 112–121, 2018.

PINHEIRO, P. P. Proteção de dados pessoais: comentários à lei n. 13.709/2018. In: . [S.l.: s.n.], 2019.

PIRAS, L.; AL-OBEIDALLAH, M.; PRAITANO, A.; TSOHOU, A.; MOURATIDIS, H.; GALLEGO-NICASIO, B.; BERNARD, J.-B.; FIORANI, M.; MAGKOS, E.; SANZ, A. C.; PAVLIDIS, M.; D'ADDARIO, R.; ZORZINO, G. Defend architecture: a privacy by design platform for gdpr compliance. In: . [S.l.: s.n.], 2019.

PRESSMAN, R. S. ***Engenharia de Software.****8. Ed*. [S.l.]: São Paulo: McGrawHill, 2016.

RIBEIRO, R. C.; CANEDO, E. D. Using mcda for selecting criteria of lgpd compliant personal data security. In: *The 21st Annual International Conference on Digital Government Research*. New York, NY, USA: Association for Computing Machinery, 2020. (dg.o '20), p. 175–184. ISBN 9781450387910. Disponível em: <https://doi.org/10.1145/3396956.3398252>.

RINGMANN, S. D.; LANGWEG, H.; WALDVOGEL, M. Requirements for legally compliant software based on the gdpr. In: PANETTO, H.; DEBRUYNE, C.; PROPER, H. A.; ARDAGNA, C. A.; ROMAN, D.; MEERSMAN, R. (Ed.). *On the Move to Meaningful Internet Systems. OTM 2018 Conferences*. Cham: Springer International Publishing, 2018. p. 258–276. ISBN 978-3-030-02671-4.

ROJAS, M. A. T.; MEDEIROS, J. K. **Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais**. Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação, v. 1, n. 13, 2021. Disponível em: <https://revistas.setrem.com.br/index.php/reabtic/article/view/391>.

SOMMERVILLE, I. ***Engenharia de Software***. [S.l.]: 8 ed. São Paulo: Pearson Addison-Wesley. Tradução de Selma Shin Shimizu Melnikoff, Reginaldo Arakaki, Edisol de Andrade Barbosa., 2007.

SRIGANESH, S.; RAMANATHAN, C. Externalizing business rules from business processes for model based testing. 03 2012.

THAYER, R.; DORFMAN, M. ***Software requirements engineering*** *IEEE Computer Society Press*. [S.l.]: Los Alamitos, CA, 1997.

VAZQUEZ, C.; SIMÕES, G. ***Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais***. [S.l.]: Brasport Rio de Janeiro, 2016.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. *Harvard law review*, p. 193–220, 1890.

APÊNDICE A – CATÁLOGO DE CONTROLES DE PRIVACIDADE

Princípios da LGPD: 1. Finalidade | 2. Adequação | 3. Necessidade | 4. Livre acesso | 5. Qualidade dos dados | 6. Transparência | 7. Segurança | 8. Prevenção | 9. Não Discriminação | 10. Responsabilização e Prestação de Contas

Tabela 22 – Catálogo de controles de privacidade

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
1	**Controle de acesso:** ao processar dados pessoais, implementar controles de acesso para garantir que os dados pessoais sejam processados apenas por partes autorizadas. ***Problema resolvido:*** impedir o processamento de dados não autorizados. ***Benefício:*** o número de pessoas com acesso aos dados pessoais é minimizado, evitando quebras de segurança e processamento ilegal.						X	X	X		X
2	**Geolocalização:** Quando um usuário deseja compartilhar ou transmitir dados de localização, implementar mecanismos para permitir que o usuário controle o contexto e o tempo para compartilhar os dados conforme sua preferência. ***Problema resolvido:*** transmitir ou compartilhar informações de localização, sem identificar locais de privacidade dos usuários. ***Benefício:*** Melhorar o controle do usuário sobre o compartilhamento de dados pessoais e impedir a divulgação de informações confidenciais.		X		X			X			
3	**Minimização:** Sempre que possível, quando houver coleta de dados pessoais com a finalidade apenas de estatísticas, os dados devem ser anonimizados, e a coleta deve ser a mínima possível, ou seja, evitando a coletar dado desnecessários. ***Problema resolvido:*** A quantidade de dados coletados é maior que o necessário para a finalidade de uso. ***Benefício:*** Melhorar a proteção da privacidade.	X		X				X	X		

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
5	**Anonimização:** Quando o período de retenção de dados expirar e desejar manter os dados pessoais para análise posterior, transforme os atributos dos dados com o objetivo de impedir irreversivelmente a identificação do indivíduo a quem se relacionam. ***Problema resolvido:*** Impedir reidentificação e ataques de vinculação. ***Benefício:*** A LGPD não se aplica a informações anônimas para que o instituto possa reter dados pessoais para análise posterior.					X		X			
6	**Notificação de acesso assíncrono:** quando um serviço rastreia/acessa a localização do usuário continuamente, implemente maneiras proativas e eficazes para notificar o usuário de que as informações estão sendo rastreadas, armazenadas ou redistribuídas. ***Problema resolvido:*** um usuário que deu permissão uma vez (ou a permissão foi forjada), mas cujas informações são acessadas repetidamente / continuamente por um serviço. ***Benefício:*** Aumentar a confiança no serviço e o conforto com a divulgação contínua de informações.	X	X				X				
7	**Credenciais baseadas em atributos:** ao verificar os dados coletados, use credenciais baseadas em atributos para autenticar de forma flexível e seletiva diferentes atributos sobre os dados, sem revelar informações adicionais e identificar o titular dos dados. ***Problema resolvido:*** evite vazamento de informações revelando mais informações do que o necessário. ***Benefício:*** a propriedade dos atributos pode ser verificada anonimamente.							X	X		
8	**Auditoria:** Quando a avaliação dos esforços de conformidade é necessária, um processo de auditoria pode ser conduzido para determinar se a organização implementou políticas e procedimentos adequados para regular o processamento de dados pessoais. ***Problema resolvido:*** demonstrar conformidade e identificar as melhores práticas para segurança da informação. Também encontrar possíveis riscos. ***Benefício:*** Melhoria da conformidade.								X		X

