Revisão Sistemática de Soluções Tecnológicas e Organizacionais para Conformidade com a LGPD

Gabriel da Silva Belarmino

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2024

Gabriel da Silva Belarmino

Revisão Sistemática de Soluções Tecnológicas e Organizacionais para Conformidade com a LGPD

Dissertação apresentada ao Programa de Pós-Graduação em Informática
do Centro de Informática, da Universidade Federal da Paraíba

Orientadores:

Prof. Dr. Gustavo Henrique Matos Bezerra Motta

Prof. Dra. Danielle Rousy Dias Ricarte

Agosto de 2024

Catalogação na publicação
Seção de Catalogação e Classificação

B426r Belarmino, Gabriel da Silva.
Revisão sistemática de soluções tecnológicas e organizacionais para conformidade com a LGPD / Gabriel da Silva Belarmino. - João Pessoa, 2024.
103 f. : il.

Orientação: Gustavo Henrique Matos Bezerra Motta, Danielle Rousy Dias Ricarte.
Dissertação (Mestrado) - UFPB/CI.

1. Informática. 2. LGPD. 3. Governança de dados. 4. Privacidade de dados. 5. Revisão sistemática. 6. Segurança da informação. I. Motta, Gustavo Henrique Matos Bezerra. II. Ricarte, Danielle Rousy Dias. III. Título.

UFPB/BC CDU 004(043)

Elaborado por Larissa Silva Oliveira de Mesquita - CRB-15/746

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Gabriel da Silva Belarmino, candidato ao título de Mestre em Informática na área de Sistemas de Computação, realizada em 01 de agosto de 2024.

Ao primeiro dia do mês de agosto do ano de dois mil e vinte e quatro, às quatorze horas, no Centro de Informática da Universidade Federal da Paraíba, reuniram-se os membros da Banca Examinadora constituída para julgar o Trabalho Final do discente Gabriel da Silva Belarmino, vinculado a esta Universidade sob a matrícula nº 20221003530, candidato ao grau de Mestre em Informática, na área de *"Sistemas de Computação"*, na linha de pesquisa *"Computação Distribuída"*, do Programa de Pós-Graduação em Informática. A comissão examinadora foi composta pelos professores: Gustavo Henrique Matos Bezerra Motta, Orientador e Presidente da banca; Gledson Elias da Silveira, Examinador Interno; Juliana de Albuquerque Gonçalves Saraiva, Examinadora Externa ao Programa; Carla Taciana Lima Lourenço Silva Schuenemann, Examinadora Externa à Instituição. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou a finalidade da reunião e passou a palavra ao candidato para que ele fizesse a exposição oral do trabalho de dissertação intitulado "**Revisão Sistemática de Soluções Tecnológicas e Organizacionais para Conformidade com a LGPD**". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Gilberto Farias de Sousa Filho, coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da Banca Examinadora. João Pessoa, 01 de agosto de 2024.

gov.br Documento assinado digitalmente
GILBERTO FARIAS DE SOUSA FILHO
Data: 07/08/2024 08:11:18-0300
Verifique em https://validar.iti.gov.br

Gilberto Farias de Sousa Filho
Coordenador do Programa de Pós-Graduação em Informática

gov.br Documento assinado digitalmente
GUSTAVO HENRIQUE MATOS BEZERRA MOTTA
Data: 01/08/2024 16:05:25-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Gustavo Henrique M. Bezerra Motta
Orientador (PPGI-UFPB)

gov.br Documento assinado digitalmente
GLEDSON ELIAS DA SILVEIRA
Data: 05/08/2024 17:09:41-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Gledson Elias da Silveira
Examinador Interno (PPGI-UFPB)

gov.br Documento assinado digitalmente
JULIANA DE ALBUQUERQUE GONCALVES SARAI
Data: 02/08/2024 09:03:51-0300
Verifique em https://validar.iti.gov.br

Prof. Drª. Juliana de Albuquerque G. Saraiva
Examinadora Externa ao Programa (UFPB)

gov.br Documento assinado digitalmente
CARLA TACIANA LIMA LOURENCO SILVA SCHUE
Data: 03/08/2024 15:24:58-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Carla Taciana Lima Lourenço Silva Schuenemann
Examinadora Externa à Instituição (UFPE)

RESUMO

A Lei Geral de Proteção de Dados Pessoais (Lei no 13.709, de 14 de agosto de 2018) dispõe sobre o tratamento de dados pessoais e descreve novos desafios e demandas sociotécnicas para modernizar o sistema jurídico, assim como, promover avanços na Governança de Dados e na Segurança da Informação, a fim de ampliar os direitos fundamentais dos cidadãos e conduzir novos princípios e diretrizes para o desenvolvimento de uma cultura organizacional capaz de garantir a proteção de dados. Para atender à LGPD, são necessárias diversas mudanças, não apenas em regulamentos e políticas empresariais com foco jurídico, mas também em questões práticas e técnicas relacionadas aos processos de trabalho, infraestrutura tecnológica e gestão de dados, que são o foco deste trabalho. Este estudo realiza uma revisão sistemática da literatura sobre a proteção de dados pessoais, com o objetivo de identificar soluções de adequação. Apresenta artefatos tecnológicos relacionados à implementação de sistemas e à gestão organizacional, preparando os processos internos para cumprir os requisitos de segurança, reduzir os riscos à privacidade e atender às demandas da LGPD. A revisão permitiu explorar 41 estudos qualificados, descrevendo soluções relevantes para a pesquisa. Com base nesses resultados, foram propostas 14 recomendações para auxiliar no processo de adequação de uma organização à LGPD. Além disso, sugerimos recomendações sobre documentação de proteção de dados e elencamos requisitos prioritários para a conformidade legislativa.

Palavras-chave: LGPD, Privacidade de Dados, Revisão Sistemática, Governança de Dados, Segurança da Informação.

ABSTRACT

The brazilian General Data Protection Law (Law No. 13,709, of August 14, 2018) governs the processing of personal data and describes new sociotechnical challenges and demands to modernize the legal system, as well as to promote advances in Data Governance and Information Security. Its objective is to expand citizens' fundamental rights and establish new principles and guidelines for developing an organizational culture capable of ensuring data protection. Compliance with LGPD requires several changes, not only in legal-focused regulations and business policies, but also in practical and technical issues related to work processes, technological infrastructure, and data management, which are the focus of this study. This paper conducts a systematic literature review on personal data protection to identify compliance solutions. It presents technological artifacts related to system implementation and organizational management, preparing internal processes to meet security requirements, reduce privacy risks, and comply with LGPD demands. The review explored 41 qualified studies, describing relevant solutions for research. Based on these results, 14 recommendations were proposed to assist organizations in their LGPD compliance process. Additionally, recommendations were made regarding data protection documentation and prioritized requirements for legislative compliance.

Keywords: LGPD, Data Privacy, Systematic Review, Information Security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABAC - Controle de Acesso Baseado em Atributos

AIPD – Avaliação de Impacto sobre a Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados

BPMN - Business Process Model and Notation

BMC – Business Model Canvas

CCPA – California Consumer Privacy Act

CMMI – Capability Maturity Model Integration

DMM - Data Management Maturity

DPO – Data Protection Officer

IA – Inteligência Artificial

IDESP - Instituto Daryus de Ensino Superior Paulista

LGPD – Lei Geral de Proteção de Dados Pessoais

PDP – Privacidade por Design e Padrão

PSI – Política de Segurança da Informação

RGPD – Regulamento Geral sobre a Proteção de Dados

RIPD – Relatório de impacto à Proteção De Dados Pessoais

RS – Revisão Sistemática

RSN - Revisão Sistemática Narrativa

SCA - Sistemas de Controle de Acesso

SGSI – Sistema de Gestão de Segurança da Informação

SI – Segurança da informação

TI – Tecnologia da Informação

TICs – Tecnologias da Informação e Comunicação

UE – União Europeia

XACML - eXtensible Access Control Markup Language

Sumário

1 INTRODUÇÃO

A forte concorrência do mercado mundial, o crescimento do mundo digital, e o rápido desenvolvimento tecnológico promovem um acréscimo constante no fluxo de informação. A transmissão de dados e informações pela internet ocorre de maneira rápida e simples e os avanços tecnológicos tornaram possível o armazenamento e processamentos diversificados sobre qualquer informação que seja fonte de interesse de uma instituição. Diante disso, constata-se a necessidade da criação de medidas para proteger e assegurar a integridade das pessoas e de suas informações.

Com a ascensão das redes sociais, do comércio eletrônico, aplicativos bancários, dentre outras ferramentas utilizadas atualmente, o volume de processamento e dados de clientes e pessoas naturais é muito relevante para empresas, órgãos intergovernamentais e governos, sendo um dos principais ativos desses, visto que, com a base de funcionamento da economia atual as organizações que possuem maior quantidade de dados detêm um poder econômico mais elevado. Esta relevância implica em uma consequência para a sociedade, pois a deixa mais exposta à falhas de segurança, ataques cibernéticos, roubo e venda de informações pessoais e publicidades indevidas (LOPES; AMARAL, 2022).

O primeiro grande marco para realização de mudanças globais, quanto ao cuidado e a proteção das informações dos cidadãos, foi a criação do Regulamento Geral sobre a Proteção de Dados (RGPD) (GDPR, 2016). O RGPD consiste em uma legislação promovida pela União Europeia (UE) em atuação desde 2018, para introduzir transformações significativas nos aspectos de dados pessoais e privacidade dos indivíduos, objetivando fornecer um maior controle aos cidadãos europeus, quanto as suas informações privadas, garantindo uma abordagem harmonizada e global de proteção de dados para todas as organizações que processem dados da UE.

Em termos de aplicação, o RGPD exige esforços e apresenta novos e complexos desafios institucionais em diversas organizações e países da Europa. A **Figura 1** apresenta os princípios elementares guiados na implementação e elaboração do regulamento europeu, como por exemplo, os princípios de confidencialidade e prestação de contas que buscam formalizar o acesso aos dados e gerar garantias e responsabilização sobre a proteção dos dados.

Em face dos novos esforços iniciados pelo RGPD, o Brasil criou a Lei Geral de Proteção de Dados (LGPD) (LGPD, 2018) sancionada em 2018 e em vigor desde setembro de 2020. A LGPD foi baseada no RGPD e ambos regulamentos são consolidados nos mesmos objetivos gerais de formulação de regras para fortalecer os direitos da privacidade. A grande maioria dos requisitos técnicos da lei europeia e da LGPD são análogos, porém algumas adaptações legislativas e territoriais foram realizadas na lei brasileira.

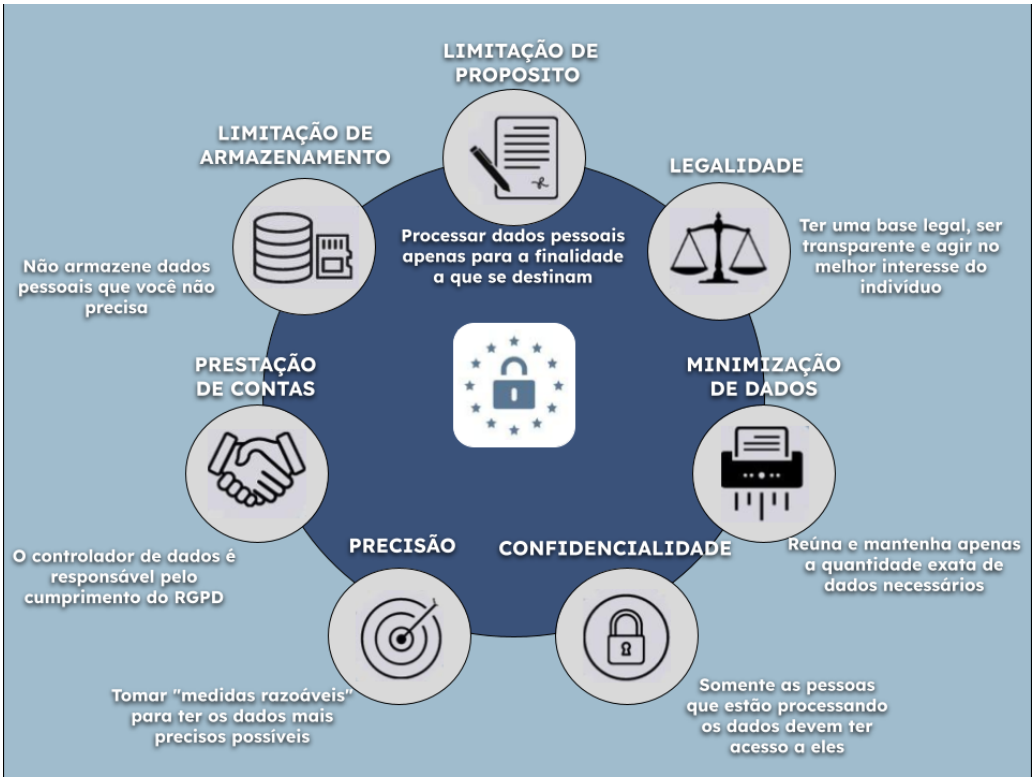

Figura 1: Princípios do RGPD
Fonte: Adaptado de CyberPilot - Data Protection Principles: The 7 Principles Of GDPR Explained (CYBERPILOT, 2022).

O escopo do regimento brasileiro é salvaguardar a forma de tratar dados pessoais, garantindo que direitos essenciais de liberdade e o desenvolvimento do cidadão sejam promovidos. A LGPD aplica-se a todas as operações de tratamento realizadas no Brasil sobre dados de indivíduos, não se limitando apenas ao meio digital, mas também abrangendo qualquer tratamento executado nas organizações públicas e privadas do país (OKANO et al., 2021).

A LGPD exige adaptações profundas para os órgãos nacionais que processam dados de pessoas, logo, muitos ajustes são necessários para cumprir as demandas do regimento que aplicará sanções e multas para organizações privadas que desrespeitem suas normas. Apesar da severidade das sanções, é importante compreender que a LGPD não serve apenas para penalizar, a lei foi desenvolvida para produzir resultados concretos na evolução do nível de proteção das informações dos cidadãos e objetiva se alinhar às metas da economia brasileira, evitando crimes e estimulando o desenvolvimento econômico e tecnológico (PAINI; ZILLES, 2021).

Apesar do debate e investimento imediato que as novas legislações geraram na Europa, no Brasil e no mundo, a implementação completa e global das disposições legislativas para todas as organizações ainda não foram totalmente concluídas. Na pesquisa nacional 2022-2023, realizada pela DARYUS (IDESP - Instituto Daryus de Ensino Supe-

rior Paulista), é indicado que 80% das organizações ainda não concluíram seus projetos de adequação à LGPD, 55% das organizações indicam que possuem adequação de pelo menos 70% dos requisitos da lei, no entanto, 21% não iniciaram seus processos de implementação, ou não souberam informar suas ações. A **Figura 2** expõe um dos gráficos de adequação da pesquisa.

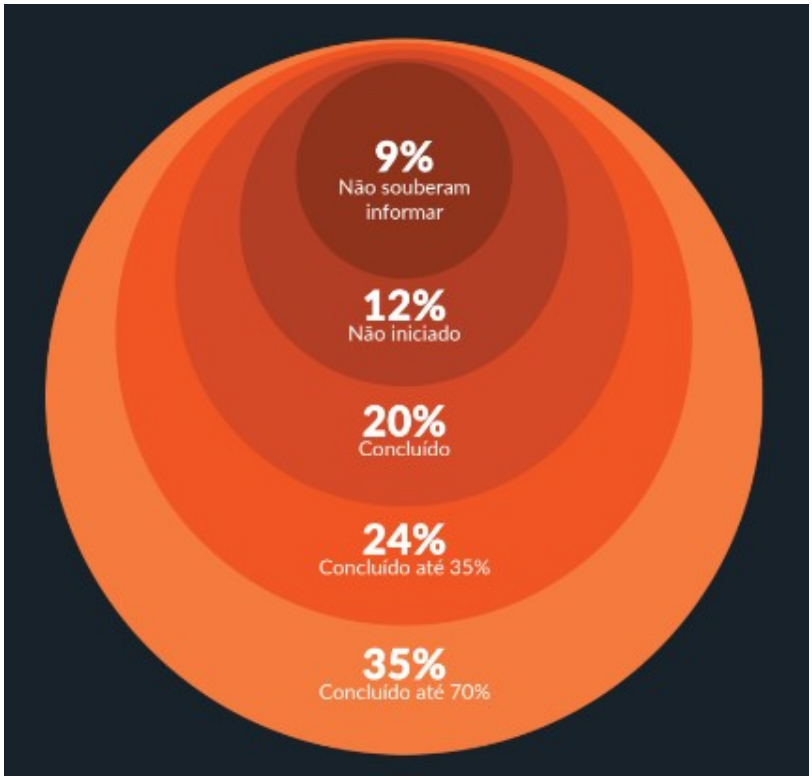

Figura 2: Nível de adequação à LGPD - Organizações Braileiras
Fonte: DARYUS - PESQUISA NACIONAL 2022 - 2023 (DARYUS, 2023).

A simplicidade da linguagem natural que estrutura as legislações (RGPD e LGPD), torna a implementação concreta complexa e indeterminada para desenvolvedores, técnicos e especialistas em Segurança da Informação e Governança de Dados. Estes profissionais encontram dificuldades em traduzir as disposições da LGPD em requisitos técnicos, especialmente caso não haja um engajamento ou conhecimento jurídico aguçado dos detalhes da Lei (DAOUDAGH; MARCHETTI, 2022).

Atualmente, a comunidade científica e as empresas, estão buscando a definição de procedimentos adequados, assim como, soluções teóricas e práticas para fazer valer a adoção dos novos regimentos e suas problemáticas de conformidade. Mais precisamente, eles reconheceram como um fator central a especificação de suportes automatizados para especificar requisitos de privacidade, e assim, controlar dados pessoais e processá-los em conformidade com a LGPD ou o RGPD. (DAOUDAGH; MARCHETTI, 2022) apontam que as maiores vulnerabilidades encontradas nas organizações é o relato de "Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação".

Com os desafios de implantação impostos, o RGPD e a LGPD promovem o interesse na gestão da Segurança da Informação nas empresas e profissionais que tratam dados pessoais. As empresas que adotam uma prática madura de gerência de projetos de segurança da informação e o desenvolvimento de soluções inovadoras, para proteger dados de seus clientes, estarão mais preparadas para o mercado competitivo, realizando todas as suas demandas jurídicas e promovendo um gerenciamento de informações, que resulta em velocidade, robustez, consistência e excelência operacional nos seus processos e sistemas de informação (MARQUES, 2020).

1.1 Problema

Muitas das discussões e estudos relacionados a leis de privacidade de dados são frequentemente relacionadas ao ordenamento jurídico, no entanto, a área de Tecnologia da Informação (TI) é uma das principais áreas que se responsabiliza pela implementação e execução da LGPD, ao garantir a segurança das informações dos usuários. Atualmente, dada a recente publicação de novas legislações de privacidade de dados pessoais como a LGPD, existem numerosas provações para o seu cumprimento. Dessa forma, é necessário avaliar quais impactos refletidos nos processos organizacionais, e quais as soluções propostas capazes de desenvolver metodologias eficientes associadas às técnicas de Tecnologia e Segurança da Informação em sua proteção de dados pessoais, tal como, quais serão os processos humanos, institucionais e culturais carecidos de transformações.

1.2 Objetivo Geral

Este trabalho tem como objetivo realizar uma revisão da conjuntura das principais soluções encontradas para implementar medidas de privacidade e processos da LGPD, considerando também os fenômenos internacionais, especialmente da União Europeia em relação às conformidades do RGPD, que possui requisitos técnicos análogos ao regimento brasileiro. As produções internacionais para cumprir o RGPD podem gerar contribuições robustas para a implementação dos requisitos da LGPD.

Com isso, é possível identificar as principais vantagens e desafios dos artefatos encontrados na revisão e, assim, avaliar as particularidades brasileiras na temática. Finalmente, elaborar recomendações, intervenções e estratégias concretas de implementação para a conformidade com a legislação, na perspectiva da Gestão de Dados e da Segurança da Informação.

1.3 Objetivos Específicos

Como objetivos específicos foram elencados:

1. Identificar implementações de metodologias, práticas e processos organizacionais de adaptação e atendimento aos requisitos do regimento nacional;

2. Identificar implementações de ferramentas tecnológicas e sistemas que solucionam requisitos técnicos das legislações de proteção de dados;

3. Abordar vantagens e desafios das soluções exploradas;

4. Propor recomendações de adequação à LGPD, tendo como base as análises das implementações encontradas na literatura.

1.4 Estrutura da Dissertação

Este trabalho está estruturado em oito capítulos, o Capítulo 2, contempla a revisão da literatura expondo os principais temas na competência da privacidade de dados pessoais, segurança da informação e no histórico de construção dos regulamentos analisados. O Capítulo 3 apresenta alguns estudos relacionados com as legislações de proteção de dados. No Capítulo 4 é apresentada a metodologia de revisão sistemática, definindo os parâmetros para a seleção de estudos e especificando o método de apresentação dos resultados.

Os Capítulos 5 e 6 expõem a apresentação e síntese dos estudos relacionados à artefatos de processos organizacionais de adequação à LGPD e soluções tecnológicas de Segurança da Informação. O Capítulo 7 apresenta as análises e interpretações dos estudos apresentados, e exibe os resultados estabelecidos pelos objetivos específicos e pelo objetivo geral do trabalho. Por fim, o Capítulo 8 apresenta as considerações finais e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada a fundamentação teórica do trabalho, para isso, é necessário elucidar as principais temáticas relacionadas ao contexto de adequação com a Lei Geral de Proteção de Dados (LGPD). Visto que o ponto de preocupação principal da nova legislação está relacionada em como as organizações, profissionais e indivíduos manipulam e analisam os dados dos cidadãos, torna-se necessário entender a concepção de dados pessoais e como eles podem ser manipulados.

Para entender o contexto de dados pessoais e como protegê-los, seguindo as diretrizes regulatórias, é preciso contextualizar suas categorias e explorar quais ações podem ser aplicadas e quais as consequências de cada operação realizada sobre os dados. As manipulações nas informações pessoais estão diretamente relacionadas com as organizações públicas ou privadas, que detém a posse dos dados e com tecnologias digitais, cada vez mais utilizadas para executar atividades de processamento de informações.

As próximas seções também se dedicam em conceitualizar a origem, propósitos e objetivos da LGPD e do regimento que serviu de base para os seus requisitos (Regulamento Geral sobre a Proteção de Dados europeu - RGPD), propondo assim uma fundação apropriada para identificar as tarefas de adequação necessárias para se adequar a lei. Os temas explorados no capítulo são:

- Dados Pessoais;
- Privacidade de Dados;
- Governança de Dados;
- Segurança da Informação;
- Regulamento Geral de Proteção de Dados;
- Lei Geral de Proteção de Dados.

2.1 Dados Pessoais

No meio organizacional e nos ambientes digitais, o compartilhamento e manipulação de dados de indivíduos ocorre frequentemente. Os dados dos indivíduos são intitulados de Dados Pessoais, e representam informações, fatos, interesses e relações que se referem a uma pessoa identificável (MONTOLLI, 2020). Exemplos de dados pessoais comuns são: nome, CPF, telefone, ocupação profissional e histórico de saúde. É relevante expressar que os dados (como dados pessoais) não são informações propriamente, em linhas gerais, dados são apenas registros sem significado. Uma vez interpretados e

analisados com contexto, dados pessoais podem promover diversas informações valiosas sobre uma pessoa.

Uma categoria de dados pessoais cada vez mais importantes para empresas e para a sociedade são os dados pessoais sensíveis. Tais dados geram uma atenção excessiva, pois caracterizam dados de caráter privado, já que são capazes de gerar informações sensíveis sobre os cidadãos. Os dados estão geralmente relacionados com questões que envolvem saúde, origem racial ou étnica, direcionamento político, religiosidade, orientação sexual, identidade de gênero, dentre outros da mesma natureza. É possível observar que são dados intrinsecamente delicados ao indivíduo, que deve deter o direito de mantê-los privados, ou reivindicar que nenhum uso indevido sobre as informações seja realizado (MONTOLLI, 2020).

As operações realizadas com estes dados são recorrentemente denominadas de 'tratamento de dados'. O tratamento simboliza quaisquer ações realizadas com o dado obtido, e podem ser listadas como: coleta, produção, compartilhamento, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, comunicação, entre outras (PAINI; ZILLES, 2021).

Um dos tratamentos de dados pessoais recorrentemente utilizados nas organizações é a anonimização de dados pessoais. Um dado anonimizado é um dado que se mantém relativo à uma pessoa, no entanto, não é mais possível identificá-la. Para realizar o processo de anonimizar dados pessoais, são utilizadas operações técnicas disponíveis entre os profissionais da organização, e assim, é executada a ocultação de informações capazes de identificar o indivíduo (LIMA, 2020).

Os dados pessoais também possuem um ciclo de vida que pode ser definido e representado para entender o fluxo de tratamentos executados pelos órgãos detentores dos dados. A Figura 3 exemplifica um ciclo de dados pessoais de um indivíduo, desde a etapa de coleta, até uma etapa de transferência, ou eliminação. Dependendo da organização, do setor e até dos objetivos ou necessidades, o ciclo de vida dos dados pode ser alterado, não tendo necessariamente a estrutura exposta na figura (FILHO et al., 2023).

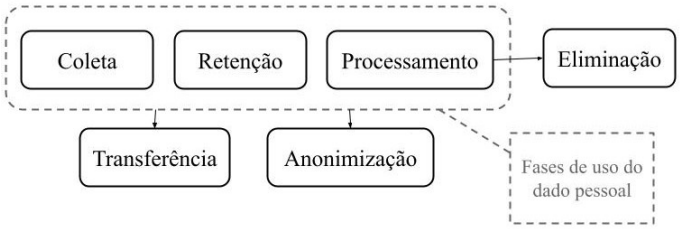

Figura 3: Ciclo de Vida de Dados Pessoais
Fonte: Adaptado de (FILHO et al., 2023).

Atualmente o foco principal do controle dos dados pessoais e de seu ciclo de vida

está relacionado em desenvolver metodologias capazes de resguardar e privar os dados pessoais, seguindo a vontade do indivíduo. Esta atividade está relacionada ao conceito de privacidade de dados apresentada em seguida.

2.2 Privacidade de Dados

OO termo privacidade é utilizado para aspectos diversificados, dependendo da área em estudo. Neste trabalho, a privacidade de dados pessoais é o direito do indivíduo de manter suas informações resguardadas, sem interferência de outras pessoas ou entidades (LIMA, 2020). Neste contexto, é vital preservar o direito de uma pessoa em ser uma figura ativa na tomada de decisão sobre o tratamento de seus dados, e assim, promover o direito de escolha sobre quais operações e quais órgãos podem processar suas informações (FERRÃO et al., 2021).

A preocupação com a privacidade de dados pessoais cresce a cada ano, graças à evolução da TI. O cumprimento deste direito encontra muitos desafios e barreiras com a alta distribuição, compartilhamento e fluxo de informações. Logo, do ponto de vista técnico, é cada vez mais prioritário alinhar sistemas e tecnologias da informação protegendo e privando os dados que gerenciam. No âmbito administrativo, normas como ISO/IEC 27701 (ISO/IEC, 2019) e ISO/IEC 27002 (ISO/IEC, 2022) formalizam procedimentos para melhorar práticas e garantir a privacidade dos dados (FERRÃO et al., 2021).

A proteção de dados é um subconjunto da privacidade, dado que, proteger informações confidenciais e dados pessoais é o primeiro passo para evitar acessos e processamentos indevidos (MENEGAZZI, 2021). A preocupação com a promoção de proteção de dados eleva o debate e o nível dos direitos humanos no cenário internacional, posto que, elaborações de novas leis sobre o tema foram executadas, dentre elas se destacam: RGPD, LGPD e *California Consumer Privacy Act* (CCPA) (BAX; BARBOSA, 2020). O principal ponto de mudança impulsionado pela temática e pelos novos regimentos é a mudança na perspectiva e nas ações institucionais, principalmente na governança de dados organizacionais, explorada a seguir.

2.3 Governança de Dados

A Governança é um conceito usado no ambiente organizacional, para descrever ações relacionadas à tomada de decisão coletiva e coordenada por indivíduos que trabalham em conjunto, atuando em atividades de interesse para toda a organização. Já a Governança de Dados, é um tipo de gestão de informação que observa a utilização de dados de forma estratégica e planejada, para estruturar a forma de coleta, armazenamento e tratamentos executados na empresa (MONTOLLI, 2020).

Essa gestão é importante pois, a partir da governança de dados, é possível visualizar as informações manipuladas como fontes valiosas para traçar estratégias e exercer o controle sobre o gerenciamento de dados. As atividades previstas nesse domínio estão relacionadas a desenvolver políticas, padrões e processos capazes de garantir a segurança, integridade e disponibilidade dos dados (SILVA, 2021).

Para uma boa execução, a governança deve envolver esforços da organização como um todo, avaliando aspectos e setores diversos, para ter um controle e uma percepção ampliada dos riscos associados aos dados e prevenir incidentes. Para isso, em muitos aspectos, é necessário alinhar a governança de dados corporativa com os recursos de TI, adotando métodos, regras e práticas tecnológicas.

2.4 Segurança da Informação

A privacidade, e a governança aliada a Segurança da Informação (SI) são temáticas em evidência, devido a grande quantidade de dados corporativos processados e distribuídos na internet e em sistemas de informação. Aliado a isso, os perigos de incidentes e de ataques nas informações organizacionais e pessoais estão cada vez maiores (MONTOLLI, 2020). A SI pode ser definida como a proteção automática a sistemas de informação, objetivando preservar a integridade, a confidencialidade e a disponibilidade de recursos do sistema, os três pilares da Segurança da Informação (LIMA, 2020).

Para a SI, a informação é um ativo valioso que precisa ser protegido e, se possível, aprimorado utilizando normas e medidas técnicas explicitadas nas políticas de segurança. Tais políticas visam minimizar qualquer dano de segurança e manter a continuidade estável das atividades corporativas (ROCHA et al., 2019). Exemplos de ativos de informação considerados pela SI são equipamentos, usuários, bases de dados e sistemas.

