UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS HUMANAS E DA EDUCAÇÃO – FAED
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO DA INFORMAÇÃO

CLARICE BUSS

REQUISITOS DE ACESSO À DADOS: IMPLEMENTAÇÃO EM BASES DE DADOS TRANSACIONAIS DE ACORDO COM A LGPD

FLORIANÓPOLIS
2023

CLARICE BUSS

REQUISITOS DE ACESSO À DADOS: IMPLEMENTAÇÃO EM BASES DE DADOS TRANSACIONAIS DE ACORDO COM A LGPD

Dissertação apresentada como requisito parcial para obtenção do título de mestra em Ciência da Informação pelo Programa de Pós-Graduação em Gestão da Informação do Centro de Ciências Humanas e da Educação – FAED, da Universidade do Estado de Santa Catarina – UDESC.
Orientador: Prof. Dr. José Francisco Salm Júnior.

FLORIANÓPOLIS

2023

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Universitária Udesc,

com os dados fornecidos pelo(a) autor(a)

Buss, Clarice
Requisitos de acesso à dados : implementação em bases de dados transacionais de acordo com a LGPD / Clarice Buss. -- 2023.
119 p.

Orientador: José Francisco Salm Júnior
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Humanas e da Educação, Programa de Pós-Graduação Profissional em Gestão de Unidades de Informação, Florianópolis, 2023.

1. Governança de dados. 2. Lei Geral de Proteção de Dados (LGPD). 3. Privacidade. 4. Ética. 5. Tratamento de dados. I. Salm Júnior, José Francisco . II. Universidade do Estado de Santa Catarina, Centro de Ciências Humanas e da Educação, Programa de Pós-Graduação Profissional em Gestão de Unidades de Informação. III. Título.

CLARICE BUSS

REQUISITOS DE ACESSO À DADOS: IMPLEMENTAÇÃO EM BASES DE DADOS TRANSACIONAIS DE ACORDO COM A LGPD

Dissertação apresentada como requisito parcial para obtenção do título de mestra em Ciência da Informação pelo Programa de Pós-Graduação em Gestão da Informação do Centro de Ciências Humanas e da Educação – FAED, da Universidade do Estado de Santa Catarina – UDESC.
Orientador: Prof. Dr. José Francisco Salm Júnior.

BANCA EXAMINADORA

Prof. Dr. José Francisco Salm Junior
Universidade do Estado de Santa Catarina – UDESC

Membros:

Prof. Dr. Alexandre Leopoldo Gonçalves
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Julio Dias
Universidade do Estado de Santa Catarina – UDESC

Florianópolis, 10 de outubro de 2023.

Dedico este trabalho ao meu pai Pedro (*in memoriam*), que vibrou comigo desde o início desse projeto e, com certeza, estará comemorando agora, em algum lugar, a conclusão e sucesso dele.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Dr. José Francisco Salm Junior por aceitar conduzir o meu trabalho de pesquisa, pelos ensinamentos constantes, pela dedicação, pelo suporte, pela paciência, pelas orientações, pela disposição em fazer reuniões com horas de diferença de fuso, e por todo o conhecimento que me proporcionou. Muito obrigada.

Aos meus pais Maria e Pedro (*in memoriam*) que sempre estiveram ao meu lado me apoiando e me incentivando ao longo de toda a minha trajetória, pela base sólida que me proporcionaram, por toda dedicação e carinho que possibilitaram meu crescimento e que foram decisivos para o sucesso e conclusão desse trabalho.

À banca examinadora desse trabalho, Prof. Dr. Alexandre Leopoldo Gonçalves e Prof. Dr. Julio Dias, pela leitura crítica e sugestões construtivas para a elaboração e evolução desse trabalho.

A todos os meus professores do curso da pós-graduação do PPGInfo da Universidade do Estado de Santa Catarina – UDESC pela excelência da qualidade técnica de cada um, pelos ensinamentos e aprendizados durante o mestrado.

A todos os meus colegas e amigos conquistados durante o curso, pelo convívio (presencial e *online*) e por toda troca e aprendizado.

Aos meus colegas de trabalho da Secretaria de Tecnologia da Informação e Comunicação (SETIC) e à própria instituição pela oportunidade de parceria com a Universidade.

Aos meus amigos, meu suporte, por me apoiarem durante todo esse processo, pela paciência, pela colaboração, pelo incentivo, por me ouvirem, por estarem ao meu lado, por confiarem e por não desistirem de mim. Em especial à nossa “panelinha”, que deu o *start* para esse projeto, às “Deusas” Mayara e Juliana, que embarcaram nessa aventura junto comigo, e aos “Deuses” Jean e Diego, que seguraram as pontas e nos mimaram sempre que possível.

À Amora, que aguentou meu mau humor nos dias mais difíceis.

Agradeço, enfim, a todos que direta ou indiretamente contribuíram para o sucesso e conclusão desse trabalho. Muito obrigada a todos vocês.

“Apenas busquem conhecimento.”
(Autor desconhecido)

RESUMO

Com avanço do uso de tecnologias de informação e comunicação para realizar a coleta e o tratamento de dados pessoais, vem surgindo no mundo um movimento no sentido de regulamentar os procedimentos de armazenamento e uso desses dados. Dessa forma, seguindo esse movimento, no Brasil, em agosto de 2018 foi sancionada a Lei Geral de Proteção de Dados Pessoais, Lei Federal n. 13.709/2018, mais conhecida como LGPD, que visa estabelecer regras e limites para o uso dos dados pessoais, dando poder de consentimento aos donos desses dados. Nesse sentido, todas as empresas e organizações, tanto do setor público, quanto do setor privado, precisam se adequar a nova lei que entrou em vigor em agosto de 2020 e começou a fazer valer suas diretrizes e sanções a partir de maio de 2021. Diante desse cenário, a Universidade do Estado de Santa Catarina (UDESC) como instituição pública que faz tratamento de dados pessoais, precisa se adequar às diretrizes da LGPD, assim, este trabalho tem como objetivo propor um modelo para implementação de requisitos de acesso à dados transacionais, em Instituições de Ensino Superior, que estejam em conformidade com os preceitos da LGPD, utilizando para isso uma base de dados de referência da UDESC para analisar o cenário atual, mapeando os riscos e vulnerabilidades de segurança dos dados armazenados, proporcionando melhorar a governança dos dados. Quanto aos aspectos metodológicos, além da pesquisa bibliográfica, esta é uma pesquisa de natureza aplicada, onde a forma de análise dos dados se dará de forma descritiva, utilizando cenários de caso e o método *Design Science Research* (DSR) como procedimentos, a fim de permitir a concepção de um artefato (modelo). Os resultados encontrados demonstraram que o modelo apresentado segue as diretrizes da LGPD e, com base em métodos e processos já referenciados por outras literaturas, demonstra que é possível sua aplicação em bases de dados transacionais de uma Instituição de Ensino Superior. Além disso, foi possível concluir que o uso adequado da Governança de Dados e a conformidade com a LGPD são essenciais para assegurar que o acesso a dados pessoais seja realizado de maneira ética, legal e segura.