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
9	**Painel de confiabilidade:** quando o sistema solicitar a inserção de dados pessoais para utilizar um serviço, apresente ao usuário a finalidade dos dados pessoais coletados, e em seguida, um painel contendo um resumo dos dados pessoais a serem enviados. ***Problema resolvido:*** os usuários superestimam a quantidade de dados pessoais necessários para usar um serviço. ***Benefício:*** Facilita a seleção de credenciais adequadas para o usuário; aumenta a transparência sobre os dados pessoais que são compartilhados.				X	X	X				
10	**Notificação de violação de dados:** sempre que ocorrer uma violação de dados, notifique a autoridade supervisora e os usuários afetados imediatamente. ***Problema resolvido:*** violação de dados. ***Benefício:*** mitigar danos, aumentar a transparência.						X				X
11	**Rastreamento de dados:** quando os usuários expõem dados pessoais, o serviço deve fornecer uma plataforma de rastreamento e de compartilhamento de dados pessoais. Também devem, ter a possibilidade de corrigir e excluir dados dos serviços. ***Problema resolvido:*** para evitar que os titulares dos dados percam os dados pessoais que divulgaram. ***Benefício:*** os titulares dos dados têm controle sobre os dados divulgados sobre eles, exercendo seus direitos de proteção de dados.		X			X					X
12	**Privacidade diferencial:** ao processar dados pessoais para análise estatística, um algoritmo pode ser fornecido para adicionar hash aleatório aos dados antes de serem disseminados para minimizar a identificação. ***Problema resolvido:*** Reidentificação de indivíduos; vazamento de informações. ***Benefício:*** Preserve a privacidade dos usuários.					X	X	X			

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
13	**Geolocalização dinâmica:** ao processar/-disseminar dados de localização, forneça mecanismos para unir dados pessoais baseados em localização para garantir que vários usuários estejam no mesmo local relatado. ***Problema resolvido:*** vazamento de informações. ***Benefício:*** Proteja a privacidade dos indivíduos.							X	X		
14	**Política de Privacidade:**Quando o usuário fornece dados pessoais após certas ações em um site (por exemplo, login, registro), uma abordagem de apresentação em várias camadas (como o padrão de Exibição da Política de Privacidade) pode ser estendida por dicas de ferramentas de informações dinâmicas que informam o usuário sobre a natureza dos dados divulgados e possíveis consequências. ***Problema resolvido:*** falta de consciência sobre as possíveis consequências ao liberar dados pessoais. ***Benefício:*** tomada de decisão mais bem informada sobre a natureza dos dados que os usuários divulgam e possíveis consequências.						X				
15	**Criptografia:** Quando os dados devem ser ocultados da visualização simples, forneça mecanismos de criptografia para embaralhar o conteúdo de uma mensagem/arquivo para que ele possa ser lido apenas na visualização autorizada, decodificando-o. ***Problema resolvido:*** visualização não autorizada. ***Benefício:*** Proteja os dados em trânsito.							X			
16	**Atividades suspeitas:** ao usar um serviço que requer autenticação, implemente mecanismos para monitorar atividades incomuns, notifique o titular da conta quando isso acontecer e use a autenticação multifator para evitar acessos suspeitos. ***Problema resolvido:*** detecção e prevenção de atividades de autenticação suspeitas. ***Benefício:*** segurança aprimorada para serviços de autenticação.						X				

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
17	**Ilustração de políticas de privacidade:** ao apresentar uma política de privacidade ao usuário, utilize ícones para descrever a política para torná-la mais fácil de entender e ser mais transparente sobre o uso de dados. ***Problema resolvido:*** as políticas de privacidade costumam extensas e complicadas. ***Benefício:*** aumente a transparência do uso de dados e melhore o processo de tomada de decisão (por exemplo, para dar/-revogar consentimento).							X			
18	**Consentimento informado:** sempre que a coleta/divulgação de dados precisar ser legitimada, forneça acordos de clique ("clique e aceite") para confirmar a compreensão ou consentimento do usuário "conforme necessário"usando ações de arrastar e soltar para divulgação de dados consentida. ***Problema resolvido:*** impedir que os usuários aceitem os termos e condições de um serviço "com muita facilidade"(devido aos longos termos legais) sem ter lido ou entendido o que eles consentiram. ***Benefício:*** garantir que os titulares dos dados entendam totalmente e concordem inequivocamente com o processamento de seus dados pessoais.	X									X
19	**Log:** sempre que o controlador de dados tiver que provar que está no controle, implemente o log para demonstrar conformidade. ***Problema resolvido:*** impedir um comportamento não conforme. ***Benefício:*** a organização pode demonstrar conformidade com a legislação de segurança da informação e prevenir fraude e outros incidentes.										X
20	**Redes Mix:** Em qualquer comunicação (via Internet) que envolva dados pessoais, forneça protocolos de roteamento que criam comunicações difíceis de rastrear usando uma cadeia de servidores proxy conhecidos como mixes. ***Problema resolvido:*** rastreamento de comunicação ponta a ponta. ***Benefício:*** Unlinkability (sem rastreio de um receptor ao remetente).							X	X		