As Políticas de Segurança da Informação (PSI) são documentos que buscam mitigar ataques às informações das organizações. O PSI é um documento capaz de descrever um conjunto de diretrizes e procedimentos, que necessitam de colaboração entre o nível estratégico da organização e os profissionais capacitados para executar atividades técnicas (ROCHA et al., 2019).

A PSI deve determinar o fluxo de informações na corporação e os princípios das políticas devem definir minuciosamente quais mecanismos são utilizados para assegurar as informações. Em muitos casos, também é necessária a criação de uma comissão de segurança da informação, formada por responsáveis de setores multidisciplinares, assim a gestão pode desenvolver uma análise correta da aplicação das políticas (ROCHA et al., 2019).

Além de seus requisitos tradicionais, atualmente a SI também deve se adequar às questões societárias e regulatórias, os novos regulamentos que influenciam neste contexto

são apresentados a seguir.

2.5 RGPD

O RGPD foi criado para substituir a Diretiva de Proteção de Dados da UE, a diretiva era focada nos requisitos de privacidade e foi adotada em 1995. A substituição pelo RGPD foi necessária, pois a lei anterior não era atualizada em algumas diretivas, especialmente sobre novos tópicos impostos pelo ambiente digital (TEIXEIRA; SILVA; PEREIRA, 2019b).

Em vigor desde 25 de maio de 2018, o regulamento aplica-se a qualquer organização do mundo que processe dados de cidadãos da UE e é aplicável para todos os Estados-Membros do bloco econômico, eliminando assim a necessidade de legislações nacionais e promovendo a unificação de regras e leis da UE (HUSSAIN et al., 2020). O RGPD desenvolve mudanças significativas no tópico de dados pessoais e privacidade de dados, objetivando uma abordagem sustentável e unificada de proteção de dados (TEIXEIRA; SILVA; PEREIRA, 2019b).

O RGPD é a alteração mais importante das últimas décadas, em relação à privacidade de dados pessoais, pois foi pioneira em produzir um regulamento qualificado, em ampliar regras e diretrizes sobre a temática, e dispõe de obrigações legais específicas de tratamento de dados, para os órgãos que processam informações pessoais. Com a legislação, os cidadãos europeus são beneficiados em questões como: o controle de seus dados, formalização de seus direitos, reformulação da forma com que as organizações tratam os dados dos cidadãos e garante uma circulação segura de dados pessoais na UE (TEIXEIRA; SILVA; PEREIRA, 2019b).

O escopo do RGPD é muito amplo, pois se aplica a qualquer organização atuante na UE. Do ponto de vista empresarial, o RGPD exige (HUSSAIN et al., 2020):

- Transparência: as políticas organizacionais devem ser claras e definidas para proteção, processamento e portabilidade de dados de qualquer informação relacionada ao cliente, empregados ou qualquer dados pessoais.
- Controle de acesso: As empresas devem possuir ferramentas de segurança adequadas, bem como processos que promovem a proteção dos dados privados dos clientes.
- Privacidade pessoal e direito de ser esquecido: um cliente com mais de 16 anos de idade tem pleno direito de definir quais dos seus dados uma empresa pode manipular. Além disso, o cliente tem pleno direito de exigir que seus dados sejam excluídos após o uso.

Apesar das exigências complexas, o RGPD não fornece diretrizes específicas quanto à sua implementação, não sendo prescritivo quais tecnologias e metodologias devem ser usadas para alcançar a adequação completa com a lei. Com essa limitação as organizações, em geral, possuem dificuldades em entender o Regulamento e como implementá-lo, em especial empresas com poucos recursos ou com grandes quantidades de dados pessoais.

O não cumprimento das disposições do regulamento europeu pode impor multas pesadas às organizações (GDPR, 2016). As empresas podem ser punidas com multas que podem chegar a 4% do faturamento anual, ou até o limite de 20 milhões de euros. Este sistema de infrações administrativas impõe atribuições pesadas para as organizações e garante que os usuários também estarão diretamente informados, quando as violações de segurança de dados pessoais implicam um alto risco para seus direitos e liberdades.

2.5.1 Privacidade por Design e Padrão

Uma diretriz inovadora desenvolvida nos termos do RGPD foi a Privacidade por Design e Padrão (PDP, *Privacy by Design*), que consiste em uma série de princípios implementados no início de todos os projetos e aplicados em todos os processos e setores de uma organização. A PDP é um método de desenvolvimento para sistemas amigáveis à proteção de dados, pois, busca mitigar preocupações tardias com informações pessoais privadas. Com este método é possível direcionar a privacidade desde o início de um projeto, ou do desenvolvimento, até a operação de um sistema (TEIXEIRA; SILVA; PEREIRA, 2019b).

O RGPD defende, explicitamente, a privacidade por design e padrão para incentivar e recomendar que a proteção de dados seja executada durante todo o ciclo de projetos, processos e sistemas. A lógica da PDP implica na dedicação humana, que não é uma coleção de meras ferramentas técnicas, e é um processo de implementação de princípios de privacidade e proteção de dados, que envolve componentes técnicos, humanos e organizacionais (HUSSAIN et al., 2020).

Embora a PDP tenha encontrado reconhecimento e se tornado um exemplo de recomendação em regulamentos influentes (GDPR, 2016), sua implementação ainda é obscura, principalmente na tentativa de abarcar metodologias gerais ou na utilização de mecanismos para integrar o desenvolvimento de proteção à dados privados (DANEZIS et al., 2015). A grande contribuição do método é exposto na constatação de que as aplicações e metodologias de proteção devem estar na configuração padrão e em todas as etapas de concepção e desenvolvimento, assim como, nas estruturas de um sistema de informação.

FILHO et al. expõe alguns princípios orientadores da PDP:

1. Proativo e não reativo - As organizações devem tratar a privacidade como padrão e

aplicá-las prontamente em suas atividades;

2. Preventivo e não corretivo - A privacidade deve ser considerada desde o início, evitando ao máximo ações corretivas após a constatação de um problema;

3. Privacidade incorporada ao design - A privacidade deve estar no planejamento e design de sistemas e projetos;

4. Segurança ponta a ponta - A proteção de dados deve ser efetuada durante todo o ciclo de vida de um sistema e de um processo;

5. Visibilidade e transparência - Os processos de uma organização devem ser sempre transparentes sobre quais medidas de privacidade estão sendo executadas;

2.6 LGPD

A LGPD foi criada para aplicar a proteção de dados pessoais em todas as organizações públicas ou privadas, que desempenham qualquer tipo de manipulação sobre os dados dos cidadãos, independente do meio de tratamento. A lei foi baseada no RGPD europeu para evoluir o nível de privacidade, em qualquer operação de coleta, transferência e tratamento de dados pessoais no território nacional (PAINI; ZILLES, 2021).

A LGPD tem sua aplicação unificada para empresas de qualquer porte, portanto, torna-se necessário o ímpeto em aplicar segurança tecnológica para evitar violações às disposições legais do regulamento (HUSSAIN et al., 2020). Além disso, faz-se crucial entender as disposições da nova norma e seus impactos práticos. Os fundamentos da disciplina da proteção de dados pessoais objetivada na LGPD estão expostos e interpretados no **Quadro 1**.

Quadro 1: Fundamentos de proteção de dados da LGPD expostos no Art. 2º

FUNDAMENTO	CONDUTA
O respeito à privacidade	Assegurar os direitos fundamentais de inviolabilidade da intimidade, da imagem e da vida profissional e privada.
A autodeterminação informativa	Expressar o direito do cidadão ao controle e arbítrio à proteção de seus dados pessoais e sensíveis
A liberdade de expressão, de informação e de comunicação	Ao desempenhar bases essenciais da democracia e direitos previstos ao cidadão na Constituição brasileira (1988)
O desenvolvimento econômico e tecnológico e a inovação	A partir da criação de um cenário de segurança jurídica em todo o país.
A livre iniciativa, a livre concorrência e a defesa do consumidor	No enriquecimento de regras claras e válidas para todo o setor privado e a transparência dos órgãos e eficiência público
Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania	O investimento na produção de um ambiente virtual valorando todos os princípios e direitos da cidadania.

Fonte: Implementado pelo Autor.

Como podemos observar, assim como o regulamento europeu, a LGPD também é uma legislação ampla e unificada para todos os órgãos do Brasil. Apesar de sua abrangência, em seu Artigo 4º, a LGPD define em quais ocasiões o tratamento de dados pessoais não possui a aplicação da lei. As exceções ao tratamento são (ROCHA et al., 2019):

- Tratamento de dados pessoais processados por pessoa natural, para intenções exclusivamente individuais e não financeiros;
- Tratamento para fins jornalísticos, acadêmicos ou artísticos;
- Utilização de dados pessoais para segurança pública, defesa nacional, segurança do estado e atividades investigativas.

Em termos cronológicos, a maioria dos artigos da legislação brasileira estão em vigor desde setembro de 2020. Já as multas e sanções (que constam nos Artigos 52 e 54), começaram a vigorar a partir de agosto de 2021. A entidade nacional responsável pela fiscalização e pela regulamentação da LGPD é a Autoridade Nacional de Proteção de Dados (ANPD) e está em execução desde dezembro de 2018 (RODRIGUES; PAULA, 2022). A ANPD foi criada com objetivo de executar a regulamentação e desenvolver maior aderência com realidade social e empresarial nacional, promovendo assim, mais estabilidade e segurança na aplicação da LGPD (PAINI; ZILLES, 2021).

Além de uma autoridade nacional para regular a adequação à LGPD, foi necessário a definição de agentes de tratamentos que ocupam papéis formais na privacidade de dados exigida pela lei. Os agentes de tratamento são Operadores e Controladores, e baseando-se no RGPD, existe o papel do Encarregado de Dados (DPO - *Data Protection Officer*). A Figura 4 apresenta os papéis citados.

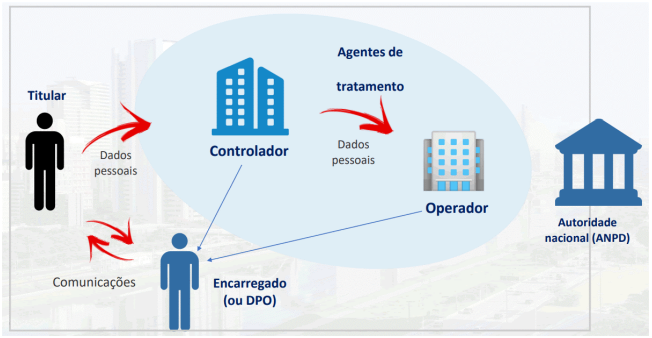

Figura 4: Entidades da LGPD
Fonte: (INOVAçãO, 2020).

- Titular de dados - Indivíduo proprietário dos dados processados por alguma organização;
- Controlador - Pessoa física ou jurídica responsável por definir a finalidade e como os dados pessoais são tratados
- Operador - Pessoa física ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado (DPO) - Indicado pelo controlador para mediar a comunicação entre titulares, ANPD e controlador. É um profissional com uma multiplicidade de funções jurídicas, técnicas e de comunicação.

É notável como a conformidade com a LGPD impõe desafios aos empresários e aos gestores públicos. Para alcançar o objetivo de cumprir todos requisitos da lei, é essencial a busca por apoio jurídico para implantação, ou atualização de regimentos internos. A atualização das políticas de SI, para abordagens mais amigáveis à privacidade de dados, torna-se importante. É primordial uma boa comunicação e disponibilização de informações para os usuários e titulares de dados sobre a coleta, utilização e tempo de posse dos dados pessoais processados (ROCHA et al., 2019).

A ANPD deve fiscalizar o cumprimento da lei por parte das empresas brasileiras, e um dos artefatos que podem ser exigidas é o "Relatório de Impacto à Proteção de Dados Pessoais" (RIPD). Este documento deve conter os processos internos, detalhando

as providências executadas sobre os dados e medidas de redução de risco de vazamentos e incidentes (RODRIGUES; PAULA, 2022).

Além da fiscalização, a ANPD é a responsável por aplicar multas e sanções para empresas que cometem infrações. A depender do grau da contravenção, as sanções podem ser executadas a partir de uma simples advertência, até multas de 2% do faturamento do último exercício de uma organização, com o limite de até R$ 50 milhões (LOPES; AMARAL, 2022). As multas e sanções impostas pela LGPD são fontes de muita preocupação para as organizações, implicando em mudanças e esforços específicos na governança corporativa e governança de dados.

2.6.1 Governança de Dados relacionada à LGPD

A LGPD influencia novos investimentos necessários para todas as organizações brasileiras de pequeno, médio e grande porte que manipulam dados pessoais. Parte dos esforços requeridos às empresas está no investimento em tecnologia da informação, assim como, em executar técnicas de adequação existentes para impedir violações com os dados, que estão salvaguardados pela legislação (ROCHA et al., 2019).

Essa mudança deve focar na geração de uma governança de dados que possui quatro pilares: estabelecimento de uma cultura organizacional inovativa; definição e estabelecimento de funções entre os profissionais que manipulam dados pessoais; técnicas de segurança da informação e técnicas que permitam um fluxo de transferência de dados seguro e transparente aos titulares (LUGATI; ALMEIDA, 2022).

As empresas brasileiras têm enfrentado desafios e transformações para corresponder à LGPD. Entretanto, não são apenas as instituições privadas que devem se adequar ao regimento. Com o amparo em artigos específicos da LGPD, a administração pública possui deveres para atender exigências relacionadas às suas atividades legais (RODRIGUES; PAULA, 2022).

Entidades públicas devem promover a adequação da LGPD, tendo como prioridade o interesse público e sempre se relacionando com a sua finalidade e os seus serviços providos. O Artigo 23 da LGPD especifica pessoas jurídicas de direito público como: os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e do Ministério Público, também incluindo as demais entidades controladas pela União, Estados e Municípios. Por fim, as autarquias, as fundações públicas e sociedades de economia mista estão incluídas na mesma base da lei (RODRIGUES; PAULA, 2022).

Quanto ao acompanhamento e a cobrança para órgãos públicos na disposição de adequação à Lei Geral de Proteção de Dados, a ANPD pode a qualquer momento emitir solicitação direcionada a órgãos públicos, para que executem atividades de tratamento de

dados pessoais. Dentre as medidas requeridas, a ANPD pode requisitar o detalhamento dos tratamentos de dados pessoais executados e informações sobre o alcance e a natureza dos dados manipulados (RODRIGUES; PAULA, 2022).

Nos casos de infração à LGPD por órgãos públicos, não são aplicadas sanções e multas como para empresas privadas. A ANPD fica encarregada de enviar informes para entidades públicas (que realizam infrações) contendo medidas cabíveis para cessar a violação. Em adição, podem pedir para que os agentes públicos orientem o desenvolvimento de processos técnicos, que viabilizem corretamente a privacidade e a proteção de dados pessoais. Mesmo com o auxílio da ANPD, a falta de sanções e multas para órgãos públicos mantêm o questionamento se entidades públicas são responsáveis confiáveis para promover uma gestão de dados eficientes para os cidadãos (ANPD, 2023).

Neste capítulo foi apresentado uma revisão dos principais tópicos relacionados à adequação com a Lei Geral de Proteção de Dados. A seguir são expostos alguns estudos com temáticas e abordagens semelhantes aos objetivos deste trabalho.

3 ESTUDOS RELACIONADOS

Neste capítulo são apresentados alguns trabalhos relacionados que exploram o uso de ferramentas que solucionam problemas de privacidade e proteção de dados. Em adição, tratamos também que identificam técnicas e fatores capazes de promover privacidade e cumprir os requisitos legislativos da LGPD e do RGPD, relatando seus objetivos e resultados.

O estudo proposto por FERREIRA; OKANO (2021), tem o objetivo de verificar o panorama de adequação das organizações brasileiras à LGPD, detectando a opinião de profissionais sobre a lei e as ferramentas, ou métodos capazes de auxiliá-los na implantação. A pesquisa foi executada durante a pandemia do Covid-19 e foi realizada por meio de uma *survey* com 216 profissionais de segmentos variados do mercado. Todas as regiões do Brasil foram contempladas na pesquisa e a análise da pesquisa evidenciou que muitas empresas brasileiras estão iniciando seus projetos de adequação, encontrando desafios complexos, principalmente quanto à sua cultura interna.

O artigo de LOPES; AMARAL (2022) investiga as bases regulamentares da LGPD e os desenvolvimentos de sistemas criados para atender tais conformidades, avaliando as tecnologias que estão surgindo para melhorar e facilitar a elaboração de medidas protetivas ,no tema de privacidade de dados pessoais. O trabalho toma como base uma organização fictícia focada em comércio eletrônico, que precisa passar pela adequação à LGPD. Ao considerar o exemplo mostrado, há diversos recursos tecnológicos para implantar um sistema voltado a assegurar o direito dos clientes e a integridade dos dados pessoais, e é evidenciado que adotar tais tecnologias é algo plausível e passará a ser um item básico nas organizações.

O trabalho desenvolvido por MENEGAZZI (2021), focou em definir um guia para as organizações entenderem as obrigações da LGPD e identificar medidas para alcançar a conformidade dos sistemas de software, principalmente se relacionando ao tema de Engenharia de Requisitos, especificamente entendendo a conformidade dos sistemas por meio de Requisitos de Negócio e Requisitos de Solução. A metodologia se baseou em levantamento bibliográfico não exaustivo. Como resultado, além de apresentar um guia com etapas que auxiliam os profissionais de Tecnologias da informação e comunicação (TIC) no alcance da conformidade com a LGPD, (o guia conta com um exemplo de ilustração demonstrando a aplicação das suas etapas no sistema de uma instituição de ensino). O trabalho apresenta uma avaliação deste guia com potenciais usuários por meio de um questionário distribuído nacionalmente (obtendo 31 respostas).

PIURCOSKY et al. (2019) procuram descrever a realidade das implementações das organizações brasileiras quanto à adequação à LGPD. A abordagem foi definida para estabelecer como as organizações do sul de Minas Gerais estão se adequando à nova

lei. A metodologia foi qualitativa e com raciocínio indutivo, objetivando compreender a realidade das empresas estudadas, coletando dados através de análise de casos múltiplos e entrevistas. O estudo evidenciou que o estado de adequação das empresas ainda é deficitário em atender aos marcos regulatórios da LGPD e foi clarificada a necessidade de modificações consideráveis em processos internos de coleta e armazenamento de dados, assim como, alterações na SI. Além disso, a escassez de recursos tecnológicos e a falta de domínio em boas práticas de SI são fatores limitadores para atender a legislação.

A pesquisa de TEIXEIRA; SILVA; PEREIRA (2019a) buscou identificar os fatores críticos de sucesso para a implementação do RGPD, que podem facilitar a realização de projetos e são fundamentais para o sucesso das adequações necessárias para a proteção de dados. A metodologia utilizada foi uma revisão sistemática que explorou 32 documentos para responder às questões propostas pela pesquisa. Como resultado, além dos fatores críticos identificados, o estudo propôs identificar as barreiras e facilitadores da implementação, assim como, descrever os benefícios em cumprir o regimento europeu. Ao todo, 8 fatores críticos foram listados para uma adequação bem sucedida ao RGPD.

ARAGÃO; SCHIOCCHET et al. (2020) buscaram em seu estudo apontar em qual medida a LGPD impacta a estrutura do Sistema Único de Saúde brasileiro (SUS). A nova lei de privacidade possui especificidades em suas bases legais para tratar tanto de órgãos públicos, como entidades que resguardam dados pessoais relacionados à saúde. Nesse domínio, muitas das necessidades na privacidade dos pacientes estão relacionadas com dados sensíveis e o trabalho identifica a necessidade de agilidade em tomar ações técnicas e de gestão, que atualizem os processos de governança, de padronização, de planejamento e de organização. A conclusão do estudo é que a LGPD exige que os gestores do SUS identifiquem as adaptações necessárias para cumprir o regimento, aliando os avanços da medicina e os avanços tecnológicos aos direitos de privacidade, no contexto de proteção da vida e de dados pessoais sensíveis.

SILVA (2021) realizaram uma pesquisa com o objetivo de analisar os avanços derivados dos impactos da LGPD na gestão das políticas públicas de dados. A análise inspecionou atividades de municípios brasileiros, e especialmente tomou como estudo de caso a cidade de Belo Horizonte/MG. A principal observação apanhada foi a visualização das mudanças na estruturação da política de governança, para isso, a pesquisa coletou documentos em portais eletrônicos públicos dos municípios e prefeituras analisadas. A principal mudança identificada com a LGPD foi a ampliação de papéis e entidades direcionadas nos processos decisórios sobre as políticas públicas de dados pessoais.

O trabalho proposto por FERRÃO et al. (2021) realizou o diagnóstico de organizações públicas e privadas no Brasil para verificar as condutas de processamento de dados e a adequação com a LGPD, a fim de permitir a percepção geral do panorama de implementação da lei, sobretudo na visão dos profissionais de TI. Coletando a opinião de

105 profissionais de TI, sobre 41 questões tratando do processamento de dados, os resultados colhidos revelam pontos de atenção para LGPD, entre eles o nível baixo de engajamento dos profissionais em tratar de dados pessoais, seguindo as diretrizes especificadas na organização. Outro ponto relevante é o desconhecimento de artefatos considerados eficientes e amigáveis à privacidade, seguindo os princípios da legislação.

Embora os autores apresentem lições aprendidas e até implementações concretas com a aplicação de vários processos, não há estudos que compilam múltiplas soluções organizacionais para garantir a privacidade. É possível verificar limitações nos trabalhos citados, principalmente em como as soluções podem ser conectadas para promover avanços na gestão de dados, mudanças na cultura organizacional e processos de negócio e Sistemas da Informação. Neste contexto, este trabalho se destaca por implantar uma revisão de soluções organizacionais e de TI para a produção de análises e recomendações a partir dos artefatos estudados.

4 METODOLOGIA

Este capítulo especifica a metodologia adotada neste trabalho, formalizando um protocolo para: a seleção dos estudos relevantes, a definição de critérios formais para o desenvolvimento do trabalho e o detalhamento da estratégia utilizada para responder às principais questões propostas.

Esta pesquisa foi conduzida por meio de uma Revisão Sistemática da Literatura (RSL), um método de estudo que busca dar coerência e sentido a uma investigação específica (CANTO et al., 2020). Para isso, foi formalizado um protocolo de pesquisa que envolve a seleção criteriosa dos estudos relevantes, a definição de critérios formais para o desenvolvimento do trabalho e a descrição detalhada da estratégia adotada para abordar as questões principais propostas.

A RSLé constituída pelas seguintes fases: (i) planejamento da RSL, que envolve a definição do protocolo de pesquisa descrevendo as questões de pesquisa, critérios de inclusão e critérios de qualidade; (ii) execução da RSL, que abrange a análise e seleção de estudos; e (iii) resultados da RSL. Neste capítulo, são detalhados os passos seguidos nas fases (i) e (ii). Os resultados e análises referentes à terceira fase são apresentados nos capítulos seguintes.

4.1 Planejamento da RS

4.1.1 Caracterização da pesquisa

Esta pesquisa examina as produções nos campos científico e organizacional, com foco na adoção de métodos e soluções tecnológicas para atender aos requisitos técnicos da nova Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira. Classificada como uma abordagem qualitativa, o estudo busca apresentar novos conhecimentos sobre a gama de soluções propostas para a adequação de sistemas, projetos e organizações à LGPD.

A metodologia utilizada é a Revisão Sistemática (RSL), um tipo de estudo que visa compreender e conferir lógica a uma investigação formulada. Para a especificação completa da RSL, é necessário criar um protocolo que inclua:

- Definição das questões de pesquisa, explicitando os critérios de inclusão e exclusão de estudos;
- Classificação do tipo de RSL, determinando o método mais viável de acordo com os tipos de estudos disponíveis;
- Definição da metodologia para apresentação da análise, dos resultados e síntese dos dados;

- Avaliação da qualidade dos estudos, com critérios claros para a admissibilidade de um estudo relevante.

Com o intuito de identificar e apresentar implementações de tecnologias, sistemas, práticas e processos organizacionais voltados à adaptação e conformidade com os requisitos da legislação nacional, bem como analisar os artefatos apresentados e compreender sua aplicabilidade às demandas da LGPD, as seguintes questões de pesquisa foram adotadas:

4.1.2 Questões de Pesquisa

- **(Q1)**: Quais são os impactos da LGPD nos processos organizacionais?
- **(Q2)**: Quais são as soluções e artefatos descritos na literatura capazes de solucionar problemáticas de privacidade de dados?
- **(Q3)**: Como as soluções podem ser conectadas para promover avanços na gestão de dados, mudanças na cultura organizacional e processos de negócio?
- **(Q4)**: Quais são as soluções tecnológicas associadas à Segurança da Informação capazes de implementar soluções para os requisitos da LGPD?

4.1.3 Elaboração de Critérios

Para selecionar os estudos mais relevantes, é preciso definir o domínio explorado na pesquisa. Os critérios do trabalho são elaborados em quatro categorias:

1. Conteúdo - explora a seleção de artigos com temáticas ligadas à exploração de informações, para solucionar a questão de investigação principal;
2. Temporal - define o período de publicação de interesse para investigação;
3. Localização - determina de que países ou regiões pode-se encontrar os estudos expressivos para o tema;
4. Configuração - Determinar idiomas, formatos e aspectos secundários dos artigos.

A) Conteúdo

Em termos de conteúdo, para explorar os dados relevantes para a análise, os trabalhos publicados devem investigar pelo menos um dos itens:

- Abordam os impactos de soluções de métodos na: gestão de dados, mudanças na cultura organizacional, processos de negócio e *frameworks* de implantação;

- Abordam os impactos em soluções de SI que solucionam problemas específicos da privacidade e/ou da proteção de dados;

Para seleção de estudos, foi definida uma *string* de busca com termos associados aos objetivos do trabalho. As palavras foram selecionadas para identificar soluções de adequação e conformidade da LGPD tanto na perspectiva de privacidade, governança de dados e segurança da informação, selecionando também estudos que indicam soluções dos fenômenos internacionais, especialmente da União Europeia em relação às conformidades do RGPD:

1. String para estudos sobre a LGPD: ((“LGPD” OR “Lei Geral de Proteção de Dados”) AND (“implementação” OR “adequação” OR“conformidade” OR “privacidade” OR “Segurança da Informação” OR “Governança de Dados” OR “Data Managment” OR “ISO”OR “Ìnteligencia Artificial” OR “IA”OR “Consentimento”));
2. String para estudos sobre o RGPD: ((“GDPR” OR “General Data Protection Regulation”) AND (“implementation” OR “compliance” OR “privacy” OR “Information Security” OR “Data Managment” OR “ISO” OR “Artificial inteligence” OR “AI”OR “Machine Learning”OR “Consent”)).

B) Localização

Em termos de localização, o trabalho analisa as soluções exploradas no Brasil para se adequar à LGPD, e também são analisados os estudos que impactam o regulamento europeu RGPD. Analisar os estudos internacionais torna-se relevante, graças a alta correspondência das legislações quanto aos seus requisitos técnicos, e em adição, podemos observar que o aspecto de internacionalização e globalização da privacidade de dados é um tema central nesta análise. Logo são estudadas:

- Soluções para atuação na Europa adequando-se ao RGPD;
- Soluções para atuação no Brasil adequando-se à LGPD;
- Soluções de organizações multinacionais que atuam para se adequar às legislações;

C) Temporal

Para selecionar estudos com aplicações mais robustas utilizados tanto na literatura, como no meio empresarial, pode-se obter as pesquisas publicadas de 2018 a junho de 2023. O ano inicial foi determinado por observarmos que o início da atuação Regulamento europeu foi realizada em 2018, logo as organizações mais eficientes e os desenvolvimentos mais completos começaram a ser apresentados a partir deste período.

D) Configuração

Para as configurações de delimitação de pesquisa, e especificação de atributos dos estudos são listados por:

- Os estudos foram escritos em Português ou Inglês (sem limitação de páginas);
- Os estudos analisados são todos gratuitos;
- Estudos analisados foram identificados pelo ambiente web, nos portais: Periódicos da CAPES que agrega os principais estudos dos repositórios acadêmicos consagrados, ao todo são agregadas 130 bases de dados diferentes, como o Oxford Journals, ACM Digital Library e Science (AAAS) . Além do Capes foi utilizado o ResearchGate e Mendeley;
- As categorias selecionadas para a seleção de estudos são artigos primários, podendo esses serem artigos de conferência, artigos de revistas/jornais e monografias.

4.1.4 Classificação da Revisão

O tipo de RSL aplicado neste trabalho é a **Revisão Mista de Convergência Qualitativa**, caracterizada por transformar os resultados de estudos qualitativos, estudos quantitativos e estudos de método misto em achados qualitativos. Este tipo de revisão é coerente para esta monografia, pois é adequada quando as pesquisas analisam temas diversificados e produção de resultados desassociados, além disso, não possuem uma padronização na análise quantitativa.

4.1.5 Critérios da Qualidade

Além dos critérios de inclusão, foram considerados os itens de qualidade essenciais para os estudos. A avaliação de qualidade consistiu em uma análise prévia do conjunto de artigos resultantes após a aplicação dos critérios de inclusão, baseada nos seguintes pontos:

- **(CQ1)**: O estudo possui uma temática e linguagem clara, além de uma metodologia possível de ser entendida e reproduzida?
- **(CQ2)**: O estudo possui uma boa base de conceituação literária em termos de direitos pessoais, privacidade de dados e Segurança da Informação (SI)?
- **(CQ3)**: O estudo contempla informações relevantes de uma implementação concreta dos regulamentos (LGPD E RGPD)?

- **(CQ4)**: O estudo apresenta dados quantitativos e qualitativos relevantes e bem estruturados sobre o artefato abordado?
- **(CQ5)**: O estudo possui uma conclusão satisfatória sobre os impactos da implementação?

