Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Transações de Dados e Privacidade à luz da Lei Geral de Proteção de Dados Pessoais (LGPD)

Evandro Thalles Vale de Castro

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Orientadora
Prof.a Dr.a Edna Dias Canedo

Brasília
2021

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Transações de Dados e Privacidade à luz da Lei Geral de Proteção de Dados Pessoais (LGPD)

Evandro Thalles Vale de Castro

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Prof.a Dr.a Edna Dias Canedo (Orientadora)
CIC/UnB

Dr.a Leticia Lopes Leites
Universidade de Brasília

Dr.a Aletéia Patricia Favacho de Araújo
Universidade de Brasília (UnB)

Prof. Dr. João José Costa Gondim
Coordenador do Curso de Engenharia da Computação

Brasília, 18 de outubro de 2021

Dedicatória

Dedico esse trabalho a meus pais, que sempre priorizaram minha educação com toda atenção, amor e carinho do mundo, e que além de tudo, apoiaram-me em todos as situações da minha vida. Dedico também aos meus amigos da faculdade que proporcionaram esses anos de faculdade mais divertidos e interessantes.

Agradecimentos

Agradeço aos meus pais, irmãos, e aos meus amigos que conheci na faculdade, por me ajudarem nessa longa e árdua jornada, e por sempre me apoiarem em toda e qualquer decisão que eu tomei na vida, já que nunca duvidaram de minha capacidade. Essa não é uma conquista exclusivamente minha, mas também é uma conquista de vocês. Agradeço também a professora Edna Dias Canedo, por ter me aceitado como orientando e pela a ajuda, todo o interesse, vontade e disponibilidade para fazer este trabalho acontecer. Sou extremamente grato à senhora por tudo.

Resumo

Atualmente, inúmeras empresas utilizam, de forma direta ou indireta, os dados pessoais de seus usuários. Dados pessoais é o conjunto de informações que podem levar à identificação de uma determinada pessoa e, por isso, geralmente, essas informações são vitais para as operações e continuidade do negócio das organizações, sendo assim, o acesso às informações dos usuários é essencial para todas as transações realizadas pelas organizações. Consequentemente, nota-se a relevância de adotar metodologias que garantam proteção e privacidade dos dados dos usuários, uma vez que se tornou frequente o uso inadequado de dados ou até mesmo a presença das ameaças cibernéticas. Como mecanismos de prevenção e proteção, leis foram elaboradas para oferecer respaldo e proteção aos dados pessoais dos usuários (titulares dos dados), são elas: Regulamento Geral Europeu de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), que determinam requisitos essenciais para que as organizações estejam em conformidade com a lei. Este trabalho tem como objetivo elaborar um guia para apoiar os profissionais de TIC na adequação das empresas em relação aos requisitos exigidos pela LGPD. Além disso, descrever as boas práticas de governança de dados. Para atingir o propósito, foi proposto um framework baseado na metodologia BEST (Business Engaged Security Transformation), com algumas adaptações. O framework possui uma abordagem sustentável e adaptável, podendo ser implementado por qualquer organização. Foi realizado um survey para coletar a percepção dos profissionais de Tecnologia da Informação e Comunicação (TIC) em relação a aderência as ações de adequações à LGPD, por parte das organizações. Como resultados, identificamos uma fragilidade em relação à metodologia de privacidade e gestão de segurança da informação implantadas nas organizações, o que futuramente, pode resultar em riscos e danos para as informações dos usuários. De acordo com os resultados obtidos, podemos concluir que o framework desenvolvido orienta os responsáveis da organização pela TIC a respeitarem os processos de manipulação de dados dos usuários, em conformidade com a LGPD, bem como melhorar os aspectos relacionados à privacidade e proteção dos dados dos usuários, que se tornaram tão essenciais na atualidade.

Palavras-chave: Lei Geral de Proteção de Dados, Privacidade dos Dados, Conformidade, Governança de TIC, Segurança da Informação, Framework

Abstract

Currently, many companies use, directly or indirectly, the personal data of their users. Personal data is the set of information that can lead to the identification of a specific person and, therefore, this information is generally vital for the operations and business continuity of organizations, thus, access to user information is essential for all transactions carried out by organizations. Consequently, the relevance of adopting methodologies that guarantee the protection and privacy of user information is noted, since the inappropriate use of user data or even the presence of cyber threats has become frequent. As prevention and protection mechanisms, laws were created to provide support and protection to the personal data of users (data subjects), they are: General European Data Protection Regulation (GDPR) and the General Personal Data Protection Law (LGPD)), which determine essential requirements for organizations to comply with the law. This work aims to develop a framework to support ICT professionals in adapting companies to the requirements demanded by the LGPD. Also, describe good data governance practices. To achieve the purpose, a framework based on the BEST methodology (Business Engaged Security Transformation) was proposed, with some adaptations. The framework has a sustainable and adaptable approach and can be implemented by any organization. A survey was carried out to collect the perception of Information and Communication Technology (ICT) professionals in relation to adherence to LGPD adaptation actions by organizations. As a result, we identified a weakness in the privacy and information security management methodology implemented in organizations, which in the future may result in risks and damage to user information. According to the results obtained, we can conclude that the developed framework guides those responsible for the ICT organization to respect user data handling processes, in accordance with the LGPD, as well as to improve aspects related to privacy and data protection of the users, which have become so essential today.

Keywords: General Data Protection Law, Data Privacy, Compliance, ICT Governance, Information Security, Framework

Sumário

1 Introdução **1**
1.1 Problema de Pesquisa 2
1.2 Justificativa 2
1.3 Objetivos 3
1.3.1 Objetivo Geral 3
1.3.2 Objetivo Específico 3
1.4 Resultados Esperados 3
1.5 Metodologia de Pesquisa 3
1.6 Estrutura da Monografia 5

2 Embasamento Teórico **6**
2.1 General Data Protection Regulation (GDPR) 6
2.1.1 Pilares e Principais Mudanças da Lei 7
2.2 Lei Geral de Proteção de Dados Pessoais (LGPD) 9
2.2.1 Fundamentos 10
2.2.2 Princípios 11
2.2.3 Tipos de Dados 12
2.2.4 Tratamento de Dados Sujeito à LGPD 13
2.2.5 Agentes de Tratamento e ANPD 14
2.2.6 Privacidade 15
2.3 Trabalhos Relacionados 16

3 Conformidade **20**
3.1 Transação de Dados 20
3.1.1 Ciclo de Vida dos Dados 20
3.1.2 Coleta 21
3.1.3 Processamento 23
3.1.4 Compartilhamento 24
3.1.5 Armazenamento 25

3.1.6 Eliminação 26

4 Metodologia BEST **28**

4.1 Implantação do Framework 29

4.1.1 Programa 1: Sistema de Gestão de Cibersegurança e Segurança da Informação 30

4.1.2 Programa 2: Proteção da Informação 32

4.1.3 Programa 3: Aprimoramento da privacidade 42

4.1.4 Programa 4: Atitudes seguras 44

4.2 Verificação do Framework Proposto 45

4.3 Limitações e Ameaças para Validação 51

5 Conclusão **52**

Referências **54**

Anexo **61**

I Questionário **62**

Lista de Figuras

1.1 Classificação da Metodologia de Pesquisa empregada (Fonte: autoria própria) 4

2.1 Modelo de Governança de Dados (Adaptado de Fonte: [1]) 7

3.1 Ciclo de Vida dos Dados (Fonte: Figura adaptada [2] página 38) 21

4.1 Visão geral do Framework (Fonte: autoria própria) 30
4.2 Ciclo de um incidente (Fonte: [3] página 108) 39
4.3 Relacionamento entre princípios da LGPD e Privacy by Design (Fonte: autoria própria) 43
4.4 Ações de adequação à LGPD, tratamento e mapeamento dos dados 46
4.5 Boas práticas de Governança de Dados 47
4.6 Estratégias de Segurança da Informação adotadas 48
4.7 Empresas que possuem certificação de gestão de Segurança da Informação(ISO ou ABNT) 49
4.8 Plano de continuidade de negócios, privacidade e treinamentos dos colaboradores 50

Lista de Tabelas

2.1 Conceitos da LGPD 19

I.1 Questões do Survey 62

Capítulo 1

Introdução

Este trabalho explanará sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Federal nº 13.709/2018 [4, 5], abordando os contextos nos quais há permissão das transações de dados e fatores importantes para sua implementação, como: fundamentos, princípios, direitos do titular da informação, segurança, privacidade, campo de aplicações, entre outros.

Primeiramente, é importante entender o que é a LGPD, que entrou em vigor a partir de 18 de setembro de 2020 e surgiu para garantir maior segurança jurídica às atividades de tratamento de dados pessoais no país, estipulando uma série de obrigações para as organizações sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, tanto online quanto offline, o que favorece o desenvolvimento econômico. Segundo o Artigo 6º da LGPD, deverão ser seguidos dez princípios básicos: finalidade, adequação, necessidade, livre acesso, quantidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas [6]. Todos esses critérios são de suma importância para a integração e adaptação da norma, enquadrando pessoas físicas e/ou pessoas jurídicas de direito público ou privado.

Sendo assim, com relação às transações de dados, os titulares da informação passarão a ter mais proteção e transparência a respeito de como serão tratados e compartilhados os seus dados para atingirem as finalidades específicas para as quais foram coletados, no qual esse princípio, sustenta dois fundamentos que são: minimização de coleta e a retenção mínima. O primeiro conceitua que os dados coletados devem ser o mínimo necessário para alcançar a finalidade em questão, já o segundo, determina que após os dados atingirem o propósito, deverá realizar a imediata exclusão das informações. Esse processamento de dados só é permitido apenas com o consentimento do titular, salvo em exceções expressamente previstas em lei [7].

O objetivo deste trabalho é explicitar o funcionamento e as diretrizes que regem a LGPD, para que as pessoas entendam os paradigmas a serem seguidos e como tais mu-

danças afetarão diferentes setores e serviços, seja no papel de indivíduo, empresa ou governo.

1.1 Problema de Pesquisa

Um dos grandes problemas que as empresas podem vir a enfrentar é a exigência de comprovar todo o processo de tratamento dos dados dos usuários, por meio do Relatório de Impacto à Proteção dos Dados (RIPD). De acordo com o Artigo 18º da LGPD [6], "o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição" [6]. Com base nisso, nota-se a relevância para as empresas de arquivar detalhadamente os dados manipulados sobre os indivíduos. Assim, este trabalho, por meio do framework a ser desenvolvido, visa esclarecer o papel significativo da segurança da informação para as organizações, além da importância de elaborar o RIPD, uma vez que por meio deste documento será possível analisar tudo o que pode gerar danos às informações dos clientes, bem como nortear o planejamento de medidas mais efetivas contra os possíveis problemas que podem ocorrer, garantindo um respaldo de todos os processos executados durante a manipulação dos dados.

1.2 Justificativa

Com a ascensão da coleta de dados, aumentaram-se exponencialmente também os crimes virtuais, estes são responsáveis em perdas estimadas em mais de 1 trilhão de dólares em 2020, segundo o relatório divulgado pela McAfee [8]. De acordo com a empresa, o valor representa um aumento de mais de 50%, se comparado ao último levantamento feito pela mesma em 2018, consequentemente, todas as empresas devem alarmar-se diante a esses fatos, pois em casos de invasão, vazamentos ou outro problemas, os riscos relacionados ao ocorrido, e até mesmo, os motivos de lentidão na comunicação do fato, se ocorrer, devem tornar-se públicos. Desse modo, as organizações devem estar organizadas e capacitadas para fornecer essas informações sempre que forem solicitadas, já que é necessário ter competência em saber precisamente onde tais dados se localizam e quais correspondem a cada indivíduo.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é oferecer um framework com os conceitos que compõem a LGPD para que os profissionais responsáveis compreendam todos os processos que compõem o tratamento de dados, isso é desde a coleta das informações até a eliminação delas em um contexto no qual garanta a segurança da informação e privacidade dos titulares dos dados em conformidade com a LGPD.

1.3.2 Objetivo Específico

Para atingir o objetivo geral deste trabalho, os seguintes objetivos específicos foram definidos:

- Descrever as principais concepções que norteiam as especificações da LGPD;
- Detalhar de maneira clara os procedimentos exigidos pela LGPD para garantir a legitimidade;
- Esclarecer detalhadamente todos os direitos dos usuários;
- Implementar um framework para que as organizações consigam atender continuamente aos requisitos da LGPD;
- Validar o framework proposto com intuito de diagnosticar a qualidade e a facilidade de integração do guia;
- Adicionar melhorias no framework proposto, caso necessário.

1.4 Resultados Esperados

O resultado esperado é oferecer um framework para apoiar as organizações na conformidade à LGPD com uma fácil integração para as empresas no âmbito de transações de dados, garantindo privacidade e proteção das informações.

1.5 Metodologia de Pesquisa

Esta pesquisa possui natureza aplicada com abordagem predominantemente qualitativa, contudo em alguns momentos do desenvolvimento, será utilizado questionários para avaliar o framework que será implementado. A análise dos dados foi realizada de forma

dedutiva para gerar conhecimento específico visando uma cadeia de raciocínio em ordem descendente, de análise do geral para o particular [9].

Em relação à tipologia, a pesquisa enquadra-se como exploratória e descritiva. É exploratório, por proporcionar mais informações sobre o assunto e possui planejamento flexível, o que permite o estudo do tema sob diversos ângulos e aspectos [9]. Em contrapartida, possui aspectos descritivos, já que inclui um levantamento para classificar e interpretar as opiniões das pessoas em relação ao guia proposto.

Este trabalho adotou os seguintes procedimentos técnicos: bibliográficos, documentais e levantamentos, isso possibilitou um aprofundamento maior sobre o tema, por utilizar fundamentalmente das contribuições de vários autores sobre determinado assunto e criar uma investigação para catalogar a percepção das pessoas em relação ao suporte fornecido por este trabalho, e mediante análise quantitativa, obteve-se conclusões correspondentes aos dados coletados [9].

A Figura 1.1 apresenta a classificação desta metodologia quanto à natureza, a abordagem, o tipo, a seleção de procedimentos e técnicas de coleta de dados adotadas, assim sendo, o trabalho seguiu os passos: O trabalho foi conduzido nos seguintes passos:

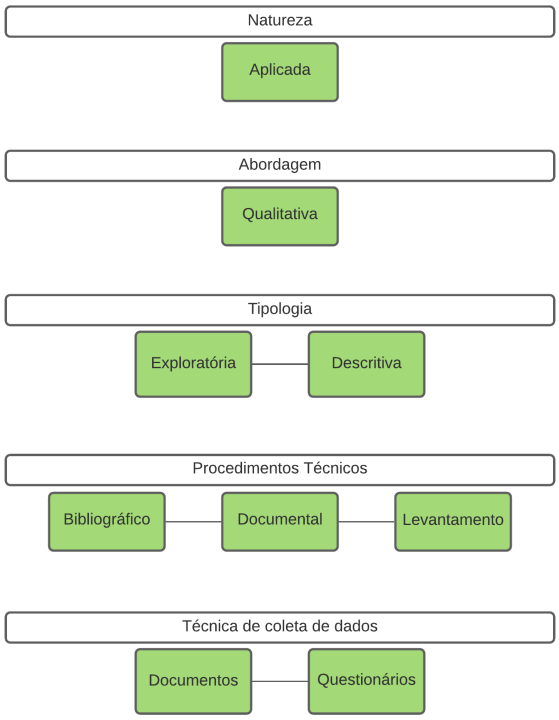

Figura 1.1: Classificação da Metodologia de Pesquisa empregada (Fonte: autoria própria)

1. Contextualização da Lei Geral de Proteção de Dados (LGPD) e General Data Protection Regulation (GDPR);

2. Destacar os principais impactos da LGPD, por meio de análise, nos serviços prestados pelas empresas;
3. Detalhar os tipos de dados existentes e quais são protegidos pela LGPD;
4. Investigação e discussão de trabalhos relacionados;
5. Implementar um framework que conduz para atender os requisitos da LGPD;
6. Conduzir uma avaliação sobre o framework implementado com intuito de analisar a adequação do mesmo;

1.6 Estrutura da Monografia

Este trabalho está organizado da seguinte maneira: O Capítulo 2 apresenta o embasamento teórico constituídos por uma descrição aprofundada da LGPD e suas diferenças com a General Data Protection Regulation (GDPR), em seguida apresentar os principais conceitos que fundamentam a LGPD, e por fim, concepções de privacidade na LGPD baseado nos direitos dos titulares.

No Capítulo 3 será descrito cada etapa do ciclo de vida dos dados, que são fundamentais para o procedimento do tratamento dos dados, bem como as suas relações diretas com a LGPD.

No Capítulo 4 será implementado a metodologia BEST [10] com algumas modificações, tal qual oferece um guia para atingir a conformidade com a LGPD. Além disso, será conduzido um questionário para avaliar o framework desenvolvido em relação aos quesitos de qualidade e eficácia de integração em atender os requisitos da LGPD. Por fim, no Capítulo 5 tem-se a conclusão, enfatizando a contribuição fornecida e a importância deste trabalho.

Capítulo 2

Embasamento Teórico

Neste capítulo serão explicados tópicos importantes que sustentam a Lei Geral de Proteção de Dados(LGPD) e General Data Protection Regulation(GDPR), assim como os direitos que os indivíduos possuem na execução da transação dos dados.

2.1 General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) é um projeto para proteção de dados e identidade dos cidadãos da União Europeia que começou a ser idealizado em 2012. Concebida em uma era anterior ao surgimento da internet comercial e muito antes da difusão dos modelos de negócio e tecnologias que se valem do uso intenso de dados pessoais e que são quase que onipresentes na vida das pessoas, precisou passar por um processo de atualização que culminou com a atual Regulação Geral de Proteção de Dados da União Europeia (GDPR) [11]. Importante ressaltar que ela possui ampla aplicação, estando submetidos a ele todos os indivíduos da União Europeia e aqueles que, mesmo não estando em território europeu, lá desenvolvem atividades de coleta e processamento de dados pessoais (artigo 3º da GDPR) [12, 13].

Uma das razões que acarretou na aprovação da lei Europeia foi a ocorrência de vários vazamentos, violações de dados pessoais e espionagem por parte dos Estados Unidos, que compartilhava esses dados de todo mundo, mediante a empresas como Apple, Google e Facebook [14]. "Revelado em 2013 por Edward Snowden, ex-analista da CIA, o escândalo ajudou a impulsionar a revisão da lei que havia começado no ano anterior" [15]. A lei entrou em vigor no dia 25 de maio de 2018, atualizando e adaptando um regulamento já existente sobre proteção dos dados denominado Diretiva Europeia de Proteção de Dados.Essa modernização na GDPR é algo necessário, pois na atualidade surgem, cada vez mais, novas formas do uso massivo das informações pessoais,tais como Big data, inteligência artificial e aprendizado de máquina [11]. Consequentemente com o alcance global

da lei, organizações de todo mundo que possuam algum formato de negócio com um país da União Europeia deverá se adequar aos regulamentos da GPDR, sendo assim, uma loja online no Brasil que deseja vender ou prestar serviços necessariamente terá que se submeter a essa legislação para que possa efetuar transações [12].

2.1.1 Pilares e Principais Mudanças da Lei

Ainda que esse procedimento de burocratização seja algo complexo em se adequar, é importante entender que GDPR tem um propósito maior implícito: o direito que as pessoas têm de verem seus dados pessoais sendo usados com responsabilidade e segurança. É composta por 3 pilares que fundamentam os regulamentos da GDPR, os quais são a governança de dados, gestão de dados e transparência.