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
21	**Roteamento Onion:** Em um sistema no qual os dados são roteados entre nós diferentes, implemente a criptografia de dados em camadas em cada estação no caminho de entrega para que todas as partes conheçam apenas o sucessor imediato e o predecessor. ***Problema resolvido:*** cada estação no caminho de entrega conhece o remetente e o destino. ***Benefício:*** comunicação anônima.							X			
22	**Projeto de plataforma para preferências de privacidade (P3P):** Ao navegar na web, permite que os sites expressem as práticas de privacidade em um formato padrão que pode ser recuperado automaticamente e interpretado pelo navegador da web e outras ferramentas de software do usuário final. ***Problema resolvido:*** diversos formatos usados para expressar políticas de privacidade em sites. ***Benefício:*** dê aos usuários mais controles sobre seus dados pessoais durante a navegação; os usuários serão mais bem informados sobre as práticas do site.						X	X			
23	**Exibição correspondente à política:** sempre que um usuário for solicitado a consentir com a divulgação de dados pessoais a um site de serviço, forneça uma ferramenta na qual os usuários insiram suas configurações de privacidade preferidas e, em seguida, ele pode ser informado de uma maneira perceptível, mas não intrusiva, sobre a distância as configurações de privacidade correspondem à política de serviços. ***Problema resolvido:*** dificuldade de identificar se os termos de uma política correspondem à privacidade e segurança esperadas de um usuário. ***Benefício:*** Melhore a compreensão e a transparência das políticas de privacidade.		X		X		X				
24	**Texto com reconhecimento de privacidade:** sempre que os usuários forem obrigados a divulgar dados pessoais em software de privacidade e segurança, use apenas frases e termos claros e compreensíveis para que o público possa entendê-los. ***Problema resolvido:*** dificuldade de entender a terminologia em software de privacidade e segurança. ***Benefício:*** Melhor controle de dados pessoais; tomada de decisão melhor informada.	X					X				

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
25	**Painel de Conscientização de Privacidade em Espaços de Trabalho Colaborativos:** Em um espaço de trabalho colaborativo, use um painel para mostrar ao usuário qual público (por exemplo, em um fórum) pode acessar sua contribuição (por exemplo, postar) e também apontar que os fornecedores têm informações identificáveis sobre o usuário (por exemplo, endereço IP, geolocalização). ***Problema resolvido:*** falta de consciência sobre o nível de anonimato e a esfera privada no espaço de trabalho colaborativo. ***Benefício:*** tomada de decisão mais bem informada (se os usuários desejam divulgar dados pessoais em suas contribuições para espaços de trabalho colaborativos).				X		X				
26	**Cliente de rede com reconhecimento de privacidade:** no domínio do navegador da web, facilite a compreensão das políticas de privacidade para os usuários, convertendo-as automaticamente em um formato claro e fácil de ler, adequado para um público mais geral. Uma solução é implementar um proxy de privacidade para analisar e interpretar as políticas para que possam ser convertidas posteriormente em um formato amigável. ***Problema resolvido:*** políticas de privacidade difíceis de entender. ***Benefício:*** aumentar o conhecimento do usuário sobre as políticas de privacidade; tomada de decisão mais informada; Detectar mud						X	X			X
27	**Codificação de cores de privacidade:** sempre que um usuário compartilha/publica dados pessoais e conteúdos em um aplicativo, use cores distintas para mostrar os efeitos da aplicação de configurações de privacidade (por exemplo, vermelho para aviso) sobre o conteúdo. ***Problema resolvido:*** as configurações de conteúdo e dados compartilhados muitas vezes não são óbvias para o usuário. ***Benefício:*** Evita que ações indesejadas ocorram ao compartilhar um conteúdo e dados.						X				

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
28	**Painel de privacidade:** quando um serviço coleta ou processa dados pessoais de usuários, forneça a eles resumos/visão geral coletados de seus dados pessoais em um painel de privacidade. ***Problema resolvido:*** os usuários podem não se lembrar ou perceber quais dados um determinado serviço, ou empresa coletou. ***Benefício:*** Usuários pode ter uma visão geral dos dados pessoais coletados sobre eles.	X			X		X				
29	**Agendamento de grupo com privacidade aprimorada:** ao usar aplicativos de agendamento, permite que os usuários planejem um evento sem revelar a "disponibilidade"das pessoas. ***Problema resolvido:*** os planejadores de eventos divulgam "padrões de disponibilidade"detalhados de seus usuários. ***Benefício:*** Garante a liberdade de escolha (evite pressão social) e sigilo dos padrões de disponibilidade.				X						
30	**Ícones de privacidade:** sempre que um aplicativo usam ícones relacionados à segurança e privacidade, torne distinguíveis, consistentes, compreensíveis e representativos da finalidade subjacente. ***Problema resolvido:*** ícones de privacidade não intuitivos usados em aplicativos. ***Benefício:*** Tomada de decisão mais bem informada sobre suas informações privadas.						X				
31	**Exibição da Política de Privacidade:** sempre que o usuário precisa inserir dados pessoais, use o formato de várias camadas (aviso curto, condensado ou completo) sob o qual cada camada deve oferecer aos indivíduos as informações necessárias para entender sua posição e tomar decisões. ***Problema resolvido:*** privacidade declaração em sites da web conténs longas frases legais que geralmente não são compreensíveis para a maioria dos usuários. ***Benefício:*** os usuários têm melhor controle dos dados pessoais; tomada de decisão mais bem informada sobre a divulgação de dados pessoais.						X				