4.2 Ameaças a viabilidade do estudo

O primeiro ponto que pode ser considerado de risco para a viabilidade da RSL é a ausência de avaliação específica de estudos de outras legislações de privacidade de dados além da LGPD e RGPD. No entanto é ressaltar que estudos gerais que impactam a segurança da informação e privacidade de dados não foram excluídos, e além disso outra legislação influente nesta temática é o California Consumer Privacy Act (CCPA) (JUSTICE, 2018), que apesar de ampla influência é uma lei estadual (aplicada ao estado da califórnia) e com exigências mais brandas do que o RGPD.

Outro ponto de ameaça para o trabalho é a avaliação dos critérios de qualidade que foram desenvolvidos pelo autor especificamente para esta RSL. Como a maioria do desenvolvimento e definições deste trabalho foi executado por apenas um autor, seria relevante para os quesitos dos critérios de qualidade a execução de uma avaliação dupla (ou com mais autores) para verificar sua aplicabilidade.

O último ponto de ameaça levantado é a quantidade limitada de repositórios explorados para seleção dos estudos, se limitando aos três portais (especificados na Seção 4.1.3 D). Entretanto, é importante realçar que o periódico Capes é agregador de repositórios abundante, e por isso, não avaliamos esta ameaça como alta para o impacto de nosso estudo.

4.3 Avaliação dos estudos

Ao todo 68 trabalhos foram analisados nesta RSL, dos quais 41 passaram nos parâmetros de qualidade e foram divididos em áreas relacionadas à: (1) processos organizacionais; (2) soluções de SI. A avaliação dos estudos foi feita utilizando a escala Likert de 1 a 5, onde 1 indica a pior avaliação do conteúdo e 5, a melhor. A pontuação foi produzida atribuindo pontos para cada itens de qualidade desenvolvidos na seção 4.1.5. O Quadro 2 expõe a pontuação dos estudos relacionados a governança de dados:

Quadro 2: Avaliação dos estudos de Governança de Dados.

Estudo	Referências	CQ1	CQ2	CQ3	CQ4	CQ5	Nota
E1	Metodologia Scrum: Uma aliada na implementação da LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E2	The critical success factors of GDPR implementation: a systematic literature review	1,0	1,0	1,0	1,0	0,5	4,5
E3	Segurança da informação e da transparência e a proteção de dados na administração pública: lgpd, acesso à informação e os incentivos à inovação e à pesquisa científica e tecnológica no âmbito do estado de minas gerais	1,0	1,0	0,5	0,5	0,5	3,5
E4	Prestação dos serviços públicos à luz da lei geral de proteção de dados (lgpd) – a case study	1,0	1,0	0,5	0,0	0,5	3,0
E5	Segurança da informação: A ISO 27.001 como ferramenta de controle para LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E6	O mapeamento do modelo data management maturity (dmm) a lei geral de proteção de dados (lgpd)	1,0	1,0	1,0	1,0	1,0	5,0
E7	Framework para identificar o nível de conformidade dasempresas brasileiras do setor químico no processo deadequação à lei geral de proteção de dados pessoais	1,0	1,0	1,0	1,0	1,0	5,0
E8	Análise da implantação da gestão de riscos na tecnologia da informação: um estudo de caso	1,0	1,0	1,0	1,0	1,0	5,0
E9	O impacto da lgpd no desenho da política de governança de dados nos municípios: o caso de belo horizonte/mg	1,0	1,0	0,5	0,0	0,5	3,0
E10	LGPD análise dos impactos da implementação em ambientes corporativos: estudo de caso	1,0	1,0	0,5	0,5	1,0	4,0
E11	From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls.	1,0	1,0	1,0	1,0	1,0	5,0
E12	A GDPR-compliant Risk Management Approach based on Threat Modelling and ISO 27005	1,0	1,0	1,0	1,0	1,0	5,0
E13	Achieving GDPR compliance of BPMN process models	1,0	1,0	1,0	1,0	1,0	5,0
E14	Lgpd o novo desafio para as organizações: Exemplos de frameworks para diagnosticar este novo cenário.	1,0	1,0	1,0	1,0	1,0	5,0
E15	Análise de conformidade de processos de negócios em relação a LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E16	Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução	1,0	1,0	1,0	1,0	1,0	5,0
E17	Diagnostic of data processing by Brazilian organizations—a low compliance issue	1,0	1,0	0,5	0,5	0,5	3,5
E18	ISO/IEC 27701: Threats and Opportunities for GDPR Certification. 2020.	1,0	1,0	1,0	1,0	1,0	5,0

Fonte: Implementado pelo Autor.

O Quadro 3 expõe a pontuação dos estudos relacionados a soluções de Segurança da Informação:

Quadro 3: Avaliação dos estudos de Segurança da Informação.

Estudo	Referências	CQ1	CQ2	CQ3	CQ4	CQ5	Nota
E19	Enterprise API Security and GDPR Compliance: Design and Implementation Perspective	1,0	1,0	1,0	0,0	0,0	3,0
E20	Implementação da Lei Geral de Proteção de Dados (Lgpd) no Brasil: Considerações Tecnológicas	1,0	1,0	1,0	0,0	0,0	3,0
E21	The Data Protection Regulation Compliance Model	1,0	1,0	1,0	1,0	0,0	4,0
E22	Impactos da Lei de Proteção de Dados (LGPD)brasileira no uso da Computação em Nuvem	1,0	1,0	1,0	0,0	0,0	3,0
E23	Tracking GDPR Compliance inCloud-based Service Delivery	1,0	1,0	1,0	0,0	0,0	3,0
E24	Automated and Personalized Privacy Policy Extraction under GDPR Consideration	1,0	1,0	1,0	1,0	1,0	5,0
E25	Automated Detection of GDPR Disclosure Requirements in Privacy Policies using Deep ActiveLearning	1,0	1,0	1,0	0,0	1,0	4,0
E26	AMNESIA: A Technical Solution towards GDPR-compliant Machine Learning	1,0	1,0	1,0	1,0	0,0	4,0
E27	How to Improve the GDPR Compliance through Consent Management and Access Control	1,0	1,0	1,0	1,0	1,0	5,0
E28	Integrating Access Control and Business Processfor GDPR Compliance: A Preliminary Study	1,0	1,0	1,0	1,0	1,0	5,0
E29	The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities	1,0	1,0	1,0	1,0	1,0	5,0
E30	Towards a Lawful Authorized Access: A Preliminary GDPR-based Authorized Access	1,0	1,0	1,0	1,0	0,0	4,0
E31	Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent	1,0	1,0	1,0	1,0	1,0	5,0
E32	Automating Cookie Consent and GDPR Violation Detection	1,0	1,0	1,0	1,0	1,0	5,0
E33	User Tracking in the Post-cookie Era: How Websites BypassGDPR Consent to Track Users	1,0	1,0	1,0	1,0	0,0	4,0
E34	Proposta de Mecanismo de Consentimento na Lei Geral de Proteção a Dados - LGPD	1,0	1,0	1,0	0,0	1,0	4,0
E35	ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT using Blockchain Technology	1,0	1,0	1,0	1,0	1,0	5,0
E36	A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR	1,0	1,0	1,0	1,0	1,0	5,0
E37	Data Protection Issues for Smart Contracts	1,0	1,0	1,0	0,0	1,0	4,0
E38	A Relação da Lei Geral de Proteção de Dados e Smarts Contracts Gerados por Blockchain nas Empresas	1,0	1,0	1,0	0,0	1,0	4,0
E39	Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework	1,0	1,0	1,0	0,0	0,0	3,0
E40	Anonymizing Machine Learning Models	1,0	1,0	1,0	1,0	1,0	5,0
E41	Data minimization for GDPR compliance in machine learning models	1,0	1,0	1,0	1,0	1,0	5,0

Fonte: Implementado pelo Autor.

4.4 Metodologia de Apresentação de Resultados e Síntese dos Dados

A metodologia desenvolvida para a síntese dos dados dos trabalhos analisados e a organização de apresentação de resultados é a Revisão Sistemática Narrativa (RSN). A RSN é capaz de considerar estudos quantitativos e mistos apresentados em diversas metodologias e em diferentes conceituações teóricas. Esse estudo busca sintetizar os resultados com um caráter descritivo, com abordagem qualitativa e um raciocínio científico indutivo, dado que, a RSN habilita a reinterpretação e interconexão em estudos que apresentam

diferentes tópicos, posibilitando uma análise investigativa capaz de realizar o cruzamento dos resultados encontrados e o desenvolvimento de novas conclusões sobre o tema. A RSLé iniciada no próximo capítulo.

5 SOLUÇÕES EM PROCESSOS ORGANIZACIONAIS

O desenvolvimento das ações necessárias para a conformidade com a LGPD é um projeto que exige uma mudança na cultura empresarial e na atualização e implementação de processos organizacionais, sobretudo na cultura da gestão e governança das informações pessoais. Tais mudanças envolvem investimentos em recursos tecnológicos, operacionais e humanos, por meio de ações planejadas e relacionadas, para assim, criar uma estratégia capaz de sensibilizar as ações sobre o tratamento de dados (MONTOLLI, 2020).

Com a utilização massiva de TI no meio empresarial, e para evoluir na perspectiva estratégica da proteção dos ativos de informação das organizações, as empresas devem oferecer um conjunto de normas e diretrizes formalizadas capazes de promover segurança em seus sistemas de segurança da informação e nos seus processos internos, que promovem a transferência de dados (ROCHA et al., 2019). Tais diretrizes e normas formam a governança de dados que ocorre por meio da institucionalização de regras, que promovem as ações dos indivíduos associados aos processos organizacionais (SILVA, 2021).

Diante das novas demandas direcionadas às organizações, com muitos ativos de informações e muitas operações sobre dados, um dos principais obstáculos enfrentados está no fato de que as transformações culturais e adaptações às regras das novas legislações de proteção de dados pessoais não são de fácil execução e geralmente não são aplicadas rapidamente como desejado. As legislações demandam o alto custo e investimento para muitas empresas e órgãos públicos em (LIMA, 2020):

- Estrutura humana e operacional;
- Contratação de novos profissionais (também existe investimento em certificações, treinamentos);
- Aquisição de equipamentos;
- Estimular o esforço conjunto entre todas as áreas da organização para promover a mudança cultural.

Este último ponto é visto por muitos como a maior dificuldade, dado que, o apoio dos profissionais para mudança cultural pode ser um problema. Recorrentemente, os funcionários oferecem resistência em mudar ações já praticadas na organização (LIMA, 2020). Este problema deve ser combatido na construção de uma governança de dados amigável à proteção de dados e com o desenvolvimento de processos internos de conformidade com a legislação, pois além dos sistemas informatizados e dos bancos de dados, os processos de trabalhos dos funcionários nos mais diversos setores e áreas devem ser levados em consideração nas atividades cotidianas (MONTOLLI, 2020).

As demandas coletivas para desenvolver processos organizacionais de adequação à LGPD é um ponto essencial para gerar uma cultura de proteção de dados, que ainda não foi consolidada (LUGATI; ALMEIDA, 2022). Logo um período de adaptação coletiva se faz necessário, visando compreender os objetivos das novas disposições sobre proteção de dados, e em adição, entender como as mudanças são aplicadas. Algumas estratégias para uma disseminação coletiva eficiente é a criação de cartilhas, elaboração de informes, produção de instruções rápidas e capacitação direcionada (ROCHA et al., 2019).

Além disso, pode ser desenvolvido um plano de conscientização de segurança da informação que deve estar ligado aos objetivos e com a visão da organização, objetivando fornecer aos funcionários sobre SI e privacidade de dados e contendo programas educacionais focados em treinamentos sobre possíveis ataques, vulnerabilidades, vazamentos e incidentes envolvendo dados pessoais (LIMA, 2020).

Para LUGATI; ALMEIDA (2022), uma mudança cultural coletiva em organização deve forcar em quatro pilares:

- Estabelecimento de uma cultura inovativa;
- Definição e consciência das responsabilidades de cada ator;
- Técnicas de segurança da informação;
- Técnicas que promovem uma comunicação clara e eficiente com os titulares de dados.

Ao estudar a implementação de uma legislação, como a LGPD em uma empresa, é importante verificar as mudanças em seus processos administrativos e de negócio, para analisar os aspectos mais diversos da organização, observando quais as maiores dificuldades encontradas e como cada membro ou divisão organizacional deve se adaptar ao processo de implementação (LUGATI; ALMEIDA, 2022).

Visto que algumas dificuldades da adequação à LGPD estão em problemas como: estabelecimento de políticas formais, gestão de dados, auditorias, mapeamento de dados e mapeamento de fluxo de dados por parte das organizações, torna-se evidente que, alguns métodos, modelos e padrões podem ser de utilidade vital para auxiliar a conformidade com LGPD. Neste capítulo, são apresentadas algumas dessas soluções aplicadas à LGPD e leis de privacidade de dados com princípios semelhantes (MARQUES, 2020). Nas próximas seções são apresentadas:

- Frameworks que desenvolvem artefatos para proteção e privacidade dados;
- Data Management Maturity (DMM) um modelo de referência abrangente para o aperfeiçoamento do gerenciamento e dados;

- Padrão ISO 27.001, norma que aplica boas práticas para Segurança da Informação;
- Metodologias Ágeis aplicada a LGPD.
- Modelagem de Negócio, estudos que utilizam a modelagem BPMN aplicada a LGPD;

5.1 *Frameworks*

Para ampliar a capacidade de desenvolvimento dos requisitos técnicos da LGPD e a diversidade de problemas de inconformidades que podem ocorrer dentro das empresas, torna-se evidente que o nível estratégico e gerencial, assim como, agentes de tratamento e os profissionais que manipulam dados pessoais, necessitam de metodologias e ferramentas que auxiliam na interpretação do estado atual da organização. Além disso, é primoroso o uso de metodologias capazes de promover a evolução na privacidade de dados.

Um dos métodos interessantes para o aumento da visualização de dados e de processos internos à luz dos requisitos da LGPD, são os *frameworks* que desenvolvem ferramentas de trabalho visual, evidenciando de forma mais clara como a privacidade de dados é abordada e qual seu nível de influência em cada atividade cotidiana da empresas. Um *framework* preparado para trazer esses benefícios é o LGPD Model Canvas.

O LGPD Model Canvas é baseado no modelo *Business Model Canvas* (BMC). O BMC desenvolve um quadro de modelos de negócios que serve como atalho visual e simplifica as atividades organizacionais, tentando, ao máximo, minimizar a carga de complexidade na variedade de processos de negócio, em especial em grandes organizações (FERREIRA; OKANO, 2021).

Os modelos produzidos no BMC são desenvolvidos em uma tela simples e visual de uma página onde é possível projetar, inovar e dialogar sobre os modelos de negócios (FERREIRA; OKANO, 2021). Além disso, são capazes de evidenciar tarefas que não estão expostas de forma transparente para os funcionários, e consequentemente, ajuda a melhorar a comunicação e o aumento da percepção nas atividades de negócio.

Inspirado em uma ferramenta visual focada para a legislação de proteção de dados, o *framework* LGPD Model Canvas também foi inspirado em métodos ágeis e no *privacy by design* proposto pelo RGPD, ou seja, um modelo de visualização que privilegia a privacidade de dados nos aspectos organizacionais, sugerindo que o cuidado com os dados pessoais devem ser resguardados desde o início do projeto e desde a concepção de todos os processos. O principal objetivo do *framework* é ser aplicado em empresas que buscam se adequar a LGPD (OKANO et al., 2021).

O *framework* é executado em duas etapas, a primeira é definida como o momento presente da organização onde todos os processos que manipulam dados pessoais são avaliados, para assim, registrar o estado atual de como a proteção de dados está sendo

efetivada. A segunda etapa é definida como um mapeamento focado no futuro, alinhando os objetivos empresariais com as lacunas e oportunidades encontradas na primeira etapa.

Para executar o LGPD Model Canvas a organização deve promover *brainstorming* para que grupos multidisciplinares possam gerar ideais distintas. Com essa atividade, os colaboradores são influenciados à cultura organizacional, focada em incluir a privacidade no centro dos processos, e ampliando a discussão sobre quais os objetivos principais da empresa e qual o valor das disposições da LGPD para a organização (OKANO et al., 2021). Outra vantagem central citada por OKANO et al. está no fato de que a criação de dinâmicas participativas geram agilidade e eficiência no cotidiano empresarial, desenvolvendo uma aprendizagem conjunta sobre os conceitos do regimento brasileiro.

Optando pela divisão em nove blocos, o *framework* LGPD Model Canvas efetiva um esforço colaborativo e define formalmente normas para o preenchimento descritivo. O preenchimento deve ocorrer para cada processo. Também é necessário alinhar os principais produtos/serviços que a empresa oferece, seus papéis como controlador/operador, assim como as entidades (internas e externas) e a complexidade envolvida nos processos que tratam os dados pessoais. A Figura 5 é um exemplo de modelo do *framework* (OKANO et al., 2021).

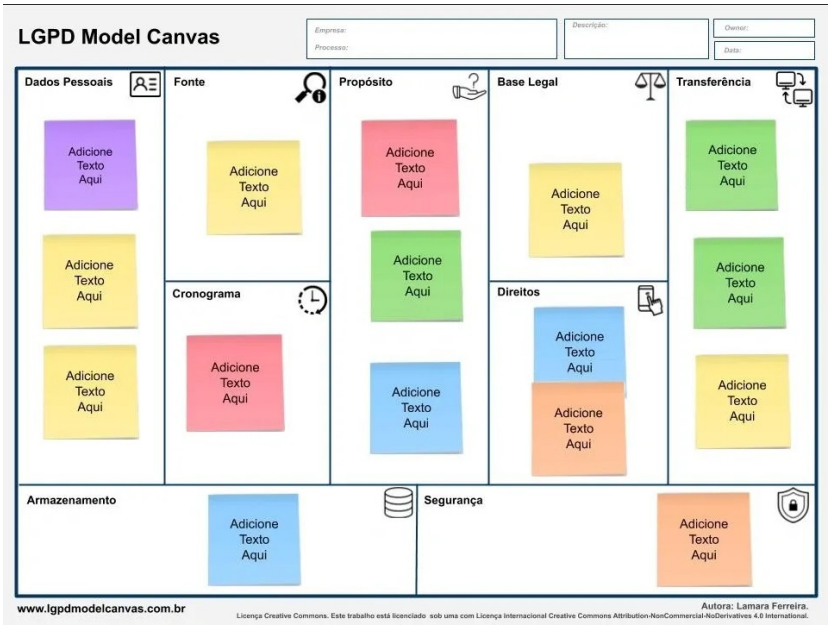

Figura 5: LGPD MODEL CANVAS.
Fonte: (OKANO et al., 2021)

Outra ferramenta explorada no estudo de OKANO et al. (2021) é FRAMEWORK LGPD, que foi criado avaliando referências e soluções em várias legislações internacionais como RGPD, CCPA (*California Consumer Privacy Act*) e LGPD, para aliar às atividades organizacionais para solucionar processos inadequados com a lei brasileira.

O FRAMEWORK LGPD desenvolvido por SILVA et al. (2021) foi criado para validar o nível de conformidade e guiar empresas para adequação com a LGPD, especificando de um conjunto de etapas e tarefas a serem executadas. A ferramenta é composta pelas fases: de iniciação, reconhecimento, validação, desenvolvimento e encerramento.

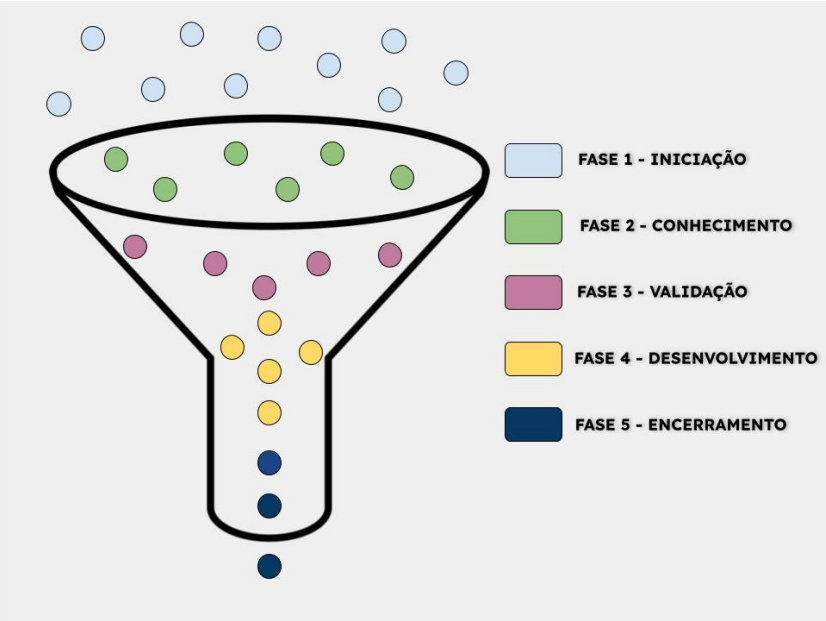

Figura 6: FRAMEWORK LGPD.
Fonte: Adaptado de (OKANO et al., 2021)

Fase 1 Iniciação - Essa fase especifica o alinhamento do nível gerencial da organização, que determina o início do projeto de adequação com a LGPD. É nesta fase que todos os funcionários e entidades relacionadas com a organização são informadas e adicionadas ao esforço de adequação, incluindo ainda a definição de um comitê de governança de dados (e suas devidas lideranças). O comitê deve conter figuras interdisciplinares capacitados, nos requisitos de proteção e privacidade de dados, assim como, indivíduos conhecedores das estratégias e organização interna (departamentos) da organização.

Fase 2 Conhecimento - Nesta fase é necessário, assim como o LGPD Model Canvas, descrever o estado atual de proteção de dados. Essa atividade deve mapear quem transmite informações pessoais, quais tipos de dados são manipulados, como é o processo de coleta, armazenamento e acesso de dados.

Fase 3 Validação - Fase que avalia se o levantamento dos dados está de acordo com os princípios da LGPD e analisar quais os impactos que a organização sofrerá das novas normas. Em muitos casos, é prudente executar auditorias (externas ou internas) para identificar riscos de proteção de dados e a privacidade dos indivíduos. Outros riscos que podem ser mapeados nesta etapa são os riscos de violação e riscos de aplicação de sanções e multas, assim como, o tratamento de dados com empresas terceiras ou órgãos públicos.

Fase 4 Desenvolvimento - Neste momento já é possível determinar as atividades específicas dos membros do comitê e dos agentes de tratamento, e em adição, produzir uma política de segurança de dados pessoais. Por fim, é desenvolvido um plano de ações com todas as atividades que serão executadas para a conformidade com a LGPD. Dependendo das necessidades da empresa, a etapa de desenvolvimento pode buscar a nomeação de um encarregado de dados capacitado a ser responsável em atender solicitações dos titulares de dados e requisições da ANPD. Outra atividade relevante do encarregado é na comunicação interna, alinhamento de objetivo e atualização de processos e documentação.

Fase 5 Encerramento - Após o desenvolvimento das etapas anteriores, a organização é capaz de atribuir esforços para a produção de uma documentação sobre a análise e os resultados obtidos. A partir desse momento, é possível alocar recursos e investir em ferramentas necessárias para promover as ações planejadas. O documento produzido deve ser um relatório com definições de recursos e funcionários destinados a projetar e operar na proteção de dados, indicando, ao final, qual o nível que a organização se encontra para a adequação com os requisitos legislativos.

A principal característica dos dois *frameworks* é avaliar os processos e verificar a adequação com a LGPD. Ambos possuem instrumentos semelhantes como *brainstorming* para realizar análises e coletas das minúcias dos processos internos, entretanto realizam métodos e produzem artefatos diferentes. A grande vantagem do LGPD Canvas Model é o seu aspecto visual enquanto o FRAMEWORK LGPD não especifica muitas ferramentas, além de modelagem de fluxo de dados e da produção de uma documentação formalizada (SILVA et al., 2021).

É possível verificar que a utilização destes métodos facilita as operações sobre dados pessoais, além de permitir uma visão mais ampla sobre os tratamentos de dados, o que favorece o diagnóstico empresarial, tornando-o mais organizado, aumentando o entendimento sobre a LGPD e realizando o engajamento de múltiplos setores e departamentos.

A pesquisa de OKANO et al. (2021) realizou entrevistas com profissionais de empresas que buscam se adequar a LGPD. O levantamento apontou que 60,2% dos entrevistados consideram métodos como o LGPD Canvas Model relevantes para auxiliar na implantação e adequação à LGPD. Apenas 8% não considerou o método relevante, no entanto, mais de 30% demonstraram desconhecimento sobre ferramentas focadas na LGPD.

A grande limitação dos *frameworks* apresentados é a sua utilização com TIC, nesse caso, maiores testes e estudos de caso devem ser empregados para associar os *frameworks* com os sistemas utilizados nas empresas (OKANO et al., 2021).

5.2 *Data Management Maturity* (DMM)

Nessa seção é explorado o modelo *Data Management Maturity* (DMM) do Instituto *Capability Maturity Model Integration* (CMMI). O DMM se define como um modelo de referência abrangente para o aperfeiçoamento de processos, que visa auxiliar uma organização a gradativamente alcançar um nível de maturidade avançado no gerenciamento de dados.

O modelo busca representar o estado atual da empresa em relação aos seus dados e define um conjunto de boas práticas para ajudar na governança das informações institucionais, ajudando as organizações a avaliar suas capacidades, identificar pontos fortes e lacunas, assim como, alavancar seus ativos de dados para melhorar o desempenho dos negócios.

A grande razão para a interconexão desse modelo com os requisitos de proteção de dados é o fato de que modelos de administração, especialmente modelos completos como o DMM, têm se tornado relevantes por promover velocidade, robustez e eficiência operacional no desenvolvimento de sistemas seguros e processos que operam sobre dados.

Outro ponto relevante é a capacidade do modelo DMM em desenvolver um gerenciamento de dados entre partes interessadas, implementando medidas precisas para gerenciar acordos e a comunicação de partes interessadas, desde a concepção dos sistemas, ou projetos de uma empresa (MARQUES, 2020). Isso é possível, pois a principal função do DMM é centralizar a gestão de dados e integrar os sistemas e processos ao modelo, gerando uma precisão de dados eficiente.

A LGPD exige medidas para proteger dados pessoais, aprimorar a rastreabilidade dos dados e promover prestação de contas com titulares e entidades como a ANPD. Logo, algumas características do DMM revelam um otimismo para o uso na conformidade com a lei brasileira, visto que as práticas funcionais do DMM são próximas dos requisitos solicitados para gestão de dados pessoais segura, propostas pelo regulamento (MARQUES, 2020).

A maturidade do gerenciamento de dados (objetivo explícito do modelo) é determinada pela capacidade da organização que aplica o modelo em conseguir controlar e gerir eficientemente seus dados de forma estratégica e planejada. O modelo está estruturado em duas estruturas principais: categorias e áreas de processos. As estruturas estão expostas na Figura 7.

CATEGORIAS	ÁREAS DE PROCESSO
Estratégia de Gestão de Dados	Estratégia de Gestão de Dados
	Comunicação
	Função de Gestão de Dados
	Caso de Negócio
	Financiamento do Programa
Governança de Dados	Gestão de Governança
	Glossário de Negócios
	Gestão de Metadados
Qualidade de Dados	Estratégia de Qualidade de Dados
	Perfil de Dados
	Avaliação da Qualidade dos Dados
	Limpeza de Dados
Operações de Dados	Definição dos Requsitos dos Dados
	Gestão de ciclo de vida dos dados
	Gestão de Provedor
Plataforma e Arquitetura	Abordagem Arquitural
	Padrões Arquiteturais
	Plataforma de Gestão de Dados
	Integração de Dados
	Dados Históricos, Arquivamento e Retenção
Processos de Suporte	Medição e Análise
	Gerência de Processos
	Garantia de Qualidade de Processos
	Gestão de Risco
	Gestão de Configuração

Figura 7: Categorias e Áreas de Processos DMM,
Fonte: Adaptado de ((CMMI), 2019).

A categoria de Estratégia de Gestão de Dados envolve processos que: definem metas e objetivos para gestão de dados, estabelecem métricas e padrões formais para comunicação e publicações, estabelecem lideranças internas, definem justificativas para o financiamento e alocação de recursos para a gestão de dados. Na categoria de Governança de Dados, os processos focam em desenvolver a estrutura operacional para que os dados sejam operados corretamente ((CMMI), 2019).

Na categoria de Qualidade de Dados, os processos são focados em determinar estratégias integradas e institucionais para manter o nível de qualidade dos dados. A qualidade é alcançada com três atividades: compreender o conteúdo e as regras dos dados geridos, desenvolver método de avaliação para qualidade dos dados e o processo de limpeza de dados, utilizado para validar e corrigir informações.

A categoria de Operação De Dados tem processos que garantem que a gestão fique alinhada com os objetivos de negócio da organização. Além disso, é relevante o processo de ciclo de vida dos dados que realiza o mapeamento e fluxo das informações desde sua entrada, até a eliminação. A categoria de Plataforma e Arquitetura foca nos processos habilitados em projetar uma abordagem arquitetônica, para cumprir todas as operações de informações necessárias pela empresa. Por fim, a categoria de Processos de Suporte especifica atividades, com o intuito de medir e analisar as técnicas de gerenciamento de

dados aplicadas.

Outra estrutura que faz parte do DMM são as capacidades dos processos que especificam um nível de maturidade para definir o quão efetivo é o gerenciamento de dados e como cada processo foi melhorado com diferentes práticas. Os cinco níveis de capacidade são ((CMMI), 2019):

- Executado - Os dados são gerenciados apenas como um requisito para a implementação de projetos ou execução de sistemas/processos.
- Gerido - Há consciência da importância do gerenciamento de dados como um ativo crítico de infraestrutura.
- Definido - Os dados são tratados no nível organizacional como críticos para o desempenho bem sucedido de uma missão na organização.
- Medido - Os dados são tratados como uma fonte de vantagem competitiva, já que nesse nível existem medições que apontam as fragilidades ou evoluções dos processos;
- Otimizado - Os dados são vistos como essenciais para a sobrevivência em um mercado dinâmico e competitivo.