O pilar da governança de dados é o sistema de gestão e monitoramento que envolve todos os níveis de uma organização, através do qual seus princípios e valores básicos são convertidos em recomendações objetivas, de modo alinhar seu interesse com a finalidade de preservá-la e otimizar o seu valor econômico de longo prazo [16], sendo assim, os processos relativos ao manuseio inapropriado das informações devem ser comunicados e sanados, resumidamente, atua como uma entidade articuladora, identificando problemas, buscando oportunidades e propondo iniciativas de melhorias. [14]. Com uma literatura relevante, sendo reconhecida internacionalmente e amplamente utilizada, de acordo com o guia DAMA – Guide to the Data Management Body of Knowledge [1], a governança de dados é representada na Figura 2.1.

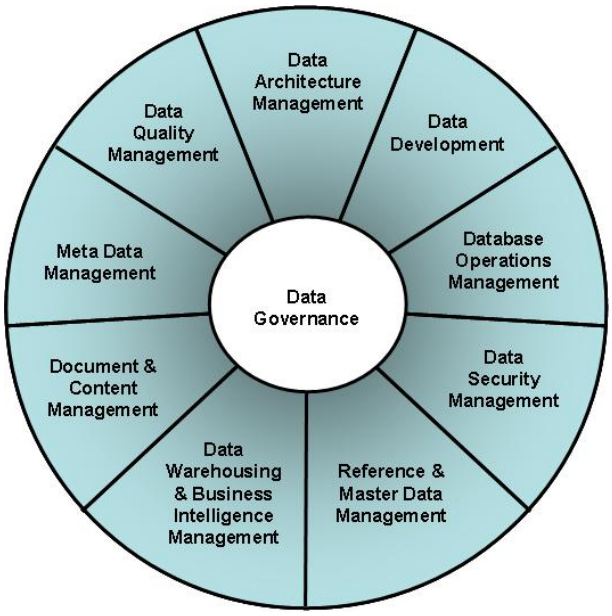

Figura 2.1: Modelo de Governança de Dados (Adaptado de Fonte: [1])

A partir da Figura 2.1, segundo o DAMA, a governança de dados é o coração do gerenciamento de ativos dos dados com intuito de definir práticas e políticas de segurança, acesso, integração e monitoramento dos dados dentro das empresas [1].

O segundo pilar é o de gestão de dados, este é baseado por operações de processamento, transações de dados e da exclusão. Novamente, segundo o guia DAMA, "gestão de dados é a função que é também conhecida como um processo de negócio de alto nível, ela consiste de planejamento e execução de políticas, práticas e projetos que adquirem, controlem, protejam, entreguem e aumentem o valor dos dados ativos e informações, tendo como objetivo de atender e aprimorar as necessidades das informações de todas partes interessadas na empresa em termos de disponibilidade, segurança e qualidade da informação". Os principais objetivos estratégicos da gestão de dados são [1]: 1. Compreender as necessidades de informação da empresa e de todos os envolvidos; 2. Coletar, armazenar, proteger, e assegurar a integridade dos dados ativos; 3. Melhorar continuamente a qualidade dos dados e informações, que incluem: precisão, utilidade, integridade e integração dos dados; 4. Garantir a privacidade e confidenciabilidade e a prevenção do uso não autorizado ou inapropriado das informações; 5. Maximizar o uso efetivo e o valor dos dados ativos e informações.

E o último pilar é o de transparência de dados, este é constituído pelos processos de consentimento, portabilidade de dados e políticas de privacidade.De forma simples, as empresas devem registrar todo o procedimento envolvido na manipulação dos dados para que disponibilizem aos seus clientes sempre que solicitados, e além disso, forneçam os métodos adotados para garantir a proteção e privacidade dos dados [12]. A amplitude da GDPR ultrapassa fronteiras geográficas, sendo assim, é importante ressaltar em como a norma europeia influencia nos serviços prestados pelas companhias que manipulam dados, pode-se citar [17]:

- O titular dos dados tem o direito de reivindicar as informações, podendo exigir a alteração, atualização e a exclusão dos seus dados para as empresas;
- Para as empresas se tornou imprescindível definir uma finalidade para o manipulação dos dados, dessa forma, a empresa precisa estabelecer e transmitir a finalidade para os usuários;
- Estabelecer medidas de segurança de dados confiáveis, pois a garantia de proteção e privacidade das informações devem estar presente em todo o procedimento de manipulação dos dados;
- Em certas ocasiões para realizar determinadas operações será obrigatório a participação do Data Protection Officer (DPO), profissional responsável pela proteção de

dados, supervisionar o tratamento dos dados pessoais, prestar informações de todo processo de uso dos dados e comunicar com as autoridades;

- As empresas tem a obrigação de notificar os titulares do dados quando ocorre incidentes relacionados a violações da privacidade dos dados, com o limite máximo de 72 horas;
- O uso de linguagem clara, objetiva e inteligível se tornou algo necessário para as empresas, para que qualquer indivíduo tenha a capacidade de compreender da maneira mais simples sobre a integridade dos seus dados e os termos de privacidade;

2.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Federal 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada em 14 de agosto de 2018 e entrou em vigor no dia 18 de setembro de 2020 [6]. Entretanto, as penalidades associadas à lei serão efetivadas somente a partir de 1 de agosto de 2021.

O texto foi exposto a várias consultas públicas de forma democrática em quatro anos, e muitas alterações foram feitas até que o texto Anteprojeto de Lei de Proteção de Dados fosse consolidado, em 2015. Neste período, ainda prevalecia a Diretiva 95/46 na União Europeia e ocorriam vários debates sobre o tema, mas em face às profundas alterações introduzidas pelo progresso tecnológico, a diretiva foi posta em xeque. No Brasil, há alguns anos atrás, o aspecto mais repercutido sobre a LGPD era a criação de um órgão competente para fiscalizar o cenário brasileiro garantindo a aplicabilidade da lei, assim como, tomar devidas providências sancionatórias. Consequentemente, como uma medida preventiva para evitar questionamentos, o presidente da república vetou os artigos que referenciavam a criação da autoridade que protegesse os dados [18], contudo com profundas análises e emendas na lei, em 2019, foi criada definitivamente, a Autoridade Nacional de Proteção dos Dados (ANPD).

Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela [19], sendo assim, ela tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. – ou seja, todo mundo [10]. A lei baseia-se na ideia de que os indivíduos tenham conhecimento e controle sobre o processo de coleta e a manipulação de seus dados, protegendo os direitos

fundamentais de liberdade, privacidade e livre formação, o que impõe várias obrigações para organizações sobre coleta, arquivamento, tratamento e transação de dados pessoais. Ainda que tenha suas próprias particularidades, foi inspirada na GDPR, ao estabelecer os princípios, direitos dos titulares, controladores e operadores do tratamento de dados pessoais, bem como exigindo o nível adequado de proteção requerido das demais jurisdições e criando a ANPD [18].

2.2.1 Fundamentos

Logo no início do capítulo 1, a lei se preocupa em definir claramente seu objetivo e escopo de atuação com o intuito de contextualizar, nivelar o vocabulário e definir a natureza dos conceitos abordados. No (Artigo 2º) [6] são descritos os fundamentos da disciplina de proteção de dados que são de suma importância para a estruturação da lei e a interpretação correta dos conceitos basilares que norteiam a lei, nos quais se porventura ocorrer qualquer ação que desrespeite tais fundamentos tornará o processo de manipulação de dados inválido [10].

São sete fundamentos que estabelecem as diretrizes da proteção de dados pessoais, o primeiro é sobre respeito à privacidade. Nesse caso, é interessante ressaltar que privacidade e proteção de dados são tópicos distintos. O autor da obra [10], argumentou um exemplo significativo, se alguém postar dados em sua página pessoal nas redes sociais, os dados serão tornados públicos. No entanto, isso não significa que os dados possam ser usados à vontade, e quem os usa deve cumprir os direitos do titular dos dados especificados na LGPD. Em vista disso, tais dados, não estão regidos pelo princípio da privacidade, mas sim sob o escopo da proteção de dados.

O segundo fundamento é o da autodeterminação informativa, que de maneira simples, constitui na possibilidade que toda pessoa tem de exercer, de algum modo, controle sobre seus dados pessoais, sendo assim, os titulares dos dados podem decidir o que será feito com a sua informação, saber quais dados as empresas possuem referentes ao cliente, como elas os utilizam e se o titular quer que seu dado esteja com elas, quer seja utilizado ou não. Ou seja, o indivíduo é o protagonista das matérias relacionadas ao tratamento de seus dados, determinando como as informações serão utilizadas [6, 10].

Assim como no Artigo 5º da Constituição federal aborda os direitos humanos, a LGPD repete alguns destes direitos em seus fundamentos com intuito de enfatizar a sua aplicabilidade, são eles: o livre desenvolvimento da personalidade, a dignidade da pessoa humana, o exercício da cidadania, a liberdade de expressão, informação e comunicação, bem como a inviolabilidade da intimidade, da honra e da imagem [10]. O último fundamento é dirigido à sociedade, o que garante desenvolvimento econômico e tecnológico, a inovação, livre iniciativa, livre concorrência e a defesa do consumidor.

No Guia de implantação [10], os autores expressam uma visão bastante interessante, ainda que dados isolados não agreguem valor, são a base quando combinados com objetivos e finalidades para análise. Portanto, os dados tornam-se informações que podem apoiar a tomada de decisões sociais, políticas e econômicas, especialmente neste último caso, como agente econômico da livre iniciativa e promotora para inovação e tecnologia, sem, contudo, negligenciar a defesa do consumidor.

2.2.2 Princípios

Os princípios que regem a lei, sem dúvidas, é uns dos aspectos mais importantes, nos quais servem de guia na forma como as organizações devem agir de acordo com as medidas previstas na lei. Além disso, exercem como fundamento legal para o órgão ANPD, em casos de possíveis violações das normas legais. Diante disso, é importante descrevê-los para melhor compreensão com a lei, sendo assim, os princípios são [6]:

1. Finalidade: todos os dados, desde o momento de coleta, deve possuir propósitos legítimos, específicos, explícitos ao titular, que justifiquem o recolhimento dos dados;
2. Transparência: o indivíduo tem direito a saber exatamente o quê, porquê e para quê seus dados estão sendo coletados.As empresas devem garantir, informações claras, precisas e acessíveis aos titulares dos dados, assim como a realização do tratamento e os respectivos agentes atuantes no processo;
3. Segurança: qualquer dado que for tratado deverá ser garantido a segurança e confidencialidade por meio medidas técnicas e administrativas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas;
4. Prevenção: é uns dos pontos mais importantes sobre segurança, pois é a adoção de medidas preventivas contra qualquer eventuais problemas no processo de tratamento de dados pessoais;
5. Adequação: o tratamento dos dados deve condizer com as finalidades informadas ao titular, conforme o contexto do tratamento;
6. Necessidade: restringe o tratamento dos dados ao mínimo necessário para alcançar suas finalidades;
7. Livre Acesso: é um complemento da transparência, já que garante ao titular o livre acesso para consultar informações sobre o tratamento de forma facilitada e gratuita, assim como a integridades de seus dados pessoais;

8. Qualidade dos Dados: as informações sobre os titulares, devem garantir que as informações sejam verdadeiras, precisas e atualizadas, de acordo com a necessidade e a finalidade;

9. Não Discriminação: o nome é auto-explicativo, ou seja, o tratamento é impossibilitado de ser feito para fins de discriminação ou gerar qualquer abuso contra o titular;

10. Responsabilização e Prestação de Contas: de forma simples, é a obrigação de prestar contas do procedimento de manipulação das informações. Determina que os agentes responsáveis devem ser capazes de demonstrar todas as medidas adotadas que comprovem o cumprimento da LGPD;

Esses fundamentos são imprescindíveis no ato de tratamento dos dados, pois orientam os agentes responsáveis nos paradigmas a serem seguidos em todas as etapas do processo de manipulação das informações.

2.2.3 Tipos de Dados

A LGPD possui uma concepção bem abrangente referente a dados, o que oferece maior durabilidade à lei e garante uma aplicabilidade maior para os reguladores e agentes responsáveis do tratamento. Contudo, não é qualquer dado que será instrumento de regulação por essa lei, somente as informações denominadas dados pessoais que serão controlados e regularizados pela mesma. De maneira simples, toda informação que permite identificar, direta ou indiretamente, a pessoa física, é considerado dado pessoal, são exemplos: CPF, nome, RG, endereço residencial, profissão, gostos, endereço IP, cookies, dentre outros, ou seja, desde o número dos seus documentos até as páginas curtidas e os perfis seguidos nas redes sociais podem ser considerados dados pessoais [20].

Há, também, uma segunda divisão do dado pessoal definida por "dados pessoais sensíveis", que são dados cujo tratamento pode ensejar a discriminação do seu titular – por se referirem, por exemplo, à opção sexual, origem racial ou étnica, saúde do indivíduo, convicções religiosas, filosóficas ou morais, ou opiniões políticas.Quando os dados forem sensíveis, o tratamento somente poderá ocorrer com o consentimento do titular, de forma especificada e destacada para as finalidades específicas [6,18].O tratamento dos dados sem o consentimento do indivíduo só será permitido nas seguintes exceções previstas no Artigo 11º da LGPD:

1. Cumprimento de obrigação legal ou regulatória pelo controlador;

2. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

3. Realização de estudos por Órgão de pesquisa;
4. Exerciício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
5. Proteção da vida ou da incolumidade fiísica do titular ou de terceiro;
6. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
7. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Outros tipos de dados relevantes são os dados anonimizados e os dados pseudo-anonimizados. O primeiro tipo é basicamente toda informação que impossibilita identificar o titular, considerando a utilização de meios técnicos razoáveis, o que inviabiliza a associação, direta ou indireta, com o indivíduo. São exemplos de dados anonimizados: estatísticas sobre a idade de pessoas que realizaram a compra de determinado produto. Essas informações anonimizadas, segundo o Artigo 12º [6, 18], não serão considerados como dados pessoais para os fins dessa lei, salvo em exceções previstas na mesma.

Os dados pseudo-anonimizados são dados que passaram por um procedimento de anonimização, que permitem associar o titular somente com o uso de informações adicionais mantidas separadamente com agentes responsáveis em local separado e seguro, por meio disso, como há a possibilidade de identificação do usuário, esse tipo de dado é protegido pela norma. Um bom exemplo é o sistema de biometria, na qual o indivíduo pode ser reconhecido apenas por um código cadastrado. A anonimização e o pseudo-anonimato são incentivados pela própria LGPD como forma de redução dos riscos e proteção dos indivíduos, já que esses dados são usados para fins de estudos no âmbito da saúde pública (Artigo 13º) [18]. Além desses conceitos explicitados, há outros de suma importância, dando destaque às definições de Banco de Dados, Relatório de impacto à proteção de dados pessoais, bloqueio e eliminação. A LGPD não restringe a apenas esses conceitos, mas são essenciais para a correta compreensão desse trabalho, sendo assim, os termos estabelecidos são Apresentados na Tabela 2.1.

2.2.4 Tratamento de Dados Sujeito à LGPD

A LGPD aplica-se em operações realizadas com dados pessoais, sendo assim, segundo o (Artigo 5º, LGPD) são definidos todas as vertentes de tratamento de dados regidos por essa norma, que é: "Toda operação realizada com dados pessoais, como as que se referem a

coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" [6], ou seja, uma abrangência ponta-a-ponta, desde a entrada do dado em determinada entidade, todo o período de permanência, até sua eventual saída.

Em vista disso, é relevante descrever que a LGPD incide sobre qualquer operação de tratamento de dados pessoais, desde que as empresas preencham pelo menos um desses requisitos, segundo o Artigo 3º da LGPD [6]: 1) A operação de tratamento seja realizada no território nacional; 2) A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; 3) Os dados pessoais objeto do tratamento tenham sido coletados no território nacional, sendo que, são considerados dados coletados no território nacional aqueles quando o titular nele se encontre no momento da coleta. Do mesmo modo que a GDPR e o Marco Civil da Internet tem os critérios do público-alvo, a LGPD não é diferente. E, nesse sentido, ela foi além, já que envolve a aplicabilidade da lei não somente aos brasileiros, mas também qualquer pessoa que esteja no Brasil, quando qualquer operação de tratamento de dados pessoais tenha sido realizada [18].

Apesar da norma ser significativamente rigorosa, existe casos no Artigo 4º, sobre tratamento de dados pessoais em que a própria lei não se aplica, como por exemplo operações de manipulações de dados pessoais realizadas por pessoa natural para fins exclusivamente particulares e não econômicos [6]. Uma situação que exemplifica isso é o ato de salvar o número de uma pessoa na agenda do celular, tal qual é um acontecimento bastante comum e de fins particulares, não sendo portanto, resguardado pela lei. Além disso, o tratamento de dados pessoais realizados com finalidades exclusivas: jornalísticas, acadêmicas, artísticas, defesa nacional, segurança pública, segurança do Estado ou matéria criminal, também são consideradas exceções à aplicação da LGPD [6]. Por fim, ficam excluídos da aplicação da lei aquelas hipóteses em que os dados estejam apenas de passagem no Brasil, ou seja, tratamento de dados pessoais "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei" [6].

2.2.5 Agentes de Tratamento e ANPD

A lei brasileira expõe três figuras como agentes de tratamento de dados pessoais, estes efetuam um papel de suma importância para o levantamento de informações de todo processo de manipulação dos dados, são eles, de acordo com o (Artigo 5º da LGPD) [6]:1)

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; 2) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, verificando a observância das próprias instruções e das normas sobre a matéria; 3) Encarregado: pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Logo, baseando-se nessas descrições legais, sem dúvidas, o Controlador é o protagonista na tomada de decisões que abrangem os dados pessoais coletados, tal qual administra como os dados serão coletados, assim como quais informações serão recolhidas; estabelece a finalidade da coleta dos dados e posteriormente estipula a forma de uso dos mesmos.Além disso, tem o papel fundamental de proteger os dados dos titulares, sendo considerado o maior responsável nessa funcionalidade e, como consequência direta,a maior parte das responsabilidades previstas na LGPD também incidirão sobre ele [20]. Já o Operador não possui a prerrogativa de controlar os dados, nem modificar a finalidade para a qual foi recolhido, dessa forma, as ações deste agente limita-se a seguir as determinações estipuladas pelo Controlador.Contudo, o operador terá liberdade para definir a metodologia, os mecanismos que serão aplicados na coleta, bem como a forma que eles serão armazenados.

Um fato importante a ressaltar que o tanto o Controlador quanto o operador, deverão registrar todas as operações de tratamento de dados pessoais que efetuarem, principalmente aquelas baseadas no legítimo interesse Artigo 37º da LGPD [6].