Palavras-chave: Governança de dados; Lei Geral de Proteção de Dados (LGPD); Privacidade; Ética; Tratamento de dados.

ABSTRACT

As information and communication technologies evolve, a global movement has arisen to regulate the storage, use and processing of personal data. In Brazil, a federal law n. 13,709/2018 known by its acronym LGPD, that stands for "*Lei Geral de Proteção de Dados Pessoais*", sets rules and boundaries for handling personal data, empowering owners to the right to consent it´s use. Subsequently, organizations in the public and private sectors needed to adapt to this new law. In August 2020 it became rule of law, and the legal system began to enforce its guidelines and sanctions started in May 2021. As a public institution that processes personal data, the Santa Catarina State University (UDESC) also needed to comply with the LGPD guidelines. This work proposes a model for implementing data access requirements in a transactional data environment in a higher education institution that comply with the premises of LGPD. This study will use as reference a database in order to analyze the current scenario, map the risks and security vulnerabilities of the stored data, and provide guidance to improve data governance. As for methodological aspects, in addition to the bibliographical research, this is applied research, where the form of data analysis will be descriptive, using the case study and the Design Science Research (DSR) method as procedures, in order to allow the design of the final artifact (model). The results found demonstrated that the model presented follows the LGPD guidelines and, based on methods and processes already referenced in other literature, demonstrates that it is possible to apply it to transactional databases of a Higher Education Institution. Furthermore, it was possible to conclude that the appropriate use of Data Governance and compliance with the LGPD are essential to ensure that access to personal data is carried out in an ethical, legal and secure manner.

Keywords: Data governance; General Data Protection Law (LGPD); Privacy; Ethic; Data processing.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CF	Constituição Federal
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados
UDESC	Universidade do Estado de Santa Catarina

SUMÁRIO

1 INTRODUÇÃO

Vivemos em um mundo hiperconectado, onde as informações estão disponíveis de maneira fácil e cada vez mais rápidas, em tempo real, podendo ser usadas por qualquer pessoa ou organização. À medida que o acesso às informações cresce, vem crescendo também a preocupação em garantir a privacidade e o manuseio dessas informações, principalmente no que diz respeito aos dados privados de pessoas e/ou organizações.

Nesse sentido, os dados estão se tornando ativos cada vez mais importantes, como estratégia de negócio para as mais variadas empresas e também pela grande versatilidade do seu uso. Para Ghavami (2020), embora a riqueza de uma organização possa ser exibida em balanços e livros eletrônicos, a verdadeira riqueza da organização está em seus ativos de informação – em dados e em quão bem a organização aproveita o valor deles.

Assim, para Barreto (2013), na medida em que os conteúdos digitais se propagam com rapidez, surge a necessidade de buscar convenções e guias que auxiliem na organização das informações disponibilizadas, principalmente na internet. Dessa forma, a Governança de Dados (GD) se apresenta como modelo de estrutura, política, processos e com uma base forte na literatura técnica e científica, que permite evoluir aspectos da qualidade, da segurança e a conformidade no uso de dados.

Conforme Ghavami (2020), sem a GD não há qualidade dos dados, e sem a integração adequada dos dados e a gestão do ciclo de vida da informação, o aproveitamento do valor dos ativos de dados fica limitado. Assim sendo, a GD envolve a definição de responsabilidades claras, a criação de estruturas de tomada de decisão, a implementação de medidas de segurança e privacidade, além do monitoramento e conformidade com as regulamentações aplicáveis.

Ainda segundo Ladley (2019), a GD garante que todos na organização cumpram as regras estipuladas, onde a própria GD fornece as proteções para usar e cuidar dos ativos de dados. Assim, à medida que a tecnologia avança e os desafios éticos evoluem, é essencial que as organizações adotem abordagens proativas e responsáveis para garantir que os dados sejam usados para o bem comum.

Contudo, de acordo com O'Keefe e O Brien (2018), as ferramentas e tecnologias de informação, que existem a disposição dos profissionais de gestão da informação, têm o potencial de trazer benefícios ou causar danos às pessoas. Em especial, se tratando da ética no tratamento de dados pessoais, esses potenciais danos levam a uma grande preocupação mundial para regular o uso de dados pessoais, tentando proteger a privacidade e os direitos fundamentais dos cidadãos.

Consequentemente, diversas leis foram surgindo no mundo para tentar regular o uso das informações pessoais dos indivíduos por empresas e instituições. A exemplo, a União Europeia criou o Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*), que entrou em vigor em 2018 e, segundo Pinheiro (2021), tem o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados, conhecida pela expressão "*free data flow*".

No Brasil, foram criadas diversas leis na tentativa de regulamentar o uso das informações pessoais, destacando-se como exemplo a criação da Lei de Acesso à Informação em 2011, o Marco Civil da Internet em 2014 e, por fim, a Lei Geral de Proteção de Dados Pessoais em 2018, Lei 13.709, mais conhecida como LGPD, que foi inspirada na GDPR. A LGPD tem como objetivo regulamentar o uso de dados pessoais e sensíveis por toda e qualquer empresa, pública ou privada, que realize o tratamento de dados pessoais, *online* e/ou *offline*.

Essas leis visam proporcionar maior segurança e privacidade para as atividades de coleta, tratamento e consulta de dados, principalmente em se tratando de dados pessoais, que vem crescendo de modo acelerado com o uso de Tecnologias de Informação e Comunicação (TIC). De acordo com Hasselbalch (2019), inúmeras iniciativas de políticas públicas de ética de dados foram criadas, indo além de questões de mero cumprimento da lei de proteção de dados para se concentrar cada vez mais na ética de big data, especialmente no que diz respeito a empresas privadas e instituições públicas que lidam com dados pessoais em formatos digitais.

Além disso, de acordo com O'Keefe e O Brien (2018), à medida que as questões éticas relacionadas com a aplicação de tecnologias e práticas de GD ganham cada vez mais destaque nas principais notícias e na discussão política, há apelos ao desenvolvimento e elaboração de novas regulamentações, incluindo abordagens éticas, para ajudar os tecnólogos a lidar com a complexidade das questões que são levantadas.

Deste modo, a tecnologia tornou mais fácil do que nunca coletar e disseminar informações, o que pode ter um impacto significativo na privacidade, na segurança e nos direitos das pessoas, levando a ética da informação a um patamar mais importante a ser trabalhado dentro das regulamentações que vem surgindo. Dessa forma, de acordo com Tsou e Walsh (2023), as referências à ética são frequentemente utilizadas como uma tentativa de antecipar os processos políticos que conduzem à regulamentação.

Diante desse contexto, percebe-se que a GD, a ética e as regulamentações, como a LGPD, estão cada vez mais interligadas, onde a LGPD estabelece o quadro legal para o tratamento de dados pessoais, a GD fornece as estruturas e os processos para atender a essas exigências legais, e a ética orienta as organizações a adotarem uma abordagem moralmente responsável em relação aos dados pessoais que coletam e processam.