O trabalho de MARQUES (2020) expõe algumas medidas do DMM que podem apoiar na promoção de conformidade com a LGPD. O principal contribuinte que a ferramenta é capaz de promover nesse tópico é a visibilidade de seus dados, assim como as fontes e fluxos das informações dos titulares em uma organização. A LGPD exige uma governança de dados direcionada aos direitos dos titulares, logo, o DMM pode resolver muitos dos problemas de tratamento de dados.

Um primeiro exemplo de como isso pode funcionar é o fato do modelo poder garantir uma gestão clara sobre como um dado pessoal é coletado, onde e por quanto tempo será arquivado e quais os processos e procedimentos que podem gerar a finalização do tratamento de dados, de forma transparente e ética. A gestão de ciclo de vida de dados no DMM pode auxiliar em requisitos específicos da LGPD, como o consentimento, o direito de ser esquecido e a consulta de informações e detalhamento de operações realizadas nos dados pessoais, o que serve não apenas para os titulares, como também, para que a organização esteja salvaguardada para qualquer demanda legal de entidades reguladoras (MARQUES, 2020).

Outra funcionalidade relevante é encontrada no mapeamento dos dados organizacionais. Essa atividade é capaz de viabilizar uma rastreabilidade interna na organização, o que melhora o controle de quais funcionários, setores ou sistemas realizaram operações de dados e quais estão com a posse ou acesso dos dados, aumentando assim o nível de

proteção de dados e de segurança da informação. Além disso, MARQUES também define que a rastreabilidade é capaz de definir quais processos internos são afetados pelos dados e quais procedimentos possuem prioridade, avaliando sempre a complexidade e criticidade na operação de dados.

As práticas funcionais recomendadas pelo DMM buscam se alinhar com os princípios empresariais e, com esforço interno, é capaz de aprimorar procedimentos que possam se adequar a aspectos específicos da LGPD, efetivando a investigação de vulnerabilidades na gestão dos dados e na especificação dos riscos encontrados durante a execução do modelo. Contudo, não há uma especificidade profunda quanto aos ajustes necessários para que o DMM possa ser completamente aplicado a LGPD, em adição, é necessário entender como a modificação dos processos organizacionais podem se alinhar com outras modelagem e normas de segurança de segurança da Informação como a ISO 27001.

5.3 Padrões de Referência

Uma das diretrizes mais relevantes da LGPD, e de muitas legislações que resguardam dados pessoais, é o desenvolvimento de medidas de segurança, sejam técnicas ou administrativas para proteção de dados. Para isso, muitas organizações optam por realizar a adoção de padrões de segurança reconhecidos internacionalmente e construídos por instituições renomadas no ramo de normas e padrões. A ISO 27001 é uma das normas mais referenciadas no meio organizacional para realizar a segurança da informação, concedendo práticas robustas para resguardar e proteger dados corporativos (incluindo dados pessoais) (TEIXEIRA; SILVA; PEREIRA, 2019b).

Os Artigos 49 e 50 da LGPD são os artigos que citam diretamente a obrigação das instituições na utilização de padrões eficientes, na promoção de segurança dos dados. Nesse contexto, a ISO 27001 é qualificada para aprimorar requisitos gerais para implementar, monitorar e melhorar a administração organizacional nos aspectos de segurança dos dados, além de possuir ferramentas para mitigação de risco, fatores interessantes para cumprir uma lei de privacidade de dados (LIMA, 2020).

Para adotar a norma, um dos primeiros passos de execução das empresas é a criação de uma política regulamentadora das práticas em SI (PIURCOSKY et al., 2019). A Política de Segurança da Informação, ou PSI, é uma documentação que determina técnicas e procedimentos sobre o fluxo de informação interno e externo e quais entidades ou sistemas processam e transferem tais informações. Os princípios da PSI precisam ser minuciosos e disseminados a todos os colaboradores da segurança das informações empresariais (ROCHA et al., 2019).

Para a criação de uma PSI coesa e efetiva, a norma 27001, que a alta administração da organização desenvolva planos de segurança envolvendo pessoal de diversos setores

como o jurídico, de engenharia, de infraestrutura, de recursos humanos, dentre outros. Em muitos casos, é recomendável a criação de uma comissão de SI para melhorar os alinhamentos internos e a tomada de decisão (PIURCOSKY et al., 2019).

A comunicação interna é mais uma obrigação da comissão à frente da segurança de dados. Nesse caso, é importante divulgar e estabelecer métodos de comunicação organizacional eficientes para informar funcionários, clientes e colaboradores terceiros, sobre qualquer mudança de diretriz ou apontar riscos e incidentes associados a SI. Treinamentos internos constantes sobre as políticas organizacionais são atividades essenciais para preservar e aprimorar a proteção das informações (ROCHA et al., 2019).

A ISO 27001 propõe instruções globais contendo subdivisão em onze seções que abordam procedimento de verificação e tratamento de riscos. Elas são listadas por: política de segurança da informação; organização da SI; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de SI; gestão de incidentes de segurança da informação; gestão da continuidade do negócio, e conformidade. A norma formaliza 7 fundamentos (ROCHA et al., 2019):

1. Análise de risco - A norma propõe analisar os riscos de segurança a cada mudança administrativa ou de processos, que causam alterações no tratamento de informações. Também é relevante descrever os riscos identificados, especificando como podem ocorrer, as decorrências e o grau de ameaça;

2. Comprometimento da alta gestão - A norma exige que a alta administração se responsabilize com o desenvolvimento do Sistema de Gestão de Segurança da Informação - SGSI e se responsabilize pela SI;

3. Definição de objetivos e estratégias - O planejamento da empresa deve conter objetivos de segurança e estratégias específicas para a finalidade.

4. Recursos e Competências - A norma requer que a organização garanta recursos técnicos e humanos para cumprir suas metas de segurança;

5. Documentação da Informação - Todas informações devem ser verificáveis, para isso, é necessária atualização constante para garantir fidelidade e desenvolver métricas para aprovação e autorização na atividade de alteração de dados;

6. Acompanhamento de desempenho - Indicadores devem ser aplicados sobre as atividades executadas para comparar com os objetivos estabelecidos;

7. Melhoria contínua - Assim que se alcance os objetivos do SGSI, é exigido que a organização implante medidas de melhoramento contínuo para corrigir inconformidades derivadas de atividades e processos futuro.

O objetivo final da norma ISO 27001 é utilizar as políticas do PSI, em conjunto com planos de tratamento de risco e auditorias internas para desenvolver o Sistema de Gestão de Segurança da Informação - SGSI. O SGSI é o sistema (não necessariamente automatizado) capaz de incluir toda abordagem organizacional nas ações de proteção para assegurar a proteção das informações empresariais, seguindo os principais princípios da SI. Como visto na pesquisa de ROCHA et al. (2019), a norma também está diretamente relacionada com os principais requisitos da LGPD.

O tempo para a preparação da certificação ISO é variável, pois requer a implementação e adoção de todos os requisitos, políticas, procedimentos, e controles requeridos para todos os âmbitos da organização. O *roadmap* típico de implementação de um SGSI é especificado pelo próprio ISO e é apresentado na Figura 8 (ISO/IEC, 2019):

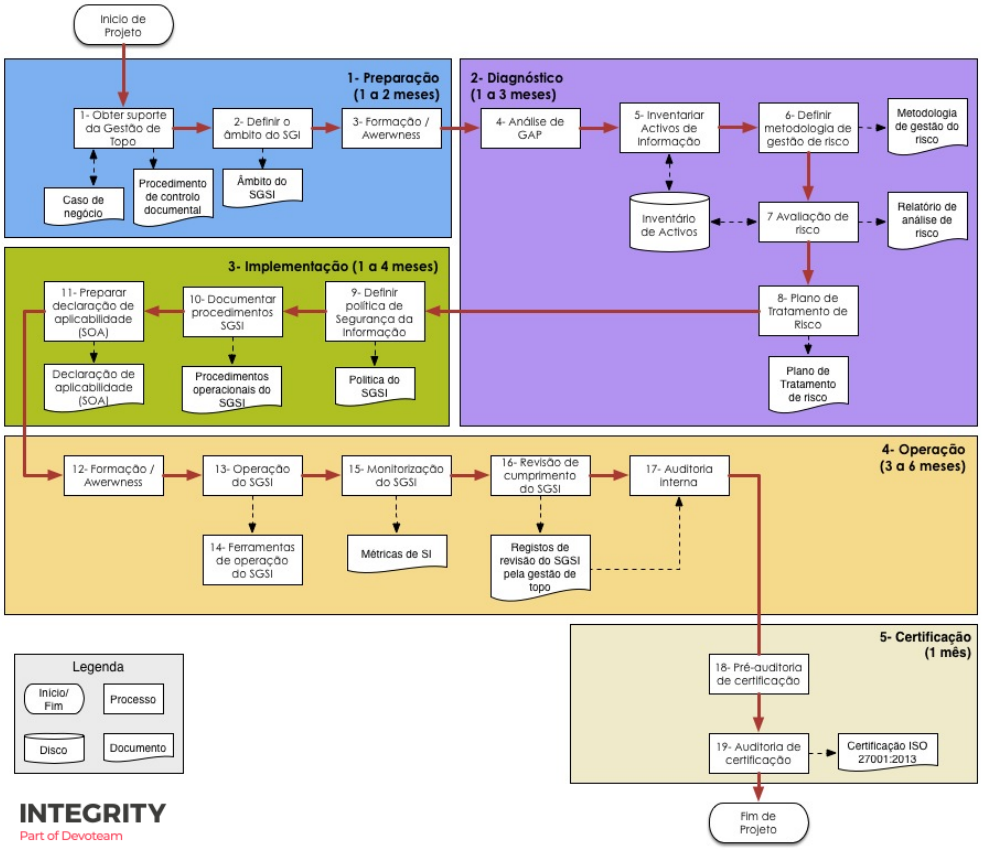

Figura 8: *Roadmap* ISO 27001
Fonte: (ISO/IEC, 2019)

A pesquisa de ROCHA et al. (2019) elaborou uma comparação entre as disposições da LGPD e da ISO 27001, para determinar diretrizes capacitadas a ajudar as empresas a cumprir os requisitos da legislação. O resultado observou que a lei brasileira possui uma correspondência direta e pode utilizar 67,86% dos itens obrigatórios da norma. Os 32% de não correspondência se referem à documentação mínima requerida pelo ISO, o que não significa que as práticas do padrão são conflituosas com a conformidade da LGPD.

Excluindo aspectos específicos, como as relações com a autoridade nacional de dados ANPD, o estudo observou que o padrão 27001 cobre 80% da lei de dados e pode ser considerada uma das melhores regras de boas práticas para o controle da adequação a privacidade e proteção de dados.

Outros padrões da série 27000 podem ser utilizados em conjunto para elaborar o SGSI, a ISO 27002 pode ser aliada a norma anterior adicionando mais controles e boas práticas que podem ser usados como guias para uma gestão de risco (DIAMANTOPOULOU; TSOHOU; KARYDA, 2020).

Já o estudo de FLORES; PERUGACHI (2023) explica a possibilidade do desenvolvimento de modelagem de ameaças para gerenciamento de riscos, usando a ISO 27005 como base para integrar os controles de segurança da ISO 27001/27002, a modelagem implementa um catálogo inicial de ameaças que possibilita um tratamento de risco mais eficiente. A modelagem é composta composta na ISO 27005 compõe um processo com as seguintes etapas:

1. Avaliação de riscos - requer a criação de perfis de ameaças e de atacantes. Neste modelo é possível definir uma árvore de decisão denominadas 'árvores de ataque' e 'árvores de defesa' para quantificar os níveis de risco inerentes e residuais. As árvores de ataque buscam determinar caminhos (ou limites) plausíveis para os invasores executarem ameaças com sucesso em um sistema vulnerável. Já as árvores de defesa descrevem controles que objetivam contra-atacar ameaças.

2. Tratamento de riscos - Envolve descobrir o risco residual após a aplicação de contramedidas, ou seja, avaliar a efetividade das ações desenvolvidas árvore de defesa correspondente.

3. Comunicação, Monitoramento e Aceitação de riscos - A comunicação e validação de uma estratégia de gestão de riscos depende da análise da eficácia dos controles. A revisão dos resultados é um processo importante para monitorar os níveis de risco e até aceitá-los ou revisá-los. Os resultados desta revisão ajudam as organizações a decidir se é necessário iniciar um novo ciclo de gestão de riscos até que os níveis de risco sejam reduzidos ou aceitar os níveis atuais.

Por último a ISO 27701, é um regimento recente de 2019 que visa gerir os processos de proteção da captura, responsabilização, disponibilidade, integridade e confidencialidade dos dados pessoais. Esta norma é mais uma comprovação de como o cuidado e a preocupação com dados pessoais se torna cada vez mais relevante, no entanto, como apontado por LACHAUD (2020) a abordagem promovida pela ISO não seja totalmente semelhante ao RGPD, o que pode gerar problemáticas quanto a correspondência entre as certificações entre a ISO e o RGPD ou até a LGPD.

A ISO 27701 torna a proteção de dados dependente da segurança da informação (criando dependência com a ISO 27001), onde promove uma abordagem baseada em riscos, oferecendo a identificação e redução dos riscos de segurança da informação aplicáveis ao gerenciamento e armazenamento de ativos de TI relacionados a dados pessoais.

Nota-se que os desafios que as organizações enfrentam para aderir aos requisitos das normas ISO e conseguir a certificação podem ser custosos, além disso, não existe um prazo definido para finalizar todas as demandas. Por isso, além dos padrões, as empresas buscam métodos ágeis para finalizar a conformidade.

5.4 Metodologias Ágeis de Gerenciamento de Equipe

Ao longo de toda a jornada que a lei brasileira de dados passou, desde de sua elaboração, aprovação e sancionamento de todos os seus artigos, muitas organizações públicas e privadas sofreram dificuldades na interpretação das definições dos requisitos e na percepção dos impactos reais causados em seus trabalhos. Diante disso, boa parte das organizações se encontram atrasadas na implementação da lei, o que influencia na busca por metodologias que promovam agilidade, a fim de evitar qualquer sanção aplicada à organização.

Para isso, a adoção de metodologias ágeis como a Metodologia Scrum pode ser vista como uma opção e uma oportunidade para realizar adaptações constantes de forma organizada para problemas complexos, envolvendo a troca de conhecimento entre profissionais com diferentes capacitações.

Enquanto o primeiro objetivo da metodologia foi agilizar o processo de desenvolvimento de software, o Scrum se demonstra versátil e útil para outras aplicações e pode ser utilizado para gerenciar projetos complexos, recursos humanos, entre outras áreas. O estudo de FILHO et al. (2023) buscou apontar as definições do Scrum, seus métodos, papéis e características para analisar sua usabilidade no gerenciamento do processo de conscientização e de conformidade com a LGPD.

Se baseando nos princípios de flexibilidade, colaboração e adaptatividade, as metodologias ágeis podem ser aplicadas para ajudar empresas a desenvolver um diferencial de mercado, se diferenciando de seus concorrentes por ganhar a confiança dos consumidores, ao desenvolver processos organizacionais eficientes. Se relacionando com a LGPD, o Scrum pode demonstrar a preocupação com o tratamento de dados pessoais, FILHO et al. (2023) abordam algumas atividades da metodologia que podem ser aplicados na gestão de dados pessoais:

- Formar uma equipe Scrum, incluindo todos os membros necessários como o Scrum Master, e membros que representem os objetivos de negócio;

- Nomeação de um encarregado pelo tratamento de dados pessoais;
- Realizar uma análise do impacto do tratamento de dados pessoais nos processos e sistemas da organização, com o objetivo de reconhecer prioridades e riscos;
- Aplicar um mapeamento e dados pessoais;
- Segurança da Informação;
- Avaliar as bases legais para o tratamento de dados pessoais da organização;
- Elaborar políticas e procedimentos internos sobre o tratamento de dados;
- Executar a revisão de contratos relacionados ao tratamento de dados;
- Treinamento de funcionários sobre a LGPD;
- Implementação de um canal de comunicação;
- Realizar revisões de cada *sprint* para demonstrar a evolução dos objetivos e viabilizar *feedback*.

Diante dos pontos levantados, fica evidenciado que a utilização do Scrum para apoiar a conformidade com a LGPD amplia mais uma vez a necessidade de uma intervenção organizacional, para uma criação de uma cultura de proteção de dados. Essa metodologia ágil pode ser uma boa opção, pois provê aos profissionais um trabalho com ciclos curtos e frequentes, com entregas colaborativas, podendo gerar impacto e mudanças rápidas nas políticas de tratamento de dados das empresas (FILHO et al., 2023).

5.5 Modelagem de Negócio

Os processos de negócio de uma organização são as atividades que especificam a execução das obrigações dos funcionários e como toda a sequência lógica de tarefas deve ser executada. Nessa direção, a modelagem dos processos de negócio propõe artefatos que simbolizam os processos da empresa e podem ser utilizados para modelar os procedimentos que envolvem questões de privacidade e requisitos da LGPD.

Uma das modelagens de negócio mais utilizadas no meio acadêmico e corporativo é o BPMN. Quando utilizado de forma a integrar processos complexos, o BPMN é capaz de gerar um programa de governança de negócio. Utilizar esse método na adequação com a LGPD gera uma investigação de conformidade, através de um padrão de linguagem visual e de fácil interpretação entre modeladores de negócio.

O trabalho AGOSTINELLI et al. (2019) verifica que muitas das modelagens de processos de negócio são adequadas para expressar a colaboração entre partes interessadas

e em compreender fluxos de dados, no entanto, pouco foi avançado para modelar processos, a fim de evitar violações de dados ou de privacidade. Diante desta demanda, o estudo defende que a proteção de dados dos cidadãos deve ser protagonista nos modelos de negócio e deve ser introduzida a partir do design dos processos e não como uma ação corretiva. O estudo propõe modelar as principais restrições de privacidade expostas no RGPD europeu (restrições que também são vistas na LGPD).

Tomando como exemplo a aplicação de modelagem BPMN, focadas no RGPD para uma companhia telefônica, são apresentados sete padrões de privacidade modelados sem que nenhum símbolo BPMN adicional fosse necessário. Os sete padrões desenvolvidos foram (AGOSTINELLI et al., 2019):

1. Violação de dados - Em caso de violação de dados, o controlador deve iniciar medidas para recuperação de dados violados, identificar o volume e quais titulares foram afetados pelo tratamento. O vazamento deve ser informado à autoridade nacional e as medidas relacionadas aos titulares afetados podem ser, desde a divulgação da violação, ou encerramento do consentimento/tratamento. O exemplo de modelagem BPMN dessa restrição de privacidade está na Figura 9;

2. Consentimento - Se for necessário, na lei, a coleta de consentimento do titular de dados para o controlador, é necessário solicitar consentimento explícito e claro antes de iniciar o tratamento. Além disso, o controlador deve explicitar os aspectos do tratamento para deixar o titular ciente antes de ceder seus dados.

3. Direito de Acesso - Ao enviar um pedido de direito de acesso sobre os seus dados, o Titular requer do controlador: recuperar dados associados ao titular, recuperar qualquer processamento realizado sobre os dados e, por fim, retornar a coleta para o titular.

4. Direito de Portabilidade - O titular ao pedir a portabilidade de seus dados para alguma organização terceira, deve esperar a comunicação entre as partes para realizar a portabilidade com sucesso.

5. Direito da finalização do Tratamento - O titular requisita o encerramento de qualquer tratamento realizado pelo controlador sobre seus dados pessoais.

6. Direito de Correção de Dados - O titular requisita a retificação de dados incorretos em posse do controlador.

7. Direito de Esquecimento - O titular de dados requisita a recuperação e o apagamento de seus dados. O operador deve avaliar as bases legais do tratamento, e caso a exclusão seja legalmente possível, o esquecimento é realizado.

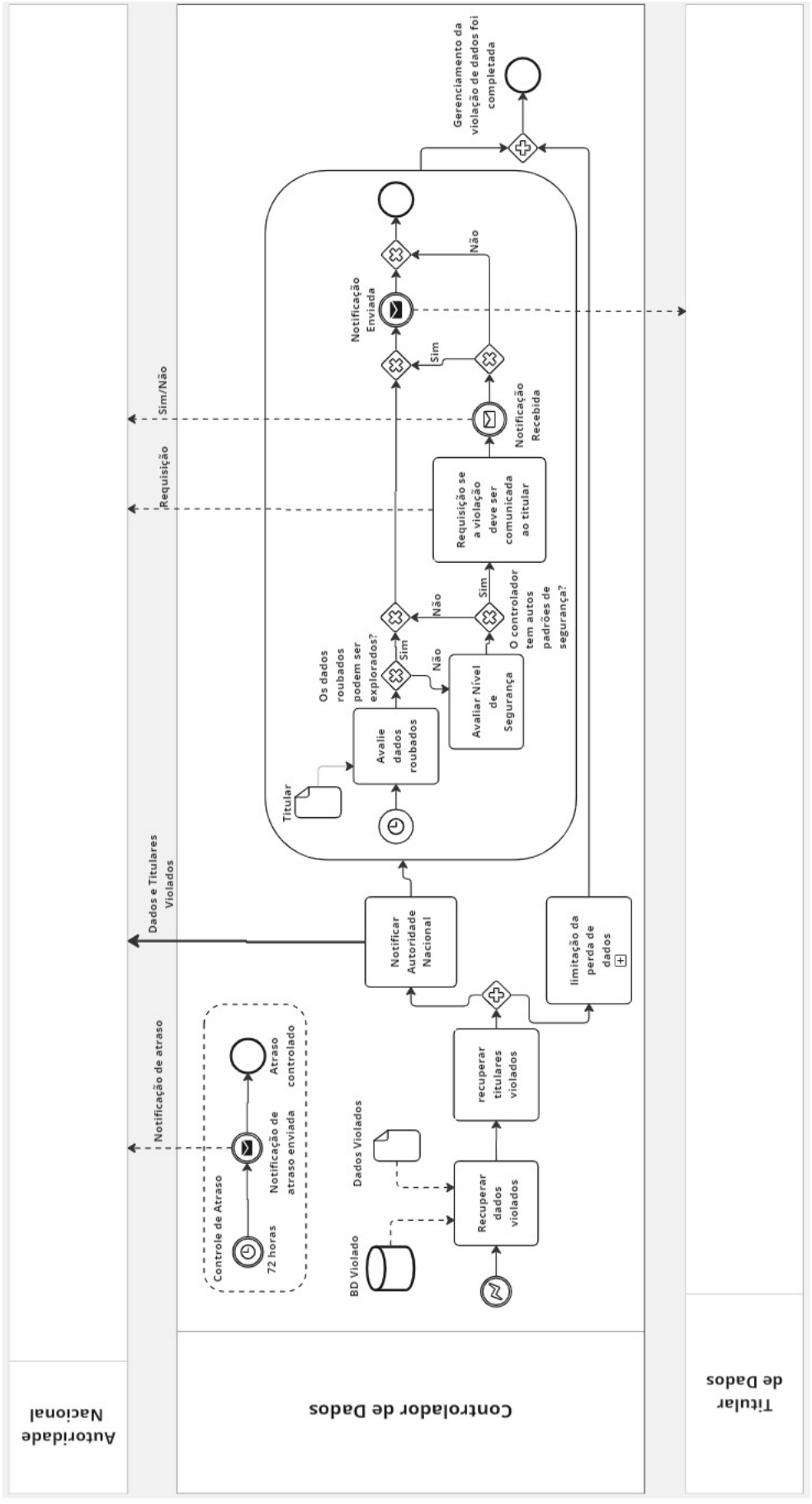

Figura 9: Padrão BPMB de Violação de Dados
Fonte: Adaptado de (AGOSTINELLI et al., 2019), tradução livre feita pelo Autor.

De forma semelhante, o estudo de JÚNIOR (2020) investiga a conformidade dos processos de negócio diante das exigências da LGPD, propondo um método de modelagens de processos utilizando a notação BPMN. Método LGPD4BP (LGPD *for Business Process*) é a modelagem proposta no trabalho, e é composto por:

- Um questionário de avaliação da conformidade dos processos em relação à LGPD;
- Um Catálogo de Padrões de Modelagem;
- Um Método de Modelagem de processos em conformidade com a LGPD.

Enquanto o questionário foi criado para avaliar se um processo de negócio está em conformidade com a LGPD, o Catálogo de Padrões e Modelagens foi criado para modelar requisitos específicos da lei. No catálogo, foram modelados 9 padrões: Consentimento, Direito de Acesso, Transferência internacional de dados, Portabilidade, Vazamento de Dados, Revisão de tomada de decisão automatizada, Retificação de Dados, Direito de Eliminação ou Esquecimento, Confirmação da existência de tratamento e direito de acesso. Na Figura 10 é exemplificada uma das modelagens.

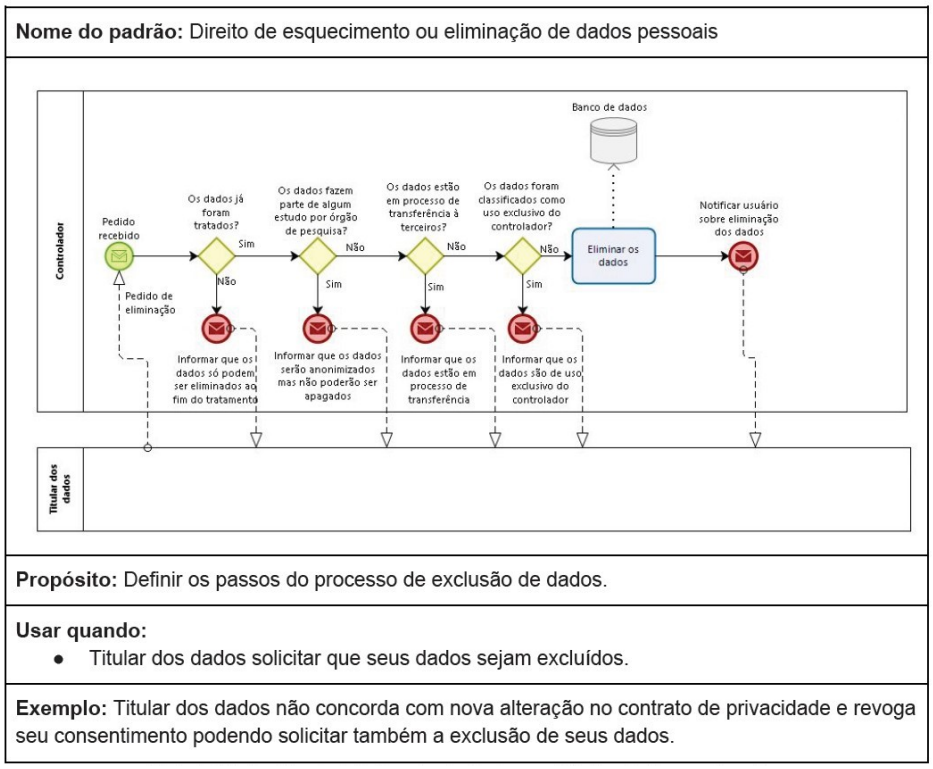

Figura 10: Padrão BPMB de Direito ao Esquecimento.
Fonte: (JÚNIOR, 2020)

Já o Método de Modelagem, é apresentado como um processo em BPMN, criado para orientar o modelador de negócio em modelar um processo, ou corrigir algum modelo não compatível com a LGPD. O método possui 16 etapas, nos quais os padrões (como os apresentados no catálogo) são vistos como artefatos de entrada. Para uma melhor interação com os modelos propostos, tanto o Catálogo de Padrões de Modelagem, como o Método de Modelagens, estão disponíveis em um site disponibilizado pelo autor (https://sites.google.com/view/lgpd4bp)

Para testar a modelagem em um exemplo concreto, o método LGPD4BP foi utilizado em uma instituição de ensino (escola de ensino fundamental e médio). Ao todo foram encontradas 12 inconformidades relacionadas, principalmente, a ausência de consentimento, indefinição de bases legais e especificidades para tratamento de dados de crianças. Todos os pontos foram corrigidos utilizando, tanto os padrões já criados no catálogo, como utilizando o método de modelagem. Ao todo foram necessárias 15 novas ações.

Com isso, o estudo de JÚNIOR avalia que o LGPD4BP pode ser usado como uma referência para modelar processos de negócios relacionado com a LGPD, no entanto, é necessário apontar que a metodologia do método ainda é manual e não automatizado, dependendo do conhecimento dos projetistas, pois o BPMN não pode ser considerada uma linguagem acessível para qualquer profissional. Outro aspecto importante é a necessidade de validar a integralidade do LGPD4BP com especialistas em privacidade.

Ao introduzir elementos de proteção de dados para BPMN, os estudos de AGOSTINELLI et al. e JÚNIOR enriquecem a capacidade de modelagem de negócios com regimentos focalizados em dados pessoais. Com isso, os processos de negócio podem ser considerados um dos pilares de segurança para o tratamento de dados adequado, e em adições as modelagens de negócio, podem estabelecer medidas organizacionais eficientes e rápidas para tratar de problemáticas sobre manipulação de dados.

Os artefatos explorados neste capítulo estão relacionados a mudanças administrativas sobre a governança de dados, para realizar impacto concreto na implementação da LGPD. No próximo capítulo, são apresentadas as soluções que executam a segurança e proteção de dados pessoais em aspectos técnicos em sistemas de informação, motivando considerações tecnológicas para cumprir requisitos específicos da LGPD.

6 SOLUÇÕES EM SEGURANÇA DA INFOMAÇÃO

O cumprimento de leis de proteção de dados como a LGPD pode ser problemática pois, considerando a natureza dos regulamentos deste âmbito, é possível observar que o texto jurídico decide especificar objetivos de qualidade, e não as definições de instrumentos técnicos capazes de ajudar as organizações a alcançar a conformidade. A grande razão para isso, é que a lei prevê garantir a proteção de dados pessoais resistindo aos avanços tecnológicos, logo, especificar soluções computacionais, artefatos de segurança ou métodos criptográficos seria algo inviável, visto que, a cada dia, os profissionais da área de SI desenvolvem novos mecanismos, cada vez mais poderosos e eficientes (BARTOLINI; LENZINI; ROBALDO, 2019).