2.2.6 Privacidade

Na sociedade atual, a informação possui um grande valor, não somente pela característica de guardar uma quantidade exorbitante de dados, mas especialmente, na capacidade de adquirir novas informações sobre os cidadãos através do tratamento desses mesmos dados [21]. É neste contexto que a privacidade possui um papel essencial para manipulação dos dados. Em sentido amplo: privacidade está relacionado aos direitos subjetivos e inerentes a todos, e nele está inserido o estilo de vida familiar, modo de vida doméstico, relações afetivas, os hábitos do indivíduo, o nome, a imagem, os pensamentos, dentre outras situações [20]. Em vista disso, surgiram duas abordagens que desempenham um papel de extrema relevância na produção de aplicativos e serviços digitais dentro do cenário moderno de proteção de dados, que são Privacy by Design e Privacy by Default. O primeira abordagem consiste em incluir recursos e metodologias de proteção de privacidade na arquitetura da tecnologia, consequentemente, todos esses componentes na proteção farão parte do próprio design da tecnologia [19]. De maneira resumida, o Privacy by Design engloba a ideia "de que a proteção de dados pessoais deve orientar a concepção de um

produto ou serviço, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais" [22]. Ann Cavoukian, em seu artigo "Privacy by Design: Essential for organizational accountability and strong business practices", implementou um guia que contém sete princípios que direcionam a concepção de privacy by design, são eles [23]:

- A adoção de medidas proativas e preventivas, não reativas, a fim de remediar as situações;
- Privacidade como default, ou seja, como padrão;
- Privacidade inserida no design e na arquitetura do sistema de tecnologia da informação e nas práticas de negócio;
- Funcionalidade completa, de modo que o resultado seja benéfico, não nulo;
- Segurança de ponta a ponta;
- Visibilidade e transparência;
- Respeito pela privacidade do usuário;

Já o Privacy by Default(privacidade por padrão), significa que, por padrão, durante o lançamento de um produto ou serviço no mercado, as configurações de privacidade devem ser fornecidas da maneira mais restrita possível. Além disso, deve informar ao usuário quais informações estão sendo coletadas e para qual finalidade. [19].

2.3 Trabalhos Relacionados

Diante da complexidade para atender as conformidades da lei brasileira nos processos de negócios, Araújo [24] realizou uma pesquisa aprofundada sobre as leis GDPR e LGPD com intuito de contextualizar e propor o método LGPD4BP (LGPD for Business Process). Esse método é composto por um questionário de avaliação e um método de modelagem com um catálogo de padrões de modelagem, conduzindo os analistas a avaliarem e modelarem processos que atendam os requisitos exigidos pela lei. Com a aplicação do método em um estudo de caso, os resultados das avaliações dos indivíduos demonstraram que a parte mais difícil é a modelagem do processo de negócio e não os componentes do método proposto.

Machado e Doneda [25] pesquisaram a fundo sobre proteção de dados pessoais e criptografia, agregando mecanismos de proteção de dados como: anonimização e pseudoanonimização. Na atualidade ocorre uma assimilação entre os conceitos de anonimato e

criptografia, principalmente ao se tratar de comunicações e interações no meio tecnológico da informação. Em vista disso, o trabalho desses autores tem por objetivo abordar a importância do anonimato e o impacto de suas respectivas técnicas no âmbito de proteção de dados, além de propor e responder perguntas, como "Em qual medida os dados pessoais submetidos a procedimento de encriptação serão considerados como tais?".No desenvolvimento do trabalho será desmembrado essas metodologias de proteção de dados e perceberá que a resposta da questão levantada anteriormente, não é tão simples, já que dados criptografados não configuram dados anônimos ou anonimizados pelo só fato de ocorrer operação de cifragem.Portanto, não foca a perspectiva relativa sobre a noção de identificabilidade da pessoa humana, mas sim os esforços e meios razoáveis empregados por outros sujeitos que não o Controlador na apreciação da potencial identificação do titular dos dados e superação das técnicas criptográficas utilizadas.

Carvalho et al. [26] abordaram o tema de Pesquisas em Análise de Redes Sociais, utilizando uma abordagem metodológica teórico-analítica. Os autores detalharam ponto a ponto os tópicos mais relevantes da LGPD associados com a epistemologia científica na Análise de Redes Sociais (ARS), além de sugerir boas práticas de pesquisas no âmbito das redes sociais, em conformidade com a LGPD, apontando os desafios de obter consentimento dos indivíduos devido ao volume de dados. Os autores mencionaram a importância do respeito à conscientização do uso de dados pessoais, sensíveis ou não, pelos pesquisadores de ARS, mencionando algumas indagações em aberto, por razões de não terem sido trabalhadas na lei ou por possuírem brechas para várias interpretações relacionadas ao contexto jurídico.

Éllen et al. [27] investigaram quais os desafios que os profissionais de Tecnologia da Informação (TI) enfrentam para garantir a conformidade dos princípios de privacidade de dados em relação a LGPD nas organizações brasileiras. Os autores elaboraram um questionário direcionado aos profissionais de TI das empresas públicas e privadas para compreender a percepção deles em relação a implementação da LGPD. Os autores identificaram que 27% das empresas em que os profissionais de TI trabalham, manipulam dados pessoais conforme os requisitos definidos pela LGPD e, em contrapartida, 16% das organizações não estabeleceram nem mesmo uma metodologia para verificar se os serviços prestados adéquam-se aos fundamentos e princípios da LGPD. Consequentemente, os resultados encontrados servem de apoio para as organizações na aplicação da LGPD, permitindo a elas ter uma visão do cenário atual e diagnosticar os pontos nos quais a empresa deve adotar para atender as conformidades da lei.

Canedo et al. [28] pesquisaram a relevância da privacidade da informação e a necessidade dos profissionais de Tecnologia da Informação e Comunicação (TIC) compreenderem as diretrizes que os softwares devem atender para adequar-se com a lei de proteção de

dados. Em vista disso, o trabalho conduziu um questionário com esses profissionais com o intuito de elaborar uma visão de como esses agentes estão implementando os conceitos de privacidade dos dados durante o planejamento do software. Os resultados revelaram que os profissionais de TIC carecem de um conhecimento sólido sobre requisitos de privacidade e como LGPD influencia no desenvolvimento de software. Esses achados demonstram uma dificuldade, por parte dos profissionais, em lidar e tratar os princípios da lei de proteção dos dados.

Paulo et al. [29] investigaram as questões tecnológicas relacionadas a transparência em um cenário no qual a lei de proteção dos dados atua, buscando abrir uma agenda de pesquisa e questionar possíveis desafios relacionados aos aspectos de TIC na área de Sistema de informação. O trabalho concluiu que a LGPD possui alguns aspectos conflitantes associadas com privacidade e transparência, sendo que a lei restringe o acesso aos dados em alguns pontos e determina a abertura em outros, simultaneamente.

Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Banco de Dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
Relatório de impacto à proteção de dados pessoais	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
Órgão de Pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Tabela 2.1: Conceitos da LGPD

Capítulo 3

Conformidade

3.1 Transação de Dados

Frequentemente as empresas executam ações de processamento e compartilhamento de dados, contudo este último é tratado de forma rígida e detalhada na LGPD, conforme apresentado no Capítulo 2. Profissionais e empresas enfrentam o desafio de transitar dos dispositivos legais e seus resultados para o cotidiano, bem como o desafio de implantar uma série de processos que farão parte do modelo padrão de processos organizacionais. Como transações de dados é uma etapa importante do ciclo de vida, é necessário primeiramente entender este processo por completo para então definir os procedimentos que devem ser adotados para adequar determinada empresa à LGPD [2].

3.1.1 Ciclo de Vida dos Dados

Compreender e categorizar corretamente os dados se tornou um processo importante para cumprir a lei, por meio da implementação de políticas, procedimentos e planos apropriados para gerenciar como coletar, processar, analisar, armazenar, compartilhar, reutilizar e descartar esses dados. Sendo assim, o gerenciamento do ciclo de vida dos dados, deve ser introduzido ao modelo de negócio, respeitando a finalidade dos seus bens e serviços a serem prestados [30]. Essas informações pessoais podem ser recolhidas e processadas de várias formas e em vários cenários, e para isso, é necessário compreender as medidas preventivas que a empresa deve tomar para garantir um serviço de qualidade e seguro, conforme previsto na LGPD [31].

A Figura 3.1 apresenta as principais etapas que compõem o ciclo de vida dos dados, este no qual envolve múltiplas formas de se esquematizar o ciclo, como: coleta, produção, recepção, classificação, uso, acesso, processamento, compartilhamento, armazenamento, modificação, eliminação, reutilização, etc. Entretanto, esses cinco tópicos são os pilares

para todo ciclo e, para fins deste trabalho, basta afirmar que o tratamento de dados pessoais imposto pela LGPD tem um início, meio e fim [19].

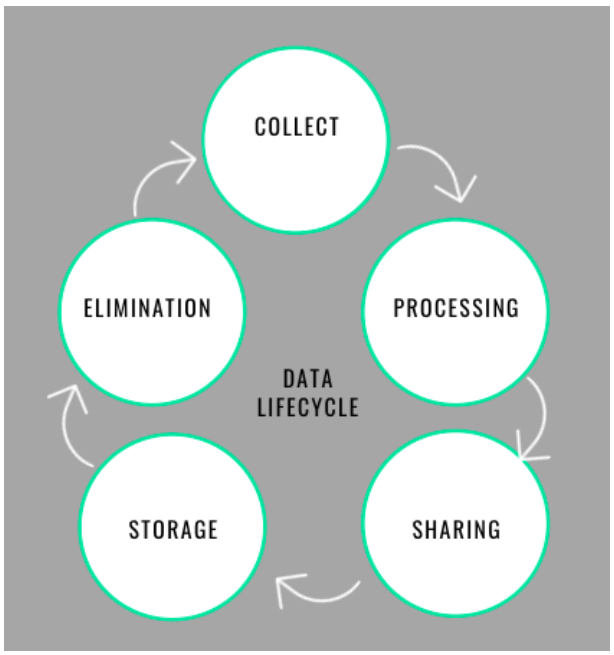

Figura 3.1: Ciclo de Vida dos Dados (Fonte: Figura adaptada [2] página 38)

3.1.2 Coleta

A etapa de coleta consiste em como os dados são inseridos na empresa, é imprescindível que os dados pessoais coletados pela empresa sejam juridicamente consistentes, ou seja, sejam legalmente coletados, e que respeitem a finalidade e transparência com seus titulares para obter seu consentimento para o uso adequado. Devido a uma massa elevadíssima de consumidores, empresas procuram diversas formas de se obterem dados sobre estes indivíduos para assim expandir a sua base de clientes, criar novos serviços, melhorar a eficiência do seu processo de produção, como também diminuir os riscos envolvidos nas operações das empresas [32, 33].

Um exemplo que retrata essa etapa são as áreas de "trabalhe conosco" nos sites das empresas, no qual há um recolhimento dos dados pessoais e dados pessoais sensíveis do indivíduo, por meio de formulários para construir um panorama sobre o perfil do usuário com intuito de executar um processo de seleção. O cadastro pode, conter informações como número de telefone, endereço de e-mail, residencial, mas alguns vão além e podem recolher dados como interesses, preferências e opiniões [34]; o que as empresas devem atentar-se é a relação entre consentimento e transparência na LGPD, o titular deve entender claramente qual é a necessidade da coleta de seus dados e como serão processados, no que é essencial a manifestação livre da pessoa [21].

Diante disso, os consumidores estão ativamente envolvidos no processo de fornecimento de suas informações à empresa, mesmo que geralmente não tenham consciência das consequências de seus atos. Os meios mais comuns que os usuários disponibilizam suas informações são: transações comerciais, censos e registros públicos, pesquisas de mercado, concursos, cookies e comercialização [18].

3.1.2.1 Transação Comerciais

Com as frequentes transações comerciais realizadas no cotidiano, muitas empresas recolhem os dados dos usuários por meio do registro do consumidor ao adquirir produtos ou serviços. Normalmente esse cadastro é pedido para garantir uma segurança maior para o usuário, caso ele efetue compras utilizando cartão de crédito ou cheques. Todavia, esses registros costumam incluir não apenas os dados do consumidor, mas também seus hábitos de consumo, no que possibilita para a empresa no futuro fornecer produtos específicos para o usuário, baseando-se nos seus gostos [35].

Ainda que as organizações consigam obter o consentimento para o recolhimento dos dados os usuários, um ponto preocupante é o monitoramento das informações e a garantia de privacidade da pessoa. A empresa Netflix, por exemplo, consegue sugerir filmes e séries pelo seu sistema de recomendações, este no qual é descrito pela empresa: "O sistema tentará ajudá-lo a encontrar facilmente uma série ou filme. Estimamos sua probabilidade de visualizar um título específico de nosso catálogo com base em uma variedade de coeficientes, tais como: sua interação com nossos serviços, outros assinantes com gostos e preferências semelhantes, informações sobre o título, como gênero, categoria, dentre outros" [36]. Diante disso, a coleta desses dados devem serem feitos conforme a LGPD exige, respeitando a finalidade e a transparência sobre o processamento das informações.

3.1.2.2 Censos e Registros Públicos

Na atualidade, o governo desempenha um papel importante no desenvolvimento da economia da informação com a aplicação de levantamentos de dados quantitativos, também nomeados como cultura de estatísticas e pesquisa de informações do cidadão, no qual essas atividades podem coletar informações do tipo: faixa etária, nível de renda, etnia, localização geográfica, tudo sem referir o nome das pessoas. Esses dados são muito importantes porque fornecem informações precisas sobre o seu público, fornecendo uma base objetiva e sólida, sem subjetivismo [32]. Além disso, é bem comum o governo transferir esses dados recolhidos de forma anônima e oficial para um órgão privado, e nisso, várias empresas do campo de análise de risco, créditos e/ou vendas desenvolvem programas computacionais específicos para criar um mapeamento demográfico com essas informações. Por conseguinte, tal situação conduz a refletir sobre possíveis problemas; primeiramente

os dados pessoais coletados para servir ao censo podem ser usados para marketing direto ou avaliação de risco sem o consentimento do titular [37].

3.1.2.3 Cookies

A coleta de dados pessoais podem ser feitas por meio de tecnologias de controle da internet (como cookies e criptografia). A internet é uma estrutura de rede de computadores aberta, que permitiu ampliar radicalmente as possibilidades de comunicação, diante disso, também estimulou o desenvolvimento de muitas tecnologias de controle, que são derivadas de interesses comerciais e governamentais, e podem resultar em restrições à liberdade do usuário; a partir de aplicativos de software baseados em protocolos de internet, é possível identificar os conteúdos que são acessados pelo indivíduo. [38].

Os cookies são pequenos arquivos de texto criados por sites visitados e que são salvos no computador do usuário, por meio do navegador, a principal função dos cookies é identificar e armazenar informações sobre esses usuários, nos quais esses sites podem usar cookies diferentes para atender às mais diversas necessidades. Eles podem armazenar informações como nome, e-mail, endereço IP, páginas visitadas, e são usados como recursos técnicos para manter adequadamente as sessões e preferências do usuário [39]. Essa coleta de informações de identificação sobre o usuário, naturalmente se enquadra na hipótese de consentimento da LGPD, ou seja, a manifestação deve ser livre, informada e inequívoca, pela qual o titular concorda com o processamento de suas informações [6]; e é por isso, as organizações devem planejarem bem antes de usar os cookies em seus sites para não violar requisitos da lei brasileira de proteção dos dados.

3.1.3 Processamento

Já fase de processamento corresponde às maneiras pelas quais são tratados os dados dos titulares, ou seja, as informações são sujeitas a várias técnicas necessárias para transformá-las em conteúdo útil para as empresas, sendo assim, a organização pode classificar os indivíduos e subdividi-los em diferentes grupos, o que distingue consumidores com maior valor para a empresa e consumidores com menor valor, respeitando sempre as hipóteses permitidas no (Artigo 7º, LGPD) [6, 19]; esses refinamentos dos dados se tornaram algo diferencial para o fornecimento de serviços e produtos variados, bem como diminuir os riscos de negócios para as empresas [10]. Pode citar como técnicas de extração dos dados: Data warehouse, Data Mining (mineração de dados), Online Analyticial Processing (OLAP), construção de perfil (Profiling) e sistema de avaliação (Scoring).

Data Warehouse(DW) é um sistema que permite armazenar informações relacionadas às atividades organizacionais de uma forma consolidada no banco de dados. A estrutura

desse banco é propício para elaborar relatórios, analisar grandes quantidades de informações, assim como construir informações estratégicas úteis para a tomada de decisões; é bastante comum combinar DW com outras técnicas de processamento, como OLAP, profiling, pois os efeitos de refinamento tornam-se mais aparentes e consistentes [40].

A mineração de dados é um processo de análise no qual volumes exorbitantes de dados são explorados para encontrar padrões relevantes ou relações sistemáticas entre as variáveis, detectando assim novos subconjuntos de dados. Basicamente, é através do uso de algoritmos de aprendizagem de máquina ou classificação baseados em redes neurais e estatística, que permite os refinamentos das informações, o que possibilita serem apresentados por diversas formas: grafos, árvores de decisão, dendrogramas, hipóteses e agrupamentos [41]. Nesse aspecto de processamento dos dados, de acordo com a LGPD, uma questão surge sobre a mineração de dados, que envolve o descumprimento do princípio da finalidade, caso esta não tiver sido esclarecida aos consumidores, o que resulta na falta de transparência com os mesmos; ou também para caso da empresa não elaborar os fins da mineração de forma acessível, clara e concisa.

O OLAP permite processar um volume enorme de dados de forma profunda e robusta, as funções mais comuns dessa técnica são: exploração, visão multidimensional dos dados e rotação; são frequentemente projetados para trabalhar com banco de dados desnormalizados, o data warehouse, por exemplo [42]. Ao passo que o DW guarda as informações, o OLAP precisa recuperá-las de forma eficiente e ágil, bem como apresentar informações, que permitem aplicar análises comparativas e facilitar a tomada de decisões.

3.1.4 Compartilhamento

A terceira etapa é o momento de difusão, transação ou interconexão dos dados pessoais, tal fato é extremamente comum e essencial em muitos casos como já citados no capítulo anterior [6]; Essa fase de partilhar os dados é um momento que exige cautela constante, mesmo que a empresa já tenha atendido a conformidade com a lei brasileira. Isso porque a LGPD oferece punições para ambas as partes (controlador e operador), para o caso de ilegitimação no processo; muitas organizações podem apresentar dúvidas quando forem executar compartilhamentos com terceiros, envolvendo procedimentos de segurança e ética, e para solucionar isso, é recomendado seguir normas internacionais de segurança da informação para prevenir incidentes entre si e os seus clientes parceiros, podendo citar a ISO/IEC 27001 [43, 44].

ISO 27001(International Organization for Standardization) é um regulamento internacional que orienta as empresas em garantir a segurança da informação; o regimento pode ser implementado em qualquer tipo de organização, independente de seu porte, seja ela pública ou privada. Esta ISO é baseada no gerenciamento de riscos e em como lidar

com esses riscos dentro da organização para proteger a integridade e a confidencialidade das informações e, talvez hoje seja a ISO que mais se associe à LGPD [45], por conter várias instruções que direcionam. Organizações que cumprem com a norma ISO 27001 e a LGPD, fornecerão produtos ou serviços com maior valor agregado, bem como ampliar a credibilidade com o cliente e a confiança na empresa [19].

O compartilhamento de dados pessoais pelas autoridades públicas é um tema que irá certamente suscitar várias questões. Os dados recolhidos através de meios informáticos são de fácil processamento, podendo ser imediatamente transmitidos e utilizados por sistemas automatizados para efetuar tratamento baseados em algoritmos, sendo, portanto, suscetíveis de infringir os direitos do titular [46]. Tal questão precisa ser organizada antes mesmo da etapa de coleta, por ser fundamental para efetuar um processo de tratamento de dados que respeitem à LGPD.

Além disso, como a LGPD afirma, para o compartilhamentos dos dados é imprescindível o consentimento do titular, salvo em exceções; caso ocorra compartilhamento não autorizado de seus dados, poderá sujeitar a empresa sanções administrativas aplicadas pela ANPD [6]. Sendo assim, aqueles que procuram adaptar os procedimentos internos da empresa às regras de governança e proteção de dados pessoais devem cada vez mais enfrentar preocupações sobre o compartilhamento dos dados do titular por uma parte (controlador), que geralmente são disponibilizados para o tratamento pela outra parte (operador) e suas responsabilidades envolvidas.