Assim, uma GD eficaz e ética é necessária para cumprir as obrigações legais estabelecidas pela LGPD, e, de acordo com Mulholland (2020), esses três pilares são requisitos fundamentais para o correto tratamento de dados pessoais, garantindo a privacidade, a segurança e a qualidade dos dados tratados. Em vista disso, a Universidade do Estado de Santa Catarina (UDESC), como instituição pública de ensino, que trata dados pessoais de alunos, professores, pesquisadores, técnicos e colaboradores, fazendo uso destes dados em sistemas transacionais, também deve se adequar às diretrizes das regulamentações, respeitando a ética e a GD, o que leva a pergunta da pesquisa e aos objetivos, principal e específicos, que serão expostos a seguir.

1.1 PROBLEMA

Como implementar requisitos de acesso à dados, em conformidade com a LGPD, em bases de dados transacionais de Instituições de Ensino Superior?

1.2 OBJETIVO GERAL

Criar um modelo para implementação de requisitos de acesso à dados transacionais, em Instituições de Ensino Superior, que estejam em conformidade com os preceitos da LGPD.

1.3 OBJETIVOS ESPECÍFICOS

a) Catalogar a fonte de dados, apontando aqueles considerados sensíveis, conforme a LGPD;

b) Analisar os riscos de acesso aos dados catalogados e considerados sensíveis, produzindo uma matriz com riscos mitigados, utilizando parâmetros escalares para a classificação dos riscos;

c) Definir um conjunto de requisitos de acesso aos dados catalogados.

1.4 JUSTIFICATIVA

Com o aumento do uso e compartilhamento de informações, principalmente através da internet, vem crescendo também o uso de tecnologias de informação e comunicação (TIC) para automatizar a coleta e o tratamento dessas informações, a fim de facilitar e acelerar o processamento destes dados no intuito de permitir uma melhor análise e uso dessas informações. Com isso, sistemas transacionais se fazem cada vez mais presentes, no intuito de facilitar o processamento e a visualização dos dados coletados.

Assim, à medida que avanços tecnológicos em transações e processamento de dados crescem, também cresce a preocupação com a privacidade e segurança das informações geradas, principalmente em se

tratando de dados e informações pessoais. Nesse contexto, diversas leis vêm surgindo a fim de regular o uso dos dados, como a LGPD, que entrou em vigor em 2021, e visa regular o tratamento de dados pessoais em instituições públicas e privadas, incluindo instituições de ensino como a UDESC.

Dessa forma, esta pesquisa se justifica no âmbito profissional onde a UDESC, como Instituição Pública de Ensino Superior e como detentora dos dados de alunos, professores, técnicos e demais colaboradores e, em algumas situações fazendo uso desses dados no âmbito da ciência de dados, deve atender aos requisitos de proteção de dados, em conformidade com o estabelecido pela LGPD.

Além disso, a coleta de dados para processamento em sistemas transacionais, torna significativo este projeto no âmbito científico, pois proporcionará ampliar a aplicação dos conhecimentos adquiridos na regulamentação dos requisitos de uso dos dados para demais sistemas dentro e fora da universidade. Já no âmbito social, esta pesquisa contribuirá para reforçar o importante papel da universidade pública em demonstrar sua eficiência em atender as regulamentações e proteger a privacidade dos indivíduos.

No âmbito do programa de Pós-Graduação em Gestão da Informação (PPGInfo), vinculado à área de Ciência da Informação, Semeler e Pinto (2019) defendem que a ciência da informação com o uso intensivo dos dados institui uma nova dimensão para os bibliotecários, e assim, de acordo com os autores:

> [...] os bibliotecários devem focar seus esforços para os dados de pesquisa digitais, pois cada vez mais eles proliferaram devido aos avanços tecnológicos da informação e da computação ligados a fazer ciência, sendo que o uso crescente da tecnologia é uma das principais fontes geradoras de dados de pesquisa. (Semeler; Pinto, 2019, p. 117).

Além disso, os autores destacam que “Dados e informação caminham de mãos dadas na Sociedade em Rede, ou Sociedade da Informação e do Conhecimento”. Isso tudo reflete na importância da pesquisa para o programa, reforçando o novo e importante papel do profissional da Ciência da Informação com o cuidado no tratamento dos dados e o impacto da LGPD no uso dessas fontes, incluindo bases científicas, procedimentos de uso, entre outros.

1.5 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada da seguinte forma:

- **Capítulo 1** – Introdução: capítulo corrente que apresenta a Introdução, o problema da pesquisa, os objetivos (geral e específicos), a justificativa para a pesquisa e a estrutura deste trabalho.
- **Capítulo 2** – Fundamentação teórica: capítulo que irá abordar os temas base desta pesquisa, que são:
  - Governança de Dados: apresentando o conceito de dados; o ciclo de vida dos dados; qualidade de dados; boas práticas e governança; governança em privacidade e compliance no contexto da Governança de Dados.
  - Lei Geral de Proteção de Dados (LGPD): apresentando os conceitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais; os fundamentos da Lei Geral de Proteção de Dados; os princípios da Lei Geral de Proteção de Dados e os direitos e liberdades dos titulares de dados.
  - Governança de Dados e as implicações éticas de seu uso: que trará a ética na tecnologia; a ética no uso de dados; a ética e a Lei Geral de Proteção de Dados.
- **Capítulo 3** – Procedimentos metodológicos: capítulo que apresentará a metodologia utilizada para conduzir esta pesquisa em cada uma de suas etapas, e apresentará o *Design Science Research* (DSR), método utilizado na pesquisa.
- **Capítulo 4** – Modelo proposto: apresentação do modelo proposto para a implementação de requisitos de acesso à dados transacionais, em Instituições de Ensino Superior, em conformidade com os preceitos da LGPD.
- **Capítulo 5** – Análise dos dados e resultados: capítulo que apresentará os processos realizados na análise dos dados estudados, resultando nos artefatos propostos no desenvolvimento desta pesquisa.
- **Capítulo 6** – Conclusão: capítulo final que apresentará as considerações finais sobre o modelo desenvolvido e os trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta sessão será apresentada a revisão de literatura referente aos principais conceitos de Governança de Dados (GD); os principais princípios e fundamentos relacionados à Lei Geral de Proteção de Dados (LGPD), que será a fonte legal usada como base desta dissertação; e as implicações ética na GD e na LGPD. Dessa forma, esta fundamentação teórica proporcionará o conhecimento necessário para o desenvolvimento desta pesquisa.