Além disso, a capacidade de criação de novos ataques e novos problemas de privacidade e segurança de dados também é uma problemática constante para a sociedade atual. Portanto, tudo que a LGPD especifica é que a área de TI se responsabiliza pela implementação e execução do regulamento. As empresas deverão evoluir suas práticas de SI, de forma urgente, e os funcionários do setor de TI devem estar focados no esforço de criar e adotar sistemas, softwares e mecanismos capazes de aprimorar as operações de dados pessoais (LOPES; AMARAL, 2022).

O resultado desta nova demanda é a ampliação de um segmento de mercado inovativo, no contexto de produção de ferramentas capazes de fornecer suporte à conformidade da LGPD e dos principais regulamentos internacionais. É primordial iniciar atividades para empregar técnicas aprimoradas de SI capazes de prover transparência aos titulares de dados (LUGATI; ALMEIDA, 2022).

Para programar sistemas e desenvolver artefatos adequados a lei, é necessário definir os requisitos legais e medidas de conformidade para um processamento de dados que (BARTOLINI; LENZINI; ROBALDO, 2019):

- Ofereçam modelos que construam ferramentas e fluxos de trabalho compatíveis com a proteção de dados;
- Construam ferramentas e metodologias que possam detectar possíveis violações;
- Proponham soluções para solucionar lacunas de privacidade.

Todos esses aspectos apontam para uma expansão tecnológica impulsionada pela LGPD para assegurar os dados pessoais (LOPES; AMARAL, 2022). Neste capítulo, serão apresentados estudos que explicam alguns dos artefatos tecnológicos recentemente desenvolvidos nos institutos de pesquisa, no mercado e na academia no contexto dos regulamentos de proteção de dados. Os artefatos apresentados nas próximas seções estão

associados aos temas de: Controle de Acesso, Consentimento, Contratos Inteligentes, Políticas de Privacidade de dados, e por fim, Anonimização e Minimização de dados.

6.1 Controle de Acesso

O controle de acesso é definido como um sistema capaz de controlar o acesso, fornecendo uma decisão a uma solicitação de autorização de acesso a algum recurso ou aplicação, normalmente baseada em políticas predefinidas. Mecanismos de controle de acesso estão embutidos em muitos sistemas diferentes, como sistemas operacionais e sistemas de gerenciamento de banco de dados (CALABRÒ; DAOUDAGH; MARCHETTI, 2019).

Estruturalmente, os Sistemas de Controle de Acesso (SCA) atendem aos princípios de confidencialidade e integridade (requisitos necessários para as legislações de privacidade de dados) pois, um conjunto de regras nos SCA são capazes de especificar quem tem acesso a quais recursos e sob quais circunstâncias (DAOUDAGH; MARCHETTI, 2022).

Um paradigma mais avançado, para tratar de um controle de acesso mais robusto avaliando vários contextos, dados e sistemas, é a abordagem ABAC (Controle de Acesso Baseado em Atributos). A ideia básica do ABAC é usar atributos de diferentes entidades para formular decisões de controle de acesso, em relação ao acesso de um sujeito, processo ou ação.

Nessa abordagem, as decisões de autorização são obtidas por meio de políticas de autorização especificadas, utilizando uma linguagem específica e especializada em descrever e avaliar diferentes contextos, processamentos e atributos. As políticas ABAC são então um conjunto de regras definidas com base nos atributos de sujeitos, objetos e operações, bem como, outros atributos contextuais ou ambientais (BARTOLINI et al., 2019).

Para especificar e aplicar as políticas de controle de acesso no ABAC, geralmente utiliza-se a eXtensible Access Control Markup Language (XACML), que é uma linguagem de especificação padronizada e apta a definir políticas que definem a decisão (à solicitações e respostas) de controle de acesso em um formato XML. Logo, uma política XACML é uma declaração específica do que é e do que não é permitido com base em um conjunto de regras, definidas em termos de atributos múltiplos. Essas regras definem a combinação de algoritmos que estabelecem o sucesso, ou a falha do acesso.

Resumidamente, uma política XACML possui uma estrutura em árvore cujos principais elementos são: *PolicySet, Policy, Rule, Target e Condition*. O PolicySet inclui um ou mais políticas. Uma Política (*Policy*) contém um Destino (*Target*) e uma ou mais Regras (*Rule*). O Destino especifica um conjunto de restrições nos atributos de uma determinada solicitação. A Regra especifica um Destino e uma Condição (*Condition*)

contendo uma ou mais funções booleanas. Caso a Condição seja avaliada como verdadeira, então o Efeito da Regra (um valor de Permitir ou Negar) é retornado, caso contrário, uma decisão *NotApplicable* é formulada (Indeterminado é devolvido, em caso de erros) (CALABRÒ; DAOUDAGH; MARCHETTI, 2019).

6.1.1 Controle de Acesso *GDPR Manager*

Os sistemas de TIC inteligente (Smart ICT Systems) estão cada vez mais aptos a inserir implementações ligadas à privacidade de dados, e atualmente contam com a integração e implementação de ferramentas e técnicas inovadoras, que podem tornar um determinado sistema inteligente capaz de fortalecer o gerenciamento do acesso a um recursos (ou dados), utilizando instalações personalizadas, ou confiando em um controle de acesso específico do sistema (DAOUDAGH; MARCHETTI, 2022). Na Figura 11 é considerado um repositório de Políticas de Controle de Acesso (PCA) definido pelo trabalho de (DAOUDAGH et al., 2021).

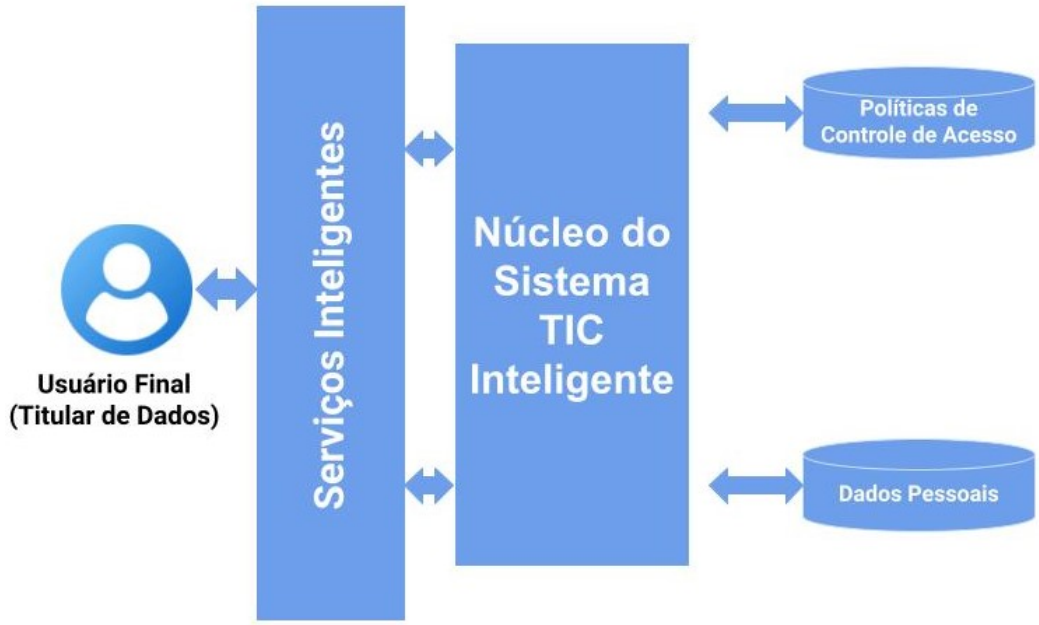

Figura 11: Sistema TIC Inteligente
Fonte: Adaptado de (DAOUDAGH et al., 2021), Tradução livre feita pelo Autor.

Para se adequar a proteção e privacidade de dados pessoais, a arquitetura genérica de Sistema de TIC Inteligente é aprimorado com uma nova camada que permite:

1. Uma interação amigável com o usuários finais;
2. A gestão de atividades e processamentos para cada domínio;
3. A derivação automática de PCA, de acordo com os dados coletados nos consentimentos.

No estudo de DAOUDAGH et al. (2021), o mecanismo de controle de acesso torna-se um meio para restringir o acesso a dados pessoais, com base nas PCA compatíveis com RGPD europeu, ou seja, um conjunto de regras que especificam quem (por exemplo, Controlador, Operador ou Titular dos Dados) tem acesso a quais recursos (por exemplo, Dados Pessoais) e sob quais circunstâncias (ou seja, as exigências do RGPD, tais como Propósito de Tratamento e Consentimento).

Para atender aos requisitos da legislação de proteção de dados, uma nova camada na arquitetura das TIC Inteligentes pode ser especificada. Esta nova camada é especializada em privacidade de dados por padrão (PDP), ou seja, a partir da fundação do sistema. Esse sistema que executa o PDP possui duas estruturas principais: (1) o núcleo do sistema inteligente e (2) uma nova camada chamada *GDPR Manager*, que é responsável pela tradução e aplicação de políticas de controle de acesso executáveis (Figura 12).

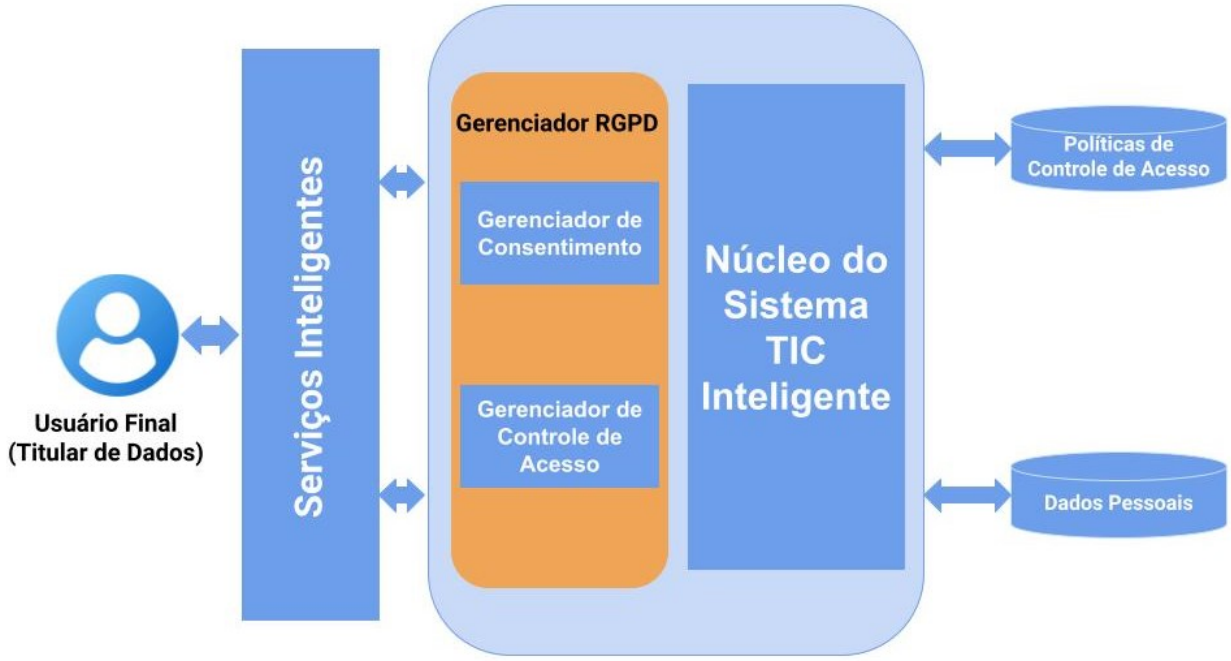

Figura 12: Sistema TIC Inteligente com PDP
Fonte: Adaptado de (DAOUDAGH et al., 2021), Tradução livre feita pelo Autor.

O *GDPR Manager* inclui dois componentes principais, o Gerenciador de Consentimento, que traduz o consentimento dos titulares de dados textual em representação estruturada e Gerenciador de Controle de Acesso, que utiliza as políticas de controle de acesso para executar apenas as operações permitidas.

O Gerenciador de Controle de Acesso tem a responsabilidade de criar PCA que sejam compatíveis com a RGPD, ou outra lei de privacidade (como a LGPD). Trabalha em conjunto com o gerenciador de consentimento recebendo, como entrada, e especificação concreta das definições dos serviços e os consentimentos dos titulares de dados relacionados. Para executar sua função, o Gerente de Controle de Acesso necessita de:

- dados pessoais categorizados (seguindo princípios da LGPD/RGPD);
- especificação de cada serviço e finalidade (projetadas pelo controlador);
- o consentimento dos titulares, em termos de seus dados pessoais e propósitos de tratamento.

Com base nessas informações, o *Access Control Manager* deve ser capaz de criar PCA específicas, para cada requisito especificado nas legislações. DAOUDAGH et al. (2021) fornecem uma prova de conceito, que consiste na integração de duas novas ferramentas provenientes dos setores industrial e acadêmico. A ferramenta de controle de acesso explorada é a GENERAL_D Framework.

A GENERAL_D Framework instancia o gerenciador de controle de acesso, e é composto por quatro componentes: *User Stories Manager; Json Manager; ACP Manager*; e *DBs Manager* como ilustrado na Figura 13.

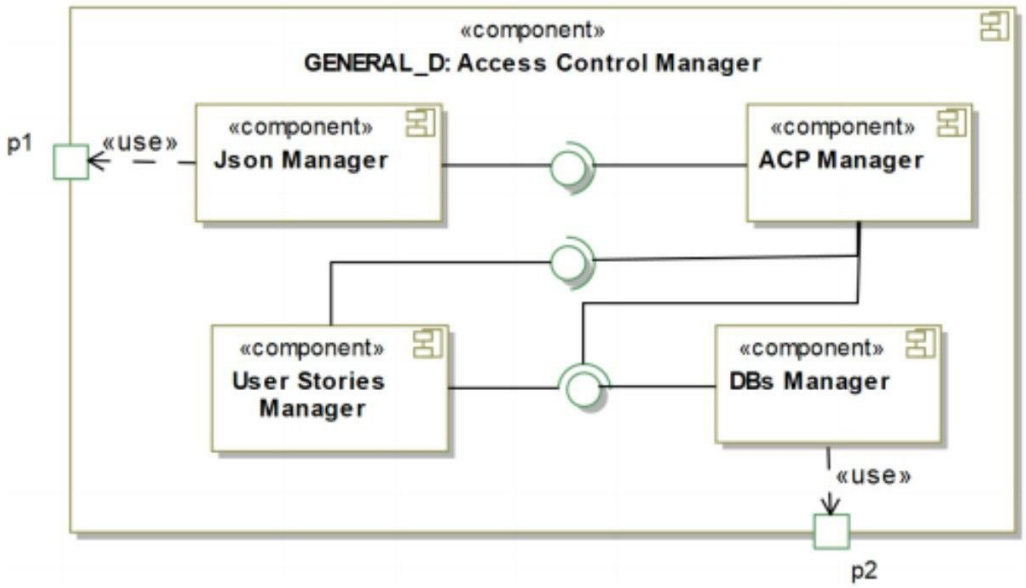

Figura 13: Estrutura geral do *Framework* GENERAL_D
Fonte: (DAOUDAGH et al., 2021).

O *User Stories Manager* gera um *backlog* de proteção de dados, que contém histórias de usuário baseadas no contexto do RGPD/LGPD (políticas específicas). Esse componente é útil para automatizar a implementação de políticas de controle de acesso padronizadas em conformidade com o regulamento. Neste estudo de caso, as histórias de usuário são modelos estruturados como políticas XACML abstratas e são armazenadas em um banco de dados interno (controlado pelo *DB Manager*).

O *Json Manager* tem a responsabilidade de interagir diretamente com o gerenciador de consentimento. Ele recebe o consentimento no formato Json e analisa esse

consentimento para extrair as informações relevantes para a geração de Políticas de controle de acesso. As informações avaliadas são a identificação e atributos do consentimento (datas, finalidades, ações e operações permitidas) e os dados fornecidos pelo titular de dados.

O *ACP Manger* é o componente central da estrutura GENERAL_D. Tem a responsabilidade de criar PCA executáveis e codificadas na linguagem XACML. Ele interage com:

1. *Json Manager* para recuperar os dados a serem processados (por exemplo, os propósitos definidos e a lista de terceiros permitidos a acessar os dados);
2. Gerenciador de histórias de usuários para receber os modelos das PCA. Portanto, o *ACP Manager* combina os dados recebidos para produzir políticas XACML, que ele armazena no repositório interno de Políticas de Controle de Acesso.

Diante dessa implementação, o *Access Control Manager* deve ser capaz de criar Políticas de Controle de Acesso específicas, para cada requisito especificado nas legislações. Diante destes métodos e linguagens, é viável objetivar a geração de um modelo de PCA baseado nos requisitos de leis de proteção de dados, para a criação de atividades aptas a analisar, projetar, implementar e testar mecanismos de controle de acesso para garantir a conformidade com legislações como a LGPD.

Este é um processo complexo pois, dependendo das peculiaridades dos cenários de aplicação e dos artigos da LGPD, pode ser necessário definir e personalizar os casos de uso para cada usuário de um sistema. Para a criação e validação de políticas concretas, significativas e executáveis, é necessário:

- Correspondência de Atributos - realizar a correspondência entre os atributos conceituais das legislações em atributos concretos. Os atributos podem ser exemplificados por: especificação de agentes de tratamento como o controlador, categorias de dados, regras de operação e especificação de propósitos;
- Criação das politicas de controle de acesso baseadas na LGPD - envolve a tradução de políticas de controle de acesso abstratas, em um formalismo ou linguagem de referência (XACML, por exemplo);
- Avaliação das políticas baseadas na lei de proteção de dados - verificar se as políticas criadas com base na LGPD, ou outra legislação, estão em conformidade com o pretendido nos direitos de acesso.

O controle de acesso é um domínio que aplica uma moderação entre as entidades que possuem acesso a sistemas e dados organizacionais, no entanto, em muitos casos,

também é necessário definir meios formais para autorizar o acesso de usuários, clientes e funcionários. Para a LGPD, em muitos casos são utilizadas técnicas de consentimento para autorizar a execução de tratamento de dados.

6.2 Consentimento

O conceito de consentimento para aprovar o tratamento de dados pessoais em organizações, sobretudo, para as operações de empresas privadas sobre os dados dos seus clientes e funcionários, foi evidenciado na aprovação do RGPD europeu. A LGPD se adequou à nova demanda e especifica o consentimento como uma de suas bases legais, ou seja, quando necessário, será obrigatória a autorização do titular dos dados, antes da obtenção de informações e do início de qualquer tratamento.

O consentimento no RGPD é especificado como uma ação válida, apenas quando ocorre livremente, quando seu contexto é específico, quando existe transparência e quando o consentimento é inequívoco (MERLEC et al., 2021). Em termos semelhantes, a LGPD define que a obtenção da permissão para o tratamento deve ser concebida de forma explícita e inequívoca (LGPD, 2018).

A ocorrência da "não necessidade de consentimento" é a exceção nas novas leis de proteção de dados, e só ocorrem quando há uma determinação legal indispensável, ou um legítimo interesse por parte do controlador para a execução de suas atividades (BAX; BARBOSA, 2020). A consequência proposta é tornar o consentimento cada vez mais comum no dia a dia das organizações e dos sistemas digitais.

Para cumprir as normas da LGPD nas disposições de permissão, para iniciar a coleta e operações sobre os dados pessoais, novas demandas em ajustes de processos e sistemas devem ser executadas. A construção de mecanismos, para obtenção e registro de consentimento eficientes, torna-se foco entre os profissionais de segurança e privacidade, pois apenas especificando um consentimento robusto e claro sobre quais os objetivos dos processamentos das organização, é possível demonstrar conformidade com a LGPD, ou seja, justificar que apenas as operações consentidas pelo titular de dados estão sendo realizadas.

Ainda que a coleta e o gerenciamento de consentimentos possa ser direta e simples para muitos sistemas ou portais, em muitas organizações complexas e sistemas com muitas integrações, é necessário desenvolver mecanismos complexos para gerir as especificidades das permissões de cada cliente. Nas subseções seguintes são apresentados alguns sistemas para a gestão das atividades de consentimento em problemas mais amplos e ecossistemas mais complexos.

6.2.1 Ferramenta Semântica de Consentimento Automatizado

O estudo de CHHETRI et al. (2022) apresentou um design de ferramenta escalável com base no consentimento informado e modelado semanticamente para a conformidade com o RGPD europeu. A conformidade nesse caso se refere em averiguar que os dados de um indivíduo são utilizados em um sistema de acordo com a autorização informada pelo titular de dados.

A contribuição inovativa deste trabalho se refere ao uso de tecnologias semânticas, em específico a tecnologia de grafo de conhecimento (*Knowledge Graph - KG*), desenvolvida com o apoio de especialistas jurídicos em representar o consentimento informado, seguindo os aspectos do regimento de proteção de dados europeu (CHHETRI et al., 2022).

Existem numerosos modelos semânticos para modelar consentimentos, neste estudo, os grafos de conhecimento fornecem uma representação de consentimento em um formato consistente para ser legível por uma máquina, o que possibilita implementar uma verificação automatizada dos acordos de concessão de dados.

Para abordar a tarefa de verificação automatizada, também é necessário traduzir as regulamentações das leis de proteção de dados em requisitos de Medidas Técnico-organizacionais (MTO), que quando bem definidas, podem ser implementadas em código. Essa tradução adiciona uma etapa de implementação de software para traduzir requisitos de MTO do RGPD em código.

A etapa principal para realizar a verificação de conformidade é a utilização do grafo de conhecimento como fonte de dados. O grafo modela os consentimentos informados e é armazenado no banco de dados GraphDB. Em termos de consentimento, o grafo de conhecimento representa (CHHETRI et al., 2022):

- O estado, como: concedido, recusado, revogado, expirado e retirado;
- A finalidade e especificidades do tratamento objetivado;
- Duração do acordo;
- Os dados solicitados e o seu tipo, como: contratos, dados de sensores e entidades envolvidas no processamento;
- Tipos de processamentos específicos (análise, marketing, coleta e vendas);
- Entidades envolvidas no consentimento, como: o controlador, o operador, o encarregado e informações do titular;
- Registros de alterações de estado do consentimento.

O módulo de consentimento automatizado proposto pela ferramenta utiliza a transformação do formato JSON, para o grafo de conhecimento que cria e armazena o consentimento. A utilização do JSON é justificada para reduzir a complexidade e dar suporte a empresas de pequeno e médio porte, que possuem pouca experiência e *expertise* em tecnologias semânticas (CHHETRI et al., 2022). A Figura 14 mostra o esquema JSON e sua representação no grafo de conhecimento do banco GraphDB. O exemplo especifica a tarefa de garantir apenas os dados necessários utilizados no tratamento, ou seja, o propósito de minimização de dados, que é requerido em muitos escopos do RGPD e da LGPD.

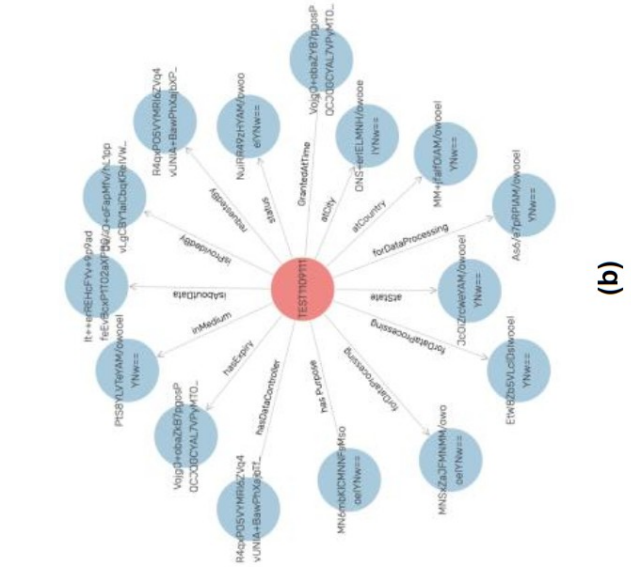

Figura 14: Estrutura JSON e GraphDB
Fonte: (CHHETRI et al., 2022).

Além do módulo de consentimento, a plataforma proposta por CHHETRI et al. (2022) dispõem de outras camadas utilizados para executar a conformidade semântica dos consentimentos:

- Camada de Serviço - Implementa a funcionalidade principal para a verificação automatizada de conformidade e operações de suporte, como a criação dos consentimentos. Ela é composta pela camada de API e pelo núcleo do sistema;
- Camada de API - Fornece uma API REST que dispõe o acesso a ferramenta;
- Camada de processamento de dados - camada de gerenciamento de dados, que dá suporte a operações de criação de consentimento, verificação de conformidade e auditorias;
- Camada de Segurança - Módulo que incorpora proteções como criptografia. As informações de consentimento devem ser criptografadas, a fim de evitar o acesso sobre informações privadas do titular de dados;
- Camada de Auditoria - Fornece a transparência sobre os processamentos de dados pessoais, de forma que estejam facilmente disponíveis, especificando detalhes do consentimento e detalhes das operação realizadas;
- Camada de Conformidade - realiza verificações para garantir que o controlador, ou operador de dados, tenha obtido o consentimento informado dos titulares para a coleta e processamento, garantindo assim a conformidade e demonstrando que nenhum acordo é violado.

Embora a ferramenta apresentada tenha sido projetada para o uso específico em uma aplicação de *Smart Cities* (Cidades Inteligentes), os autores criaram um sistema que pode ser generalizado, no entanto, a grande limitação levantada no trabalho é a possibilidade de restrições para requisitos de consentimento em domínios específicos (CHHETRI et al., 2022). Além disso, embora os termos de consentimento sejam análogos na LGPD, é necessário avaliar o método de codificação dos requisitos do RGPD, para utilizar o sistema em diferentes regimentos de proteção de dados.

6.2.2 Gerenciador de consetimento: CaPe

Integrado com o Gerenciador de Controle de acesso GENERAL_D Framework apresentado na Seção 6.1.1, o estudo de DAOUDAGH et al. (2021) apresenta o CAPE como Gerenciador de Consentimento. O principal objetivo de um Gerenciador de Consentimento é gerenciar e controlar os dados pessoais durante a interação entre os titulares

de dados e controladores representando entidades ou serviços públicos ou privados. Esta estrutura permite a gestão e o acompanhamento da capacidade de conceder e retirar consentimento para que terceiros possam realizar os tratamentos de dados pessoais de um indivíduo.

Em serviços de TIC Inteligentes o consentimento é guiado por propósitos específicos bem definidos para cada operação e os dados necessários para realizar as tarefas, visto que o controlador deve garantir a minimização de dados e a limitação de finalidade. Assim, o Gestor de Consentimento deve incluir uma interface centrada no usuário, baseada em consentimento, que permite:

1. titulares de dados aptos a gerenciar e rastrear seus próprios dados e seus consentimento associados;

2. Controladores/operadores de dados utilizam o consentimento para compartilhamento de dados entre serviços e processamentos utilizando dados pessoais apenas quando atenderem aos requisitos do RGPD/LGPD.

O CaPe fornece um conjunto de soluções TIC para gerenciamento de dados pessoais centrado no usuário e baseado em consentimento, assegurando as seguintes características:

1. O consentimento autoriza que Fontes de dados sejam transferidas para Consumidores de dados e autoriza o Solicitante de Dados a processá-los;

2. O consentimento refere-se a uma Política de Uso de Dados que pode ser vinculada à formalização do consentimento;

3. O consentimento é dado de forma clara, de modo a permitir que o responsável pelo tratamento de dados demonstre a validade do consentimento;

4. O registro de consentimento inclui claramente 1. Quem consentiu; 2. Quando consentiram; 3. O que foi consentido; 4. Como foi consentido; 5. Se ocorreu uma retirada de consentimento.

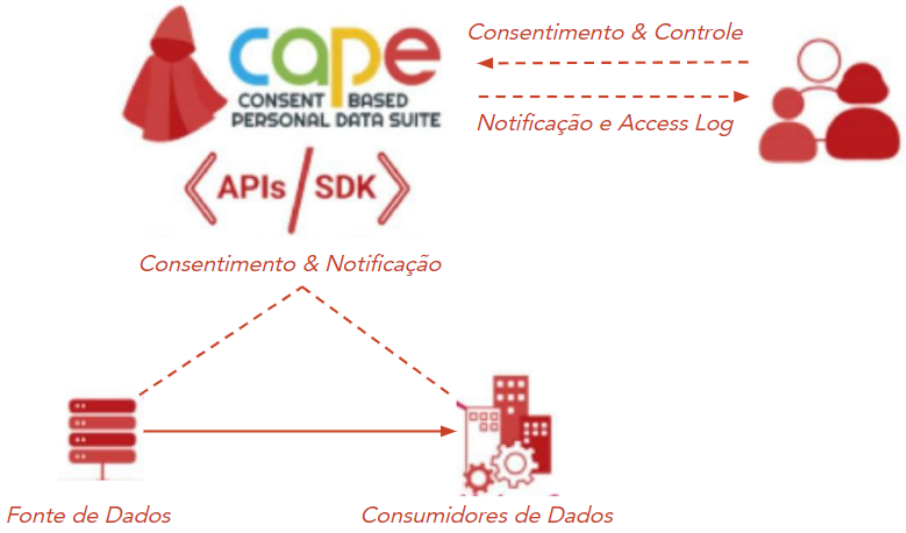

Figura 15: Lógica Cape
Fonte: Adaptado de (DAOUDAGH et al., 2021), Tradução livre feita pelo Autor.

Um uso geral do CaPe utiliza um *Data Controller Dashboard*. Com esse Dashboard dois painéis separados podem ser utilizados, de um lado, o Controlador de dados para visualizar e gerenciar todos os consentimentos recolhidos. Por outro, o Titular dos Dados, através do Painel de autoatendimento do usuário, para verificar quais dados são usados, como e para qual finalidade e para gerenciar os consentimentos relacionados.