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
32	**Link privado:** quando os usuários desejam compartilhar conteúdos privados (acessível online) usando os mecanismos de comunicação existentes, forneça ao usuário um link privado ou URL indescritível para um determinado conjunto de seus dados pessoais. ***Problema resolvido:*** compartilhe conteúdo privado com contatos que não podem ser facilmente autenticados. ***Benefício:*** compartilhe informações sem ampla visibilidade pública e fácil controle de acesso autenticado.					X	X				
33	**Proteção contra rastreamento:** quando o usuário interage com a web, restringe o uso de cookies no lado do cliente, excluindo cookies regularmente para remediar que informação pessoalmente identificável é rastreado por meio de ferramentas de software, protocolos ou outros mecanismos (por exemplo, cookies). ***Problema resolvido:*** os sites coletam informações sobre os usuários que afetam a privacidade e o anonimato. ***Benefício:*** rastreamento limitado.					X	X				
34	**Pseudonimização:** Sempre que houver tratamento de dados pessoais, substituir as características de identificação dos dados por um pseudônimo, ou seja, por um valor que não permita que o titular dos dados seja diretamente identificado. ***Problema resolvido:*** os dados podem ser vinculados a um determinado indivíduo. ***Benefício:*** Manter o anonimato até certo ponto. Reduza a intromissão de privacidade.						X	X			
35	**Senhas seguras:** ao usar interfaces de alteração de senha, utilize mecanismos (passivo [botão de ajuda], estático [pop-ups] ou dinâmico [mensagem de ajuste dinâmico como medidor de força]) para ajudar os usuários a criar senhas seguras. ***Problema resolvido:*** os usuários escolhem senhas fáceis. ***Benefício:*** senhas mais seguras, o usuário obtém feedback sobre a segurança da senha.									X	

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
36	**Selecione antes de coletar:** Em situações cuja criação de perfil pode ocorrer, os dados necessários para cumprir uma finalidade devem ser selecionados antes da coleta. ***Problema resolvido:*** evite a coleta indiscriminada de dados confidenciais para evitar qualquer forma de processamento automatizado de dados pessoais, como perfis. ***Benefício:*** a quantidade de dados pessoais coletados é reduzida e também são as consequências implícitas que podem prejudicar o titular dos dados.									X	
37	**Acesso seletivo de controle de acesso/-privacidade aprimorada:** em plataformas cujos usuários podem postar/compartilhar conteúdo (fórum, OSNs), forneça aos usuários a opção de definir o público de suas contribuições (alterar as configurações de privacidade), especificando as regras de acesso aos seus próprios tópicos e publicações para aumentar a privacidade dos usuários. ***Problema resolvido:*** falta de controles de privacidade ao divulgar dados em provedores de fóruns. ***Benefício:*** controle aprimorado sobre a divulgação de dados pessoais.				X	X		X			
38	**Políticas fixas:** quando os dados são transmitidos por meio das fronteiras organizacionais, anexe condições e restrições (que descrevem como os dados devem ser tratados) aos dados para melhorar o controle sobre as informações pessoais dos usuários. ***Problema resolvido:*** torne o gerenciamento de privacidade eficaz quando as informações são transmitidas entre as partes. ***Benefício:*** melhor controle sobre as informações pessoais dos usuários.					X					

ID	Controles de Privacidade	1	2	3	4	5	6	7	8	9	10
39	**Retirar metadados invisíveis:** quando um serviço requer que um usuário importe dados de fontes externas (por exemplo, fotos, tweets, documentos), os usuários não estão cientes que diferentes categorias de metadados podem ser transmitidos, revelando mais informações sobre eles. A remoção de todos os metadados que não são diretamente visíveis durante o upload ou durante o uso do serviço ajudaria a proteger os serviços de vazamentos e responsabilidades. ***Problema resolvido:*** compartilhamento de mais informações do que o necessário ao transmitir dados. ***Benefício:*** proteja os serviços de vazamentos e responsabilidades.						X	X	X		
40	**Avaliação de confiança por parte dos serviços:** ao usar plataformas que gerenciam os dados dos usuários (por exemplo, sites de e-commerce, softwares), implemente ferramentas que integrem funções de avaliação de confiança para avaliar a confiabilidade e garantia dos sistemas e seus parceiros de comunicação. Essas funções podem avaliar os sistemas em práticas e confiabilidade de privacidade. ***Problema resolvido:*** faça com que as pessoas confiem nas afirmações sobre recursos de melhoria de privacidade em sistemas. ***Benefício:*** estabeleça a confiança confiável nos parceiros de comunicação.				X	X	X	X			X

Fonte: Adaptado de Ayala-Rivera (2018)

APÊNDICE B – REQUISITOS DE SOLUÇÃO

Tabela 23 – Cenário 1 - [I - Princípio da Finalidade]

ID do requisito:	**SREQ-1**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **finalidade** que deve ser específica e informada explicitamente ao titular, sem possibilidade de tratamento de dados posterior de forma incompatível com essas finalidades, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-1, mapeado da Lei 13.709 - LGPD Art. 6º, inciso I. Esse requisito especifica que o Instituto Federal deve ter pelo menos uma base legal válida para processar dados pessoais. O Instituto deve determinar a base legal antes de iniciar o processamento e documentação de dados pessoais. A escolha da base jurídica dependerá da finalidade do processamento de dados. Se a finalidade for alterada, o Instituto deverá reavaliar a base ou poderá manter a base original somente se a nova finalidade for compatível com a finalidade inicial. Para ajudar a satisfazer a BREQ-1 no contexto do cenário 1, o profissional implementará o controle **consentimento informado** (identificado pelo ID **18** do catálogo de controles de privacidade) para resolver o problema de os usuários aceitarem os termos e condições de um serviço "com muita facilidade" sem terem lido ou entendido o que estavam aceitando. Esse controle de privacidade envolve que sempre que a coleta de dados precisar ser legitimada, forneça contratos de clique ("clique e aceite") para confirmar o entendimento ou consentimento do usuário "conforme necessário", usando ações de arrastar e soltar para consentir a divulgação de dados. Como resultado, a organização pode garantir que os titulares dos dados entendam totalmente e concordem com o processamento de seus dados pessoais.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Consentimento informado, Finalidade, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 24 – Cenário 1 - [II - Princípio da Adequeação]