2.1 GOVERNANÇA DE DADOS

A implementação da Governança de Dados (GD) nas organizações foi muito impulsionada pelo aumento do uso das tecnologias de informação e comunicação (TIC), pela crescente quantidade de dados gerados, compartilhados e coletados pelas organizações, pela necessidade de cumprir normas e regulamentações cada vez mais rigorosas e, ainda, pela preocupação com a privacidade dos dados. De acordo com Barbieri (2020), a GD tem uma definição ampla e plural, onde:

> É um conceito em evolução, que envolve o cruzamento de várias disciplinas, com foco central em qualidade de dados no sentido mais amplo deste conceito. Passa por busca de maturidade da empresa na gerência desses recursos, melhoria na valoração e produção dos dados, monitoração de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de compliance, associadas a eles. Para tal, as empresas deverão definir objetivos organizacionais e processos institucionalizados, que serão implementados dentro do equilíbrio fundamental entre TI e áreas de negócios, entendendo que os dados não são mais do domínio de tecnologia e sim um ativo organizacional. (Barbieri, 2020, p. 42)

A *Data Management International* (DAMA-DMBOK, 2017) também define a GD como uma disciplina que trata do planejamento, supervisão e controle sobre o gerenciamento de dados e de uso de dados, sendo um conjunto de práticas, políticas, estruturas e tecnologias que ajudam a garantir a integridade, disponibilidade, segurança e confiabilidade dos dados em uma organização. Também para Mendes (2022), a GD se refere ao gerenciamento, disponibilidade, uso e segurança dos dados e como eles são compartilhados dentro de uma organização.

Contudo, alguns autores confundem a definição de GD com Gestão de Dados. De acordo com Rêgo (2020), a Gestão de Dados se concentra na tecnologia e nos processos para gerenciar os dados, enquanto a GD é mais ampla, e se concentra nos aspectos éticos e regulatórios. Dessa forma, segundo Barbieri (2020), um levantamento das necessidades de Gestão de Dados dentro da organização deve guiar a implantação de um programa de GD, permitindo uma delimitação do escopo para a atuação da GD.

Nesse contexto, Ladley (2019) afirma que a GD é um requisito obrigatório para o sucesso de uma organização, pois ela envolve a definição de responsabilidades e processos para a gestão dos dados, incluindo a sua classificação, armazenamento, uso, proteção e destruição. Com isso, a GD tem um papel importante para assegurar que os dados sejam utilizados de forma ética e eficiente, garantindo assim que a organização possa tomar suas decisões estratégicas baseadas em informações precisas e confiáveis.

Ainda de acordo com Mendes (2022) a GD é voltada para o uso estratégico dos dados, e é um tema responsável por criar as diretrizes e manter a organização diligente com leis e regulamentações. Nesse sentido, Barbieri (2020) afirma que:

> [...] a GD estabelece políticas, padrões, processos, procedimentos [..] e diretrizes corporativas, legislando sobre os dados e atribuindo papéis específicos para se tratar esses elementos com responsabilidade e *accountability* (responsabilidade objetiva e direta). (Barbieri, 2020, p. 43)

Para Rêgo (2020), a GD representa o exercício da autoridade ao controle de estratégias, políticas, padrões, processos, métricas e indicadores envolvidos com os ativos dos dados. Assim também, Ladley (2019), afirma que a GD é a organização e implementação de políticas, procedimentos, estrutura, papéis e responsabilidades que delineiam e reforçam as regras de comprometimento, direitos decisórios e prestação de contas para o gerenciamento eficaz dos ativos de dados.

Ainda nesse contexto, Ghavami (2020) reforça que a GD trata de uma estrutura de políticas, práticas e regras de negócios sobre como coletar, proteger e aplicar dados para viabilizar os negócios. Em vista disso, as políticas de governança corretas darão suporte e complementarão a estratégia da gestão de dados garantindo que as regras sejam cumpridas.

De acordo com Fernandes, Diniz e Abreu (2019):

> [...] A GD é a organização e implementação de políticas, procedimentos, comitês, papéis e responsabilidades que delineiam e reforçam regras de comprometimento, direitos decisórios e prestação de contas para garantir o gerenciamento apropriado dos ativos de dados. (Fernandes; Diniz; Abreu, 2019, p.242-243)

Ainda para os autores, o foco da GD pode variar de acordo com a organização, onde alguns programas de governança centram-se em privacidade, *compliance* e segurança da informação. Também para Ghavami (2020), a GD fornece importantes controles de qualidade de dados, permitindo assim que as empresas tenham conjuntos de dados consistentes e confiáveis, que permitem decisões gerenciais mais rápidas e melhores. Mahanti (2021) também afirma que uma melhor qualidade e segurança dos dados é resultado de uma GD bem evoluída e amadurecida, que permite a criação e aplicação de políticas, processos, funções e responsabilidades.

Diante desse contexto, para entender melhor o contexto da GD, faz-se necessário conceituar seu elemento fundamental: o dado, para então considerarmos as boas práticas e governança necessárias para atender as diretrizes das políticas e regulamentações envolvidas.

2.1.1 Conceito de dados

A definição mais comum e simples encontrada na literatura sobre dados, de acordo com Buckland (1991), é de que “dados são registros ou representações simbólicas de objetos, eventos ou processos”. De acordo com Mahanti (2021), para entender o significado de um dado, deve-se entender não apenas o que os dados devem representar, mas também as convenções de representação que eles empregam para transmitir significado.

Para Barbieri (2020), dado é a representação mais elementar e orgânica de um fato que ainda não possui nenhum significado ou contexto específico. Também segundo a DAMA-DMBOK (2017), os dados são um meio de representação, onde eles podem ser tanto uma interpretação dos objetos que representam quanto um objeto que deve ser interpretado. Assim, quando o dado é apresentado com um contexto ele ganha significado, ele se transforma em informação.

Nesse sentido, o contexto que transforma o dado em informação pode ser definido como metadado, onde, de acordo com Turban *et al*. (2009), os metadados descrevem a estrutura e significados a respeito de dados, contribuindo para que seu uso seja eficiente ou ineficiente, e oferecendo informações que gerem conhecimento. Dessa forma, os metadados podem incluir informações sobre formato, data de criação, autor e outras informações que ajudam a entender e gerenciar os dados.

Contudo, para Ghavami (2020), os metadados não se limitam apenas a nomes, definições e rótulos, segundo o autor, os metadados devem incluir informações mais abrangentes sobre o conjunto de dados, a tabela de dados e a coluna de dados.

Para o guia DAMA-DMBOK (2017), os metadados são essenciais para gerenciar a qualidade dos dados. Assim, Barbieri (2020), reforça que todos os dados devem ter metadados bem definidos, analisados e preservados sob o prisma da qualidade. Nesse contexto, os autores concordam que os metadados são tipos de dados e, como tal, devem ser regidos como outros tipos de dados.

Outra classificação dos dados é apresentada por Barbieri (2020), como uma forma de facilitar o seu entendimento e melhorar sua percepção na forma de como gerenciá-los:

1. **Dados Mestres**: são os dados base ou pilares das empresas. Chamados dados de fundação (*foundational*), tendem a ser mais estáveis e através deles são produzidos os Dados Transacionais.
2. **Dados Referenciais**: têm associação com os Dados Mestres e, devido a sua volatilidade, merecem um gerenciamento especial. Geralmente utilizados com o objetivo de padronização, são normalmente obtidos de fontes externas definidas por entidades oficiais, mas podem ser produzidos internamente, de acordo com o negócio da empresa.
3. **Dados Transacionais**: são dados dinâmicos, produzidos em função da movimentação de negócios da empresa. Conectados com a dimensão tempo, têm data como elemento essencial para caracterizar um evento e estabelecem relacionamentos entre Dados Mestres. Têm valores e cálculos como atributos.