A Figura 16 exemplifica o extrato genérico do modelo de consentimento derivado de CaPe.

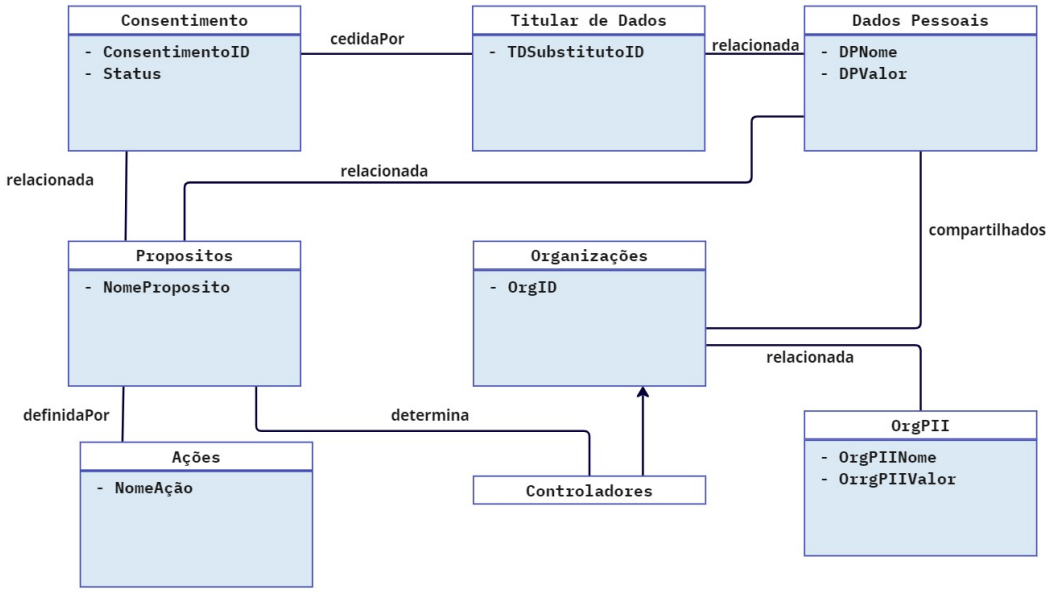

Figura 16: Modelo estrutural da Cape
Fonte: Adaptado de (DAOUDAGH et al., 2021), Tradução livre feita pelo Autor.

Na figura estão expostas as seguintes estruturas:

- Um Titular de Dados é identificado por seu ID e está relacionado a um conjunto de Dados Pessoais, cada um representado por um par nome/valor;
- O Titular dos Dados pode dar um Consentimento para processar o seus dados para um propósito específico definido pelo Controlador;
- Cada Propósito tem um nome e é implementado por meio de um conjunto de Ações;
- Durante a fase de consentimento, o Titular dos Dados pode escolher também compartilhar seus Dados Pessoais com uma ou mais Organizações, para que o controlador possa eventualmente alcançar os fins definidos.

O titular também pode pode retirar um consentimento a qualquer momento (dado a natureza do consentimento ou da entidade e com as bases legais estipuladas). Na implementação atual, o CaPe codifica as instâncias do modelo definido como arquivos Json e, em seguida, fornece esses arquivos para o GENERAL_D Framework com o objetivo de tornar o consentimento diretamente executável pelo Sistema.

6.2.3 ADVOCATE

O artigo de RANTOS et al. (2019) propõe o ADVOCATE, uma solução que auxilia controladores e operadores a desenvolver uma estrutura para consentimentos de dados pessoais garantindo integridade. O *framework* é um serviço em nuvem, que também pode ser utilizado como uma ferramenta para usuários, que no papel de titular de dados, pode controlar de forma acessível os consentimentos executados sobre os dados pessoais no ecossistema de Internet das Coisas (IdC).

O ecossistema de IdC é um ambiente complexo para a privacidade de dados pessoais, pois atualmente existe uma escalada de popularidade na utilização de dispositivos de IdC, capazes de transmitir uma quantidade massiva de dados, incluindo os dados pessoais dos usuários.

A conformidade com legislações, como a LGPD e o RGPD, se relaciona com o ambiente de IdC, dado que as principais aplicações utilizadas pelos clientes são relacionadas à saúde, casas inteligentes e localização. O compartilhamento de dados com dispositivos dessa natureza pode causar danos graves à privacidade dos usuários como: monitoramento indevido de atividades e comportamentos; a falta de conhecimento/autorização na criação de perfis dos indivíduos e a execução de decisões automatizadas.

A conformidade com os requisitos das legislações de proteção de dados pessoais no ambiente IdC é o objetivo do AVOCATE, sobretudo no aspecto de desenvolver um ambiente de controle de consentimento, para ajudar usuários e organizações no gerenciamento

de dados (RANTOS et al., 2019). Com o *framework* controladores de dados poderão solicitar a autorização para a coleta de dados e deixar transparente informações sobre:

- Quais dados estão em processamento e as fontes de origem;
- Finalidades, prazos e bases legais definidas no tratamento;
- As entidades que operam sobre os dados;
- Destinatários ou categorias de destinatários de dados.

Já os titulares podem utilizar a ferramenta para:

- Se informar sobre as solicitações de processamento de seus dados pessoais;
- Criar preferências de privacidade e definir regras específicas de processamento de dados;
- Conceder consentimento;
- Ter a oportunidade de exercer os direitos de acesso, correção, eliminação, restrição e oposição ao tratamento;
- Estar ciente da segurança e qualidade dos acordos que consentiu.

O AVOCATE fornece uma arquitetura composta por: (1) os responsáveis pelo tratamento (os controladores que desenvolveram os dispositivos de IdC); e (2) uma plataforma para gerar os consentimentos com todos os seus dados e requisitos pré-estabelecidos. No lado dos titulares, eles podem utilizar o sistema para interagir e gerir seus consentimentos. A Figura 17 apresenta a abordagem do *framework*:

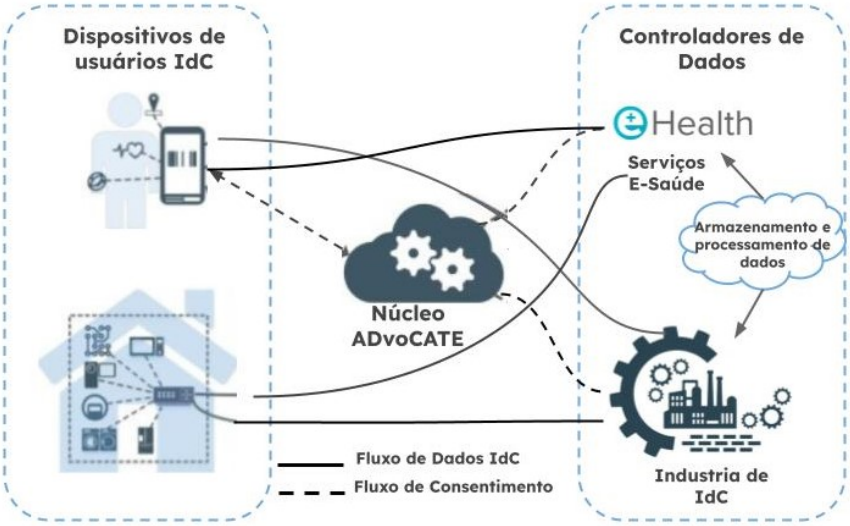

Figura 17: Arquitetura ADVOCATE
Fonte: Adaptado de (RANTOS et al., 2019), Tradução livre feita pelo Autor.

Nesse contexto, o ADVOCATE é visto como uma plataforma com os seguintes componentes (RANTOS et al., 2019):

- Gerenciamento de Consentimento - Componente que gerencia geração, atualizações e retiradas de consentimento;
- Certificação de Consentimento - Componente criado para garantir a integridade e validade dos consentimentos. Para isso, a plataforma utiliza assinaturas digitais e o uso da tecnologia blockchain;
- Componente de Inteligência - Estrutura de inteligência computacional utilizada para distinguir regras/políticas contraditórias ou conflitantes nos consentimentos de um usuário.

Uma implementação de referência para o componente de gerenciamento de consentimento, utilizando o Node.js e MongoDB, está disponível em https ://github.com /AnthonyK95 /adplatform. Na próxima seção é explorado um método específico de aquisição e gestão de consentimento, que é executado por meio de contratos inteligentes.

6.3 CONTRATOS INTELIGENTES

Com a aplicação das sanções e multas aplicadas pelas legislações de proteção de dados pessoais, muitas organizações estão dispostas a utilizar tecnologias capazes de prover segurança e um histórico de registros que assegura que todos os tratamento e operações de dados executados foram devidamente acordadas entre clientes, entidades públicas e empresas terceiras (BENTO, 2020).

Uma ferramenta capaz de prover essa funcionalidade é o contrato inteligente, e a corrente de adoção dessa tecnologia é denominada *Legal informatics*, que tem por objetivo apresentar uma visão de informática jurídica, uma área que relaciona o Direito, Tecnologia, Inovação e Economia (BENTO, 2020).

Os contratos inteligentes são programas de computador, que uma vez iniciados, executam de forma automática e obrigatória as condições específicas de acordos e negociações cadastradas. A operação ideal do programa deve evitar interrupções, fraudes ou interferência indevidas de sistemas externos (MERLEC et al., 2021).

No domínio de dados pessoais, os contratos inteligentes não possuem a finalidade de armazenar os dados pessoais como um ativo, são apenas coletados os dados relevantes para executar autonomia nas relações de consentimento/contratuais (VOSS, 2021).

Tecnologia de contrato inteligente é baseada em *blockchain* e permite que as partes envolvidas transfiram, acessem e armazenem as informações em uma rede de computadores distribuída (CORRALES; JURČYS; KOUSIOURIS, 2019). *Blockchain* é uma tecnologia distribuída qualificada para registrar uma lista de transações em cadeia. As transações são armazenadas e protegidas criptograficamente, e assim, cada bloco de transação armazenada deve bloquear alterações nos registros, mantendo todo o histórico da cadeia intacto (MERLEC et al., 2021).

Um sistema de gerenciamento de consentimento dinâmico, baseado em contrato inteligente com apoio da tecnologia *blockchain* foi proposto no trabalho de MERLEC et al. (2021). O sistema é centrado no usuário e permite o controle, a partir da coleta de dados pessoais, e provê um histórico de transações registrados nos contratos inteligentes, fornecendo a determinação da origem do acordo, definições de responsabilidades e a rastreabilidade de dados, mantendo as informações fidedignas e invioladas.

Os contratos inteligentes são adequados para o controle de consentimento, quando é necessário executar acordos específicos, informados e engajados entre as partes interessadas. O objetivo central no contexto de dados pessoais é prover transparência e segurança. Para isso, alguns desafios são encontradas para alinhar essa abordagem com legislações de privacidade de dados, como:

1. Fornecer acordos de consentimento personalizados e adequados aos tipos de dados e entidades relacionadas;
2. Garantir flexibilidade e dinamismo da tecnologia;
3. Permitir o controle sobre as definições de coleta, acesso e uso de dados, especificando prazos, parâmetros e regras para executar as atividades.

Para desenvolver um sistema eficiente e uma boa utilização da tecnologia *blockchain*, alguns requisitos de design são especificados:

1. Identificação das partes envolvidas no acordo e qual a função de cada envolvido;
2. Gerenciamento de consentimento centrado no usuário, possibilitando que os titulares sejam capazes de controlar a coleta e acordos de tratamento sobre os seus dados;
3. O acordo e os direitos dos indivíduos devem ser descritos no contrato de forma explícita e legível, por um humano ou programa de computador;
4. Os titulares devem ter acesso aos contratos e histórico de atividades realizadas;
5. Qualquer violação de consentimento deve ser comunicada;

6. Permitir a retirada do consentimento quando ocorrem violações, ou quando as obrigações e operações já foram cumpridas.

Para cumprir os requisitos, o sistema implementa uma camada de processamento de dados pessoais. As atividades desse módulo são de pesquisa, adesão de recursos de processamento e análise de dados. Além disso, uma API é desenvolvida nessa camada para habilitar aplicações externas descentralizadas à acessar os contatos inteligentes (MERLEC et al., 2021).

Outra camada importante do sistema é a camada de gerenciamento de consentimento dinâmico, que serve para apresentar os consentimentos dos contratos inteligentes na *blockchain*. Para isso, são especificados perfis e funções de usuários e um gerenciamento de contrato, que manipula os consentimentos durante todo o ciclo de vida dos dados. O gerenciamento de contrato é composto por: o solicitante do acordo; o acesso aos acordos para interação do titular de dados; um rastreador de consentimento, que rastreia os logs de transação de consentimento armazenados no registro da *blockchain* e por fim, o atualizador de consentimento, que permite aos titulares dos dados atualizar e adaptar seus acordos.

Essa camada corresponde a todo o processamento para a expressão de consentimento dos usuários. O modelo do acordo e a expressão de regras e direitos é desenvolvido utilizando a eXtensible Access Control Markup Language (XACML). Na parte dos operadores e controladores de dados, este módulo permite a criação de solicitação de consentimento que é processada no contrato inteligente e registrada na *blockchain* (MERLEC et al., 2021).

O pedido de consentimento deve conter os identificadores do titular dos dados e do solicitante, finalidades, período e base legal para coletar e/ou usar dados pessoais. Ao receber o pedido, o titular pode aceitar ou recusar livremente o acordo proposto.

A arquitetura do sistema também prevê uma camada de segurança e privacidade que contém recursos relacionados à segurança de dados, como autenticação, autorização e confidencialidade. Outro componente é controle de acesso, protegendo dados pessoais, autorizando o acesso depois de avaliar as políticas e regras incorporadas no consentimento. Por fim, também é incorporado um gerenciador de auditoria capaz de auditar o histórico de processamentos executados nos contratos. Um protótipo do sistema foi projetado com o objetivo de demonstrar sua viabilidade. O código é disponibilizado publicamente no site https://github.com/ mlecjm/sc-dcms.

Uma das principais limitações para o uso de contratos inteligentes no cumprimento dos requisitos da LGPD é o direito de esquecimento e retificação de informação (BENTO, 2020). O direito de apagar dados gera problemas no contexto dos contratos, pois a tecnologia *blockchain* é construída para criar confiança e impedir a exclusão, ou modificações

de registros sem quebrar a cadeia de transações (VOSS, 2021).

Embora o sistema apresentado possua o seu escopo na finalização dos consentimentos, MERLEC et al. (2021) também evidencia a necessidade que mais pesquisas sejam efetivamente aplicadas e implementadas, para assegurar de forma completa o direito de esquecimento e possibilitar adaptabilidade e atualização nos contratos inteligentes.

Outra limitação apontada é a vulnerabilidade dos contratos inteligentes, que por serem programas de computador, podem estar sujeitos a falhas e mau-funcionamento. Além disso, à medida que a popularidade na utilização da tecnologia cresce, novos ataques e vulnerabilidades de segurança podem surgir.

Após a apresentação das múltiplas abordagens para gerir e executar o consentimento, é possível explorar as políticas de privacidade de dados, artefatos criados para divulgar e informar as especificidades do tratamento de dados pessoais no momento do consentimento.

6.4 POLÍTICA DE PRIVACIDADE

Um dos requisitos mais importantes para os novos regimentos de proteção de dados é a divulgação dos riscos de privacidade para os usuários de sistemas digitais e o detalhamento dos propósitos na coleta de dados (RAHAT; LE; TIAN, 2021). Para isso são criadas as Políticas de Privacidade, que servem como um canal de comunicação e um contrato formal, que especifica como os princípios de tratamento de dados requeridos pela LGPD são atendidos.

Muitas empresas atualizaram sua política de privacidade após a aplicação dos novos regulamentos internacionais, entretanto, a linguagem utilizada nas políticas é massante e possui jargões jurídicos de difícil acesso. Além disso, muitas organizações omitem especificidades das operações sobre os dados. Esses dois fatores promovem, na prática, a omissão da leitura das Políticas de Privacidade por parte dos clientes e usuários dos sistemas.

Para o Serviço Federal de Processamento de Dados (SERPRO) a elaboração da política de privacidade nos sistemas e serviços é fundamental para o contexto de adequação aos princípios da LGPD. Para isso é necessário mapear os dados pessoais para especificar a finalidade, as bases legais que legitimam o tratamento e o modo de atendimento aos direitos do titular de dados. É importante garantir que a política esteja facilmente disponível e com uma linguagem clara. Esse processo deve ter auxílio da área jurídica e avaliar outras legislações que são aplicadas à organização (SERPRO, 2019).

Evidenciando as ineficiências dos sistemas e serviços em disponibilizar uma política de privacidade completa, o estudo de RAHAT; LE; TIAN (2021) explorou os requisitos do RGPD para verificar se os termos de portais da internet cumprem integralmente as

obrigações legais. Coletando 9.761 políticas de privacidade dos principais sites vinculados ao Reino Unido, e comparando com os 18 principais requisitos da lei, demonstraram que apenas 3% das políticas compreendem integralmente os aspectos legais. Também foram identificadas seis principais categorias de requisitos do RGPD, aos quais apenas 15-20% dos sites dispõe em suas políticas.

A solução de CHANG et al. (2019) objetivou em seu estudo a concepção de uma solução prática capaz de atender às preocupações de privacidade dos usuários para extrair automaticamente as descrições das políticas de privacidade, de acordo com o perfil do indivíduo e qual a natureza da aplicação que especifica os termos do acordo.

O primeiro passo executado no estudo é a criação de perfis de indivíduos, determinando com especificidade qual o nível de preocupação com a privacidade e o cuidado de seus dados. Os diferentes tipos de perfis foram obtidos através de entrevista e *crowdsourcing*, ou seja, obtenção de informações e opiniões de grupos na internet e mídias sociais. O conjunto de dados produzidos teve apoio de 252 participantes (CHANG et al., 2019).

Depois da especificação, os tipos de perfis são armazenados na base de dados e o módulo de Geração de Perfil de Preocupação com a Privacidade é criado, como um mecanismo apto a realizar a correspondência entre perfis a um novo usuário. A cada novo usuário na plataforma, são feitas 5 perguntas selecionadas dinamicamente, de acordo com as respostas, e um perfil de privacidade do banco de dados é associado com o usuário ao final.

A segunda contribuição da pesquisa de CHANG et al. (2019) foi projetar uma Rede Neural Convolucional para analisar automaticamente as políticas de privacidade em grande escala e extrair com precisão a política que é relevante para o usuário em determinada aplicação. O módulo responsável para essa tarefa é o módulo de extração de política de privacidade. Esse módulo tem como entrada os segmentos de privacidade dos usuários do servidor, gerado pelo módulo de Geração de Perfis, e uma base de dados com 115 políticas de privacidade com 23 mil anotações de especificidade rotuladas por especialistas jurídicos especialmente focados no RGPD europeu.

O resultado da análise da rede neural é uma saída que corresponde às descrições da política de privacidade da aplicação pesquisada, que está diretamente relacionada com a preocupação do usuário quanto aos seus dados pessoais. Para testar o módulo, o trabalho realizou um estudo de campo com 96 participantes, atingindo 0,81 de precisão na apresentação da política requerida. Um exemplo de saída do sistema para esse módulo é apresentado na Figura 18:

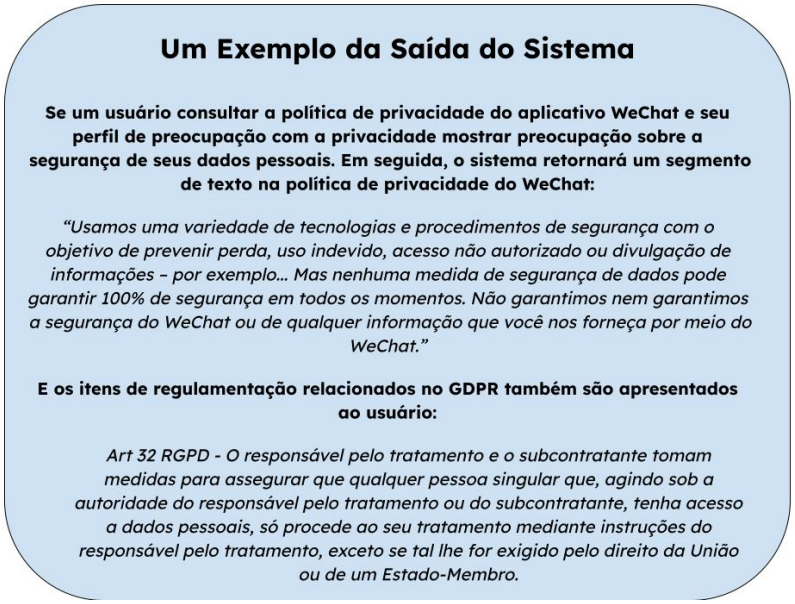

Figura 18: Exemplo de Saída da Rede Neural
Fonte: (CHANG et al., 2019), Tradução livre feita pelo Autor.

Com os estudos apresentados, fica evidente os problemas atuais para a disposição de políticas de privacidade de dados completa e de fácil acesso aos usuários dos sistemas digitais. É evidente que metodologias para auxiliar as organizações em elaborar políticas mais acessíveis e adequadas às legislações de privacidade de dados pessoais ainda são necessárias. A principal contribuição do estudo de CHANG et al. é minimizar a carga de leitura e informações irrelevantes, expondo apenas as informações relevantes para um indivíduo, que pretende resguardar seus dados.

Nesta seção foram apresentadas algumas técnicas que utilizam a Inteligência Artificial (IA) para melhorar a privacidade de dados. Seguindo nesse sentido, a próxima seção apresenta técnicas de IA para as demandas de minimização e anonimização de dados.

6.5 MINIMIZAÇÃO E ANONIMIZAÇÃO

A utilização de IA para solucionar problemas de privacidade é um dos campos de maior interesse na academia e em empresas e corporações, que investem em inovações tecnológicas complexas. Desenvolver inovações no campo da IA é muitas vezes inviável para a maioria das empresas, devido a complexidade e o custo das soluções, por isso algoritmos e mecanismos de IA, como a Aprendizagem de Máquina (*Machine Learning - ML*), são do interesse de organizações de grande porte, que investem em pesquisa e em grupos de desenvolvedores focados em inovações.

Um exemplo de organização que investe nesse contexto é a IBM. O AI Privacy Toolkit da IBM é um conjunto de ferramentas de código aberto projetadas por desen-

volvedores de modelo de aprendizagem de máquina para ajudar as organizações a criar soluções de IA mais confiáveis. Em seu estado atual, as duas principais ferramentas de privacidade desenvolvidas pelo projeto são relacionadas a minimização de dados e a anonimização de dados (IMB, 2022).

A minimização de dados (*data minimization*) significa o efeito de minimizar ou reduzir dados a proporções mínimas, seguindo uma necessidade jurídica ou de lógica de negócios. Esse processo contempla uma tarefa relevante para estes novos termos legislativos e para a privacidade de dados pessoais, pois é preciso especificar os propósitos e as necessidades de tratamento de qualquer dado relacionado a uma pessoa natural. Em seus termos, a lei brasileira indica: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

Podemos identificar que as definições de minimização de dados foram inseridas no contexto de dados pessoais, para limitar o processamento e tratamento excessivo, desnecessário, antiético e vicioso, que qualquer organização possa realizar com os dados pessoais que possui. A LGPD não determina quanto é suficiente minimizar, ou quais operações a minimização são necessárias. Cabe a cada organização identificar qual é o conjunto de dados pessoais mínimos necessários para atingir o propósito daquele determinado tratamento.

Já no quesito de anonimização, a LGPD define um dado anonimizado como "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento", enquanto o processo de anonimização é definido por "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (LGPD, 2018).

A aplicação desta técnica é um recurso valioso no âmbito de proteção de dados, pois é utilizando esse método que operadores de dados podem privar a identidade de dados pessoais, o que pode ser uma atividade conveniente e muitas vezes necessária para tratar e compartilhar dados pessoais. Um exemplo concreto de anonimização pode ser encontrado na aplicação de pesquisas demográficas, onde os registros das bases de dados com dados pessoais são processadas para retirar qualquer identificador pessoal como Nome ou CPF, e assim, apenas os dados em foco da pesquisa como idade, gênero, escolaridade, etnia podem ser observados.

Em muitos contextos, a anonimização é referida na lei brasileira, e também no RGPD europeu, como uma ação amigável aos dados privados dos cidadãos, e é recomendada diretamente em casos como: estudos por órgão de pesquisa e na finalização do tratamento, visto que, ao realizar a tarefa de esquecimento e revogação de tratamento,

algumas organizações ainda podem manter registros e dados derivados do usuário que interferem no negócio, desde que realize a anonimização para que ele não possa ser identificado.

No entanto, os processos de anonimização e minimização de dados podem ser complexos e de difícil implementação, pois os dados pessoais de uma empresa necessitam de um mapeamento profundo, já que o tratamento/processamento é toda operação realizada com dados pessoais. O AI -Privacy-Toolkit da IBM visa ajudar as organizações e ser utilizado por desenvolvedores de modelos (como cientistas de dados), como parte de seus processamentos de dados com ML. O *toolkit* foi desenvolvido como uma biblioteca Python que pode ser usada com diferentes estruturas e *frameworks* da linguagem (scikit-learn, PyTorch e Keras.).

A implementação está disponível em https://github.com/IBM/ai-privacy-toolkit/ e os detalhes dos modelos de anonimização e minimização foram apresentados em artigos científicos GOLDSTEEN et al. (2021b) e GOLDSTEEN et al. (2021a).

6.5.1 Minimização de dados com Aprendizagem de Máquina

As legislações de privacidade especificam a minimização de dados como um princípio norteador para a exigência da utilização apenas dos dados necessários, contudo é difícil determinar a quantidade mínima de dados necessários e quais informações não devem ser manipuladas. O estudo de GOLDSTEEN et al., 2021b utiliza a aprendizagem de máquina para reduzir a quantidade de dados necessários com previsões, para tomar a decisão de exclusão ou generalização de dados, e produzir como saída um modelo minimizado. Os objetivos específicos do método são:

- Ser capaz de produzir a minimização que pode reduzir a quantidade e a granularidade dos dados de entrada, executando previsões de modelos de ML. Neste método, a minimização é executada apenas nos dados coletados para a análise (dados em tempo de execução), não nos dados de treinamento do modelo. Essa abordagem fornece uma solução mais simplificada e prática para ser executada e/ou integrada a um sistema;
- Utilizar conhecimento codificado do modelo para gerar uma minimização (ou generalização) com pouco ou nenhum impacto em sua precisão. Logo, o método visa manter ao máximo a precisão do modelo original, enquanto se esforça para reduzir a quantidade de dados coletados.

Em alguns casos pode haver a ocorrência de manutenção de todos os dados, pois todos podem ser avaliados como necessários, no entanto, o modelo é capaz de aplicar

a generalização na maioria dos casos, e assim propiciar um processamento que melhora a privacidade dos dados. Além da privacidade, a execução do modelo pode viabilizar benefícios às organizações, como: na redução do armazenamento de dados e na agilidade e segurança no compartilhamento de dados (GOLDSTEEN et al., 2021b).

O processo de minimização é uma árvore de decisão que inicia treinando um modelo generalizado, a partir dos dados de treinamento (rotulado com previsões do modelo alvo), ou seja, é executado o treinamento de um modelo para realizar as previsões do modelo destino. A Figura 19 apresenta a estrutura geral.

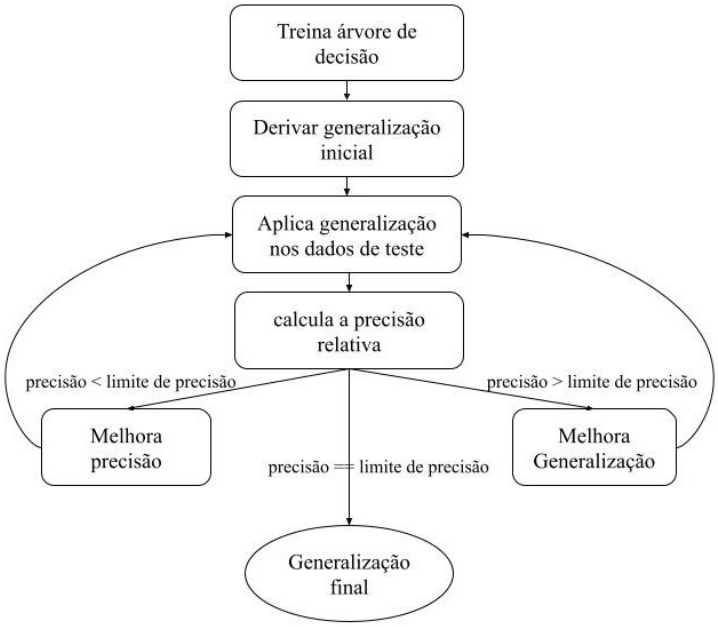

Figura 19: Estrutura do modelo de minimização de dados
Fonte: Adaptado de (GOLDSTEEN et al., 2021b), tradução livre feita pelo Autor.

6.5.2 Anonimização de dados com Aprendizagem de Máquina

O artigo apresentado por GOLDSTEEN et al., 2021a especifica um novo método de anonimização, com um modelo de ML que tem como principal objetivo executar seu processamento com duas características:

- Desenvolver uma técnica capaz de gerar um modelo com precisão alta - A ML deve aplicar uma anonimização guiada por precisão específica do modelo ao conjunto de dados de treinamento, em seguida, retrata o modelo nos dados anônimos para produzir um modelo anônimo. Este modelo anônimo não contém mais nenhum dado pessoal e pode ser livremente usado, ou compartilhado com terceiros.
- Ser uma abordagem genérica - Uma solução prática para anonimizar modelos de ML que são completamente flexíveis para o tipo de modelo treinado. Como não é

necessário realizar modificações no processo de treinamento para utilizar o modelo, a ferramenta pode ser aplicada em uma ampla variedade de casos de uso, tornando o aprendizado de máquina anônima uma opção viável para muitas empresas.