ID do requisito:	**SREQ-2**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **adequação** que deve usar os dados de modo compatível com a finalidade informada ao titular, e de acordo com o contexto do tratamento dos dados. Ou seja, os dados não podem ser utilizados para outros fins, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-2, mapeado da Lei 13.709 - LGPD Art. 6º, inciso II. Esse requisito especifica que o Instituto Federal deve usar os dados de modo compatível com a finalidade informada ao titular, e de acordo com o contexto do tratamento dos dados. Ou seja, sua justificativa deve fazer sentido com o caráter da informação solicitada. Assim, o tratamento de dados deverá ser condizente à destinação a qual se refere, não apresentando de forma contraditória à finalidade destinada. A coleta de dados deverá ser compatível com a atividade fim do tratamento, não podendo apresentar uma relação divergente entre o titular dos dados e o controlador. Para ajudar a satisfazer a BREQ-2, no contexto do cenário 1, o profissional implementará o controle **exibição correspondente à política** (identificado pelo ID **23** do catálogo de controles de privacidade) para resolver o problema da dificuldade de identificar se os termos de uma política de privacidade correspondem à privacidade e segurança esperadas de um usuário de acordo com a finalidade. Esse controle de privacidade aplica-se sempre que um usuário for solicitado a consentir com a divulgação de dados pessoais a um site de serviço, forneça uma ferramenta na qual os usuários insiram suas configurações de privacidade preferidas e, em seguida, poderá ser informado de uma maneira perceptível, mas não intrusiva, sobre a distância as configurações de privacidade correspondem à política de serviços. Como resultado, a organização melhora a compreensão e a transparência das políticas de privacidade.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Adequação, Política de privacidade, Princípio, Transparência.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 25 – Cenário 1 - [III - Princípio da Necessidade]

ID do requisito:	**SREQ-3**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **necessidade** para evitar o acúmulo de dados redundantes ou desnecessários e minimizar os riscos de uma violação de dados, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-3, mapeado da Lei 13.709 - LGPD Art. 6º, inciso III. Esse requisito especifica que o Instituto Federal deve realizar o tratamento de dados pessoais somente se for necessário e relevante para a realização da finalidade definida. Sempre que possível, a coleta deve ser a mínima possível, coletando somente dados necessários para cumprir o propósito. Para ajudar a satisfazer a BREQ-3 no contexto do cenário 1, o profissional implementará o controle **minimização** (identificado pelo ID **3** do catálogo de controles de privacidade) para resolver o problema de coletar mais dados do que o necessário para a finalidade de uso. Esse controle de privacidade diz que, sempre que possível, quando houver coleta de dados pessoais com a finalidade apenas de estatísticas, os dados devem ser anonimizados, e a coleta deve ser a mínima possível, ou seja, evitando a coletar dado desnecessários. Como resultado, essa solução irá melhorar a proteção da privacidade e a minimização dos dados.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Finalidade, Minimização de dados, Necessidade, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 26 – Cenário 1 - [IV - Princípio do Livre acesso]

ID do requisito:	**SREQ-4**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado(a) a cumprir o princípio do **livre acesso** e garantir aos titulares dos dados uma consulta, de forma fácil e gratuita, sobre a forma como é realizado o tratamento de dados e sua duração, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-4, mapeado da Lei 13.709 - LGPD Art. 6º, inciso IV. Este requisito especifica que o Instituto Federal deve garantir aos titulares dos dados uma consulta de forma fácil e gratuita, sobre a forma como é realizado o tratamento de dados e sua duração. Ou seja, o Instituto Federal não deve manter os dados pessoais por mais tempo do que o necessário para atingir a finalidade específica, exceto nos casos em que tenha uma base legal, ou legislação vigente para justificar o armazenamento dos dados. O Instituto Federal também deve tomar medidas técnicas para proteger a integridade dos dados pessoais. Para ajudar a satisfazer a BREQ-4 no contexto do cenário 1, o profissional implementará o controle **painel de privacidade** (identificado pelo ID **28** do catálogo de controles de privacidade) para resolver o problema de os usuários esquecerem ou não perceberem quais dados um determinado serviço ou empresa coletou. Esse controle de privacidade diz que quando um serviço coleta ou processa dados pessoais de usuários, deve fornecer a eles resumos ou uma visão geral dos seus dados pessoais coletados em um painel de privacidade. Como resultado, os usuários podem ter uma visão geral dos seus dados pessoais coletados.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Dados coletados, Livre acesso, Painel de privacidade, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 27 – Cenário 1 - [V - Princípio da Qualidade dos dados]

ID do requisito:	**SREQ-5**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **qualidade dos dados** e implementar medidas para garantir aos titulares, exatidão, clareza, relevância e atualização dos dados, que deve ser especificada e informada ao titular, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-5, mapeado da Lei 13.709 - LGPD Art. 6º, inciso V. Esse requisito especifica que o Instituto Federal deve implementar medidas para garantir aos titulares, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Para ajudar a satisfazer a BREQ-5, no contexto do cenário 1, o profissional implementará o controle **avaliação de confiança por parte dos serviços** (identificado pelo ID **40** do catálogo de controles de privacidade) para resolver o problema de confiabilidade nas afirmações sobre recursos de melhoria de privacidade dos sistemas. Esse controle de privacidade envolve ao usar plataformas que gerenciam os dados dos usuários (por exemplo, sites de e-commerce, software), implemente ferramentas que integrem funções de avaliação de confiança para avaliar a confiabilidade e garantia dos sistemas e seus parceiros de comunicação. Essas funções podem avaliar os sistemas em termos de práticas de privacidade e confiabilidade da privacidade. Como resultado, a organização estabelece uma confiança nos parceiros de comunicação.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Confiabilidade, Integralidade, Qualidade dos dados, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 28 – Cenário 1 - [VI - Princípio da Transparência]