4. **Dados Históricos**: são dados originados dos dados Mestres, Referenciais e Transacionais que são guardados em uma linha do tempo. São dados que permitem tomadas de decisão.

Barbieri (2020), classifica ainda os dados de acordo com o seu formato armazenado, que podem ser: **Estruturado**, **Semiestruturado**, **Não estruturado**. O autor também cita a classificação dos dados quanto à origem (**Internos** ou **Externos**) e quanto à gênese (**Primários** ou **Derivados**), sendo Primários os dados básicos e Derivados os dados produzidos, via um tratamento, a partir dos dados básicos.

As diferentes categorias de dados, segundo Mahanti (2021), precisam ser gerenciadas adequadamente, e as organizações geralmente têm muitas iniciativas de dados em execução em paralelo, por exemplo, gerenciamento de metadados para gerenciar os metadados, gerenciamento de dados mestres para gerenciar dados mestres, iniciativas de segurança de dados para garantir que os dados estejam seguros, iniciativas de qualidade de dados e assim por diante. Ainda segundo o autor, essas iniciativas precisam estar alinhadas, suas dependências precisam ser compreendidas e um ritmo de trabalho precisa ser estabelecido.

Dessa forma, os dados precisam ser precisos e confiáveis, ou seja, precisam ter “valor” para terem significado relevante e serem úteis, produzindo resultados confiáveis para a correta tomada de decisão das organizações. Nesse sentido, Ladley (2019) afirma que o "valor" dos dados aparece na forma como são utilizados, e assim, esses dados passam a ser considerados "ativos". Com isso, ainda para o autor, a GD desempenha um papel fundamental na definição e tratamento de ativos de dados.

Para Mahanti (2021), os dados também podem ser facilmente compartilhados, transformados e excluídos, não se esgotam e podem ser reutilizados, pois os dados não são consumidos à medida que são usados - na verdade, seu valor aumenta com o compartilhamento e o uso.

2.1.2 Ciclo de vida dos dados

De acordo com Barbieri (2020), os dados, assim como outros ativos, têm um ciclo de vida. O ciclo de vida do dado descreve as diferentes etapas pelas quais um dado passa desde sua criação até sua utilização e eventual descarte. Segundo o DAMA-DMBOK (2017), as etapas do ciclo de vida dos dados podem compreender: extração, exportação, importação, migração, validação, edição, atualização, limpeza, transformação, conversão, integração, agregação, referenciação, revisão, análise, garimpo, armazenamento, recuperação, arquivação, restauração e eliminação.

Conforme destacado por Mahanti (2021), a GD melhora a visibilidade em cada fase do ciclo de vida do ativo de dados. Para o autor, o escopo da governança abrange o ciclo de vida dos ativos de dados desde a criação/aquisição e captura, passando pelo processamento e armazenamento, acesso e distribuição, manutenção e arquivamento, exclusão e limpeza, bem como o atendimento aos requisitos de qualidade, segurança, acessibilidade e divulgação.

De acordo com a DAMA-DMBOK (2017), diferentes tipos de dados têm diferentes características de ciclo de vida, e por esse motivo, eles têm diferentes requisitos de gerenciamento. No contexto da LGPD, todas as operações realizadas com dados pessoais são consideradas parte do tratamento de dados pessoais, conforme artigo 5º, inciso X:

> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...] (Brasil, 2018, Art. 5º, inciso X)

Dessa forma, para garantir a privacidade dos dados e estar em conformidade com a LGPD, algumas etapas do ciclo de vida dos dados são consideradas fundamentais, pois estão diretamente relacionadas com as operações de tratamento de dados pessoais da LGPD, conforme apresentado no Quadro 1 a seguir.

Quadro 1 - Ciclo de vida do dado e suas operações de tratamento de dados pessoais, de acordo com a LGPD

Ciclo de vida do dado	Tratamento de dados – LGPD – art. 5º	Conceito
Coleta	Coleta, produção, recepção	É uma etapa crítica para garantir que os dados sejam obtidos de forma lícita e com consentimento adequado do titular dos dados, e de forma precisa e completa. É importante definir padrões para a coleta de dados, bem como diretrizes para garantir que os dados coletados sejam confiáveis.
Armazenamento	Arquivamento e armazenamento	A etapa de armazenamento envolve a garantia da segurança e confidencialidade dos dados, bem como a adoção de medidas de proteção adequadas para prevenir o acesso, a alteração ou o vazamento de dados pessoais ou sensíveis.
Gerenciamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação	A etapa de gerenciamento envolve a adoção de políticas e procedimentos para garantir a qualidade dos dados e sua precisão, bem como a atualização e correção de dados que possam estar incompletos ou desatualizados.
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão	Essa etapa envolve a garantia de que os dados sejam compartilhados apenas com terceiros que tenham uma justificativa legítima para o acesso a esses dados e que tenham adotado medidas de segurança e privacidade adequadas.
Descarte	Eliminação	O descarte adequado dos dados é crítico para evitar a exposição de informações pessoais. Os dados devem ser descartados de forma segura, de acordo com os requisitos legais e regulatórios aplicáveis.

Fonte: elaborada pela autora (2023)

Estas etapas também são importantes para garantir a qualidade dos dados ao longo do seu ciclo de vida, permitindo que as organizações obtenham o máximo benefício dos seus dados. Assim, o ciclo de vida do dado deve ser considerado um processo contínuo, onde cada modelo é usado como uma estrutura para a gestão de dados, permitindo que as organizações gerenciem efetivamente seus dados ao longo de todo o seu ciclo de vida. Para Mahanti (2021), também é importante avaliar a condição atual do ativo de dados, o custo

envolvido na manutenção do ativo de dados, seu valor comercial atual e oportunidades para uso estendido e futuro.

Assim como o ciclo de vida é um aspecto fundamental dentro da GD, a qualidade de dados e as suas métricas também são parte integrante do contexto da GD. A seguir apresenta-se o conceito da qualidade de dados e suas métricas.

2.1.3 Qualidade de dados

A qualidade dos dados é primordial para a correta tomada de decisão pelas empresas. Nesse sentido, Rêgo (2020) afirma que os dados possuem qualidade quando eles satisfazem os requisitos para os quais foram criados, e, com isso, a qualidade dos dados é definida sobre a visão de negócio da empresa, envolvendo esforços integrados através de pessoas, processos e tecnologia com o propósito de gerar valor para a organização a partir dos dados armazenado.

Heinrich *et al*. (2018) também definem qualidade de dados como sendo uma construção multidimensional, compreendendo diferentes dimensões de qualidade de dados, como precisão, integridade, consistência e atualidade. Ainda para Loshin (2010), a qualidade dos dados é a medida em que os dados atendem às necessidades de negócios em termos de sua adequação, precisão, integridade e consistência.