3.1.5 Armazenamento

Esta etapa é uma questão complicada que a lei brasileira não responde de forma clara e prática, sendo assim, muitos fatores específicos de negócios precisam ser analisados para obter uma resposta correta; pode-se dizer que a LGPD visa limitar o armazenamento desnecessário e de longo prazo de dados e informações pessoais. É um dos fundamentos da lei, e que segundo ela, o motivo do armazenamento devem ser apresentados na etapa de coleta de dados; o artigo 15º da LGPD [6], prevê sobre as hipóteses do fim do tratamento dos dados pessoais e, logo no primeiro inciso, ela descreve que uns dos motivos do fim do tratamento é quando os dados deixaram de ser relevantes para o tratamento, o que naturalmente encerra o armazenamento destas informações também.

Ou seja, o tempo de armazenamento dos dados deve atender o consentimento do titular dos dados e o objetivo da coleta; um bom exemplo é que se uma empresa planeja guardar alguns dados dos clientes para o envio de promoções e anúncios, é importante estimar um período de tempo durante o qual o anúncio permanecerá ativo para assim garantir a transparência e legitimidade do processo de manipulação dos dados pessoais [35].

A GDPR trata um princípio acerca desse etapa de armazenamento que é princípio de limitação de armazenamento, este que por sua vez, pode servir como um guia para conduzir as empresas brasileiras nos procedimentos que envolvem o armazenamento, além de prepará-las com boas práticas de governança de dados. Resumidamente, essa limitação de armazenamento é uma forma de padronização dos dados, semelhante aos princípios de minimização, não podendo manter os dados pessoais por mais tempo do que o necessário. Se armazenar dados pessoais além da finalidade inicial, para finalidades compatíveis ou outras, devem ser aplicados técnicas de anonimização ou pseudoanonimização nas informações para garantir os direitos dos titulares dos dados, bem como realizar análises periódicas nos dados armazenados [17, 47]. Diante disso, as organizações brasileiras, tem uma base, em como proceder, caso seja necessário o armazenamento por períodos prolongados, deste modo, o ideal para as empresas seguirem é: solicitar o consentimento do titular dos dados acerca desse período de armazenamento, assim como estimar um período de armazenamento para as informações recolhidas.

3.1.6 Eliminação

A etapa de exclusão é qualquer operação para excluir dados, e para isso, é preciso avaliar ativos que armazenam dados pessoais, que podem ser eliminados a pedido do titular ou pedido de descarte. Segundo a LGPD, existe quatro hipóteses para o término do tratamento dos dados pessoais [6]:

- verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- fim do período de tratamento;
- comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público;
- determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

No artigo 18, há um ponto que fala que o titular tem o direito de requisitar ao controlador procedimentos de correção, anonimato, bloqueio ou eliminação de dados pessoais desnecessários, ou tratados em desconformidade e, isso, não se aplicam apenas ao controlador, mas também às empresas que compartilham informações com ele [6]. Assim que o titular solicitar qualquer um desses processos, o controlador deve notificar imediatamente as organizações envolvidas no tratamento dos dados, por exemplo, as informações pessoais podem ser armazenados em banco de dados, documentos físicos, sistemas, ou até

mesmos armazenamento em “nuvem”, e neste último, é necessário informar a organização contratada desse serviço para a exclusão das informações também [48].

Permitir que os usuários controlem seus dados pessoais, e até mesmo conceder que indivíduos solicitem a eliminação desses dados do banco de dados da empresa, é uma das tendências que abordam a ênfase global na privacidade [49]. Diante do risco de vazamento de informações, as pessoas estão prestando cada vez mais atenção a esse problema, portanto, negligenciar as determinações legais do direito de exclusão de dados não é apenas uma multa da ANPD que será aplicada, mas também um grande dano à imagem da empresa.

Capítulo 4

Metodologia BEST

Um dos grandes desafios das organizações é atender as exigências da LGPD e para isso, neste trabalho, será utilizado a metodologia BEST (Business Engaged Security Transformation), um sistema de gestão que respeite todas as áreas de negócios, incluindo processos, pessoal e tecnologia, de forma clara, contínua e sustentável. Esse sistema abrange a construção de um projeto de transformação que envolve que envolve áreas, como: cibersegurança, segurança da informação e continuidade de negócios. A metodologia foi concebida pela fundação Vanzolini, com o objetivo central nos tópicos de cibersegurança e à privacidade de dados. O grande destaque da abordagem é viabilizar a conscientização e a participação dos colaboradores na autotransformação de seus negócios e procedimentos com intuito de obedecer os quesitos de garantia da integridade, transparência, privacidade das informações compartilhadas, processadas e armazenadas. A metodologia BEST é composta por oito princípios [10]:

1. Mindset e Cultura: é por meio de adoções de atitudes proativas, por partes dos colaboradores com seus clientes que possibilitará uma estabilidade com o atendimento das obrigações de cibersegurança.

2. Responsabilidade: os colaboradores possuem total responsabilidade na execução das atividades de negócio que forneçam satisfação com todos seus clientes.

3. Engajamento que é necessário ter comprometimento e percepção, já que se os requisitos de cibersegurança forem negligenciados, todas as atividades não serão capazes de entregar resultados aos seus clientes.

4. Agente de transformação: é um agente externo que umas das suas principais funções é facilitar a superação das dificuldades pessoais da equipe, organizacionais e tecnológicas, canalizando as ações tudo em prol da conscientização dos integrantes.

5. Velocidade: a execução e os objetivos da transformação necessitam ser consistentes e atrelados com as demandas e processos de negócios, reduzindo atritos com os clientes.

6. Metodologia adequada: é essencial escolher a metodologia que melhor concilia com suas aplicações, e por isso, métodos ágeis se adaptam melhor para esse cenário, por providenciar uma resposta ágil a determinadas demandas e permitir uma flexibilidade maior nas atividades de transformação de cibersegurança.

7. Alinhamento estratégico: a alta administração e os gestores precisam integrar em seu modelo de análise do sucesso das atividades de negócio e o nível de qualificação dos colaboradores na conformidade dos requisitos de segurança.

8. Melhoria contínua: é necessário consolidar um procedimento de melhoria contínua de avaliação de processos, no qual todos possuem a responsabilidade de reconhecer oportunidades de aprendizado e a importância do fluxo de eventos envolvidos da cibersegurança aplicado aos negócios.

Com o foco de capacitar todos os integrantes envolvidos no processo de manipulação dos dados, essa visão da metodologia BEST, diminui consideravelmente a responsabilidade exclusiva do DPO, relacionados em atender as exigências da LGPD, dessa forma, respeitar os parâmetros da lei se torna um propósito de toda empresa, e não apenas de alguns indivíduos.

4.1 Implantação do Framework

O framework proposto neste trabalho é baseado na metodologia BEST [10] com algumas adaptações, podendo destacar como diferenças o controle (Subseção 4.1.2.8) sobre a ISO/IEC 27001:2013 [50] e o Programa 3 [23] que descreve abordagens em como melhorar a privacidade dos dados na organização. Ao todo constituirá de quatro programas diretamente conectados com as exigências da LGPD, permitindo que as organizações treinem seus integrantes e forneçam seus serviços de forma segura, legítima e com maior qualidade; os controles são: 1. Programa de Sistema de Gestão de Cibersegurança e Segurança da Informação(SGCSI); 2. Programa de Proteção da Informação; 3. Programa de Aprimoramento da privacidade; e 4. Programa de Atitudes Seguras.

Os controles estão na ordem lógica de instauração, o programa de cibersegurança não é diretamente abordado na parâmetros da LGPD, contudo ele é fundamental para a consistência e cumprimento, de forma precisa, dos princípios, além de ter boas práticas de governanças requisitadas no artigo 50 [6]. Em seguida na ordem cronológica é o controle sobre proteção das informações, este no qual contém a maior parte dos requisitos

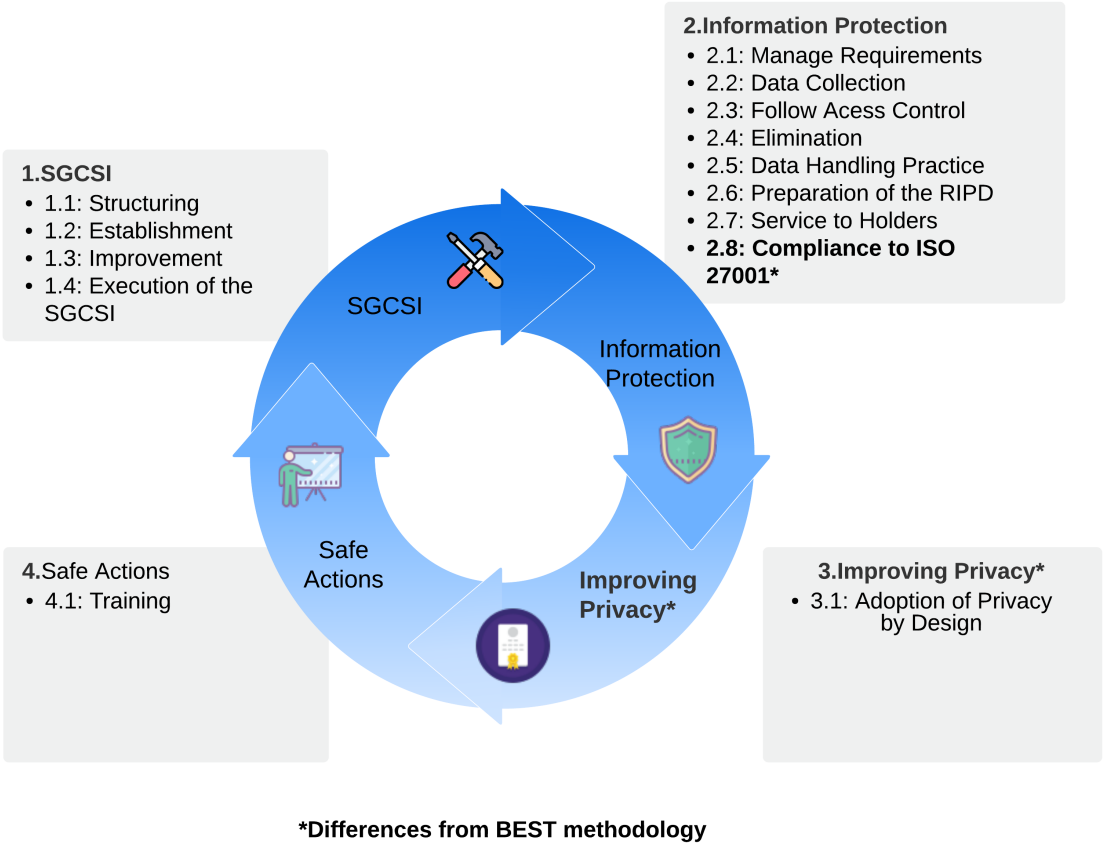

Figura 4.1: Visão geral do Framework (Fonte: autoria própria)

envolvidos à LGPD, sendo assim, é o programa que exige maior atenção da empresa, por englobar vários detalhes e procedimentos para sua correta implantação. Já os dois programas restantes servem para garantir uma persistência de legitimidade sobre as ações das organizações e capacitar progressivamente os integrantes envolvidos com conteúdos de segurança da informação e seu papel de extrema relevância.

4.1.1 Programa 1: Sistema de Gestão de Cibersegurança e Segurança da Informação

Este passo consiste em preparar as empresas em garantir a segurança das informações em todos âmbitos da organização, além de preparar procedimentos a possíveis ameaças que venham a ocorrer; como dito no início desse trabalho, ocorre com muita frequências ataques cibernéticos ou vazamento de dados, diante disso, é um tópico que não pode ser negligenciado por nenhuma empresa. Portanto o controle do sistema de gestão de

cibersegurança e segurança da informação (SGCSI) trata-se de planos, estratégias, políticas, medidas e controles voltados para a segurança da informação [10, 51] que têm o intuito de implementar, monitorar, analisar, manter e melhorar a segurança da informação corporativa [52], sendo composto de 4 fases: estruturação, instauração, manutenção e execução.

4.1.1.1 Estruturação do SGCSI

4.1.1.1.1 Qual SGCSI seguir: O primeiro de tudo é estabelecer um SGCSI, que a empresa irá adotar, pois direciona toda a empresa em como será o escopo do gerenciamento durante o ciclo de atuação da organização, consequentemente, instaura um protocolo consistente que guia todos os integrantes na empresa e permite uma melhora contínua dos processos [53]; um ponto essencial para a implantação é determinar as responsabilidades dos indivíduos em concordância com a estrutura organizacional, já que a depender do momento, existe a possibilidade da organização precisar adaptar sua infraestrutura que aplica seu SGCSI, por motivos de surgir eventualidades, como: incidentes ou novas tomadas de negócios da organização. Portanto, a empresa deve analisar sobre o seu estágio atual e definir meios para preparar a estrutura da empresa para integrar novas mudanças, já que a procedimentos de segurança da informação é algo imprescindível para que todos os processos internos empresariais se mantenham seguros [10].

4.1.1.1.2 Qual política da SGCSI seguir: Este controle consiste em elaborar políticas base a serem seguidas e devem ser planejadas de forma meticulosa e precisa, dado que essas diretrizes são a sustentação de todas as ações de segurança na organização. Protocolos de autenticação, modelos de segurança em ambientes cooperativos, técnicas e tecnologias de segurança da informação são conteúdos que devem ser discutidos e instaurados nessa etapa [54].

4.1.1.2 Instauração e manutenção do SGCSI

Para uma implantação correta, primeiramente, deve estimar um prazo para a instalação, o que implica numa organização maior e mais eficiente. Após essa definição de data, é importante acompanhar o processo de implantação, analisando se foram atendidos os tópicos planejados e aplicar revisões contínuas para adequação das prioridades da empresa; é sempre importante documentar esse procedimento, pois assim, a organização poderá levantar diversas informações, como: o que foi implantando, justificativas da não implementação de tópicos planejados, atendimento das políticas bases da empresa, e a partir disso, a empresa terá indícios se haverá necessidade de redefinir a data das implantações, aplicando manutenções nesses conteúdos relacionados [10]. Aprimoramento do SGCSI é

algo natural no decorrer da instauração, visto que os esforços devem ser da organização como um todo, é como uma nova cultura a ser implementada, todos precisam participar, seja a qual escalão pertencerem na empresa.

4.1.1.3 Execução do SGCSI

E, por fim, na execução deve realizar uma análise completa dos controles e avaliar a eficiência destes de acordo com o prazo, após isso, se tudo estiver em concordância com os passos anteriores, deve divulgar as políticas e normas dentro da organização com intuito de preparar os integrantes para a aplicação da cibersegurança [10].

4.1.2 Programa 2: Proteção da Informação

Essa fase é a que compõe o maior número de controles a serem avaliados, portanto é onde localiza os principais detalhes do guia para atender a maior parte dos requisitos da LGPD, abordando assuntos como: quais dados pessoais a organização está processando, quais tipos de dados estão sendo coletados, quem está compartilhando os dados, como os dados são armazenados, portanto é a etapa onde as organizações dedicarão um esforço maior para atender as orientações deste programa.

4.1.2.1 Gerenciar requisitos para as informações protegidas

4.1.2.1.1 Mapear o valor das informações: Esse controle trata sobre determinar o tipo de informações coletadas com intuito de diferenciar precisamente entre dados pessoais (resguardado pela LGPD) das demais informações, bem como estimar o valor que representa esses dados; resumidamente, é a execução de um mapeamento completo dos dados coletados para então prosseguir no tratamento das informações. Os dados pessoais são um pouco "flexíveis", já que possuem várias classificações a depender do contexto referido, como: dados cadastrais, informações do histórico de consumo, informações médicas, e até mesmo financeiras [10]. Além dessas, há outro grupo de classificação que é o níveis de acesso das informações, no qual estes é um preparo para atender boas práticas da ISO 27001 já comentada [45], sendo assim a empresa torna-se mais preparada para lidar com os dados de seus clientes e a organização dos dados será elevada, dado que com o mapeamento permite uma acessibilidade das informações significativamente maior; os níveis estão ordenados de forma do mais alto nível de confidencialidade pro mais baixo, são eles respectivamente: confidencial, restrita, uso interno e pública [3].

4.1.2.1.2 Definir os tipos de arquiteturas: A definição das arquiteturas é um conteúdo sobre engenharia de software e consiste num passo importante para a organização

já que é dividida em dois tipos: arquitetura funcional e técnica [10]. A funcional trata-se de planejar as metodologias de funcionamento na qual é uma descrição ou modelo de como solucionar os problemas dos clientes e pode ser utilizado nas mais diversas situações, ou seja, define como deve tratar as necessidades propostas por esses clientes [55]. A organização que conseguir ser um diferencial para o mercado e demonstrar seus atrativos será a que sairá na frente e é a chave para alcançar mercados existentes e conquistar clientes que já possuem uma destas soluções, e é por essa razão, que é recomendável para as organizações planejarem e incorporarem a arquitetura funcional em sua infraestrutura [56].

Já a arquitetura técnica trata dos elementos específicos da aplicação que sustentam a execução das funcionalidades pela arquitetura funcional, ou seja, recursos como: estrutura de dados computacionais, logísticas de armazenamento, tipo de rede, forma de processamento de dados, distribuição da aplicação; em outras palavras, são todos os recursos essenciais para a execução das atividades da empresa [55]. Além disso, é de fundamental importância definir nessa fase a localização geográfica da realização do processamento de dados e o armazenamento, pois como já descrito no artigo 3º da LGPD [6], há uma restrição territorial de sua aplicabilidade, portanto é necessário definir esse contexto já aqui; mesmo que as informação não sejam tratadas no território nacional, se há referência com pessoas situadas no Brasil, a LGPD é aplicável.

4.1.2.1.3 Indicar os agentes responsáveis: A nomeação do encarregado, controlador e operador é realizado nessa fase. Primeiramente é interessante eleger o controlador para gerenciar as decisões referentes ao processamento de dados, já que este possui um peso maior nas responsabilidades a serem exercidas [6]. Em seguida é necessário indicar o operador, este que exerce suas funções de tratamento de dados em nome do controlador; como o controlador e o encarregado podem ser pessoas física ou jurídica, a empresa tem a opção de si nomear como tal. E, por último, o encarregado é a pessoa que é indicada pelo controlador e operador que tem como funcionalidades de ser a ponte de comunicação com a controlador, titulares e a ANPD.

4.1.2.2 Coleta de dados

4.1.2.2.1 Manter salvo todos os procedimentos aplicados as informações sensíveis: Esse controle é onde a empresa deve incorporar boas práticas de governança, logo ações de processamento, armazenamento, compartilhamento e transmissão que envolvam dados pessoais sensíveis devem ser salvos e documentados [10], o que eventualmente possibilita gerar com essa base de dados o próprio RIPD, caso seja necessário.

4.1.2.2.2 Definir fins da coleta: A finalidade é um ponto fundamental para a execução da manipulação dos dados, sendo o primeiro princípio do tratamento de dados abordado (artigo 6º,LGPD), logo é um esforço a ser definido antes do tratamento e deve possuir propósitos legítimos, explícitos e não discriminatório, bem como determinar características sobre fins privados ou específicos, já que o artigo 4º delimita ressalvas na qual a LGPD não se aplica [6]. É importantíssimo documentar essas parâmetros de finalidades definidos, para posteriormente comprovar para seus clientes e para ANPD sobre o fins da coleta, caso for necessário.