ID do requisito:	**SREQ-6**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **transparência**, garantindo aos titulares informações claras e precisas sobre o tratamento de seus dados pessoais, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-6, mapeado da Lei 13.709 - LGPD Art. 6º, inciso VI. Este requisito especifica que o Instituto Federal deve atender ao princípio da transparência, garantindo aos titulares informações claras e precisas sobre o tratamento de seus dados pessoais. Caso a organização tenha o consentimento do titular, é necessário informar qual a finalidade de uso dos seus dados e essa informação deve ser de fácil compreensão. Sempre que houver uma mudança da finalidade, o usuário deve ser informado da mudança e deve realizar um novo consentimento para a nova finalidade. Também é necessário que a organização adote medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. Para ajudar a satisfazer a BREQ-6 no contexto do cenário 1, o profissional implementará o controle **painel de confiabilidade** (identificado pelo ID **9** do catálogo de controles de privacidade) para resolver o problema dos usuários superestimam a quantidade de dados pessoais necessários para usar um serviço. Esse controle de privacidade diz que quando um sistema solicitar a inserção de dados pessoais para utilizar um serviço, deve apresentar ao usuário a finalidade de uso dos dados pessoais a serem enviados e, em seguida, deve apresentar um painel contendo um resumo desses dados pessoais. Como resultado, isso facilita a seleção de credenciais adequadas para o usuário e aumenta a transparência sobre os dados pessoais que serão compartilhados.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Confiabilidade, Princípio, Transparência.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 29 – Cenário 1 - [VII - Princípio da Segurança]

ID do requisito:	**SREQ-7**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **segurança**, garantindo medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-7, mapeado da Lei 13.709 - LGPD Art. 6º, inciso VII. Este requisito especifica que o Instituto Federal deve garantir medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, incluindo situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Atua junto ao princípio da prevenção, uma vez que realiza-se a contratação de mecanismos de segurança exatamente para mitigar e poder prevenir de eventuais incidentes. Para ajudar a satisfazer a BREQ-7, no contexto do cenário 1, o profissional implementará o controle **criptografia** (identificado pelo ID **15** do catálogo de controles de privacidade) para resolver o problema de visualização não autorizada. Esse controle de privacidade aplica-se quando os dados devem ser ocultados da visualização simples, forneça mecanismos de criptografia para embaralhar o conteúdo de uma mensagem/arquivo para que possa ser lido apenas na visualização autorizada, decodificando-o. Como resultado, proteja os dados em trânsito.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Criptografia, Prevenção, Princípio, Segurança.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 30 – Cenário 1 - [VIII - Princípio da Prevenção]

ID do requisito:	**SREQ-8**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **prevenção**, garantindo medidas técnicas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-8, mapeado da Lei 13.709 - LGPD Art. 6º, inciso VIII. Este requisito especifica que o Instituto Federal deve garantir que as medidas técnicas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, ou seja, a organização deve agir antes dos problemas e não somente depois. Para ajudar a satisfazer a BREQ-8, no contexto do cenário 1, o profissional implementará o controle **atividades suspeita** (identificado pelo ID **16** do catálogo de controles de privacidade) para resolver o problema da detecção e prevenção de atividades de autenticação suspeitas. Esse controle de privacidade envolve ao usar um serviço que requer autenticação. Implementar mecanismos para monitorar atividades incomuns, que notifique o titular da conta quando isso acontecer e use a autenticação multifator para evitar acessos suspeitos. Como resultado, segurança aprimorada para serviços de autenticação.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Prevenção, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 31 – Cenário 1 - [IX - Princípio da Não Discriminação]

ID do requisito:	**SREQ-9**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **não discriminação**, a organização quando realizar um tratamento de dados, não poderá discriminar ou promover abusos contra os titulares dos dados, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-9, mapeado da Lei 13.709 - LGPD Art. 6º, inciso IX. Este requisito especifica que o Instituto Federal quando realiza um tratamento de dados pessoais, não poderá discriminar ou promover abusos contra os titulares dos dados. O princípio diz respeito, principalmente, pelo tratamento de dados sensíveis, ou seja, não é permitido utilizar o dados para fins que gerem discriminação. Para ajudar a satisfazer a BREQ-9, no contexto do cenário 1, o profissional implementará o controle **selecione antes de coletar** (identificado pelo ID **36** do catálogo de controles de privacidade) para resolver o problema de coleta indiscriminada de dados confidenciais para evitar qualquer forma de processamento automatizado de dados pessoais, como perfis. Esse controle de privacidade envolve-se em situações cuja criação de perfil pode ocorrer, os dados necessários para cumprir uma finalidade devem ser selecionados antes da coleta. Como resultado, a quantidade de dados pessoais coletados é reduzida e também as consequências implícitas que podem prejudicar o titular dos dados.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Dados sensíveis, Não discriminação, Princípio.