Contudo, segundo Barbieri (2020), a falta de qualidade dos dados é um ponto importante de se entender, pois impacta em problemas como influência da sua reputação ou programas, aspectos críticos de regulação (*compliance*) e mesmo, aspectos de segurança. Redman (2016) foi além, afirmando que dados ruins são como vírus, pois não há como dizer onde aparecerão ou quais danos causarão, o autor ainda afirma que decisões ruins são tomadas com base em dados ruins.

No contexto da LGPD, a qualidade dos dados faz parte de um dos dez princípios fundamentais presentes em seu art. 6º, inciso V, que estabelece:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> [...]
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e

> para o cumprimento da finalidade de seu tratamento; [..] (Brasil, 2018, Art. 6º)

Dessa forma, para atingir a qualidade desejada para os dados são usadas métricas de dimensões de qualidade, onde, de acordo com Heinrich *et al*. (2018) cada dimensão de qualidade de dados fornece uma perspectiva específica sobre a qualidade das exibições de dados. Como exemplo, o guia DAMA-DMBOK (2017) prevê onze dimensões que são: acuracidade, completude, consistência, valor corrente, precisão, privacidade, razoabilidade, integridade referencial, em tempo adequado, unicidade e validade.

Assim, para fins de garantir a qualidade dos dados pessoais e sensíveis, permitindo que as organizações atendam às exigências legais de proteção de dados pessoais (LGPD) e protegendo a privacidade dos dados, é possível considerar algumas métricas de dimensões de qualidade de dados, como: Precisão; Completude; Consistência; Integridade; Confiabilidade; Relevância e Segurança (Quadro 2).

Quadro 2 - Dimensões da qualidade de dados no contexto da LGPD

Dimensão	**Conceito**
Precisão	Os dados devem ser precisos e corretos, sem erros ou inconsistências que possam prejudicar a sua qualidade ou usabilidade.
Completude	Os dados devem ser completos e abrangentes, sem informações relevantes ausentes.
Consistência	Mede a uniformidade dos dados em diferentes fontes ou momentos no tempo. Os dados devem ser confiáveis, com controle de acesso e medidas de segurança adequadas.
Integridade	Os dados devem ser consistentes em todo o seu ciclo de vida, desde a coleta até o armazenamento e uso posterior.
Confiabilidade	Os dados devem ser completos e consistentes, sem duplicatas ou informações conflitantes que possam comprometer a sua integridade.
Relevância	Os dados devem ser relevantes para o propósito para o qual foram coletados, evitando a coleta excessiva ou desnecessária de dados pessoais ou sensíveis
Segurança	Os dados devem ser protegidos contra acessos não autorizados, perda, vazamento ou alteração

Fonte: Elaborada pela autora (2023) baseada no guia DAMA-DMBOK (2017)

Conforme o guia DAMA-DMBOK (2017), as dimensões incluem algumas características que podem ser medidas objetivamente (completude, validade, conformidade de formato) e outras que dependem fortemente do contexto ou da

interpretação subjetiva (usabilidade, confiabilidade, reputação), ainda segundo o guia, quaisquer que sejam os nomes usados, as dimensões de qualidade se concentram em se há dados suficientes (completude), se estão corretos (precisão, validade), quão bem eles se encaixam (consistência, integridade, singularidade), se estão atualizados (temporalidade), acessíveis, utilizáveis e seguros.

Nesse sentido, de acordo com Barbieri (2020), aspectos de privacidade e ética já estão sendo discutidos como elementos associados à qualidade dos dados, assim como os aspectos de dados usados como amostra estatística para definição de modelos de aprendizagem de máquina na Inteligência Artificial (IA). Ainda para Ghavami (2020), para ter sucesso na utilização dos dados é essencial dominar a qualidade dos dados, gerenciamento de dados, privacidade e uso ético de dados e disponibilidade de dados.

Com isso, de acordo com Ghavami (2020), empresas que acertarem na GD poderão gerar benefícios e resultados financeiros substanciais, incluindo custos operacionais reduzidos e economia de tempo, maior confiança nos dados, adoção mais rápida de novas estratégias e retorno acelerado do investimento. Em consequência, buscam-se cada vez mais medidas de boas práticas e governança para administrar os dados e seu ciclo de vida, agregando a qualidade e o valor necessário para a sua consistência e auxílio na tomada de decisão.

2.1.4 Boas práticas e governança

Como observado por Seiner (2014), as melhores práticas de GD formam a base e a diretriz para a execução de um programa de GD, onde essas medidas permitem planejar e implementar diretrizes e padronizações internas no tratamento dos dados, assegurando a viabilidade do acesso a esses dados e garantindo a sua consistência e qualidade, bem como a rapidez e eficiência no seu tratamento. De acordo com Ghavami (2020), a GD é um processo contínuo e repetível para gerenciar dados adequadamente e mitigar riscos potenciais, assim, políticas de governança corretas dão suporte e complementam a estratégia geral de dados.

Nesse sentido, Fernandes e Abreu (2014), ainda em 2014, quando entrou em vigor o Marco Civil da Internet, defendiam que a GD se tornaria um requisito regulatório, e que as práticas de GD deveriam ser comprovadas a órgãos fiscais e de auditorias regulares. Naquele mesmo ano, alguns projetos de lei já se encontravam tramitando no congresso, até culminarem, em 2018, na Lei 13.709, Lei Geral de Proteção de Dados (LGPD).

O conceito de governança adotado nos parâmetros da LGPD, de acordo com Fernandes, Diniz e Abreu (2019), registra três verbos em sequência: avaliar, dirigir e monitorar, que devem servir de padrão mínimo às empresas em busca da conformidade às obrigações da lei. Os conceitos básicos sobre dados também são definidos pela LGPD, em seu artigo 5º, como forma de regular o tratamento dos dados para a implementação de programas de qualidade efetivos e para o aprimoramento das boas práticas de GD (capítulo 2).

Nesse contexto, conforme Mahanti (2021), as organizações têm muitos dados que devem ser conceituados e agrupados por suas características semelhantes, necessitando de um gerenciamento adequado. Assim, ainda segundo o autor, a GD supervisiona essas iniciativas e ajuda a estabelecer políticas, funções, responsabilidades, direitos de decisão, processos e métricas que facilitam a implementação de boas práticas de gerenciamento de dados.

Assim, de acordo com Palmeira (2020), a LGPD busca trazer um nivelamento mínimo para todos que tratam dados pessoais, além de trazer orientações gerais para programas de boas práticas e governança. Em seu artigo 50, a LGPD trata das boas práticas e governança, incentivando que os agentes de tratamento de dados pessoais (controladores e operadores), no âmbito de suas competências, elaborem regras de boas práticas e governança dentro das organizações. De acordo com a Lei:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (Brasil, 2018, Art. 50)

Nesse sentido, Cots e Oliveira (2019) afirmam que, a disposição do artigo 50 vem ao encontro das atuais políticas empresariais de governança e *compliance*, buscando realizar uma gestão de dados adequada por meio de boas práticas.

Diante desse contexto, para Pinheiro (2021), a instituição de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção dos dados pessoais sejam efetivados. Sendo assim, de acordo com a LGPD, conforme identificado por Giovannini Junior (2019), os agentes de tratamento deverão definir o conjunto de boas práticas que será utilizado pelas suas organizações, levando em consideração, com relação ao tratamento de dados dos titulares, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos, bem como os benefícios decorrentes de tratamento de dados do titular.