4.1.2.2.3 Informar tratamentos, compartilhamentos ao titular e obter consentimento do mesmo: Tópico primordial para a execução de coleta, então é necessário informar ao titular dos dados sobre as especifidades do tratamento que serão efetivamente executados, bem como possibilidade de ocorrer transação de dados com terceiros, e importante ressaltar que essa notificação deve ocorrer também no cenário digital [10, 45]. Após a comunicação sobre o procedimento, a organização precisa solicitar o consentimento do titular ou do responsável(hipótese quando os dados referem-se a indivíduos de menor de idade), e existindo a concordância do titular, é de suma importância registrar essa manifestação da vontade do titular de forma escrita ou com outros meios, tendo a consciência que esse consentimento pode ser revogado a qualquer momento pelo titular(artigo 8º) [6].

4.1.2.3 Acompanhamento do controle de acesso dos dados

No decorrer do tratamento de dados, é necessário gerenciar o repertório de acesso à informação para construir um panorama sobre quais informações são acessadas pelas aplicações e/ou por quais usuários. Então esse passo consiste em gerenciar, atribuir ou remover permissões de acesso aos dados para as aplicações ou usuários. Para controlar se os usuários que acessam os dados realmente possuem autorização para tal ação, a organização necessita registrar esses acessos à informação, e diante disso, o mais aconselhável é dentro do próprio banco de dados para assim, a empresa ter uma gerência maior dessas aquisições de informações e confirmar se tal usuário tem a permissão para acesso [10]. Como há possibilidade de acessos por terceiros devidamente autorizados, para o registro de acesso é viável também o uso de leitores, dispositivos que realizam o controle de acesso através de cartão, leitura facial, impressão digital ou senha, no qual enviam essas credenciais para as controladoras realizarem a autenticação do usuário [57]. Outra forma de controle de acesso são as transferências (SFTP, HTTPS), para manter a lista de acessos sempre atualizada, já que com a utilização do SFTP, por exemplo,utiliza-se do protocolo de rede SSH (Secure Shell) para autenticar o contato e estabelecer uma conexão segura

para a transmissão dos dados entre as máquinas, o que garante uma segurança e controle de acesso maior [58].

4.1.2.4 Eliminação da informação

Os casos mais comuns para a eliminação dos dados é quando o próprio titular requisita a exclusão de suas informações ou quando o tratamento dos dados atingiu sua finalidade inicial. Aqui a organização deve disponibilizar mecanismos que permitam os usuários solicitarem informações, incluindo a remoção destas de forma clara e segura. Em alguns casos os dados podem ser mantidos, de acordo com artigo 16º da LGPD [6], há 4 casos que permitem a conservação: 1. cumprimento de obrigação legal ou regulatória pelo controlador; 2. estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; 3. transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; 4. uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Por isso, é sempre importante comunicar o titular sobre as possibilidades de conservação dos dados para execução de atividades para que ele tenha total consciência de ponta a ponta do processo de manipulação de seus dados.

4.1.2.5 Práticas de manuseio de dados

Nesse momento ocorre o tratamento dos dados, e por isso, seguir o código de ética definido no SGCSI é importante não somente para prevenir desvios de comportamentos compatíveis com a segurança da informação, mas também para garantir a legitimidade do processo de manuseio de dados [53], o que permite que a organização comprove pros seus clientes que o tratamento de seus dados respeitem os princípios prescritos na LGPD, como: finalidade, necessidade, transparência, livre acesso e gratuito, qualidade dos dados, segurança; todas essas prerrogativas são uma parcela do total defendida pela LGPD [6] e devem ser garantidas neste controle.

4.1.2.5.1 Garantia da qualidade dos dados e necessidade Neste princípio é importante analisar continuamente os dados sensíveis dos titulares que recebem tratamento, pois estes devem estar devidamente atualizados, bem como apresentar características de: exatidão, clareza, relevância (artigo 6º, inciso V) [6]. Oportunamente, como este passo consiste em avaliações, a empresa precisa avaliar também a necessidade dos dados, em outras palavras, se a informação é mínima, compatível com o mínimo necessário para a alcançar a finalidade [6, 46]. A organização pode basear-se em perguntas como [10]: 1) as informações sensíveis capturadas estão corretas?; 2)todos os dados pessoais sensíveis coletados são necessários para o serviço oferecido e utilizados nos tratamentos?; 3)todos os

dados pessoais sensíveis capturados estão atualizados? Dessa forma, a empresa entenderá os dados essenciais para suas atividades e coletará apenas estes.

4.1.2.5.2 Garantia de livre acesso e transparência: A empresa deve evidenciar em todas as etapas do tratamento dos dados o direito de livre acesso e transparência de forma gratuita, nítida, e simplificada [46]. Os tipos de informações fornecidas para os titulares podem conter, conforme o artigo 9º: finalidade do tratamento, forma e duração do tratamento, identificação e informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador e a finalidade, responsabilidades dos agentes de tratamento, bem como os direitos garantidos do titular [6, 18].

Um fato interessante que a organização precisa ter consciência que caso ocorra mudança da finalidade não compatíveis com o consentimento original, o controlador deverá comunicar com antecedência o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações (artigo 9º §2º, [6]); em outras palavras, esse controle consiste em ser transparente e atribuir apropriadamente responsabilidades, dado que facilita a prestação de contas, tanto aos titulares (com base em seus direitos previstos em lei) quanto para a própria ANPD.

4.1.2.5.3 Garantia de anonimização: Aplicar técnicas de anonimização é incentivada pela própria LGPD, tanto que para esses tipos de dados, a lei brasileira não se aplica, conforme o artigo 12º: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" [6]. A lei somente traz a anonimização como uma opção em determinadas circunstâncias(realização de estudos por órgão de pesquisa, por exemplo), mas não é um procedimento obrigatório para quem deseja tratar dados pessoais. O grande atrativo da anonimização é justamente a não incidência da LGPD sobre dados anonimizados, portanto, caso a sua empresa não precise identificar diretamente os titulares dos dados, é aconselhável a anonimização, pois é benéfico para os titulares e pode ser melhor para a organização também, já que evita vários riscos de privacidade [54].

4.1.2.5.4 Manter o registro (log) dos tratamentos efetuados: Adicionalmente, a LGPD em seu artigo 37º solicita que os agentes controladores e operadores devem registrar as operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse [6]. Portanto, as organizações devem criar uma espécie de inventário de dados(logs) onde é compilação estruturada das informações relacionadas às operações de tratamento de dados pessoais e que complemente as informações citadas pela artigo 9º [10, 59]. Uma lista de informações que poderiam acrescentar esse inventário

de dados, são: Identificação do responsável pelo preenchimento do inventário, identificação da base legal atribuída a cada operação do tratamento, descrição da operação de tratamento e informações de transferência internacional(se houver) [18].

4.1.2.6 Elaborar o RIPD

O relatório de impacto à proteção de dados é explicado pelo artigo 5º, inciso XVII: "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" [6]. Esse relatório apoia-se no princípio da responsabilidade e prestação de contas, o que ajuda as organizações provarem que tomam medidas técnicas e organizacionais, sendo assim, é usado para avaliar os riscos a direitos e liberdades dos titulares de dados que resultam do processamento de dados, e também podem ser úteis na implementação de novos processos ou tecnologias no ambiente corporativo [31,38]. A LGPD não especifica em como elaborar o RIPD, mas tem determinadas informações que são relevantes, como:

- Identificar a necessidade (justificativa);
- Descrever o fluxo de informações;
- Descrever a natureza, o escopo, o contexto e os propósitos do processamento (fundamentalmente, a base legal);
- Identificar os riscos para os direitos e liberdades dos titulares de dados (como a privacidade do titular seria ameaçada, neste processo);
- Identificar soluções para reduzir ou eliminar esses riscos (alternativas de mitigação do risco);
- Apresentar possíveis soluções de proteção de dados (quando cabível).

Portanto, é importante mencionar que a finalidade da RIPD não é eliminar riscos, mas prever e mitigar riscos de forma a minimizá-los. Não deve ser usado apenas como um documento burocrático para o cumprimento da legislação, mas deve ser usado como uma ferramenta para as melhores práticas e aprimoramento de processos e soluções relacionadas à proteção de dados. Neste ponto, tem uma ideia relevante deste trabalho, que o RIPD é extremamente útil para conscientizar a empresa dos riscos existentes e ajuda a evitá-los, já que ameaças cibernéticas ou vazamentos de dados tornaram-se cada vez mais frequentes na atualidade, conforme visto no início do trabalho.

4.1.2.7 Atendimento a solicitações e reclamações de terceiros

É importante poder identificar se o pedido feito pelo titular dos dados é aplicável de acordo com a LGPD e quando pode ser rejeitado, bem como desenvolver um plano estruturado para responder aos pedidos, reclamações e correções, e é neste controle que a empresa precisa evidenciar a existência de mecanismos que atendam solicitações dos titulares e da ANPD. Sendo assim, é aconselhável que as organizações integrem em suas estrutura fatores como [30]: canais adequados para receber todas solicitações, treinamento para funcionários que realizarão essas operações de atendimento, recursos de identificação do titular, gerenciamento do tempo de recebimento e resposta, criação de evidências do recebimento e respostas com intuito de proteger as ferramentas de segurança da informação e promover operações responsivas para respeitar todos os direitos do titular [10].

4.1.2.7.1 Comunicar pedidos do titular com agentes terceiros: Como há possibilidades de agentes terceiros manipularem as informações durante o tratamento, conforme o artigo 18º §6º, a solicitação do titular e da ANPD deve ser comunicada imediatamente ao agente de processamento com o qual o controlador compartilha os dados. Essa comunicação deve incluir correções, exclusões, anonimato ou bloqueio de dados, exceto nos casos que a comunicação for comprovadamente impossível ou resulte em esforço desproporcional [6], portanto, os meios de comunicação utilizados ao atendimento dos titulares devem ser flexíveis o suficiente para suportar essa possibilidade também.

4.1.2.7.2 Notificar incidentes: Essa situação é onde que as organizações precisam manter calma para lidar com os problemas, já que tais situações não podem ser negligenciadas, tampouco omitidas. Em casos de incidente de segurança que tenha possibilidades de acarretar riscos ou danos significativos aos titulares, o controlador tem a responsabilidade de notificar a ANPD e o titular dos dados (artigo 48º) [6]; a LGPD afirma que o prazo dessa comunicação tem que ser em um prazo razoável e as informações a serem repassadas, são como: riscos relacionados ao incidente, informações sobre os titulares envolvidos, bem como a descrição da natureza dos dados pessoais afetados; indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados. Sendo assim, as organizações precisam implantar processos de gerenciamento de incidentes que assegurem que incidentes e deficiências relacionadas aos sistemas de informação sejam conhecidos, de forma que ações apropriadas possam ser tomadas em tempo hábil. Primeiramente, é importante compreender o processo de incidente e que ele é composto de quatro etapas: ameaça, incidente, dano e restauração [54], e é exemplificado na Figura 4.2 para melhor compreensão.

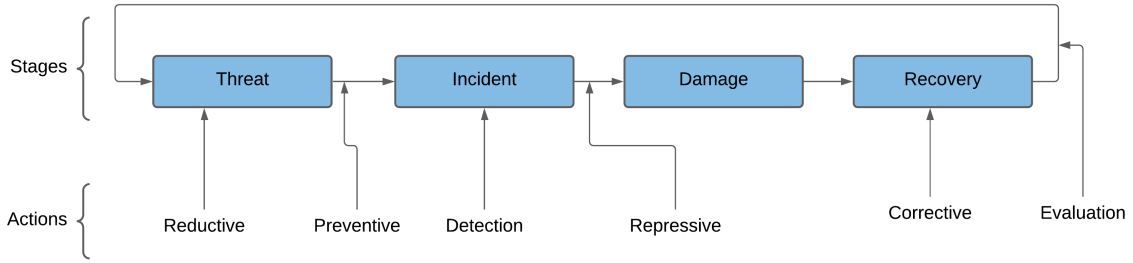

Figura 4.2: Ciclo de um incidente (Fonte: [3] página 108)

A etapa de ameaça consiste em identificar possíveis ameaças cibernéticas e se preparar para evitar incidentes. É muito comum não haver preparação suficiente para ameaças existentes, e isso certamente, poderá causar problemas em momentos futuros; a próxima etapa é o fato do incidente em si que pode acontecer de diferentes maneiras, e uma das questões chave é em responder a ameaça com a utilização de ações repreensivas, para solucionar o incidente da forma mais eficiente possível. Após isso, será necessário reconhecer os danos causados pelo o incidente, iniciando medidas corretivas para restaurar as "lesões" sofridas [3]. E por fim, métodos de avaliações devem ser aplicadas após a restauração com intuito de documentar e construir provas dos procedimentos internos adotados, consequentemente, com essas evidências em mãos, colabora na análise do próprio incidente e ensina as organizações a corresponder melhor a esses tipos de eventos [60]. As organizações precisam esforçar em manter uma comunicação clara e acessível com seus clientes, além de executar esse gerenciamento de incidentes, já que fazem toda a diferença na hora de solucionar os problemas.

4.1.2.8 Adequação para ISO/IEC 27001:2013

Se a organização almeja construir uma boa reputação em termos de disponibilidade, confidencialidade e integridade, agregando diferencial competitivo e valor à sua marca e/ou produto, a ISO/IEC 27001:2013 será uma grande aliada para a imagem da empresa, já que ao obter a certificação dessa ISO, a organização terá vantagem competitiva na visão de clientes que são sensíveis a questão de manter suas informações seguras [44, 61].

4.1.2.8.1 Criptografia: Devida a importância de manter segurança nos dados, a criptografia é uma das melhores formas de manter a integridade das informações, sendo recomendado aplicar em todos os dispositivos utilizados pela empresa, dessa forma, existe vários tipos de criptografia, como: chave simétrica e assimétrica, IDEA (International Data Encryption Algorithm) e AES (Advanced Encryption Standard), entre outras [54].

A chave simétrica é o modelo mais comum e simples, entre eles, o remetente e o destinatário da mensagem usam a mesma chave, ou seja, ela é usada para codificar e decodificar os dados ao mesmo tempo; na assimétrica a chave privada é usada para descriptografar a mensagem e a chave pública é usada para criptografar o conteúdo. Portanto, quem precisa enviar conteúdo para alguém, precisará apenas da chave pública do destinatário, que usa a chave privada para descriptografar a mensagem. O que torna esse sistema tão especial é que a chave pública pode ser conhecida pelo mundo inteiro, contanto que a chave privada seja mantida em segredo [62].

O IDEA é uma chave simétrica que pode operar em blocos de informação de 64 bits e usa uma chave de 128 bits. Funciona de diferentes maneiras, criptografa textos, protege informações e evita rearranjos para que sejam lidos corretamente, criando uma espécie de confusão para quem tentar decifrar. O cifrador IDEA tornou-se popular e é amplamente utilizado, sendo aplicado com certa frequência, dado que esse técnica é bastante complexa; e por fim, o AES é um dos algoritmos de criptografia mais seguros da atualidade e é usado por inúmeras organizações de segurança. Sua criptografia é feita em blocos de 128 bits, mas a chave também pode ser aplicada em 192 bits e 256 bits, o que torna a chave extremamente difícil de quebrar em ataques cibernéticos, por esse motivo, é extremamente aconselhável para as empresas usar essa técnica de cifração [53, 62].

4.1.2.8.2 Análise de vulnerabilidades e Pentest: Vulnerabilidade pode ser vista como qualquer variável que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos, e por isso, que torna esse conceito de avaliação de fraquezas tão importante na atualidade. A análise de vulnerabilidade consiste em um programa rotineiro, na maioria das vezes, é automatizado por um software chamado escaneadores(scanners), que servem para localizar o ponto de falha, criando relatórios sobre vulnerabilidades em hosts locais e remotos , ou seja, detecta possíveis brechas que podem ser utilizadas para invasão por cibercriminosos. Os escaneadores podem ser configurados para monitorar um único endereço IP ou vários endereços IP, eles podem realizar os seguintes tipos de análises: Escaneamento de conexao Protocolo de Controle de transmissão (TCP), Escaneamento semiaberto, Escaneamento de Protocolo Datagrama de usuário (UDP), Escaneamento do protocolo IP, Escaneamento de ping e Escaneamento discreto [63]. Além dos scanners, há outras abordagens para detectar vulnerabilidades nos softwares, como [64, 65]:

- Exploits: Programas automatizados que buscam causar um comportamento acidental ou imprevisto na execução de um sistema, podendo ocorrer roubo de dados;
- Envenenamento de DNS: altera uma tabela de endereçamento do DNS, desviando o tráfego dos servidores legítimos e direcioná-lo a caminhos falsos;

- Buffer overflow: O estouro de buffer ocorre quando um programa, ao gravar dados em um buffer, ultrapassa os limites do buffer e sobrescreve os locais de memória adjacentes, permitindo executar programas indesejados;
- Negação de serviço: Conhecido como ataque Denial of Service ou DoS, basicamente busca sobrecarregar um determinado sistema, localmente ou remotamente, para que o serviço fique indisponível.

Com todos esses mecanismos existentes, a organização deve avaliar qual destas técnicas melhor se enquadram com sua estrutura, permitindo assim, detectar e elencar as ameaças de acordo com a sua criticidade. Além dessas análises de vulnerabilidades, a organização deve considerar em utilizar testes de penetração(pentest), o pentest é conhecido como ataque controlado, no qual existe um roteiro pelo qual o responsável de segurança da informação se guiará, verificando se é possível invadir ou obter alguma informação sem nenhuma autorização, em outras palavras, o pentest é uma simulação de um ataque real onde verifica como o hacker poderia utilizar uma determinada falha para abrir caminho até seus dados sensíveis [66]. Alguns exemplos de ataques cibernéticos: Code Injection – injeção de códigos (SQL, PHP, LDAP); XSS/CSS (cross site scripting) – usado para obter sessões de usuário, obter cookies; Força bruta (Brute Force) – usado para quebra de senha, exploração de senhas fracas [67]. Portanto, um procedimento que as organizações poderiam adotar é fazer uma análise de vulnerabilidades para reduzir seus riscos, complementando com o pentest para a avaliação de riscos residuais que não puderam ser eliminados na análise.

4.1.2.8.3 Continuidade de negócios: A possibilidade de crise no novo cenário é muito grande e muitas organizações precisam se reorganizar para garantir a sustentabilidade dos negócios, o objetivo da gestão de continuidade de negócios é prevenir a interrupção das atividades da empresa, proteger os processos críticos das consequências mais agravantes do sistema de informação, bem como permitir uma recuperação rápida. O gerenciamento de continuidade é geralmente dividido em duas partes independentes, mas profundamente relacionados, são elas [68]: Planejamento de continuidade do negócio (Business Continuity Planning – BCP) , no qual consiste em identificar os processos do negócio que são garantidos, e o segundo é o planejamento de recuperação de desastres (Disaster Recovery Planning – DRP), onde é organizada a recuperação após um desastre. Para contextualização, o BCP trata-se de um plano que irá guiar a gestão da continuidade do negócio em situações de imprevisto que vão desde a temporária falta de energia elétrica até desastres naturais, pandemia, incêndios, pane nos sistemas de segurança, acidentes, entre outros [69]; são considerados incidentes por ser situações que afetam a vida e o trabalho diário dos indivíduos.