Desenvolver um modelo de aprendizagem com dados anonimizados, geralmente resulta em perda de precisão, no entanto o método utilizado usa o conhecimento codificado no modelo treinado e orienta o processo de anonimização para reduzir o impacto na precisão do modelo. O método utilizado é o k-anonimato (*k-anonymity*), que foi criado para reduzir a probabilidade de qualquer pessoa ser identificada, mantendo a utilidade dos dados (GOLDSTEEN et al., 2021a) .

O k-anonimato é uma abordagem baseada na generalização de atributos e em alguns casos na exclusão de registros de dados, com objetivo de tornar impossível a distinção entre os registros. Uma das limitações do método é aceitar apenas dados estruturados, incluindo dados numéricos, discretos e categorizados. O processo geral de anonimização é representado na Figura 20:

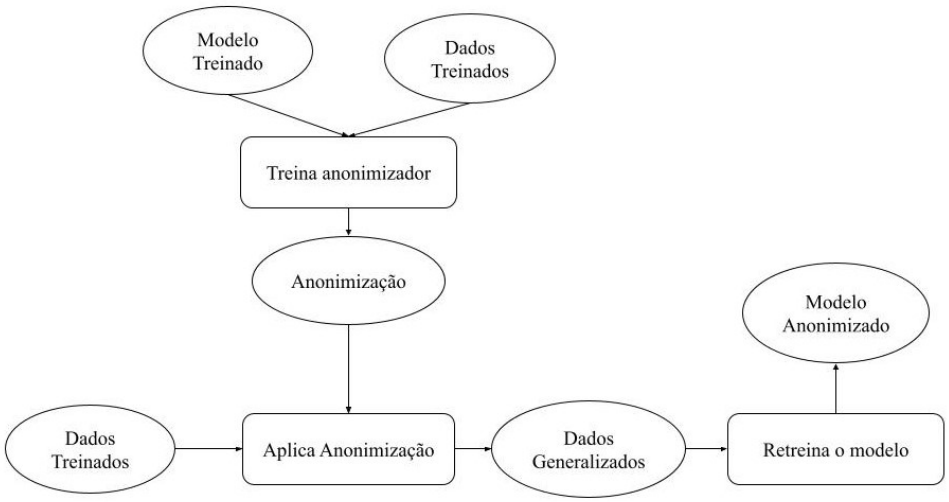

Figura 20: Estrutura do modelo de anonimização de dados
Fonte: Adaptado de (GOLDSTEEN et al., 2021a), tradução livre feita pelo Autor.

Este capítulo conclui a apresentação dos trabalhos da revisão sistemática. O Capítulo 7 expõe a análise e novos resultados obtidos diante das soluções encontradas.

7 ANÁLISE DOS RESULTADOS

Este capítulo descreve a análise dos artefatos identificados durante a revisão sistemática, com potencial para auxiliar resultados concretos no alcance da conformidade com a LGPD. A análise exposta é dividida entre os artefatos relacionados aos processos organizacionais de adequação à lei brasileira, e as soluções tecnológicas relacionadas à Segurança da Informação. Por fim, cada seção oferece recomendações de implementação à legislação nacional reveladas ao longo do estudo.

7.1 Análise das Soluções em Processos Organizacionais

O início da implementação da adequação à LGPD requer primordialmente, ou seja, antes da adoção de qualquer método, ou ferramenta metodológica/tecnológica, a inclusão de profissionais e gestores da organização para especificar os objetivos e metas pretendidas com o novo contexto emplacado pela legislação. Em seguida, também é necessário o envolvimento de atores internos à organização para aperfeiçoar as manipulações de informações e criar uma cultura organizacional motivada em cumprir os requisitos da LGPD.

A partir da atribuição de papéis, grupos e profissionais focados na conformidade da LGPD, é possível iniciar as mudanças internas, especialmente nos processos organizacionais que influenciam na operação de dados e na tomada de decisão dos procedimentos de negócio executados.

Muitos dos artefatos coletados no Capítulo 5 evidenciam que qualquer metodologia adotada para que um órgão se adeque às cláusulas estipuladas pela LGPD, deve promover o alinhamento de objetivos e incluir a privacidade de dados pessoais em processos vitais da empresa. Para isso, em muitos casos, torna-se necessário descrever ou modelar os processos atuais para atualizá-los e utilizá-los diante das novas metas estabelecidas. A modelagem dos processos é uma ferramenta poderosa para institucionalizar a execução de tarefas de adequação à proteção de dados.

Além do mapeamento dos processos, muitos dos artefatos apresentados na revisão estimulam a produção de documentação que detalha o mapeamento de dados e o fluxo de dados, além do mapeamento de riscos e inconformidades. A documentação e artefatos produzidos podem conceber informações relevantes para a produção de registros obrigatórios pela autoridade nacional ANPD, como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

As soluções mais complexas, relacionadas aos processos de adequação organizacionais, demandam a produção de um controle total dos dados pessoais em grandes organizações ou conglomerados, que possuem inúmeros recursos, procedimentos e sistemas. Neste caso, as soluções estabelecidas buscam formalizar uma Política de Segurança da

informação (PSI), que define regras administrativas para tratar da proteção de dados.

Para as organizações que possuem recursos técnicos e profissionais e se deparam com muitos processos sensíveis às demandas da LGPD, é possível prospectar a adoção de normas de segurança para transformar a PSI, em conjunto com planos de tratamento de risco e auditorias internas, e desenvolver o Sistema de Gestão de Segurança da Informação - SGSI. O desenvolvimento do SGSI é um processo difícil e pode requisitar das empresas a utilização de modelos complexos para compreender toda a estrutura operacional, estabelecer padrões de comunicação e planejamento.

Nos quadros seguintes (4 a 8) são descritas os benefícios e desafios identificadas nos artefatos coletados no Capítulo 5:

Quadro 4: Análise do FRAMEWORK LGPD.

SOLUÇÃO	*FRAMEWORK* LGPD
CONTEXTO DE APLICAÇÃO	Inicialização do processo de adequação com a LGPD integrando agentes para validar o nível de conformidade e guiar empresas para identificar suas necessidades e melhorar seus processos.
BENEFÍCIOS	O *framework* possibilita a definição de papéis entre funcionários, departamentos multidisciplinares e o nível gerencial para mapear dados e procedimentos executados. Com a implementação de suas etapas, é possível documentar riscos e identificar as necessidades de privacidade, o que pode auxiliar na produção do RIPD. Por fim, a documentação final do *framework* pode detalhar a alocação de recursos e descrever o planejamento de conformidade.
DESAFIOS	Dependendo do porte da empresa, é necessário implementar grande quantidade de documentação para detalhar o fluxo de dados e dos processos, o que dificulta a organização e aplicação prática das demandas de adequação encontradas.

Fonte: Implementado pelo Autor.

Quadro 5: Análise do LGPD Model Canvas.

SOLUÇÃO	LGPD Model Canvas
CONTEXTO DE APLICAÇÃO	Ferramenta de trabalho visual, que busca evidenciar como a privacidade de dados é abordada e qual seu nível de influência em atividades vitais ou corriqueiras da organização.
BENEFÍCIOS	O *framework* é capaz de descrever as atividades atuais e prospectar novos quadros com atividades otimizadas, a serem implantadas e integradas à organização, de acordo com objetivos definidos. É uma solução que busca privilegiar as demandas da LGPD na criação de cada tarefa das empresas.
DESAFIOS	A solução demanda um esforço coletivo para executar um preenchimento descritivo de processos, incluindo a integração com produtos e serviços fornecidos. Além disso, a quantidade de quadros a serem implementados e sua característica descritiva pode tornar a utilização da solução ineficiente para empresas de grande porte.

Fonte: Implementado pelo Autor.

Quadro 6: Análise do BPMN.

SOLUÇÃO	BPMN
CONTEXTO DE APLICAÇÃO	A utilização da metodologia BPMN, como notação dos processos de adequação com a lei de proteção de dados gera uma investigação visual e padronizada capaz de desenvolver artefatos, que descrevem o passo a passo das avaliações de dependências com a LGPD, dos atores relacionados ao tratamento de dados e dos procedimentos executados.
BENEFÍCIOS	Com as modelagens, é possível institucionalizar processos e procedimentos que podem ser acessados por funcionários e operadores de dados. A disseminação das sequências de atividades modeladas podem ser padronizadas na organização e novos atores podem ser instruídos para executar as operações planejadas. Além disso, a modelagem dos negócios possibilita que as organizações identifiquem e priorizem os procedimentos e demandas mais complexas ou mais importantes no quesito de tratamento de dados.
DESAFIOS	Com a criação dos modelos, a dificuldade imposta pela utilização do BPMN é que, apesar de ser uma notação padronizada, os modelos implementados não são de fácil interpretação para qualquer profissional, logo, a interpretação e transcrição dos passo a passo para executar os processos torna-se uma atividade essencial. O treinamento e qualificação dos operadores de dados e profissionais envolvidos nos processos de adequação da LGPD deve ser prioridade para executar de forma prática as modelagens propostas na organização. Os procedimentos especificados devem ser disseminados de forma clara, para que os atores aumentem sua maturidade na execução de suas tarefas, e assim, possam compreender e fixar a sequência de ações programadas para atender as exigências organizacionais no tratamento de dados pessoais.

Fonte: Implementado pelo Autor.

Quadro 7: Análise dos Padrões de Referência.

SOLUÇÃO	ISO SÉRIE 27000
CONTEXTO DE APLICAÇÃO	O Padrão 27001 para sistema de gestão da segurança da informação que pode certificar organizações com interesse em adotar normas capazes de aprimorar requisitos gerais para implementar, monitorar e melhorar a administração organizacional nos aspectos de segurança dos dados. Outras normas da série 27k podem criar ferramentas para mitigação de risco, modelagens e requisitos específicos de privacidade de dados.
BENEFÍCIOS	O padrão impõe o envolvimento da alta gestão organizacional para produzir as políticas analisando e descrevendo os riscos de proteção e privacidade de dados, além de especificar o constante dever de monitoramento e atualização das diretrizes criadas. A associação direta da LGPD com os aspectos do padrão de segurança (como visto na Seção 5.3) é um bom benefício para as organizações que buscam aderir a norma.
DESAFIOS	A adoção completa da norma, apesar de demonstrar esforço organizacional e uma implantação eficaz para a LGPD, não é viável para muitas organizações de pequeno ou médio porte, visto que, muitas não possuem profissionais com disponibilidade de tempo, ou capacidade técnica para implementar todas as exigências de um SGSI completo. Logo, a abordagem demanda a capacidade de uma empresa em alocar muitos recursos e investimentos, o que geralmente pode ser acessível apenas para grandes corporações.

Fonte: Implementado pelo Autor.

Quadro 8: Análise do DMM.

SOLUÇÃO	Data Management Maturity - DMM
CONTEXTO DE APLICAÇÃO	Ao implementar todas as estruturas do DMM, as organizações são capazes de definir o estado atual do gerenciamento de dados e definir o conjunto de práticas a serem executadas na governança das informações para elevar o nível de capacidade de cada tipo de processo especificado.
BENEFÍCIOS	Fornece um modelo de dados capaz de formalizar a multiplicidade de percepções sobre aspectos enraizados e significativos das organizações. O DMM pode ser identificado como uma ferramenta poderosa, especialmente para grandes conglomerados e grandes corporações que possuem processos e operações de dados pessoais massivos sobre uma grande quantidade de sistemas e procedimentos, além de fluxos e transferência de dados pessoais entre entidades internas e externas. O modelo ainda prevê integrar os sistemas de informação utilizados na organização aos processos adaptados e otimizados.
DESAFIOS	A principal barreira para a consolidação do DMM para adequação com a lei de dados é sua viabilidade e tempo de implementação, fatores que dependem da complexidade e magnitude da empresa, quantidade de riscos a serem tratados, a quantidade de mudanças a serem aplicadas e os recursos humanos capacitados em colaborar e implementar todos os processos do modelo para o nível de capacidade otimizado. Como especificado na Seção 5.2, o nível otimizado significa desenvolver os processos de governança de dados, tratando as informações como ativos essenciais para as ações da organização e percebendo a segurança e privacidade dos dados pessoais como indispensável e inegociável.

Fonte: Implementado pelo Autor.

Com a análise obtida sobre as soluções relacionadas aos processos organizacionais de adequação, este trabalho lista as seguintes recomendações para a conformidade com LGPD:

R1. **Integração de Atores para Inicialização da Conformidade com a LGPD**

Descrição:

- Ao iniciar o projeto de conformidade com a LGPD, é necessária a inclusão de atores para criação de uma cultura organizacional amigável à privacidade de dados e desenvolver: a especificação de objetivos, a construção do planejamento, as execuções de todas as requeridas na legislação;
- Os atores são profissionais, gestores, auditores internos e externos, agentes de tratamento especificados na LGPD (controladores e operadores) e encarregados de dados.

Soluções envolvidas:

- *Framework* LGPD Model Canvas que envolve setores, funcionários e entidades para atualizar processos internos;
- Metodologia Scrum que especifica as atribuições para realização de atividades e entregas coletivas;
- *Framework* LGPD que especifica a criação de um comitê interdisciplinar de governança de dados;

- ISO 27001 que especifica a necessidade do envolvimento da alta administração nos esforços de conformidade.

Recomendado para: Todas as organizações que demandam engajamento de funcionários, gestores, administradores, agentes de tratamento para as ações de adequação.

R2. **Mapeamento de Dados e Fluxo de Dados**

Descrição: Para atender aos requisitos da LGPD, é vital verificar a natureza dos dados processados e o fluxo de coleta, processamento, análise e compartilhamento de dados.

Soluções envolvidas:

- O *Framework* LGPD MODEL CANVAS pode apoiar a descrição dos tipos de dados e seus fluxo, tanto para empresas de médio e de pequeno porte, ou até Microempreendedores individual que processam dados pessoais armazenados em um único sistema, ou em documentos físicos;
- Para organizações de grande porte. ou órgãos públicos com quantidade massiva de dados de cidadãos o DMM apoia os mapeamento, sobretudo nas categorias de processo de qualidade de dados e operação de dados.

Recomendado para: O processo de mapeamento de dados é essencial para qualquer organização que pretende a adequação com a LGPD.

R3. **Relatório de Impacto à Proteção de Dados Pessoais - RIPD**

Descrição: A construção do RIPD é um processo especificado na LGPD para prestação de contas das organizações com a autoridade nacional ANPD. A documentação deve prover detalhes do estado presente de conformidade, identificando os riscos de violação dos princípios da lei e os procedimentos de salvaguarda. As modelagens de processo e a documentação das ações e recursos alocados para atender à proteção de dados são recursos que facilitam a construção do RIPD.

Soluções envolvidas:

- *Framework* LGPD e LGPD MODEL CANVAS para criação de um RIPD inicial ou atualizado com a evolução da conformidade;
- O modelo DMM é mais viável para apoiar a produção do documento em grandes corporações, visto que, o RIPD precisa gerar detalhes completos sobre aspectos minuciosos de muitos setores e sistemas.

Recomendado para:

- Qualquer organização que armazena uma quantidade significante de informações pessoais para receber demandas ou cobranças da autoridade nacional;
- É especialmente necessária para órgãos públicos e empresas com sistemas de informação que processa dados de usuários.

R4. **Modelagem de Processos de Conformidade à LGPD**

Descrição: Diagnosticar as exigências estabelecidas pela LGPD nos procedimentos organizacionais, visando modelar processos adaptados à proteção e privacidade de dados, utilizando a notação BPMN, por exemplo. É imperativo que as instituições delineem claramente suas necessidades e modelem os processos essenciais para garantir o cumprimento dos direitos dos titulares de dados, atendendo, assim, às demandas da autoridade nacional.

Soluções envolvidas:

- Modelagem de negócio com a notação BPMN;
- Metologia ágil Scrum e o *framework* LGPD Model Canvas podem ser utilizados para traduzir as modelagens de processos em linguagem natural, para disseminar os procedimentos e possibilitar o treinamento e instrução das atividades.

Recomendado para: Empresas de médio e grande porte com multiplicidade de processos serem adaptados aos requisitos da LGPD.

R5. **Criação de Política de Segurança da Informação - PSI**

Descrição: O desenvolvimento da PSI emerge de uma documentação que descreve as regras, delineando procedimentos e ações adotadas para garantir a SI. Essa documentação abrange minuciosamente o fluxo e o ciclo de vida dos dados, incluindo uma lista detalhada de entidades, artefatos e sistemas que processam e compartilham informações. A precisão desse detalhamento é intrinsecamente ligada à Lei Geral de Proteção de Dados, pois ao especificar os pormenores das informações organizacionais, os dados pessoais são correlacionados às exigências específicas de segurança.

Soluções envolvidas: A adoção da Norma 27001 especifica o desenvolvimento de PSI nos primeiros passos para a certificação do padrão de segurança.

Recomendado para:

- Empresas de médio e grande porte com multiplicidade de processos e regras a serem adaptados aos requisitos da LGPD;
- Empresas que possuem, desenvolvem e/ou gerenciam sistemas da informação ou são baseadas em produção de tecnologia (sistemas digitais / aplicações para internet).

R6. **Desenvolvimento do Sistema de Gestão de Segurança da Informação - SGSI**

Descrição: O SGSI é um sistema (não necessariamente um sistema automatizado) que descreve e engloba todos os procedimentos e políticas organizacionais para a SI. A correlação dos requisitos impostos pela LGPD com as diretrizes estabelecidas pela norma ISO 27001, que formaliza a implementação do SGSI, representa uma garantia sólida da pertinência e utilidade desse sistema na proteção efetiva dos dados.

Soluções envolvidas: O objetivo final da norma ISO 27001 é o desenvolvimento do SGSI. Outros padrões da série ISO 27000 podem ser adotados para implementar um SGSI mais completo e mais robusto para a segurança da informação.

Recomendado para: Grandes corporações que buscam a certificação de padrões e normas de segurança conceituados.

R7. **Modelo de Governança de Dados**

Descrição: As organizações podem utilizar um modelo de governança de dados capaz de analisar, sistematizar e aprimorar a maturidade no gerenciamento de dados. O modelo deve ser capaz de representar o estado atual da organização, em relação a manipulação e gestão de seus dados. Além do seu estado, deve definir práticas que auxiliem na governança das informações e identificar as oportunidades, pontos fortes e lacunas, para assim, possibilitar a melhora no desempenho de governança e execução das atividades de negócio.

Soluções envolvidas: O DMM para a análise documentação, implementação e melhoramento de processos internos, relacionados à governança e processamento de dados.

Recomendado para: Grandes corporações com entidades, departamentos e fluxo de dados complexo. Dotada de profissionais especializados em governança de dados, aptas a realizar capacitação e treinamentos contínuos, e por fim aptas em destinar recursos tecnológicos e humanos para adaptar seus processos.

A Figura 21 expõe a associação entre as recomendações e os artefatos envolvidos em suas soluções. A primeira coluna representa as recomendações desenvolvidas neste capítulo, já a última coluna está relacionada com os estudos que serviram de referência para a criação das recomendações. Por fim, as células em azuis indicam a existência do relacionamento entre a recomendação e os artefatos estudados.

	FRAME-WORK LGPD	LGPD Model Canvas	*Scrum*	Normas ISO	DMM	BPMN	Referências
R1	■	■	■	■			E3, E5, E7, E14 e E16
R2		■			■		E5, E6, E14 e E17
R3	■	■			■		E1, E7, E9, E14 e E 16
R4	■	■				■	E13, E14, E15 e E16
R5				■			E5
R6				■			E5, E11, E12 e E18
R7					■		E2, E6 e E10

Figura 21: Associação entre recomendações de processos organizacionais e artefatos

Fonte: Implementado pelo Autor.

7.2 Análise de Segurança da Informação

Com o objetivo de implementar novos sistemas e ferramentas digitais ou adaptar as tecnologias já utilizadas na organização para conformidade com a proteção de dados e Segurança da Informação especificadas na LGPD, os controladores e agentes de tratamento devem, a partir do planejamento de uma nova governança de dados que atualize os processos internos, especificar os objetivos organizacionais e as bases legais que autorizam os processamentos de dados. Só após a análise das necessidades do contexto é possível saber quais desenvolvimentos são necessários nos instrumentos tecnológicos.

A especificação das bases legais pela administração das organizações é um ponto chave na especificação de tecnologias, pois, as bases tornam possível a determinação de quais operações podem ser realizadas, e se precisam de consentimento ou se devem se basear em contratos ou em legítimos interesses especificados pelos controladores.

Outro ponto relevante para iniciar os processos de SI para se adequar a LGPD, é a avaliação das capacidades organizacionais e das dificuldades encontradas ao garantir a privacidade dos dados pessoais manipulados na instituição. Os fatores que impactam nas na complexidade dos sistemas e tecnologias da informação estão geralmente relacionados a utilização de uma multiplicidade de sistemas e ambientes de TI, isso pode impactar nas seguintes necessidades:

- Interoperabilidade - Quando mais de um sistema ou setores manipulam dados pessoais com tecnologias diferentes, surge a necessidade de garantir a interoperabilidade dos dados, ou seja, aumentar capacidade dos sistemas de se comunicar e cooperar para a segurança das informações;

- Fluxo de dados - Garantir um compartilhamento e transferência de dados entre tecnologias de forma segura, transparente e seguindo os requisitos e acordos amparados pela LGPD (compartilhando apenas os dados pessoais essenciais para o tratamento das atividades de negócio);

- Dependências Externas - Quando a organização precisa tramitar dados pessoais com tecnologias ou órgãos externos, também é necessário determinar minuciosamente as operações corretas de compartilhamento que não causem nenhuma violação aos dados dos titulares;

A adequação na SI também sofre influência da complexidade nos processos internos, e possui uma dependência direta sobre os investimentos institucionais, tanto sobre seus recursos tecnológicos, como na capacitação dos profissionais de TI para desenvolver e gerenciar as tecnologias.

Como muitas empresas já utilizavam sistemas de informação antes da aprovação da LGPD, as organizações não têm opção a não ser adaptar e atualizar as tecnologias para garantir a privacidade de dados pessoais. No entanto é observável que no momento atual as empresas têm a oportunidade de garantir a Privacidade por Design e Padrão, desenvolvendo o zelo pela proteção e privacidade a cada novo sistema e na criação de novos projetos.

Nos quadros seguintes (9 a 13) são descritas os benefícios e desafios identificadas nos artefatos coletados no Capítulo 6:

Quadro 9: Análise do Sistema de Controle de Acesso.

SOLUÇÃO	Sistema de Controle de Acesso - GENERAL_D Framework
CONTEXTO DE APLICAÇÃO	O sistema de controle de acesso apresentado é aplicado em sistemas TIC Inteligente que incorpora princípios do RPGD ao adotar o GENERAL_D Framework que instancia o Gerenciador de Controle de acesso que pode manipular políticas de controle de acesso que sejam amigáveis à privacidade de dados.
BENEFÍCIOS	Com a aplicação do GENERAL_D Framework o SCA é capaz de automatizar o gerenciamento do controle de acesso de acordo com os princípios das leis de privacidade de dados. A utilização de um controle de acesso construído para atender a proteção de dados pessoais pode aumentar a efetividade da adequação organizacional e destacar o nível de maturidade no âmbito de SI em uma organização.
DESAFIOS	A atuação correta do controle de acesso baseado no GENERAL_D Framework pode ser custosa e extensa, pois, é necessário implementar e validar as políticas de controle de acesso correspondentes com os requisitos legislativos do RGPD europeu. Para adaptar para a LGPD é necessário reavaliar cada requisito e aplicar as PCAs de acordo com as particularidades brasileiras.

Fonte: Implementado pelo Autor.

Quadro 10: Análise do CaPe.

SOLUÇÃO	CaPe
CONTEXTO DE APLICAÇÃO	Gerenciador de consentimento que atua integrado ao GENERAL_D Framework para realizar a gestão de dados pessoais durante a vigência do consentimento entre titular e controlador.
BENEFÍCIOS	O CaPe possibilita a utilização de um dashboard duplo, o primeiro para que titulares possam acompanhar e manipular os seus consentimentos e o segundo para que os controladores possam manipular seus múltiplos tipos de consentimento. Os consentimentos criados no CaPe também tem função para o sistema de controle de acesso.
DESAFIOS	Para grandes corporações é necessário ver a viabilidade quanto a experiência de usuário por parte dos controladores devido a grande demanda e a variedade na natureza dos consentimentos.

Fonte: Implementado pelo Autor.

Quadro 11: Análise do ADVOCATE.

SOLUÇÃO	ADVOCATE
CONTEXTO DE APLICAÇÃO	O ADVOCATE é uma solução que cria uma estrutura para consentimento de dados pessoais no ecossistema de Internet das Coisas, que, assim como o CaPe, busca promover funcionalidades para organizações e titulares de dados.
BENEFÍCIOS	Além do gerenciamento de consentimento (similar ao desenvolvido no CaPe), o ADVOCATE proporciona uma certificação de consentimento, apoiando a tecnologia blockchain para assegurar a integridade dos consentimentos, e em adição, um componente de inteligência que busca capturar inconsistências nos consentimentos.
DESAFIOS	A aplicação apesar de pioneira e com potencial para influência de novas soluções, o ADVOCATE foi criado para atender a um contexto específico, associando os objetos da IdC dos usuários ao âmbito do consentimento. Apesar de ambicioso, o estado atual da privacidade de dados ainda necessita validar como a indústria e os usuários estão preparados para gerir consentimentos com a interconexão digital de objetos cotidianos.

Fonte: Implementado pelo Autor.

Quadro 12: Análise de Contratos Inteligentes.

SOLUÇÃO	Contratos Inteligentes
CONTEXTO DE APLICAÇÃO	Os contratos inteligentes são programas de computador que automatizam a produção de acordos e negociações, apoiado pela tecnologia blockchain, a principal função dos contratos é armazenar os dados relevantes para executar autonomia nas relações de consentimento/contratuais.
BENEFÍCIOS	O sistema é capaz de armazenar os acordos e consentimentos formalizados provendo um histórico de transações seguro, possibilitando rastreabilidade de dados e a integridade dos contratos.
DESAFIOS	Os contratos inteligentes possuem limitações quanto ao direito de esquecimento visto que a base da tecnologia blockchain é manter a inviolabilidade. Além disso, por ser um software os contratos inteligentes devem possuir constantes atualizações e manutenções para manter a operação e segurança do programa.

Fonte: Implementado pelo Autor.

Quadro 13: Análise de Minimização e Anonimização.

SOLUÇÃO	Minimização e Anonimização
CONTEXTO DE APLICAÇÃO	Os processos de minimização e anonimização de dados estudos são o desenvolvimento de modelo de aprendizagem de máquina de alta precisão para retirada de dados pessoais irrelevantes para o contexto ou para preservar a identidade dos indivíduos.
BENEFÍCIOS	Com a automação dos processos de anonimização e minimização de dados é possível realizar operações e transferências de dados pessoais de forma segura e com mais controle. A aplicação das modelagens pode empoderar os operadores e controladores de dados ao promover estratégias e demandas de acordo com o contexto e com as necessidades de cada operação. Além disso, as operações podem promover a redução do armazenamento de dados e agilidade no compartilhamento de dados.
DESAFIOS	A utilização destas operações possuem limitações quanto à sua abrangência, visto que, as operações são aplicáveis apenas a dados estruturados. Além disso, para utilizar as ferramentas é necessário ter capacitação humana quanto aos algoritmos de aprendizagem de máquina e como manipular os dados de treinamento e os modelos treinados para gerar os modelos anonimizados e minimizados (generalizados).

Fonte: Implementado pelo Autor.

Com os resultados analisados, as seguintes recomendações relacionadas a Segurança da Informação e Tecnologias da Informação no contexto da LGPD são apresentadas:

R8. **Inventário de Necessidades de TI**

Descrição:

Para iniciar a implementação e atualização das tecnologias da informação com requisitos adequados à LGPD é necessário avaliar as mudanças de processos internos e a disponibilidade de alocação de recursos humanos e tecnológicos. Após avaliar o contexto organizacional é viável criar um inventário de necessidades para aquisição de sistemas e artefatos tecnológicos, a fim de implementar os procedimentos de proteção de dados e Segurança da informação aplicadas à LGPD.

Soluções envolvidas: Soluções de governança de dados que possam evidenciar a necessidade de sistemas de informação como:

- A modelagem de processos utilizando modelagem BPMN;
- Descrição dos processos com LGPD Model Canvas que especifica as tecnologias de armazenamento, segurança e transferência de dados usadas em cada procedimento;
- Modelos de dados como o DMM, que especifica a integração da governança de dados com os sistemas da informação utilizados no processamento de dados.

Recomendado para: Qualquer organização que opera dados pessoais com sistemas da informação ou necessita de recursos tecnológicos para se adequar a LGPD.

R9. **Implementação de Privacidade por Design e Padrão**

Descrição:

Para ampliar a capacidade de atingir os requisitos de forma ágil e eficiente é vital realizar a implementação de sistemas e o desenvolvimento de projetos considerando os problemas de privacidade e proteção de dados pessoais. As novas tecnologias adotadas na organização devem prover a partir de suas concepções soluções que maximizem a segurança das informações e e proteção de dados.

Soluções envolvidas:

- Implementar Gerenciamento de Controle Acesso, planejando e especificando os direitos de acesso de cada perfil de usuário e classificando recursos privados e dados sensíveis;
- Gestão de Consentimento para definir as operações permitidas para os dados pessoais processados nos sistemas;
- Anonimização e Minimização de dados em processos que podem violar a privacidade dos dados;
- Especificação de políticas de privacidade que descreve aos titulares todos os processamentos realizados pelo sistema;
- Inspeções de segurança e integridade nos sistemas de informação;
- Manutenção e backups de bases de dados.

Recomendado para: Qualquer organização que fomenta o desenvolvimento e implementação de sistemas da informação e projetos com soluções tecnológicas.

R10. **Interoperabilidade de Dados**

Descrição:

Organizações que possuem múltiplos sistemas que tratam dados pessoais devem garantir uma boa comunicação e cooperação nos processamentos de dados. Para uma boa interoperabilidade é necessário verificar os diferentes sistemas estão abarcado nas mesmas bases legais da LGPD e se possuem os mesmo consentimentos associados, caso contrario, é necessário realizar processamento sobre os dados pessoais para que nenhum direito ou consentimento do titular seja violado.