Com isso, a LGPD, ainda em seu artigo 50, incentiva a adoção e aplicação de controles para governança em privacidade, que atentem para a estrutura, escala, volume e segurança das operações realizadas pelas organizações, como forma de reforçar as regras de boas práticas e governança para o tratamento de dados.

2.1.5 Governança em privacidade

Como observado por Dennedy, Fox e Finneran (2014), a privacidade de dados é uma parte fundamental da GD para informações pessoais, dessa forma, a GD e a privacidade estão intimamente relacionadas, já que a privacidade é uma preocupação central na gestão dos dados. De acordo com Rêgo (2020), a governança em privacidade (GP) é aplicada nos dados considerados pessoais, tendo como um direito humano fundamental: a privacidade, e seus objetivos se dão prioritariamente ao cumprimento dos requisitos legais estabelecidos pela LGPD. Em vista disso, a GP deve atender todos os preceitos legais da LGPD, seguindo um conjunto de melhores práticas, a fim de promover o *compliance*, gerando impactos positivos e agregando valor à organização.

Os programas de governança em privacidade devem sempre levar em consideração a estrutura de GD existente na organização, assim, segundo

Garbaccio, Vadell e Torchia (2022), a decisão de uma organização em se dedicar à temática governança é crucial para sua perenidade no mercado, dos profissionais que irão se interessar em fazer parte de sua missão, bem como dos consumidores que pretende atingir. Por isso, é muito importante que as empresas estejam em conformidade com as regulamentações vigentes, como no Brasil com a LGPD, adotando medidas eficazes de GD para proteger a privacidade dos dados de seus clientes e usuários.

As regulamentações de privacidade, como a LGPD, destacam a importância da GD, fornecendo orientações e requisitos para proteger os dados pessoais. Neste seguimento, a LGPD, em seu Capítulo VII – Da Segurança e das Boas Práticas, em sua Seção II – Das Boas Práticas e da Governança, traz um destaque para a adoção e implementação de um Programa de Governança em Privacidade, a fim de atender os princípios de segurança e prevenção presentes na lei.

Para ajudar na implantação de um Programa de Governança em Privacidade, a LGPD traz, ainda em seu art. 50, § 2º, alínea I, as características mínimas para a criação desse programa:

> [...] I – implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. (Brasil, 2018, Art. 50, I)

Para Garbaccio, Vadell e Torchia (2022), estes são parâmetros mínimos que devem ser seguidos por cada organização, mas de acordo com a sua realidade, além do que o programa deve ser monitorado e

aperfeiçoado de acordo com aquilo que ocorre na organização, inclusive com as falhas de conformidade e com eventuais incidentes de segurança.

Dessa forma, de acordo com Blum e Moraes (2021), o Programa de Governança em Privacidade pode ser entendido como o conjunto de regras de boas práticas e de governança que atendem aos princípios da LGPD e que o programa:

> [..] (i) contenha demonstração do comprometimento do controlador com a proteção de dados; (ii) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo em que se realizou sua coleta; (iii) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; (iv) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; (v) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; (vi) esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; (vii) conte com planos de resposta a incidentes e remediação; e (viii) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. (Blum; Moraes, 2021, p.558)

Ainda de acordo com Rêgo (2020), a implantação de um Programa de Governança em Privacidade é facilitada com a adoção da GD, que tem um escopo de atuação mais amplo junto aos dados. Isso reforça que a governança em privacidade, apresentada na LGPD, está intrinsecamente ligada à GD, pois um dos pilares da GD é *compliance*, onde o conjunto de regras e boas práticas sobre o tratamento de dados da organização deve estar de acordo com os marcos regulatórios mais recentes, sendo usadas de forma ética e legal.

2.1.6 *Compliance* no contexto da Governança de Dados

De acordo com Fernandes, Diniz e Abreu (2019), um dos significados mais comuns para o termo *compliance*, presente no cotidiano de empresas, governo, órgão de fiscalização e em leis, de forma geral, é de: “programa de conformidade”. Segundo os autores:

> Conformidade, então, nessa acepção mais comum entregue ao *compliance*, liga-se na forma de programa ético, que estabelece o conjunto de regras e comportamentos que devem ser objeto de conscientização e de procedimentos para implementação em determinado ecossistema e seu objetivo: transações íntegras. (Fernandes; Diniz; Abreu, 2019, p. 287)

Para Artese (2021) *compliance* é um termo incorporado ao nosso idioma que significa, na melhor das traduções, “conformidade” e, segundo o autor:

> A conformidade não se atinge tão simplesmente pela observância de leis. Se dá, também, por meio da adoção de um conjunto de disciplinas e estratégias voltadas a que se faça cumprir as normas legais e regulamentares a que se sujeita uma organização. Também se atinge a conformidade por meio do estabelecimento e cumprimento, *motu proprio*, de políticas e diretrizes de natureza procedimental e ética estabelecidas pela própria organização. (Artese, 2021, p.501)

Ainda conforme o DAMA-DMBOK (2017), *compliance* é garantir que a organização possa atender aos requisitos de conformidade regulatória relacionados a dados. Dessa forma, segundo Mahanti (2021), *compliance* geralmente se refere a ações que garantem o comportamento em conformidade com as regras estabelecidas, bem como o fornecimento de ferramentas para cumprir as normas regulatórias.

Nesse contexto, as dimensões do *compliance* se conectam com a GD, conforme afirmam Fernandes, Diniz e Abreu (2019), e interligam-se com a estratégia das organizações em relação ao plano de comportamentos éticos, integradas às normas costumeiras, jurídicas e regulatórias direcionadas ao horizonte de atos íntegros. Ainda segundo os autores, “o *compliance* impõe a conformidade de cumprimento, de respeito e de obediência às normas que as organizações e seus membros devem respeitar”.

Nesse sentido, segundo o DAMA-DMBOK (2017), a GD orienta a implementação de controles adequados para monitorar e documentar a conformidade com os regulamentos relacionados a dados, uma vez que toda empresa é afetada por regulamentações governamentais e do setor, incluindo regulamentações que determinam como os dados e as informações devem ser gerenciados.

Muito embora *compliance* diga respeito ao cumprimento de leis e normas, de acordo com Artese (2021), é mais oportuno indicar que o *compliance* se refira, sobretudo, ao conjunto de esforços voltados a fazer com que uma organização, e seus membros, assumam comportamentos virtuosos ou desejáveis, associando com isso o protagonismo da ética em seus objetivos.