No BCP, o focal total é em manter a empresa funcionando, mesmo que apenas parcialmente, a partir do momento em que o desastre ocorre até quando a empresa estiver totalmente recuperada, isso é fundamental para assegurar o que chama de resiliência organizacional. Em outras palavras, por meio do BCP é possível identificar ameaças e prever cenários que podem exercer impacto sobre as operações da empresa, permitindo uma preparação mais eficiente e a continuidade de seus processos [70]. Já o DRP [71] é usado para recuperação imediata após um desastre, sendo posto em prática enquanto o desastre está em andamento, com o intuito de identificar o prejuízo e fazer o sistema funcionar novamente. Para garantir a continuidade dos negócios e a disponibilidade dos recursos-chave durante o incidente, o plano deve ser documentado e testado com antecedência; isso ajudará a acelerar o processo no caso de um desastre ou emergência real [69]. Dessa maneira, o grande destaque do DRP é minimizar a interrupção das operações comerciais e os riscos de atrasos, além de ajudar na restauração das operações com maior velocidade, e é por isso, que as organizações precisam pensar em sua continuidade de negócios para poder aplicar suas operações com maior segurança e flexibilidade, diminuindo o dano dos incidentes surgidos.

4.1.3 Programa 3: Aprimoramento da privacidade

4.1.3.1 Adoção do Privacy by Design

Como já vimos anteriormente no Capítulo 2, a concepção de Privacy by Design (PbD) resume em uma abordagem, divida em princípios que visa garantir a proteção da privacidade dos indivíduos, tal metodologia recebeu tanta notoriedade que ganhou reconhecimento mundial [72], sendo incorporado seus conceitos até mesmo pela GDPR, e por esse motivo, as organizações brasileiras devem dedicar esforços para adotarem essa política de privacidade, já que ela também é uma grande aliada na adequação da LGPD, por conter boas práticas no procedimento de tratamento de dados pessoais [49]. Para oferecer uma compreensão mais sólida, será relacionado os princípios do PbD com os controles já abordados nesse framework para construir uma interconexão entre programas. O primeiro princípio é sobre medidas proativas e preventivas, bem como não reativas; resumidamente para as empresas, o ideal é prevenir incidentes de privacidade antes que eles ocorram, e para que isso ocorra, é preciso desenvolver métodos para detectar vulnerabilidades e gerência de riscos, e é aqui que este princípio relaciona-se diretamente com o controle 4.1.2.8.2 (análise de vulnerabilidade), que ao atendê-lo, também cumprirá requisitos do PbD consequentemente.

O princípio da Privacy by Default estipula que a privacidade deve ser configuração padrão de qualquer prática de negócio ou sistema, não sendo obrigatório a participação

manual pelo usuário, em outras palavras, as organizações já devem inserir por padrão aspectos de privacidade para seus produtos e/ou serviços. Alguns aspectos importante a enfatizar que o Privacy by Default, possui semelhanças que compartilham correlações aos princípios da LGPD, por exemplo, ele apresenta conceitos sobre especificação da finalidade, explanando que o tratamento de dados deve ter fins específicos, claros, limitados e relevantes às circunstâncias, o que naturalmente correlacionamos com o princípio de finalidade da LGPD [73]. Além disso, trata também requisitos de limitação da coleta, o que remete ao princípio da necessidade, abordando que o recolhimento de dados pessoais devem ser justo e limitado para os fins estipulados. Outro princípio do PbD é o privacidade incorporada ao design sugere que a privacidade deve ser empregada à tecnologia, operações e arquitetura de informações de uma maneira abrangente e integrada ao projeto como um todo, adicionando o uso da criatividade para promover a inclusão de seu público na privacidade e proteção dos dados, muito enfatizado nas políticas de privacidade das corporações, pois maximiza o entendimento dos titulares sobre as suas disposições [23].

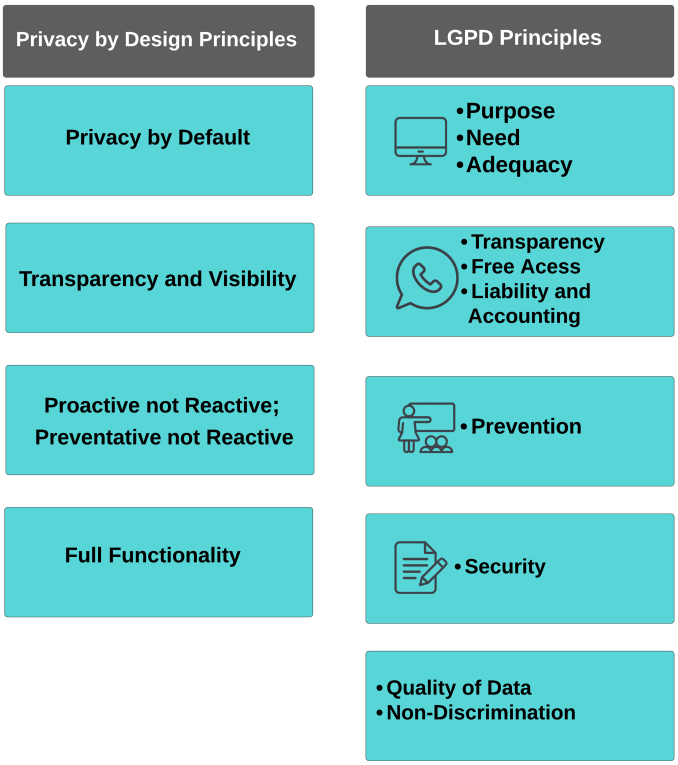

Figura 4.3: Relacionamento entre princípios da LGPD e Privacy by Design (Fonte: autoria própria)

A funcionalidade completa é o quinto fundamento do PbD, é umas das essências promovida pela LGPD que simplesmente mostra que privacidade e segurança não se opõem, mas são somadas para melhor atender às expectativas dos titulares dos dados, e nisso, cria-se uma relação mais consistente e próxima com os indivíduos, em outras palavras, organizações que constroem privacidade sabem como criar valor econômico ao mesmo tempo em que protegem a privacidade individual [74]. A transparência e visibilidade do PbD é uma extensão do princípio anterior e são essenciais para demonstrar responsabilidade, honestidade e gerar confiança com os usuários, consequentemente mostra para estes que a organização está aberta sobre o que pratica, defende suas afirmações e responde de forma clara e ágil quando surgem qualquer tipo de dúvidas. Desta maneira, correlaciona-se intuitivamente com os fundamentos da LGPD sobre transparência, livre acesso, responsabilização e prestação de contas, já que a ideia central é manter uma relação direta e transparente com os clientes. O princípio de segurança de ponta a ponta do PbD, consiste em garantir a segurança das informações durante todo o ciclo de vida do processamento dos dados pessoais, por meio de tecnologias como criptografia apropriada, anonimização, controles de acessos precisos, diante disso, reforça-se ainda mais a eficácia da incorporação da ISO 27001, dado que como foi visto, há vários técnicas de ciframento das informações, ampliando a segurança dos dados armazenados [44, 68].

Por último, o princípio do PbD de respeito pela privacidade do usuário é entendido como a conclusão dos demais fundamentos, já que o titular dos dados devem ser respeitados, juntamente com o esclarecimento das medidas de seguranças adotadas, resumidamente, a organização deve coletar, usar, armazenar, compartilhar e retirar informações de uma maneira que seja consistente com o respeito pela privacidade do indivíduo [73].

Em meio a isso, o intuito desse programa é perceber a convergência clara entre os princípios da LGPD e essa sistemática de privacidade dos dados, já que quando a organização adere ao compliance da LGPD, ela atende a vários aspectos sobre privacidade, ao passo que o oposto também é verdade, pois ao cumprir fundamentos do Privacy by Design, ela atende naturalmente vários princípios da LGPD e o artigo 46º em específico [6].

4.1.4 Programa 4: Atitudes seguras

4.1.4.1 Treinamento

Embora a organização tenha investido pesadamente em recursos de segurança de dados e em políticas de gestão de cibersegurança, se os funcionários não forem treinados para identificar e prevenir ameaças cibernéticas, tal negligência podem causar gravíssimos problemas como: vazamentos ou roubo de informações [2], e é por esse motivo, que esse programa é tão relevante para o ambiente corporativo. Muito desses incidentes são cau-

sadas pela insuficiência de conhecimento sobre a LGPD, contudo vale ressaltar também a engenharia social, esta é uma ação empregada por cibercriminosos e pode ser definida como o ato de manipular seres humanos, muito frequente com o uso de persuasões psicológicas, infecções dos computadores da vítima com malware e/ou envio de links infectados, tudo para obter acesso do sistema que contém dados pessoais que não deveriam ser acessados por indivíduos não autorizados [10, 75], dessa forma, a proteção para combater a engenharia social é por meio do treinamento, resumidamente, os colaboradores da organização(funcionários, contratados e visitantes) devem ser instruídos a nunca clicar em links suspeitos; proteger suas credenciais de login, excluindo qualquer solicitação de informações financeiras ou senhas; analisar a fonte dos e-mails(revisar o cabeçalho do e-mails, por exemplo), definir seus filtros de spam como alto para evitar conteúdos suspeitos, dentre outros aspectos relacionados a atitudes seguras [76].

A própria LGPD estabelece no artigo 50º que os controladores e operadores, no contexto de suas competências, podem formular regras de boas práticas e governanças como: ações educativas, mecanismos internos de supervisão e de diminuição de riscos [6]; portanto, todos colaboradores são responsáveis pela segurança dos dados da empresa, por isso é fundamental o treinamento sobre a LGPD e outros aspectos relacionados a engenharia social, para garantir assim uma segurança maior para os indivíduos e as informações.

Em virtude do que foi proposto neste guia, antes de colocar em prática cada um dos pontos abordados neste framework, avalie sua realidade e molde essas habilidades de acordo com suas necessidades, para que sua organização seja capaz de atender todos os aspectos de cibersegurança, proteção da informação, Privacy by Design e os treinamentos propostos por este guia.

4.2 Verificação do Framework Proposto

Para avaliar o framework proposto, foi conduzido um survey I.1, de forma online, no qual as questões foram baseadas nos tópicos abordados pelos programas e controles do modelo proposto, como segurança, privacidade, conformidade e boas práticas de Governança de ICT. O survey ficou disponível online durante 45 dias e o tempo médio para respondê-lo foi de 12 minutos. No total, 53 profissionais de ICT responderam o questionário. De acordo com as percepções dos profissionais de TIC, a maioria das organizações apresentam algumas características importantes para uma infraestrutura consistente e em conformidade com a LGPD.

De acordo com a questão 3 apresentada na Figura 4.4 é possível observar que 88% dos participantes concordaram que suas organizações manipulam dados pessoais, o que é necessário dedicar atenção para tal fato. Com relação à questão 6 na Figura 4.4, observou-

se que cerca de 88% das organizações já iniciaram medidas de adequações com a LGPD. Esse resultado nos permite inferir que a conscientização e conformidade em relação a LGPD está amadurecendo cada vez mais no cenário organizacional.

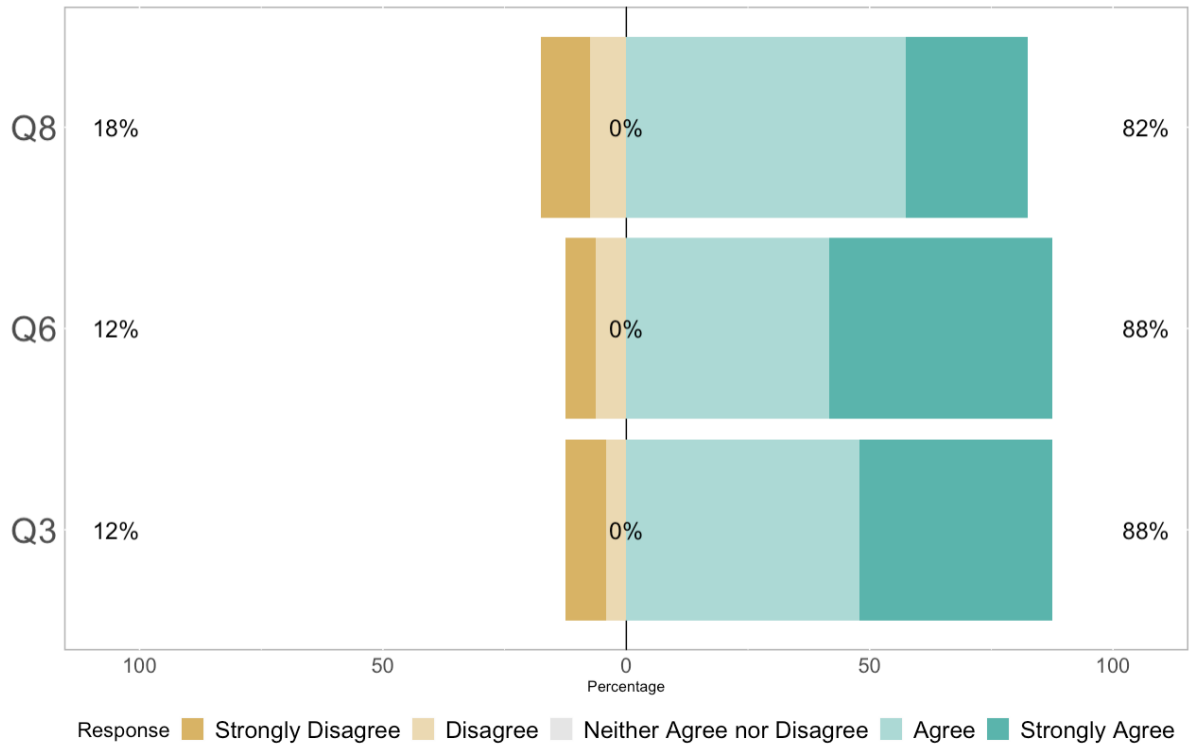

Figura 4.4: Ações de adequação à LGPD, tratamento e mapeamento dos dados

82% das organizações preocupam-se em mapear os dados, o restante das organizações ou não sabem ou não ocorre o mapeamento das informações, conforme apresentado na questão 8 da Figura 4.4. Esse achado pode gerar problemas futuros para as organizações, já que identificar e classificar os dados que são tratados pela organização, é fundamental para melhoria dos processos organizacionais de segurança da informação, aumento na confiabilidade dos processos e na governança de TIC da organização.

26% das organizações descuidam-se em compreender como funcionam e quais são os equipamentos que compõem a sua própria infraestrutura de tecnologia da informação, conforme apresentado na questão 10 da Figura 4.5. É por isso, que é um conceito tão importante do framework, pois com a documentação, facilita a leitura e entendimento do contexto tecnológico da empresa, além de construir um ambiente mais estruturado, permitindo a acessibilidade e gerência informacional do sistema de forma bem mais eficaz.

Em relação aos mecanismos de comunicação dentro da empresa, questão 11 da Figura 4.5, a grande maioria dos profissionais afirmaram que em suas organizações é de extrema relevância os meios de comunicação e a transparência fornecida à seus clientes, isso é um ponto excelente, dado que a relação entre empresa e cliente é essencial não só para

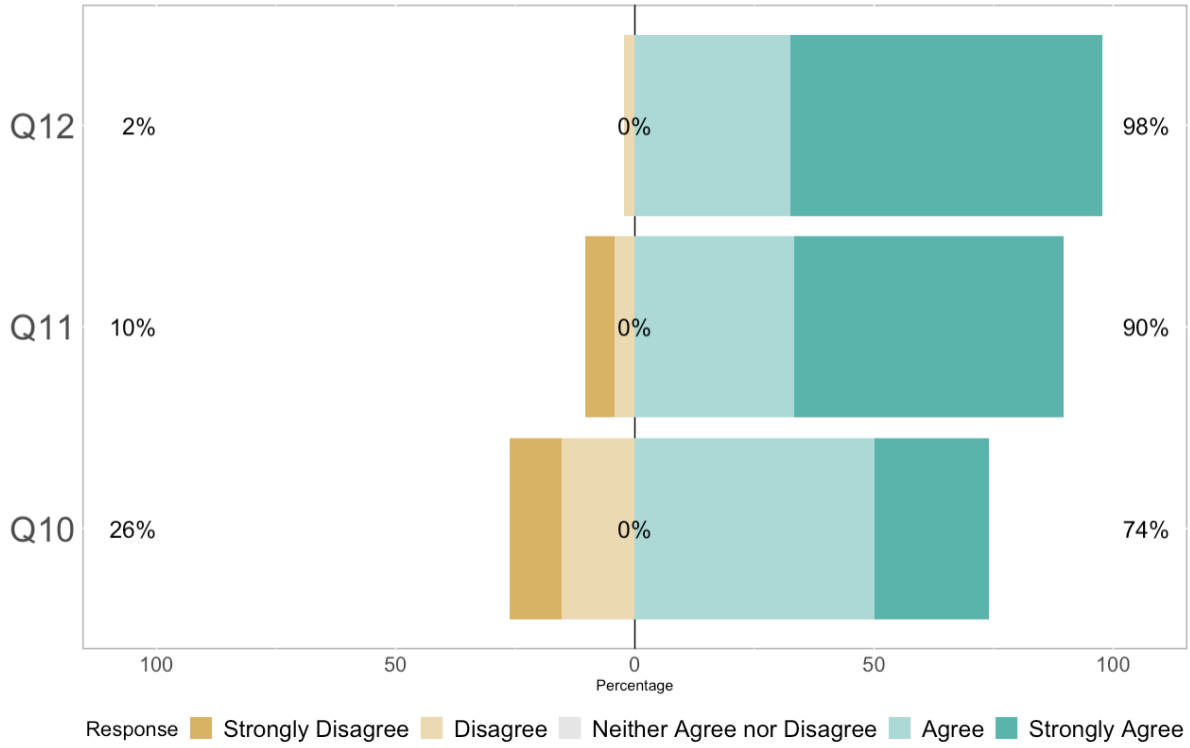

Figura 4.5: Boas práticas de Governança de Dados

o compliance com a LGPD, mas também para estabelecer uma relação de confiança e íntegra entre as duas partes. Em relação ao tópico de logs, tema abordado na questão 12 da Figura 4.5), a maioria dos profissionais (98% deles) concordaram que as organizações devem incorporar técnicas de armazenar registros relacionados as operações executadas de tratamento de dados. Separar os dados relevantes dos comuns é algo que requer atenção e, até mesmo, experiência; e com um inventário de logs e a configuração correta, auxiliará não só no desenvolvimento, operação e segurança na maioria dos ambientes tecnológicos, mas também fornece uma evidência real de que um evento ocorreu nas informações dos titulares.