Fonte: Adaptado de Ayala-Rivera (2018)

Tabela 32 – Cenário 1 - [X - Princípio da Responsabilização e Prestação de Contas]

ID do requisito:	**SREQ-10**
Declaração de requisitos:	De acordo com a LGPD, o Instituto Federal Catarinense (IFC) é obrigado a cumprir o princípio da **responsabilização e prestação de contas**, onde a organização deve documentar as medidas usadas para tratamento dos dados pessoais e ser capaz de demonstrar a sua conformidade com a LGPD, podendo sofrer as sanções administrativas previstas no art. 52 da lei, caso o princípio não seja atendido. Este princípio é expresso pelo requisito BREQ-10, mapeado da Lei 13.709 - LGPD Art. 6º, inciso X. Este requisito especifica que o Instituto Federal deve documentar as medidas usadas para tratamento dos dados pessoais e ser capaz de demonstrar sua conformidade com a LGPD. Sempre demonstrando sua boa-fé. Para ajudar a satisfazer o BREQ-10 no contexto do cenário 1, o profissional implementará o controle **notificações de violação de dados** (identificado pelo ID **10** da entrada do catálogo de controles de privacidade) para resolver o problema de violação de dados. Esse controle de privacidade diz que sempre que ocorrer uma violação de dados, é mandatório notificar a autoridade supervisora e os usuários afetados imediatamente. Como resultado, isso irá mitigar danos e aumentar a transparência.
Autor:	Diego Menegazzi
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Documentação, Notificações, Princípio, Responsabilização e prestação de contas.

Fonte: Adaptado de Ayala-Rivera (2018)

APÊNDICE C – MODELO DE MAPEAMENTO DE DADOS

ID	Dados Coletados	Base Legal	Sensível?	Categoria	Forma de Coleta	Setor Responsável	Compartilha?
1	Nome completo	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
2	Endereço	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
3	RG	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
4	CPF	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
5	E-mail	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
6	Curso	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
7	Campus	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
8	Ampla Concorrência	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
9	Sistema Cotas	-	Sim	Cadastrais	Sistema Web	CGAI	Sim, RACI
10	Deslocamento	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
11	Processo Seletivo	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI
12	Urbana ou Rural	-	Não	Cadastrais	Sistema Web	CGAI	Sim, RACI

Fonte: Elaborada pelo Autor (2021)

APÊNDICE D – QUESTIONÁRIO DE AVALIAÇÃO DO GUIA

1º Conjunto - Perfil e Experiências
1. Qual é o seu papel atual na organização? ( ) Analista de negócios ( ) Líder de negócio ( ) Scrum master ( ) Gerente de projetos ( ) Gerente de requisitos ( ) Engenheiro ( ) Arquiteto ( ) Desenvolvedor ( ) Gerente de Teste/Testador ( ) Product owner ( ) Epic Owner ( ) Product Manager ( ) Outros
2. Qual a sua área de atuação? ( ) Finanças ( )Setor público ( ) Saúde ( ) Comércio eletrônico ( ) Telecomunicações ( ) Automotiva ( ) Logística ( ) Empreendimento ( ) Recursos Humano ( ) Transporte ( ) Segurança ( ) Agricultura ( ) Jogos ( ) Engenharia ( ) Jurídica ( ) Tecnologia ( ) Outros
3. Quantos anos de experiência profissional você tem na área ? ( ) Entre 1-5 ( ) Entre 6-10 ( ) Entre 11-15 ( ) Mais de 15 anos
4. O seu setor de trabalho precisa estar em conformidade com a Lei 13.709 - Lei Geral de Proteção de Dados (LGPD)? ( ) Sim ( ) Não ( ) Não sei responder
5. Qual o seu grau de familiaridade com os Princípios Lei Geral de Proteção de dados - LGPD (Artigo 6)? ( ) Nem um pouco (não tem conhecimento desta Lei) ( ) Familiaridade limitada (consciente, mas não conhece os detalhes) ( ) Familiar (conhece alguns detalhes) ( ) Experiente (bastante familiar, mas não conhece todos os detalhes) ( ) Especialista (profundo conhecimento da Lei e detalhes)
2º Conjunto - Quão ÚTIL você classifica as diferentes etapas do guia?
6. Etapa 1 do Guia | Auditoria de dados ( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder
7. Etapa 2 do Guia | Análise de Lacunas ( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

8. Etapa 3 do Guia | Planejamento e Preparação

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

9. Etapa 4 do Guia | Revisão do Plano de Ação

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

10. Etapa 5 do Guia | Execução

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

11. Etapa 6 do Guia | Revisão Pós-Implementação

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

3º Conjunto - Quão ÚTIL você classifica os diferentes componentes do guia?

12. Requisitos de negócio

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

13. Requisitos de solução

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

14. Catálogo de controles de privacidade

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

15. Exemplo de ilustração de uso do Guia

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

16. Vídeo de explicação de uso do Guia

( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

17. Qual foi o componente mais ÚTIL do Guia e por quê?
R:

4º Conjunto - Quão DIFÍCIL de compreender você classifica os componentes do Guia?

18. Requisitos de negócio
( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

19. Requisitos de solução
( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

20. Catálogo de controles de privacidade
( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

21. Exemplo de ilustração de uso do Guia
( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

22. Vídeo de explicação de uso do Guia
( ) Extremamente útil ( ) Muito útil ( ) Moderadamente útil ( ) Nada útil ( ) Não sei responder

23. Qual foi o componente mais difícil do Guia e porquê?
R:

5º Conjunto - Últimas perguntas

24. Algum componente do Guia pode ser considerado desnecessário para apoiar o alcance da conformidade com a LGPD? (Os componentes do Guia são Requisitos de negócio, Requisitos de solução, Catálogo de controles de privacidade, Exemplo de ilustração de uso e Vídeo de explicação de uso)
( ) Sim, qual?_____ ( ) Não ( ) Não sei responder

25. Você acha que precisaria de treinamento para executar as etapas deste Guia? (As etapas do Guia são: Auditoria de dados, Análise de Lacunas, Planejamento e Preparação, Revisão do Plano de Ação, Execução e Revisão Pós-Implementação)
( ) Definitivamente sim ( ) Provavelmente sim ( ) Provavelmente não ( ) Definitivamente não ( ) Não sei responder

26. Você acha que precisaria de treinamento para utilizar os componentes deste Guia?
( ) Definitivamente sim ( ) Provavelmente sim ( ) Provavelmente não ( ) Definitivamente não ( ) Não sei responder