Soluções envolvidas:

- Modelagem de processos com BPMN para modelar transferências de dados entre sistemas internos;

- Controle de Acesso (se possível automatizado) para gerenciar os acessos a recursos e dados de cada tecnologia;
- Anonimização e minimização caso seja necessário pré-processar os dados pessoais entre sistemas com diferentes permissões de tratamento.

Recomendado para: Organizações com estruturas internas complexas e que gerenciam ou utilizam múltiplos sistemas e tecnologias que processam dados pessoais.

R11. **Compartilhamento de dados com entidades externas**

Descrição:

Realizar o compartilhamento e transferência de dados pessoais com órgãos externos como: empresas parceiras, órgãos públicos e em demandas de portabilidade de dados. O compartilhamento deve avaliar as especificações das bases legais que autorizam a operação e os processo de transferência deve conter ferramentas de segurança para evitar vazamentos e corrupção dos dados.

Soluções envolvidas:

- Gestão de Consentimento para verificar a viabilidade do compartilhamento;
- Modelagem de processos com BPMN para modelar transferências de dados rotineiras e planejadas;
- Anonimização e minimização caso seja necessário pré-processar os dados pessoais antes do compartilhamento.

Recomendado para: Organizações com processos de transferência de dados pessoais com órgãos externos;

R12. **Gestão de Consentimento**

Descrição:

Os controladores de dados devem coletar os consentimentos dos titulares de forma explícita e especificar todos os objetivos de tratamento sobre os dados para promover transparência e evitar que o proprietário dos dados cometa equívocos.

Para pequenas e médias organizações que armazenam dados em poucos sistemas o consentimento pode ser coletado no início de tratamento, e o gerenciamento deve avaliar o prazo ou a finalização dos propósitos de tratamento especificados. Para organizações com processos complexos é viável desenvolver uma gestão de consentimento que capacite controladores e titulares de dados em realizar tarefas como: acompanhamento do acordo, atendimento a requisições de acesso aos dados, alteração de parâmetros dos dados e dos consentimentos e encerramento do acordo.

Soluções envolvidas: Soluções de Gestão de consentimento como-o ADVOCATE (seção 6.2.3) e CaPe (seção 6.2.2) ou até softwares que manipulam acordos formais como Contratos Inteligentes (seção 6.3);

Recomendado para: Organizações que coletam dados pessoais tendo como uma das bases legais da LGPD o Consentimento.

R13. **Verificação de Consentimento**

Descrição:

Os controladores de dados que necessitam aplicar gerenciar e muitos consentimentos, com diferentes origens e especificações precisam desenvolver ferramentas para realizar verificação constante de violação de acordos. Caso algum consentimento seja violado o controlador deve divulgar o incidente a autoridade nacional para determinar quais ações serão tomadas a favor do titular de dados.

Soluções envolvidas:

- Implementação de Sistema ou rotinas (scripts) para verificar violações de consentimento;
- Solução de verificação de consentimento automatizado com ferramenta semântica (seção 6.2.1) ou contratos inteligentes.

Recomendado para: Organizações que coletam dados pessoais a partir de Consentimento e possuem processos complexos e extensos para gerenciar os acordos.

R14. **Implementação de Sistema de Controle de Acesso**

Descrição:

As organizações devem prover ferramentas de controle de acesso que criem perfis de usuários e caracterize os recursos que podem acessar e manipular dados pessoais. Para sistemas da Informação com processamentos complexos e dados pessoais massivos é recomendável a implementação de um sistema de controle de acesso que possua uma base de Políticas de Controle de Acesso (PCA), atualizadas aos requisitos da LGPD.

Soluções envolvidas:

- Ferramentas de controle de controle de acesso tradicionais que garantem barreiras de acesso aos recursos bloqueados pelos administradores;
- Solução de controle de acesso com Tecnologia da Informação Inteligente capaz de criar PCA traduzidas em XACML (apresentada na seção 6.1.1).

Recomendado para: O controle de acesso é um recurso essencial para qualquer sistema que armazena dados pessoais a fim de garantir proteção e privacidade das informações processadas.

A Figura 22 expõe a associação entre as recomendações relacionadas a Segurança da Informação e os artefatos envolvidos em suas soluções:

	Contratos Inteligentes	BPMN	Controle de Acesso	DMM	Gestão de Consenti-mento	Anonimização /Minimização	Referências
R8		■		■			E6, E13, E14, E16
R9			■		■	■	E24, E26, E27, E28, E29, E31, E33, E34, E35, E36
R10		■	■			■	E13, E15, E26, E27, E28, E29, E39, E40
R11	■	■			■	■	E13, E15, E31, E32, E34, E35, E39, E40
R12	■				■		E26, E34, E35, E36, E37, E38
R13	■				■		E30, E34, E35, E36, E38
R14			■				E26, E27, E28, E29

Figura 22: Associação entre recomendações relacionadas a Segurança da Informação e artefatos.

Fonte: Implementado pelo Autor.

7.3 Documentação relevante para LGPD

Em seu escopo a LGPD motiva ou requisita a criação de documentos capazes de melhorar a proteção de dados ou pessoais, ou servir como registros e até como prestação de contas na aderência de todas as demandas legislativas. Como resultado deste trabalho, a RS executada também foi capaz de nos fornecer algumas recomendações para os documentos mais relevantes para as organizações (Quadro 14).

Quadro 14: Recomendações de documentações para a LGPD.

DOCUMENTOS	DESCRIÇÃO	RECOMENDAÇÕES	REFERÊNCIAIS
Mapeamento de Dados Pessoais	O mapeamento dos dados pessoais podem ser registrados em uma documentação capaz de auxiliar o monitoramento e atualização dos ativos de informações pessoais de uma instituição	Recomenda-se, primeiramente, que as organizações avaliem quais dados serão processados, considerando a perspectiva de negócios, a legitimidade do tratamento pretendido e o legítimo interesse. Outro ponto importante é o reconhecimento do princípio da necessidade, ou seja, limitar a coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades. Para uma boa descrição do documento, é necessário entender e descrever o fluxo, a categoria dos titulares de dados e o ciclo de vida dos dados.	E1, E2, E3, E4, E6, E9, E13, E14 e E16
Registro de operações de tratamento e Inventário de Dados Pessoais	Documentação de registro de operações de tratamento e inventário de dados pessoais, que atende a determinação explícita da LGPD referente ao levantamento e registro do tratamento realizado pela instituição.	Esta documentação deve descrever as atividades de processamento de dados pessoais, fornecendo informações valiosas para as instituições, como: (1) Os atores envolvidos, incluindo os agentes de tratamento e o encarregado; (2) As bases legais que justificam o tratamento e a finalidade (o que a instituição faz com o dado pessoal); (3) A descrição dos dados utilizados; (4) Os locais em que os dados pessoais estão armazenados; (5) O tempo de retenção dos dados pessoais; (6) A descrição dos dados e das instituições que fazem parte do processo de compartilhamento de informações pessoais; (7) Uma descrição geral das medidas de segurança atualmente adotadas.	E5, E11, E12, E13, E14, E15 e E18, Art. 37 da LGPD
Política de segurança da informação	Políticas que buscam orientar quanto à adoção de controles e processos para atendimento dos requisitos de Segurança da Informação	As PSI devem ser capazes de orientar a adoção de controles e processos estabelecidos nas melhores práticas de SI, como os definidos na ISO/IEC 27001. Se possível, é importante definir políticas robustas que possam instituir um Sistema de Gestão de Segurança da Informação (SGSI). Para isso, é necessário: (1) Especificar as diretrizes e orientações estratégicas de proteção de dados a serem aplicadas tanto ao ambiente físico quanto ao digital; (2) Indicar um plano de tratamento de risco, utilizando os controles especificados na ISO 27002, o catálogo de ameaças desenvolvido pela ISO 27005, e as medidas de redução de riscos de SI aplicáveis ao gerenciamento e armazenamento de ativos de TI em relação a dados pessoais, como definido na ISO 27701. (3) Realizar auditorias internas periódicas para o aperfeiçoamento e desenvolvimento de novas políticas; (4) Detalhar normas específicas, como: Norma de Controle de Acesso (que pode definir Políticas de Controle de Acesso específicas para a proteção de dados), Norma de Backup, e Norma de Gestão de Incidentes e Violações de Dados Pessoais.	E5, E11, E12, E18, E19, E22, E23, E24, E28, E29 , E30.
Política Interna de Privacidade e Proteção de Dados Pessoais	Documentação que deve descrever as diretrizes necessárias para atender aos requisitos da LGPD de forma integral para todos os níveis da organização	Quando bem executada, esta política deve instituir um Programa de Conformidade com a LGPD. Este documento é desenvolvido com base nas demandas internas de privacidade e proteção de dados, adaptado às peculiaridades da organização e sempre assegurado e aprovado pela alta gestão. As diretrizes podem incluir normas relacionadas a: (1) Gestão de terceiros (garantindo conformidade em qualquer atividade envolvendo parceiros e entidades públicas dependentes); (2) Cláusulas contratuais de proteção de dados pessoais; (3) Gestão de consentimento; (4) Procedimentos para atendimento dos direitos dos titulares; (5) Procedimentos para atendimento das requisições da ANPD.	E1, E5, E6. E7, E30, E31, E32, E33, E34, E35, E36, E37 e E38
Política Externa de Privacidade	Conhecido popularmente apenas como "Políticas de Privacidade", este documento possui o objetivo de exercer transparência ao informar os titulares de dados sobre o detalhamento das atividades de tratamento de dados pessoais executadas pelas organizações.	É essencial garantir que a política esteja facilmente disponível e escrita em linguagem clara. O documento deve especificar como todos os princípios de tratamento de dados requeridos pela LGPD são atendidos. É altamente recomendável que as organizações minimizem a carga de leitura e utilizem uma linguagem acessível e direta para atender aos interesses dos titulares. Em geral, uma boa Política de Privacidade deve conter: (1) A especificação dos tipos, condições e duração dos tratamentos de dados; (2) Os dados de contato da organização, incluindo a especificação do encarregado de dados e como contactá-lo; (3) A especificação de qualquer compartilhamento de dados pessoais com empresas ou serviços externos à organização; (4) As medidas de segurança da informação e proteção de dados adotadas. (5) A especificação dos direitos e reivindicações dos titulares.	E3, E6, E11, E24 e E25
Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)	O relatório é uma responsabilidade legal criada pela LGPD. Ele é desenvolvido para especificar todos os processos envolvidos no tratamento de dados pessoais que podem trazer risco às liberdades civis. O RIPD é a principal fonte de transparência e de prestação de contas para comprovação de adequação com a LGPD.	Para o desenvolvimento do Relatório de Impacto à Proteção de Dados (RIPD) e para a prestação de contas à ANPD quanto à adequação à legislação, é recomendado que o documento detalhe: (1) Descrição dos tipos de dados coletados, validade do tratamento e a metodologia de coleta de dados; (2) Detalhamento de categorias especiais de dados pessoais, como dados sensíveis ou dados de crianças e adolescentes; (3) Garantias de segurança das informações, com descrições detalhadas do gerenciamento de risco, integridade, vazamentos e controle de acesso; (4) O relatório deve ser realizado periodicamente e preceder o desenvolvimento de novos processos e a implementação de novos sistemas e projetos na organização.	E6, E8, E9, Art. 38 da LGPD

Fonte: Implementado pelo Autor.

7.4 Aspectos Prioritários

Analisando os aspectos prioritários no processo de aderência a LGPD em uma empresa, foi possível identificar os requisitos apresentados no Quadro 15. Salienta-se que esses requisitos podem ter prioridades distintas dependendo do contexto ou finalidade do negócio, no entanto, a coluna 'TIPO' elenca a prioridade identificada para os requisito discutidos neste trabalho classificando como: (1) 'E' o requisito de alta importância, podendo ser considerados até essenciais para qualquer organização; (2) 'A' os requisitos de alta importância que devem ser implementadas para uma implementação completa e robusta da LGPD; e (3) 'B' requisitos de baixa prioridade, ou requisitos que se tornam importantes (ou até essenciais) dependendo do contexto organizacional e do tipo de tratamento necessário.

Quadro 15: Requisitos prioritários para a LGPD.

FOCO	REQUISITOS PRIORITÁRIOS	TIPO	REFERÊNCIAIS
PROCESSOS ORGANIZACIONAIS	Mapeamento de dados	E	E1, E2, E6, E7, E14
	Definição de uma equipe multidisciplinar para Implementar LGPD	E	E6, E7, E14
	Adaptação de processos internos	E	E6, E7, E11, E12, E13, E14, E18
	Privacidade por Design e Padrão	E	E14, E17
	Especificação de bases legais	E	LGPD Art 7
	Elaboração da Política de Privacidade	E	E24
	Adaptação nas modelagens de negócio	A	E13, E15
	Gestão de riscos	A	E1, E5, E6, E8, E11, E12, E18
	Criação de PSI	A	E11
	Formalização do Board de Segurança da Informação	B	E6, E7, E14
	Metodologias ágeis na implementação da LGPD	B	E1
	Desenvolvimento do SGSI	B	E5, E11, E12, E18
	Avaliação de qualidade de dados	B	E6
TECNOLOGIA DA INFORMAÇÃO	Integridade dos dados	E	E5, E6, E18, E27, E28, E29, E30
	Controle de Acesso	E	E27, E28, E29, E30
	Dados Históricos, backup, arquivamento e retenção	E	E5, E6, E27, E36
	Adaptações na abordagem arquitetural	A	E6, E19, E27
	Criptografia	A	E5
	Auditorias de SI	A	E5, LGPD
	Portabilidade dos dados	A	E27, E35, E40, E41
	Interoperabilidade de dados	A	E5, E11, E27, E35, E40, E41
	Gestão de Consentimento	B	E30, E31, E32, E33, E34, E35, E36, E37, E38, E39
	Anonimização e Minimização	B	E40, E41
	Consentimentos formalizados por Contratos Inteligentes	B	E37, E38, E39

Fonte: Implementado pelo Autor.

8 CONSIDERAÇÕES FINAIS

O aumento do processamento de dados pessoais tanto nas demandas públicas, quanto na esfera de negócio, e nas áreas de pesquisa, promoveu o debate no tema de privacidade de dados. Isso impulsionou a implementação de legislações capazes de formular diretrizes de boas práticas e responsabilizar condutas antiéticas e danosas aos indivíduos, assim como, no desenvolvimento de ferramentas capazes de construir modelos e sistemas que assegurem a segurança das informações pessoais.

Esse crescimento na utilização dos dados pessoais levantou sérias preocupações sobre os problemas sócio-técnicos, tanto na perspectiva de direitos humanos, quanto nos direitos do consumidor para assim garantir o exercício integral da cidadania. Na perspectiva de quem detém, ou processa dados, também é relevante o cuidado com o desenvolvimento econômico e tecnológico, a inovação e a livre concorrência, em qualquer órgão privado que detenha dados da sociedade.

A implantação de uma nova lei de proteção de dados do Brasil passa a ser um item básico nas organizações. A lei concebe um avanço, tanto para a tecnologia, especialmente no tema de segurança da informação, quanto aos aspectos econômicos, onde empresas terão uma normas estáveis para melhorar a segurança e efetividade de seus processos internos, e consequentemente, apurar o vínculo com os consumidores.

Este trabalho executou uma RS com objetivo de coletar as técnicas e soluções capazes de mitigar os riscos à privacidade e atender as demandas da LGPD, com artefatos tecnológicos e organizacionais. Os estudos apresentados exploram desde tecnologias que implementam medidas específicas de SI para proteção de dados, até metodologias capazes de planejar e executar processos complexos na estrutura interna das organizações.

Os artefatos apresentados no Capítulo 5 auxiliam em condutas organizacionais para prover o planejamento e análise dos dados pessoais seguindo as preocupações e requisitos criados na LGPD. Já as soluções descritas no Capítulo 6 descrevem artefatos voltados a implantar um sistema capaz de assegurar a integridade, confidencialidade, autenticidade e legalidade dos dados. Com isso atendemos aos objetivos específicos (1) e (2) que buscaram identificar metodologias, práticas, processos organizacionais e ferramentas (Seção 1.3).

A revisão evidenciou que a diversidade de estratégias implementadas nos últimos anos, em muitos casos, foi desenvolvida de forma desconexa. Diante desse cenário, as soluções de conformidade com as legislações foram concebidas de maneira paralela, revelando uma lacuna na especificação de todos os recursos e artifícios necessários para uma implementação abrangente da LGPD, alinhada às exigências específicas das organizações. Para cada artefato discutido no trabalho foi possível elencar vantagens e desvantagens em sua utilização, alcançando, dessa forma, o objetivo específico 3 da Seção 1.3.

Também como resultado da RS, a análise proposta no Capítulo 7 identificou 14 recomendações de implementação, visando executar boas práticas de privacidade e estabelecer processos seguros e alinhados aos requisitos da LGPD. Espera-se que essas recomendações contribuam para a implementação da LGPD de forma consistente e eficiente. Em acréscimo, foram apresentadas no quadro 14, as recomendações para o desenvolvimento de documentos relevantes para LGPD, e por fim, no quadro 15, a análise da classificação por prioridade dos requisitos exigidos na legislação.

Este trabalho serviu de base para a construção de artigos científicos relacionados à proteção de dados no âmbito das empresas e organizações. Nesta perspectiva nossa pesquisa já foi bem avaliada possuindo uma aceitação de publicação no WICS - 5º Workshop sobre as Implicações da Computação na Sociedade, e possui mais um artigo em análise para uma revista científica.

8.1 Limitações e Trabalho Futuro

As principais limitações enfrentadas neste trabalho residem no processo de coleta de estudos, que se restringiu aos três portais que disponibilizam acesso livre aos artigos, além da restrição aos idiomas português e inglês. Como a RS executada neste estudo explorou múltiplos artefatos e artigos, é possível considerar a limitação em alguns estudos, onde não há uma aplicação ou verificação completa dos artefatos quanto à sua aplicabilidade total para a LGPD ou RGPD. Neste caso, todos os artigos que expressam tais restrições possuem justificativa e a exposição das limitações na apresentação de seus conceitos (Capítulo 5 e 6).

A área de privacidade de dados e LGPD apresenta muitas oportunidades e lacunas para pesquisas acadêmicas e estudos de caso. Aqui apontamos alguns caminhos possíveis para trabalhos futuros ao considerar os artefatos que exploramos neste trabalho como ponto de partida para novas investigações:

- Analisar criteriosamente o impacto em infraestrutura de TI que a LGPD impõe para manter a conformidade;
- A criação de uma arquitetura de sistemas ou de suporte à privacidade de dados (genérica ou aplicada à um estudo de caso), contando com as recomendações e resultados explorados nesta RS;
- Aplicar as recomendações descritas na seção 7.1 e 7.2 em uma organização que detenha dados pessoais, para assim, realizar a integração dos processos organizacionais com técnicas de SI;

- Utilizar as soluções organizacionais e de SI encontradas em nossa RS, para avaliar a interseção e solucionar conflitos do uso de inteligência artificial e big data com a privacidade de dados;
- Investigar de forma mais aprofundada, a utilização do GENERAL_D Framework, ADVOCATE, CaPe e Contratos Inteligentes testando seu uso concreto no contexto brasileiro.

Referências

AGOSTINELLI, S. et al. Achieving gdpr compliance of bpmn process models. In: SPRINGER. **Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, June 3–7, 2019, Proceedings 31**. [S.l.], 2019. p. 10–22.

ANPD. **Autoridade Nacional de Proteção de Dados.** 2023. Disponível em ⟨https://www.gov.br/anpd/pt-br⟩. Acesso em: 15 set 2023.

ARAGÃO, S. M. d.; SCHIOCCHET, T. et al. Lei geral de proteçao de dados: desafio do sistema único de saúde. 2020.

BARTOLINI, C. et al. Towards a lawful authorized access: A preliminary gdpr-based authorized access. **ICSOFT**, v. 2019, p. 331–338, 2019.

BARTOLINI, C.; LENZINI, G.; ROBALDO, L. The data protection regulation compliance model. **IEEE Security & Privacy**, IEEE, v. 17, n. 6, p. 37–45, 2019.

BAX, M. P.; BARBOSA, J. L. Proposta de mecanismo de consentimento na lei geral de proteção de dados-lgpd. In: UNIVERSIDADE FEDERAL DE MINAS GERAIS. **Seminar on Ontology Research in Brazil; Doctoral and Masters Consortium on Ontologies**. [S.l.], 2020.

BENTO, C. M. C. **A relação da Lei Geral de Proteção de Dados e Smarts Contracts gerados por blockchain nas empresas**. 2020. Tese (Doutorado) — Centro Universitário de Brasília, 2020.

CALABRÒ, A.; DAOUDAGH, S.; MARCHETTI, E. Integrating access control and business process for gdpr compliance: A preliminary study. In: **ITASEC**. [S.l.: s.n.], 2019.

CANTO, G. et al. **Revisões sistemáticas da literatura: guia prático**. [S.l.]: Curitiba (Paraná): Brazil Publishing, 2020.

CHANG, C. et al. Automated and personalized privacy policy extraction under gdpr consideration. In: SPRINGER. **Wireless Algorithms, Systems, and Applications: 14th International Conference, WASA 2019, Honolulu, HI, USA, June 24–26, 2019, Proceedings 14**. [S.l.], 2019. p. 43–54.

CHHETRI, T. R. et al. Data protection by design tool for automated gdpr compliance verification based on semantically modeled informed consent. **Sensors**, MDPI, v. 22, n. 7, p. 2763, 2022.

(CMMI), T. C. M. M. I. I. **DATA MANAGEMENT MATURITY (DMM)SM MODEL**. 2019. Disponível em ⟨https://stage.cmmiinstitute.com/getattachment/cb35800b-720f-4afe-93bf-86ccefb1fb17/attachment.aspx⟩. Acesso em: 21 fev 2023.

CORRALES, M.; JURČYS, P.; KOUSIOURIS, G. Smart contracts and smart disclosure: coding a gdpr compliance framework. **Legal Tech, Smart Contracts and Blockchain**, Springer, p. 189–220, 2019.

CYBERPILOT. **Sanção da Lei Geral de Proteção de Dados.** 2022. Disponível em ⟨https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/⟩. Acesso em: 2 fevereiro 2023.

DANEZIS, G. et al. Privacy and data protection by design-from policy to engineering. **arXiv preprint arXiv:1501.03726**, 2015.

DAOUDAGH, S.; MARCHETTI, E. The gdpr compliance and access control systems: Challenges and research opportunities. In: **ICISSP**. [S.l.: s.n.], 2022. p. 571–578.

DAOUDAGH, S. et al. How to improve the gdpr compliance through consent management and access control. In: **ICISSP**. [S.l.: s.n.], 2021. p. 534–541.

DARYUS. **Pesquisa nacional 2022-2023 - Privacidade e Proteção de Dados Pessoais.** 2023. Disponível em ⟨https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados⟩. Acesso em: 5 abril 2023.

DIAMANTOPOULOU, V.; TSOHOU, A.; KARYDA, M. From iso/iec27001: 2013 and iso/iec27002: 2013 to gdpr compliance controls. **Information & Computer Security**, Emerald Publishing Limited, v. 28, n. 4, p. 645–662, 2020.

FERRÃO, S. É. R. et al. Diagnostic of data processing by brazilian organizations—a low compliance issue. **Information**, MDPI, v. 12, n. 4, p. 168, 2021.

FERREIRA, L.; OKANO, M. T. Um panorama da implementação da lgpd no brasil: uma pesquisa exploratória com 216 profissionais. 2021.

FILHO, D. R. de M. et al. Metodologia scrum: Uma aliada na implementação da lgpd. **Research, Society and Development**, v. 12, n. 4, p. e22712441189–e22712441189, 2023.

FLORES, D. A.; PERUGACHI, R. A gdpr-compliant risk management approach based on threat modelling and iso 27005. **arXiv preprint arXiv:2306.04783**, 2023.

GDPR. **Intersoft Consulting - General Data Protection Regulation (GDPR).** 2016. Disponível em ⟨https://https://gdpr-info.eu⟩. Acesso em: 28 abr 2021.

GOLDSTEEN, A. et al. Anonymizing machine learning models. In: SPRINGER. **International Workshop on Data Privacy Management**. [S.l.], 2021. p. 121–136.

_____. Data minimization for gdpr compliance in machine learning models. **AI and Ethics**, Springer, p. 1–15, 2021.

HUSSAIN, F. et al. Enterprise api security and gdpr compliance: Design and implementation perspective. **IT Professional**, IEEE, v. 22, n. 5, p. 81–89, 2020.

IMB. **AI Privacy Toolkit da - IBM.** 2022. Disponível em ⟨https:https://research.ibm.com/blog/ai-privacy-toolkit⟩. Acesso em: 1 dez 2022.

INOVAçãO, C. **Cria Inovação - Lei Geral de Proteção de Dados(LGPD)**. 2020. Disponível em ⟨https://criainovacao.com.br/lei-geral-de-protecao-de-dados/⟩. Acesso em: 21 jun 2023.

ISO/IEC. **ISO/IEC 27701:2019 Security techniques .** 2019. Disponível em ⟨https://www.iso.org/standard/71670.html⟩. Acesso em: 27 abril 2023.

_____. **ISO 27002: Boas práticas para gestão de segurança da informação.** 2022. Disponível em ⟨https://www.iso.org/standard/75652.html⟩. Acesso em: 27 abril 2023.

JÚNIOR, E. A. da C. **Análise de conformidade de processos de negócios em relação a LGPD**. 2020. Tese (Doutorado) — UNIVERSIDADE FEDERAL DE PERNAMBUCO, 2020.

JUSTICE, S. of California Department of. **California Consumer Privacy Act (CCPA).** 2018. Disponível em ⟨https://oag.ca.gov/privacy/ccpa⟩. Acesso em: 28 abr 2023.

LACHAUD, E. **ISO/IEC 27701: Threats and Opportunities for GDPR Certification. 2020**. 2020.

LGPD. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2018. Disponível em ⟨http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm⟩. Acesso em: 21 set 2020.

LIMA, V. H. Lgpd análise dos impactos da implementaçao em ambientes corporativos: Estudo de caso. Pontifícia Universidade Católica de Goiás, 2020.

LOPES, F.; AMARAL, M. A. A. Implementação da lei geral de proteção de dados pessoais (lgpd) em uma instituição sem fins lucrativos, atuante na área da educação básica. **PROJETOS E RELATÓRIOS DE ESTÁGIOS**, v. 4, n. 1, p. 21–21, 2022.

LUGATI, L. N.; ALMEIDA, J. E. de. A lgpd e a construção de uma cultura de proteção de dados. **Revista de Direito**, v. 14, n. 01, p. 01–20, 2022.

MARQUES, L. N. O mapeamento do modelo data management maturity (dmm) à lei geral de proteção de dados (lgpd). Pontifícia Universidade Católica de Goiás, 2020.

MENEGAZZI, D. **Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução**. 2021. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2021.

MERLEC, M. M. et al. A smart contract-based dynamic consent management system for personal data usage under gdpr. **Sensors**, MDPI, v. 21, n. 23, p. 7994, 2021.

MONTOLLI, C. Â. Segurança da informação e da transparência e a proteção de dados na administração pública: Lgpd, acesso à informação e os incentivos à inovação e à pesquisa científica e tecnológica no âmbito do estado de minas gerais. **REVISTA ELETRÔNICA DA PGE-RJ**, v. 3, n. 3, 2020.

OKANO, M. T. et al. Lgpd o novo desafio para as organizações: Exemplos de frameworks para diagnosticar este novo cenário. **South American Development Society Journal**, v. 7, n. 20, p. 380, 2021.

PAINI, G. S.; ZILLES, M. H. B. A lei geral de proteção de dados: Comentários acerca do propósito e da aplicabilidade. **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, v. 6, p. e27804–e27804, 2021.

PIURCOSKY, F. P. et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de negocios**, Fundación Universitaria Konrad Lorenz, v. 10, n. 23, p. 89–99, 2019.

RAHAT, T. A.; LE, T.; TIAN, Y. Automated detection of gdpr disclosure requirements in privacy policies using deep active learning. **arXiv preprint arXiv:2111.04224**, 2021.

RANTOS, K. et al. Advocate: a consent management platform for personal data processing in the iot using blockchain technology. In: SPRINGER. **Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers 11**. [S.l.], 2019. p. 300–313.

ROCHA, C. P. d. et al. Segurança da informação: A iso 27001 como ferramenta de controle para lgpd. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78–97, 2019.

RODRIGUES, A. C.; PAULA, A. P. de. Prestação dos serviços públicos à luz da lei geral de proteção de dados (lgpd). **Academia de Direito**, v. 4, p. 1039–1055, 2022.

SERPRO. **Como elaborar uma política de privacidade aderente à LGPD?** 2019. Disponível em ⟨https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais⟩. Acesso em: 03 abril 2023.

SILVA, B. S. d. S. **O impacto da LGPD no desenho da política de governança de dados nos municípios: o caso de Belo Horizonte**. 2021. Tese (Doutorado), 2021.

SILVA, R. H. d. et al. Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais. 2021.

TEIXEIRA, G. A.; SILVA, M. M. da; PEREIRA, R. The critical success factors of gdpr implementation: a systematic literature review. **Digital Policy, Regulation and Governance**, Emerald Publishing Limited, 2019.

TEIXEIRA, G. A.; SILVA, M. Mira da; PEREIRA, R. The critical success factors of gdpr implementation: a systematic literature review. **Digital Policy, Regulation and Governance**, Emerald Publishing Limited, v. 21, n. 4, p. 402–418, 2019.

VOSS, W. G. Data protection issues for smart contracts. **Smart Contracts: Technological, Business and Legal Perspectives (Marcelo Corrales, Mark Fenwick & Stefan Wrbka, eds., Hart Publishing/Bloomsbury, 2021), https://www. bloomsburycollections. com/book/smart-contracts-technological-business-and-legal-perspectives**, 2021.