42% das organizações (questão 13 da Figura 4.6) ainda não elaboraram o seu próprio Relatório de impacto à proteção de dados (RIPD). O RIPD é um documento de fundamental importância para a compliance com a LGPD. É por meio de um RIPD que a empresa será capaz de compreender totalmente todo o ciclo de vida dos dados, além de analisar possíveis fatores que podem afetar a liberdade dos clientes e até mesmo os direitos básicos dos indivíduos que devem ser garantidos, e é por isso que é um conceito tão importante do framework proposto. A maioria das organizações já aplicam em seus dados coletados estratégias de criptografia e anonimização (82%), conforme apresentado na questão 15 da Figura 4.6. Esse resultado é ótimo em quesitos de segurança e proteção da privacidade dos dados, em razão de desassociar as informações que permitem identificar diretamente

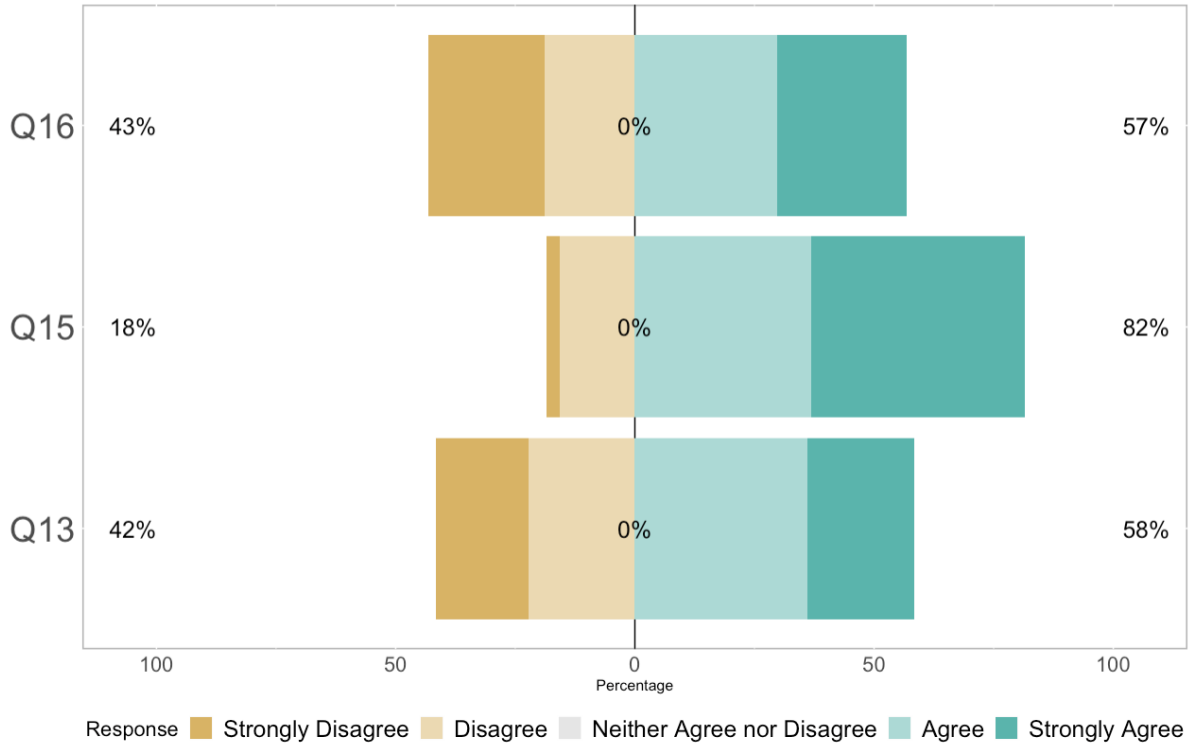

Figura 4.6: Estratégias de Segurança da Informação adotadas

o indivíduo, de forma definitiva e buscando, inclusive, apagar possíveis registros e rastros remanescentes que possam levar à recuperação de tais dados. Essa desassociação refere-se a anonimização, já em relação a criptografia, ela oferece uma segurança mais sólida para os dados que a empresa manipula e armazena, dado que, atualmente, é muito comum que aconteçam ataques cibernéticos e acessos indevidos a backups. 43% das organizações ainda não tem o hábito de realizar avaliações periódicas de vulnerabilidades em seus sistemas, conforme questão 16 da Figura 4.6. Esse achado é um ponto preocupante, já que com a existência de várias tipos ameaças cibernéticas, as empresas não podem negligenciar os assuntos relacionados à Segurança da Informação. Por isso, na seção do framework que trata sobre esse tópico, foi abordado vários tipos de técnicas que as organizações podem aplicar em seus sistemas de TIC, com o objetivo de compreender a importância dessas medidas de segurança que, além reduzir a probabilidade de vazamento de dados, garante também uma confiabilidade maior nos serviços prestados pela organização.

49% das empresas não possuem certificação em gestão de Segurança da Informação, conforme apresentado na Figura 4.7. Esse resultado representa um ponto negativo, uma vez que a ISO é um padrão que normaliza produtos e serviços. Na atualidade, um dos maiores recursos organizações são as informações que as organizações possuem, e quando não há segurança para o seu tratamento, pode colocar em risco toda as operações da organização. Diante disso, cuidar da segurança da informação é o que torna a implementação

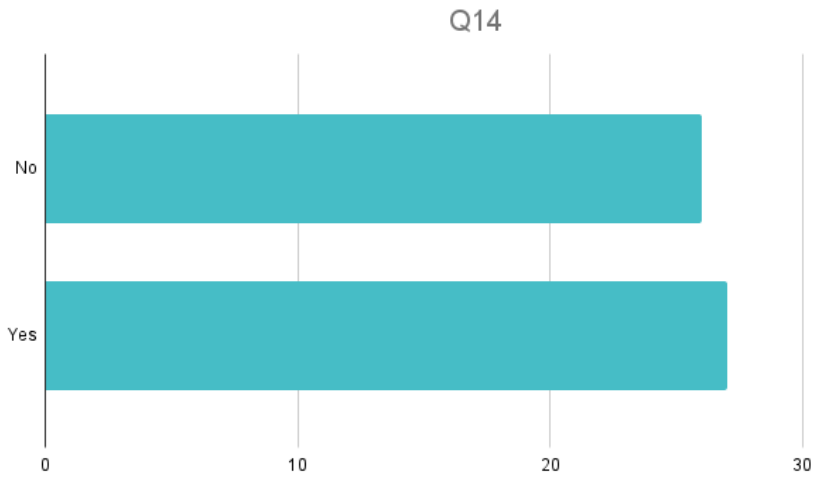

Figura 4.7: Empresas que possuem certificação de gestão de Segurança da Informação(ISO ou ABNT)

da ISO 27001 tão importante para a infraestrutura da organização, e é por isso que é uns dos tópicos principais do framework proposto.

80% das organizações possuem alguma estratégia de continuidade para manter a operações da empresa em funcionamento, caso ocorram desastres, conforme apresentado na questão 17 da Figura 4.8. As organizações com essa consciência, possuem preparação para a recuperação de dados e sistemas dentro de um curto prazo, bem como minimizar os efeitos de paralisação em casos de incidentes. Consequentemente, possuir um plano de continuidade é outro aspecto que reforça ainda mais a implementação da ISO 27001 pelas organizações, pois está dentro do seu escopo.

Uma parte significativa das organizações não incorporaram ainda o Privacy by Design, conforme apresentado na questão 18 da Figura 4.8. Esse resultado talvez seja por desconhecerem os benefícios que essa metodologia proporciona para os serviços oferecidos pela organização. conforme mencionado anteriormente, a LGPD possui semelhanças com a Privacy by Design (Figura 4.3), não sendo coincidência, pois a própria GDPR incorpora dentro do seu escopo essa mesma metodologia de privacidade [17], o que torna um tópico tão relevante para as organizações em conscientizarem e integrarem em sua infraestrutura e, por esse motivo, foi proposto a etapa 3 do Framework (Figura 4.1), que é específico ao Privacy by Design, por se adequar com vários requisitos da LGPD.

60% das organizações possuem um plano de treinamento para os colaboradores (questão 19 da Figura 4.8) e, isso é fundamental, pois assim como a própria empresa deve estar em conformidade com à LGPD, isso deve se estender para os seus colaboradores. Afinal, os agentes de tratamento de dados (controlador, operador e encarregado) devem ter ciência de suas responsabilidades, e quais os procedimentos necessários para atingi-las. E, por

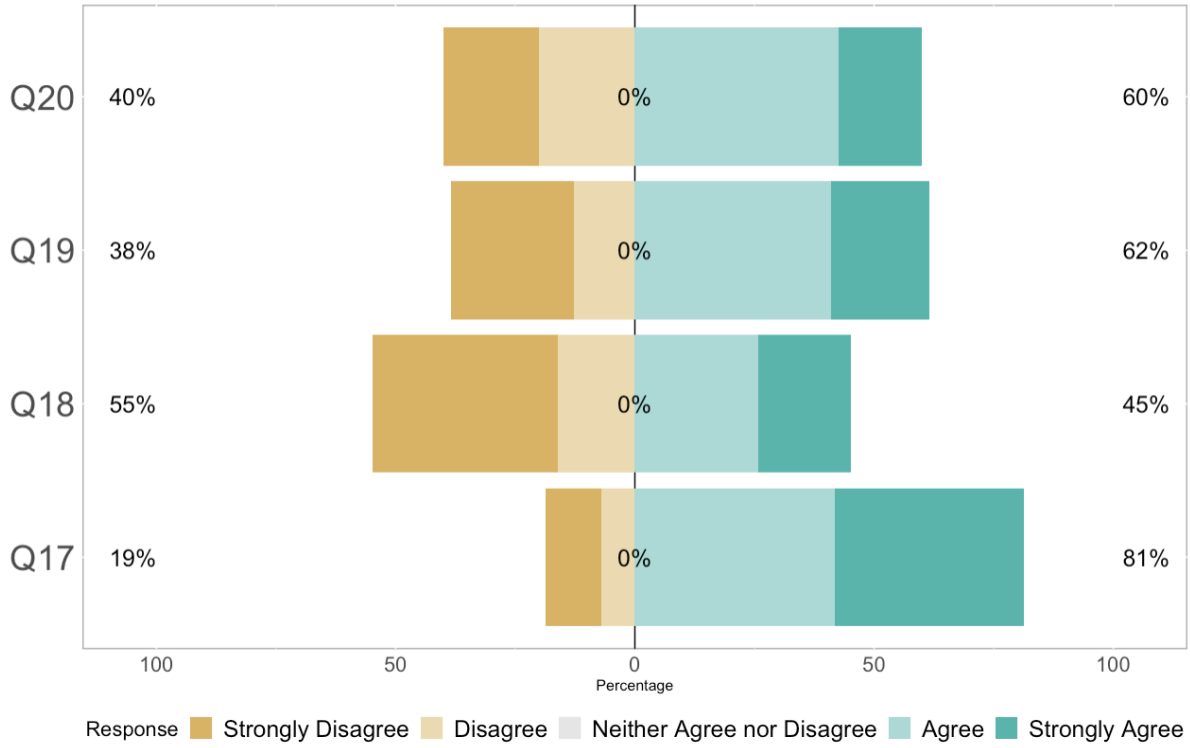

Figura 4.8: Plano de continuidade de negócios, privacidade e treinamentos dos colaboradores

fim, 60% das organizações treinam os seus colaboradores a protegerem-se contra atitudes maliciosas, minimizando os riscos de incidentes, bem como garantindo maior segurança e proteção dos dados pessoais, conforme apresentado na questão 20 da Figura 4.8.

Nossos achados são semelhantes aos achados por Tamburri [17] em relação ao quesito apoiar os profissionais de TIC a remodelarem a infraestrutura de sua organização para adequarem-se aos requisitos da lei de proteção de dados. Além disso, os autores mencionaram que o Privacy by Design é extremamente relevante para as organizações.

Outro trabalho interessante é o Gestão da segurança da informação em empresas do setor de TIC e não TIC [77], pois dedicaram em ampliar os conhecimentos sobre a importância de implementar a ISO/IEC 27001 para dentro das organizações, além de apresentar motivos e obstáculos relacionados à implementação da ISO, utilizando dados de uma pesquisa feita com empresas que já possuem certificação na ISO 27001. Nisso, pode correlacionar com o nosso trabalho no aspecto de evidenciar a relevância dessa ISO para a infraestrutura das empresas, bem como formas de integrá-las para as operações executadas pelas mesmas.

4.3 Limitações e Ameaças para Validação

De acordo com o survey aplicado, as percepções dos profissionais de TIC reforçam o escopo do framework, assim como, a importância de incorporar todos esses fatores de segurança, privacidade e boas práticas para os costumes da organização. Entretanto, é necessário ressaltar que o framework proposto possui algumas limitações. A ISO 27001 é um dos principais tópicos que consistem o modelo proposto, e por isso, há uma correlação fortíssima com ela, na qual se a organização não implementar tal padrão de sistemas de gestão(ISO), por motivos de não visualizar necessidade para isso, deixará de ser aproveitado vários conhecimentos de segurança da informação e boas práticas que a ISO 27001 tem a oferecer, o que pode limitar certas operações da organização.

Outro aspecto que limita é a falta de experiências dos colaboradores, dado que há muitos conceitos específicos e complexos envolvidos, que são necessários o conhecimento para a correta integração dos controles do guia proposto e, conforme pode ser observado no resultado do survey, há uma porcentagem muita alta ainda em relação a falta de treinamento dos colaboradores, dificultando a capacitação e a implementação dos requisitos da LGPD. Por fim, a falta de comunicação pode ser considerada como fator limitante, principalmente com os clientes da organização, já que a transparência é uns dos pontos fundamentais da LGPD, e que se não respeitada e atendida, viola vários direitos dos indivíduos, além de procedimentos sugeridos pelo framework desenvolvido.

Assim como todos os normativos sofrem mudanças frequentes, as leis não são diferentes e, por isso, é um elemento que pode ser uma ameaça para validação, já que o framework proposto foi desenvolvido com base na última versão da LGPD, futuramente, podem ser aplicadas modificações, inserções e/ou exclusões de termos, o que pode prejudicar as instruções e conceitos fornecidos pelo framework proposto. Uma forma de lidar com essa situação um pouco volátil, é investir em treinamentos para os colaboradores da organização com o intuito de prepará-los a garantir a segurança da informação dos titulares dos dados, além de serem capazes de solucionar e adaptar a situações imprevistas do cotidiano.

Capítulo 5

Conclusão

Este trabalho realizou uma pesquisa detalhada sobre a LGPD, assim como todas as etapas que compõem o tratamento de dados em relação ao compliance da LGPD. Além disso, boas práticas de governança de dados e de privacidade foram explanados com intuito de garantir uma proteção e confiança maior no processo de manipular os dados para as organizações. Existem vários conceitos e procedimentos envolvidos para uma correta integração e atendimento aos requisitos da LGPD e, que se negligenciados, as organizações apresentarão dificuldades para legitimar seus serviços prestados, bem como ganhar credibilidade no mercado.

Os resultados desse trabalho, nos permite concluir que, embora uma grande parcela das empresas já iniciaram ações de adequação à LGPD, uma porção significativa não aderiram ainda metodologias que garantam a proteção das informações, como: integração da ISO 27001, elaboração do RIPD e de planos de continuidade de negócios, assim como programas de treinamentos de seus colaboradores; sendo assim, o framework proposto auxilia essas mesmas organizações a compreenderem a relevância desses procedimentos para sua infraestrutura, os quais são primordiais para aumentar a proteção dos dados, garantir a privacidade das informações de seus clientes e reduzir riscos oriundos a vazamentos e invasão de cibercriminosos.

Este trabalho cumpriu todos os objetivos elencados no início, uma vez que, o framework desenvolvido ofereceu instruções que guiam as organizações nos procedimentos mais importantes para estar em conformidade com os requisitos da LGPD, além de fornecer boas práticas de gestão de cibersegurança e Segurança da Informação, de forma clara e concisa.

Apesar dos resultados terem mostrado que ações de adequação são essenciais no processo de atender a LGPD, é necessário realizar outros estudos envolvendo mais participantes e organizações com o objetivo de obter resultados com um nível de significância maior em relação ao nível de conformidade das organizações com a LGPD. Outro traba-

lho futuro é o desenvolvimento de uma ferramenta automatizada baseada no framework proposto para apoiar as organizações na adequação aos requisitos da LGPD e na busca contínua da melhoria nas ações de tratamento de dados executadas por elas.

Referências

[1] Mosley, Mark e Michael Brackett: *The DAMA Guide to The Data Management Body of Knowledge*, volume first edition. Technics Publications LLC, 2009, ISBN 978-0-9771400-8-4. x, 7, 8

[2] Donda, Daniel: *Guia prático de implementação da LGPD*, volume 1. São Paulo: Editora Labrador, 2020, ISBN 978-65-5625-046-5. `https://plataforma.bvirtual.com.br/Leitor/Publicacao/185745/pdf/0`, Acesso em: 3 de junho 2021. x, 20, 21, 44

[3] Hintzbergen, J., K. Hintzbergen, A. Smulders e H. Baars: *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*, volume 1. Rio de Janeiro: Brasport, 2018, ISBN 9788574528670. x, 32, 39

[4] BRASIL: *Guia de boas práticas – lei geral de proteção de dados (lgpd).* Comitê Central de Governançã de Dados. Secretaria de Governo Digital, 1–65, 2020. `https://https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd`. 1

[5] Macedo, Pereira Neto: *Brazilian general data protection law (lgpd).* National Congress, accessed in May 18, 2020, 1:1–5, 2018. `https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf`. 1

[6] Brasil: *Lei nº 13.709, de 14 de agosto de 2018.* Diário Oficial da República Federativa do Brasil, 2021. `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm`, Acesso em:1 de Fevereiro, 2021. 1, 2, 9, 10, 11, 12, 14, 15, 23, 24, 25, 26, 29, 33, 34, 35, 36, 37, 38, 44, 45

[7] FIESP e CIESP: *Cartilha de Protecão de Dados Pessoais.* Acesso: 2 de fevereiro de 2021, 2020. 1

[8] Zhanna Malekos, Eugenia Lostri e James A. Lewis: *The hidden costs of cybercrime.* Acesso em:5 de Fevereiro, 2021, página 38, 2020. `https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf`, Acesso em:5 de Fevereiro, 2021. 2

[9] Freitas, Cleber Cristiano Prodanov Ernani Cesar de: *metodologia do trabalho científico:Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico*, volume 2. Novo Hamburgo: Feevale, 2013, ISBN 978-85-7717-158-3.

https://aedmoodle.ufpa.br/pluginfile.php/291348/mod_resource/content/3/2.1-E-book-Metodologia-do-Trabalho-Cientifico-2.pdf. 4

[10] Laura Rocha, Edson Aguilera Fernandes, Rafael Augusto e Marcos Ribeiro: *Lei Geral de Proteção de Dados - Guia de Implantação.* São Paulo: Editora Edgard Blücher Ltda, 2020. https://integrada.minhabiblioteca.com.br/#/books/9786555060164/. 5, 9, 10, 11, 23, 28, 29, 31, 32, 33, 34, 35, 36, 38, 45

[11] Renato Leite: *Existe um direito à explicação na lei geral de proteção de dados do brasil.* Instituto Igarapé, 2018, ISSN 2359-098X. https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. 6

[12] europe: *General data protection regulation.* eur, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, Acesso: 2 de fevereiro de 2021. 6, 7, 8

[13] Paulo Marcos Rodrigues Brancher e Ana Claudia Beppu: *Proteção de dados pessoais no Brasil: Uma nova visão a partir da lei Nº 13.709/2018.* Belo Horizonte: Fórum, 2019, ISBN 978-85-450-0647-3. 6

[14] Juliana Gonçalves e Sabrina Lapa: *Análise dos impactos da lei geral de proteção de dados pessoais sobre a governanÇa e seguranÇa de dados.* UNIRIO, 2020. https://bsi.uniriotec.br/wp-content/uploads/sites/31/2020/05/202002JulianaSantosSabrinaLapa.pdf, Acesso em:4 de Fevereiro, 2021. 6, 7

[15] Rogério Christofoletti: *Riscos Éticos em tempos de delações, vazamentos e clamor pela transparência.* Associação Brasileira de Pesquisadores em Jornalismo, 12(2), 2016. https://core.ac.uk/download/pdf/192901742.pdf. 6

[16] Truong, Nguyen, Kai Sun, Siyao Wang, Florian Guitton e YiKe Guo: *Privacy preservation in federated learning: An insightful survey from the gdpr perspective.* Computers & Security, 110:102402, 2021, ISSN 0167-4048. https://www.sciencedirect.com/science/article/pii/S0167404821002261. 7

[17] Tamburri, Damian A.: *Design principles for the general data protection regulation (gdpr): A formal concept analysis and its evaluation.* Information Systems, 91:101469, 2020, ISSN 0306-4379. https://www.sciencedirect.com/science/article/pii/S0306437919305216. 8, 26, 49, 50