27. Alguma etapa que não exista no Guia poderia ser acrescentada para apoiar o alcance da conformidade com a LGPD?
( ) Sim, qual?_____ ( ) Não ( ) Não sei responder

28. Algum componente que não existe no Guia poderia ser acrescentado para apoiar o alcance da conformidade com a LGPD?
( ) Sim, qual?_____ ( ) Não ( ) Não sei responder

29. Você recomendaria o uso do guia a alguém?
( ) Definitivamente sim ( ) Provavelmente sim ( ) Provavelmente não ( ) Definitivamente não ( ) Não sei responder

30. Qual recomendação você gostaria de deixar para o autor do Guia?
R:

APÊNDICE E – QUESTIONÁRIO DE ANÁLISE DE LACUNAS

Princípios	**Perguntas**
Finalidade Transparência	**1** - Quando o usuário realiza o cadastro no sistema, é apresentado quais dados pessoais estão sendo coletados e para qual a finalidade? ( )Sim. (**X**) Não. ( ) Não se aplica.
Finalidade Transparência	**2** - Caso não consiga enquadrar a coleta de dados em uma das 9 bases legais e apenas restou a hipótese do consentimento, antes de o usuário inserir seus dados para o cadastro, é apresentando a ele um termo de consentimento? ( )Sim. (**X**) Não. ( ) Não se aplica.
Finalidade Adequação	**3** - Os dados pessoais coletados, são compatíveis com a finalidade informada para o usuário? Por exemplo, no caso do sistema de processo seletivo, a finalidade é proporcionar educação profissional, atuando em ensino, pesquisa e extensão. Dificilmente será justificável pedir dados sobre opinião política ou vida sexual. Então, se não é compatível, o tratamento se torna inadequado. (**X**)Sim. ( ) Não. ( ) Não se aplica.
Finalidade Adequação Necessidade	**4** - Caso o sistema faça a coleta de algum dado inadequado, é informado ao usuário o motivo? ( ) Sim. ( ) Não. (**X**) Não se aplica.
Finalidade Necessidade Transparência	**5** - O sistema coleta apenas os dados pessoais necessários para cumprir seu propósito? ( )Sim. (**X**) Não. ( ) Não se aplica.
Finalidade Necessidade	**6** - Caso os dados coletados sejam necessários para cumprir o propósito, é informado qual a finalidade e hipótese legal para o tratamento dos dados pelo sistema? ( ) Sim. ( ) Não. (**X**) Não se aplica.

Livre acesso Transparência	**7** - Após realizar o cadastro, o usuário consegue acessar o sistema para saber quais dados pessoais estão sendo tratados? ( )Sim. (**X**) Não. ( ) Não se aplica.
Finalidade Livre acesso Transparência	**8** - Existe um painel no sistema para o usuário saber para qual a finalidade de cada dado coletado, e a confirmação do consentimento do uso? ( )Sim. (**X**) Não. ( ) Não se aplica.
Livre acesso Qualidade dos dados	**9** - O usuário consegue realizar a correção de dados incompletos ou desatualizados no sistema? ( )Sim. (**X**) Não. ( ) Não se aplica.
Finalidade Qualidade dos dados Transparência	**10** - Após cumprir a finalidade, os dados são anonimizados ou excluídos do sistemas? ( )Sim. (**X**) Não. ( ) Não se aplica.
Transparência	**11** - As informações coletadas pelo sistema, ficam claras, precisas e verdadeiras para o usuário? ( )Sim. (**X**) Não. ( ) Não se aplica.
Transparência	**12** - Caso seja compartilhado os dados pessoais com setores ou empresas terceiras, o titular é informado sobre este compartilhamento? ( )Sim. (**X**) Não. ( ) Não se aplica.
Segurança Prevenção	**13** - O sistema utiliza meios tecnológicos que garantam a proteção dos dados pessoais de acessos não autorizados por terceiros? (**X**) Sim. ( ) Não. ( ) Não se aplica.
Segurança Prevenção	**14** - Existe algum dado pessoal, que utilize criptografia para aumentar a segurança da informação? (**X**) Sim. ( ) Não. ( ) Não se aplica.
Segurança Prevenção	**15** - A organização possui alguma política de Segurança da Informação, para o desenvolvimento de sistemas? (**X**) Sim. ( ) Não. ( ) Não se aplica.

Segurança Prevenção	**16** - A organização possui regras de firewall, onde apenas conexão por VPN pode acessar o banco de dados? (**X**) Sim. ( ) Não. ( ) Não se aplica.
Não Discriminação	**17** - Caso faça a coleta de dados pessoais sensíveis, a organização é contra discriminar ou promover abusos contra os seus titulares? (**X**) Sim. ( ) Não. ( ) Não se aplica.
Não Discriminação	**18** - Caso a organização faça algum tratamento diferente com dados pessoais sensíveis, exite alguma lei que permite esta ação? Por exemplo, no tratamento de dados de alunos optantes por cotas, perante a Lei de Cotas 12.711/2012, a condição de tratamento de dados pessoais será a partir de seu histórico educacional, sendo ele oriundos integralmente do ensino médio público. (**X**) Sim. ( ) Não. ( ) Não se aplica.
Transparência Prevenção Responsabilização e Prestação de Contas	**19** - A organização possui um relatório de impacto à proteção de dados pessoais (RIPD), para comprovar que está tomando medidas necessárias para alcançar a conformidade com a LGPD? ( ) Sim. (**X**) Não. ( ) Não se aplica.
Responsabilização e Prestação de Contas	**20** - Alguns bons exemplos comprovam que a organização está em busca da conformidade da lei, a organização já iniciou o processo de alcançar a conformidade com a LGPD? (**X**) Sim. ( ) Não. ( ) Não se aplica.