[18] Adalberto Simão, Augusto Tavares, C. Prado, E. Eduardo e G. Bezerra: *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com Alteração da Lei n. 13.853/2019.* Almedina Brasil, 2020, ISBN 9788584935796. 9, 10, 12, 13, 14, 22, 36, 37

[19] Laura Schertel e Danilo Doneda: *Tratado de proteção de dados pessoais.* Editora Forense Ltda, 2020, ISBN 978-85-309-9219-4. 9, 15, 16, 21, 23, 25

[20] Barbara Santini, Clarice Cardim, Helio Andre e Joana Maria: *O que estão fazendo com meus dados:Importância da LGPD*. Comissão de direito de tecnologia da informação - OAB(Pernambuco), 2019, ISBN 978-85-66599-12-1. https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf#page=78, Acesso em 11 de Abril de 2021. 12, 15

[21] Mendes e L. S: *Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental*, volume 1. Editora Saraiva, 2014. https://integrada.minhabiblioteca.com.br/#/books/9788502218987/, Acesso em: 26 de abril de 2021. 15, 21

[22] Ricardo e B. B.: *Proteção de Dados Pessoais - A Função e os Limites do Consentimento*, volume 2. Rio de Janeiro: Grupo GEN, 2019, ISBN 978-85-309-8876-0. https://integrada.minhabiblioteca.com.br/#/books/9788530988777/, Acesso em: 27 de abril 2021. 16

[23] Cavoukian, A., S. Taylor e M.E. Abrams: *Privacy by design: essential for organizational accountability and strong business practices*. Identity Inf. Soc, página 405–413, 2010. https://doi.org/10.1007/s12394-010-0053-z, Acesso em: 27 de abril 2021. 16, 29, 43

[24] Eric Araújo da Costa Júnior: *Análise de conformidade de processos de negócios em relação a lgpd*. Universidade Federal de Pernambuco (UFPE), 2020. https://www.cin.ufpe.br/~tg/2020-3/TG_SI/tg_eacj.pdf. 16

[25] Machado, Diego e Danilo Doneda: *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados*, páginas 99–125. Thomson Reuters Brasil, janeiro 2019, ISBN 978-85-203-6888-6. 16

[26] Luiz Paulo Carvalho, Jonice Oliveira e Claudia Cappelli: *Pesquisas em análise de redes sociais e lgpd, análises e recomendações*. Anais do Brazilian Workshop on Social Network Analysis and Mining (BraSNAM), 2020. https://sol.sbc.org.br/index.php/brasnam/article/view/11164. 17

[27] Ferrão, Sâmmara Éllen Renner, Artur Potiguara Carvalho, Edna Dias Canedo, Alana Paula Barbosa Mota, Pedro Henrique Teixeira Costa e Anderson Jefferson Cerqueira: *Diagnostic of data processing by brazilian organizations—a low compliance issue*. Information, 12(4), 2021. https://www.mdpi.com/2078-2489/12/4/168. 17

[28] Canedo, Edna Dias, Angélica Toffano Seidel Calazans, Eloisa Toffano Seidel Masson, Pedro Henrique Teixeira Costa e Fernanda Lima: *Perceptions of ICT practitioners regarding software privacy*. Entropy, 22(4):429, 2020. Acesso 18 de abril de 2021. 17

[29] Luiz Paulo, Jonice Oliveira, C. Cappelli e V. Majer: *Desafios de transparência pela lei geral de proteção de dados pessoais*. Anais do Workshop de Transparência em Sistemas (WTranS), 2019. https://sol.sbc.org.br/index.php/wtrans/article/view/6438. 18

[30] Graef, Inge e Jens Prüfer: *Governance of data sharing: A law & economics proposal*. Research Policy, 50(9):104330, 2021, ISSN 0048-7333. https://www.sciencedirect.com/science/article/pii/S004873332100130X. 20, 38

[31] M.F: *Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos*, volume 1. Rio de Janeiro: Grupo GEN, 2020, ISBN 9788597026009. https://integrada.minhabiblioteca.com.br/#/books/9788597026009/, Acesso em: 09 Jun 2021. 20, 37

[32] Mendes, L. S: *Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental*, volume 1. São Paulo: Editora Saraiva, 2014, ISBN 978-85-02-21898-7. https://integrada.minhabiblioteca.com.br/#/books/9788502218987/, Acesso em: 13 Jun 2021. 21, 22

[33] Anja Czymmeck, Antônio Jorge, Estevão de Rezende e F. Anastasia: *Proteção de Dados: Privacidade versus avanço tecnológico*, volume 3. Rio de Janeiro:Fundação Konrad Adenauer, 2019, ISBN 978-85-7504-230-4. 21

[34] Arndt, Aaron D., John B. Ford, Barry J. Babin e Vinh Luong: *Collecting samples from online services: How to use screeners to improve data quality*. International Journal of Research in Marketing, 2021, ISSN 0167-8116. https://www.sciencedirect.com/science/article/pii/S0167811621000203. 21

[35] Ducato, Rossana: *Data protection, scientific research, and the role of information*. Computer Law & Security Review, 37:105412, 2020, ISSN 0267-3649. https://www.sciencedirect.com/science/article/pii/S0267364920300170. 22, 25

[36] *Netflix: sistema de recomendações*. https://help.netflix.com/pt/node/100639. Acesso em: 17 Jun 2021. 22

[37] Li, Yuanxin e Darina Saxunová: *A perspective on categorizing personal and sensitive data and the analysis of practical protection regulations*. Procedia Computer Science, 170:1110–1115, 2020, ISSN 1877-0509. https://www.sciencedirect.com/science/article/pii/S187705092030497X, The 11th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops. 23

[38] Fosch-Villaronga, Eduard e Tobias Mahler: *Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots*. Computer Law & Security Review, 41:105528, 2021, ISSN 0267-3649. https://www.sciencedirect.com/science/article/pii/S0267364921000017. 23, 37

[39] Strycharz, Joanna, Edith Smit, Natali Helberger e Guda van Noort: *No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies*. Computers in Human Behavior, 120:106750, 2021, ISSN 0747-5632. https://www.sciencedirect.com/science/article/pii/S0747563221000728. 23

[40] AlMeghari, Mayada, Sanaa Taha, Hesham Elmahdy e Xuemin(Sherman) Shen: *A proposed authentication and group-key distribution model for data warehouse signature, dws framework*. Egyptian Informatics Journal, 2020, ISSN 1110-8665. https://www.sciencedirect.com/science/article/pii/S1110866520301547. 24

[41] Santos-Pereira, Judith, Le Gruenwald e Jorge Bernardino: *Top data mining tools for the healthcare industry*. Journal of King Saud University - Computer and Information Sciences, 2021, ISSN 1319-1578. https://www.sciencedirect.com/science/article/pii/S131915782100135X. 24

[42] Cuzzocrea, Alfredo e Elisa Bertino: *Privacy preserving olap over distributed xml data: A theoretically-sound secure-multiparty-computation approach*. Journal of Computer and System Sciences, 77(6):965–987, 2011, ISSN 0022-0000. https://www.sciencedirect.com/science/article/pii/S002200001100033X. 24

[43] A., Calder.: *Nine Steps to Success: an ISO 27001 Implementation Overview*, volume 3. IT Governance, 2006, ISBN 978-1905356126. 24

[44] Syreyshchikova, Nelli V., Danil Yu. Pimenov, Tadeusz Mikolajczyk e Liviu Moldovan: *Information safety process development according to iso 27001 for an industrial enterprise*. Procedia Manufacturing, 32, 2019, ISSN 2179-8966. https://www.sciencedirect.com/science/article/pii/S2351978919302501, Acesso: 2 de Agosto de 2021. 24, 39, 44

[45] Lima, Ana Paula Moraes Canto de, Marcelo Crespo e Patricia Peck Pinheiro: *LGPD Aplicada*, volume 1. GEN - Grupo Editorial Nacional, 2020. https://integrada.minhabiblioteca.com.br//#/books/9788597026931/%7D. 25, 32, 34

[46] Fornasier, Mateus de Oliveira e Norberto Milton Paiva Knebel: *O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na lei geral de proteção de dados*. Revista Direito e Práxis [online], 2021, ISSN 2179-8966. https://doi.org/10.1590/2179-8966/2020/46944, Acesso: 2 de Agosto de 2021. 25, 35, 36

[47] Regulation, General Data Protection: *Eu data protection rules*. European Commission, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, Acesso: 9 de fevereiro de 2021. 26

[48] B, Matheus: *Lei geral de proteção de dados: uma análise sobre os direitos dos titulares e os deveres das organizações perante a lei*. Campina grande: UFCG, 2021. http://dspace.sti.ufcg.edu.br:8080/xmlui/handle/riufcg/19884, Acesso: 24 de julho de 2021. 27

[49] O'Connor, Yvonne, Wendy Rowan, Laura Lynch e Ciara Heavin: *Privacy by design: Informed consent and internet of things for smart health*. Procedia Computer Science, 113:653–658, 2017, ISSN 1877-0509. https://www.sciencedirect.com/science/article/pii/S1877050917317398, The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2017) / Affiliated Workshops. 27, 42

[50] ABNT: *Abnt nbr iso/iec 27001 – tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2019. 29

[51] Matos, P. C. de A.: *A cibersegurança: Políticas públicas para uma cultura de cibersegurança nas empresas*. [Dissertação de mestrado, Iscte - Instituto Universitário de Lisboa], 2018. `https://repositorio.iscte-iul.pt/handle/10071/17630`, Acesso: 6 de Agosto de 2021. 31

[52] Fontes, Edison: *Políticas e normas para segurança da informação*, volume 1. Rio de Janeiro: Brasport, 2012. 31

[53] Peck, P. P.: *Segurança Digital - Proteção de Dados nas Empresas*, volume 1. São Paulo: Grupo GEN, 2020. `https://integrada.minhabiblioteca.com.br/#/books/9788597026405/`, Acesso em: 17 Jul 2021. 31, 35, 40

[54] Santos, B.J. D., Z. Aline, M.I. S. e V.A. D Souza: *Fundamentos de segurança da informação*, volume 1. São Paulo: Grupo A, 2018, ISBN 9788595025875. `https://integrada.minhabiblioteca.com.br/#/books/9788595025875/`, Acesso em: 07 de Agosto de 2021. 31, 36, 38, 39

[55] Roger, P.; Bruce, M.: *Engenharia de Software*, volume 8. Porto Alegre: Grupo A, 2016. `https://integrada.minhabiblioteca.com.br/#/books/9788580555349/`, Acesso em: 03 de Agosto de 2021. 33

[56] Cortellessa, V., A. Di Marco, P. Inverardi, F. Mancinelli e P. Pelliccione: *A framework for the integration of functional and non-functional analysis of software architectures*. Electronic Notes in Theoretical Computer Science, 116:31–44, 2005, ISSN 1571-0661. `https://www.sciencedirect.com/science/article/pii/S1571066104052752`, Proceedings of the International Workshop on Test and Analysis of Component Based Systems (TACoS 2004). 33

[57] Junior, E: *Introdução a Sistemas de Supervisão, Controle e Aquisição de Dados*, volume 1. Rio de Janeiro: Editora Alta, 2019, ISBN 9788550807744. `https://integrada.minhabiblioteca.com.br/#/books/9788550807744/`, Acesso em: 07 de Agosto de 2021. 34

[58] E., C. D.: *Redes Computadores e Internet*, volume 6. Porto Alegre: Grupo A, 2016. `https://integrada.minhabiblioteca.com.br/#/books/9788582603734/`, Acesso em: 05 de Agosto de 2021. 34

[59] HOFFMANN-RIEM, Wolfgang.: *Teoria geral do direito digital*, volume 1. Rio de Janeiro: Grupo GEN, 2020, ISBN 978-85-309-9225-5. `https://integrada.minhabiblioteca.com.br/#/books/9788530992262/`, Acesso em: 07 de Agosto de 2021. 36

[60] Fernandes, A.A. e V.F. Abreu: *Implantando governança de TI da estratégia à gestão dos processos e serviços*, volume 3. Rio de Janeiro: BraSport, 2012. 39

[61] OLIVEIRA, Frank Ned Santa Cruz de.: *Gestão de riscos no direito fundamental à privacidade de dados pessoais no processo judicial eletrônico / diário de justiça eletrônico*. Dissertação (Mestrado Profissional em Computação Aplicada)—Universidade de Brasília, 2020. https://repositorio.unb.br/handle/10482/39152, Acesso: 17 de Agosto de 2021. 39

[62] Katz, J. e Y. Lindell: *Introduction to Modern Cryptography*, volume 1. CRC Press, 2008, ISBN 978-1-58488-551-1. 40

[63] Basta, A., N. Basta e M. Brown: *Segurança de Computadores e teste de invasão*, volume 2. São Paulo: Cengage Learning Brasil, 2014, ISBN 9788522121366. https://integrada.minhabiblioteca.com.br/#/books/9788522121366/, Acesso em: 14 de Agosto de 2021. 40

[64] Melo, Laerte Peotta de.: *Proposta de metodologia de gestão de risco em ambientes corporativos na área de ti*. Dissertação (Mestrado em Engenharia Elétrica)-Universidade de Brasília, 2008. https://repositorio.unb.br/handle/10482/1628, Acesso: 16 de Agosto de 2021. 40

[65] Nicula, Stefan e Răzvan Daniel Zota: *Exploiting stack-based buffer overflow using modern day techniques*. Procedia Computer Science, 160:9–14, 2019, ISSN 1877-0509. https://www.sciencedirect.com/science/article/pii/S1877050919316527, The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2019) / The 9th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2019) / Affiliated Workshops. 40

[66] CRUZ, Carlos Magno Bispo Rosal da.: *Auditoria de segurança da informação em sistemas e aplicações*. Dissertação (Mestrado Profissional em Computação Aplicada)—Universidade de Brasília, 2017. https://repositorio.unb.br/handle/10482/25258, Acesso: 16 de Agosto de 2021. 41

[67] Stuttard, D. e M. Pinto: *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, volume 2. Wiley Publishing, 2011. 41

[68] D, Kosutic.: *secure & simple a small-business guide to implementing iso 27001 on your own*, volume 1. Advisera Expert Solutions, 2017. 41, 44

[69] Margherita, Alessandro e Marikka Heikkilä: *Business continuity in the covid-19 emergency: A framework of actions undertaken by world-leading companies*. Business Horizons, 64(5):683–695, 2021, ISSN 0007-6813. https://www.sciencedirect.com/science/article/pii/S0007681321000227. 41, 42

[70] Marinho, Fernando: *Guia de Plano de Continuidade de Negócios (PCN)*. Rio de Janeiro: Grupo GEN, 1st edição, 2018, ISBN 9788595152540. https://integrada.minhabiblioteca.com.br/#/books/9788595152540/. 42

[71] Prazeres, Antero e Eurico Lopes: *Disaster recovery – a project planning case study in portugal*. Procedia Technology, 9:795–805, 2013, ISSN 2212-0173. https://www.sciencedirect.com/science/article/pii/S2212017313002429,

CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013 - International Conference on Project MANagement/ HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies. 42

[72] Polverini, D., F. Ardente, I. Sanchez, F. Mathieux, P. Tecchio e L. Beslay: *Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process.* Computers & Security, 76:295–310, 2018, ISSN 0167-4048. https://www.sciencedirect.com/science/article/pii/S0167404817302614. 42

[73] Pilton, Callum, Shamal Faily e Jane Henriksen-Bulmer: *Evaluating privacy - determining user privacy expectations on the web.* Computers & Security, 105:102241, 2021, ISSN 0167-4048. https://www.sciencedirect.com/science/article/pii/S0167404821000651. 43, 44

[74] Stallings, William: *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.* Addison-Wesley Professional, 1st edição, 2019, ISBN 0135302153. 44

[75] Washo, Amy Hetro: *An interdisciplinary view of social engineering: A call to action for research.* Computers in Human Behavior Reports, 4:100126, 2021, ISSN 2451-9588. https://www.sciencedirect.com/science/article/pii/S2451958821000749. 45

[76] Grassegger, Tanja e Dietmar Nedbal: *The role of employees' information security awareness on the intention to resist social engineering.* Procedia Computer Science, 181:59–66, 2021, ISSN 1877-0509. https://www.sciencedirect.com/science/article/pii/S1877050921001381, CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020. 45

[77] Mirtsch, Mona, Knut Blind, Claudia Koch e Gabriele Dudek: *Information security management in ict and non-ict sector companies: A preventive innovation perspective.* Computers & Security, 109:102383, 2021, ISSN 0167-4048. https://www.sciencedirect.com/science/article/pii/S0167404821002078. 50

Anexo I

Questionário

Tabela I.1: Questões do Survey

ID	Enunciado
Q1	Qual a natureza de atuação da sua organização?
Q2	Selecione o seu cargo na organização
Q3	Sua empresa já iniciou, de maneira formal, ações de adequação a LGPD?
Q4	Você considera essencial sua empresa instaurar um sistema de gestão de cibersegurança e segurança da informação para estruturar todo o decorrer do período de processamento dos dados?
Q5	Considerando que, para a LGPD, o conceito de "tratamento de dados" é toda operação realizada com dados pessoais, como as que se referem à coleta, classificação, utilização, acesso, reprodução, processamento, armazenamento, eliminação, controle da informação, entre outros, a sua empresa realiza tratamento de dados?
Q6	Considerando que, para a LGPD, o conceito de "dados pessoais" é o de qualquer informação relacionada à pessoa natural identificada ou identificável (nome, endereço, e-mail, telefone, números de documentos), a sua empresa trata dados pessoais?

Continua na próxima página

Tabela I.1 – Questões do Survey

ID	Enunciado
Q7	Considerando que, para a LGPD, o conceito de "dados pessoais sensíveis" é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, a sua empresa trata de dados pessoais sensíveis?
Q8	Ao executar a coleta de dados,sua empresa realiza procedimentos de mapeamento dos dados ?
Q9	Os dados pessoais tratados pela sua empresa, foram coletados no Brasil ou passaram por uma das fases do processo de tratamento de dados em território nacional?
Q10	A empresa mantém toda a documentação, devidamente atualizada, de seu ambiente tecnológico (infraestrutura, hardwares e softwares)?
Q11	Mecanismos que facilitem a comunicação entre os agentes de tratamento com os titulares dos dados, permitindo um acesso e transparência mais simplificado para os clientes, são importantes para empresa?
Q12	Você acha necessário a organização ter o costume de realizar registros de Logs dos tratamentos executados nos dados pessoais?
Q13	Sua empresa elabora o Relatório de impacto à proteção de dados (RIPD) com intuito de avaliar possíveis riscos no sistema?
Q14	A sua empresa possui algum certificado de gestão de segurança da informação, como ISO ou ABNT?
Q15	Sua empresa tem o hábito de aplicar nos dados coletados, técnicas de segurança da informação como: anonimização, criptografia?
Q16	A empresa conduz periodicamente avaliações de vulnerabilidade e testes de penetração(pentest) em seus sistemas?
Q17	Há um Plano de Continuidade do Negócio e de Recuperação em caso de Desastres em sua organização?

Continua na próxima página

Tabela I.1 – Questões do Survey

ID	Enunciado
Q18	É incorporado na organização metodologias de Privacidade por Design(Privacy by Design) em seus serviços?
Q19	Existe um Plano de Treinamento dos colaboradores para a correta adequação da LGPD?
Q20	Ocorre treinamentos dos funcionários para atitudes seguras associadas a Engenharia Social?