Em se tratando da LGPD, *compliance* se refere à conformidade com as normas e princípios estabelecidos na lei, incluindo a obtenção de consentimento explícito dos titulares dos dados, a garantia da segurança das informações e o

cumprimento de requisitos específicos para o tratamento de dados sensíveis. Assim, no contexto da GD, as empresas e organizações devem implementar medidas para garantir que seus processos e práticas relacionados à gestão de dados estejam em conformidade com a LGPD.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais, Lei Federal n. 13.709/2018, mais conhecida como LGPD, foi publicada em 14 de agosto de 2018. De acordo com Pinheiro (2021), é uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas. A Lei brasileira regula o tratamento dos dados pessoais conforme seu artigo 1º:

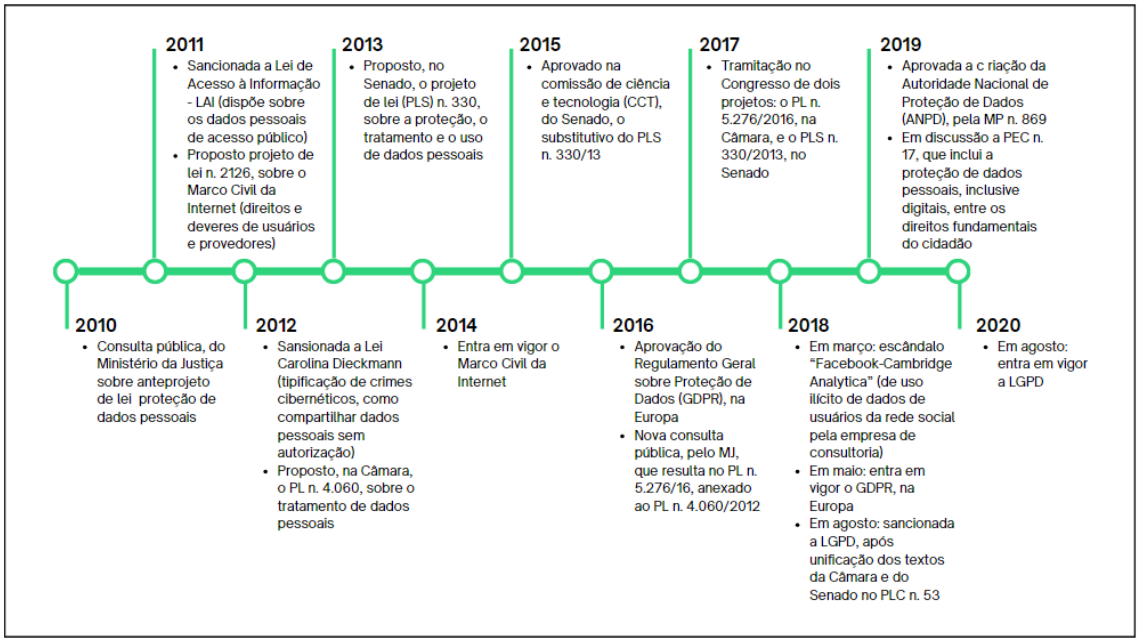
> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018, Art. 1º)

A LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*) da União Européia, que entrou em vigor em 2018 e, segundo Pinheiro (2021), tem o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecida pela expressão "*free data flow*". Além da Regulamentação Européia, outras leis criadas antes da LGPD ajudaram a consolidar sua legislação e unificar as disposições referentes à proteção e privacidade de dados, entre elas estão, em 2011, a criação da Lei de Acesso à Informação[1] e em 2014 o Marco Civil da Internet[2], como pode ser observado na Figura 1, que mostra a linha do tempo da proteção de dados pessoais e da LGPD, no Brasil.

[1] Lei de Acesso à Informação – LAI (Lei nº 12.527/2011) – regula o acesso a dados, dentre os quais as informações pessoais (Terra; Castro, 2020, p.217).

[2] Marco Civil da Internet (Lei nº 12.965/2014) – estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Terra; Castro, 2020, p.217).

Figura 1 - Linha do tempo entre o Projeto de Lei (PL) e a entrega em vigor da Lei Geral de Proteção de Dados Pessoais, no Brasil



Fonte: Elaborada pela autora com base no site da SERPRO (2019)

Estas leis visam proporcionar maior segurança para as atividades de coleta, tratamento e consulta de dados, principalmente em se tratando de dados pessoais, que vem crescendo de modo acelerado com o uso de tecnologias de informação e comunicação (TIC). O principal objetivo da LGPD, segundo Garcia *et al*. (2020), é proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Em vista disso, a lei dispõe sobre o tratamento de dados pessoais, exigindo das empresas que lidam com esses dados maior transparência sobre os procedimentos adotados no tratamento dos dados coletados.

Dessa forma, a LGPD se aplica a todas as empresas privadas, órgãos do setor público e demais instituições que realizam operações de tratamento de dados pessoais, as quais devem se adequar para atender às diretrizes da lei. De acordo com Garcia *et al*. (2020), qualquer empresa, organização, instituição pública ou privada que coleta ou que utiliza dados de pessoas físicas precisa se adaptar a lei. Também para Shintaku *et al.* (2021), é evidente o dever das instituições de informar com clareza e transparência o que fazem com os referidos dados, que são reconhecidamente pertencentes aos usuários titulares.

Nesse sentido, a UDESC, como universidade pública, que faz tratamento de dados pessoais de seus alunos, professores, técnicos e profissionais

terceirizados também deve aderir e se adequar a legislação para que o tratamento dos dados ocorra de modo efetivo, sem infringir a privacidade das pessoas e a proteção dos dados pessoais. Assim, a LGPD traz alguns conceitos e disposições importantes, que serão apresentados a seguir, destacando os principais termos e princípios e fundamentos a serem seguidos pelas universidades públicas, que é o tema central desta pesquisa.

2.2.1 Conceitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais

As disposições gerais da LGPD são citadas no Capítulo I da lei, onde, segundo Garcia *et al*. (2020), na condição de capítulo introdutório, sua principal função é nivelar o vocabulário e definir a natureza dos conceitos abordados.

Assim, em seu art. 5º, a LGPD traz alguns conceitos importantes para o melhor entendimento da lei, como os principais conceitos sobre os dados:

> I - **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
> II - **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - **Dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - **Banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (Brasil, 2018, Art. 5º, grifo nosso)

Quanto aos principais conceitos sobre os dados, vale destacar o conceito de **Anonimização**, definido no artigo 5º da LGPD, inciso XI, como “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”. Na LGPD, de acordo Branco (2020), a anonimização e/ou pseudoanonimização de dados, deve ser garantida, sempre que possível, principalmente quando o tratamento de dados envolve estudos por órgão de pesquisa, dessa forma diferentes dados vinculados ao titular do dado podem ser associados a um determinado pseudônimo.

Ainda em seu artigo 5º a lei define os principais papéis dos envolvidos. O ator principal de que trata a lei, o **Titular dos dados**, que é definido como “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (Brasil, 2018, Art. 5º, V). A lei ainda define os **Agentes de tratamento**, em seu inciso IX, como “o controlador e o operador”; respectivamente definidos como:

- **Controlador**: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Brasil, 2018, Art. 5º, VI, grifo nosso);
- **Operador**: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (Brasil, 2018, Art. 5º, VII, grifo nosso).

Outro papel essencial para o adequado cumprimento da LGPD é o **Encarregado**, definido pelo artigo 5º como “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (Brasil, 2018, Art. 5º, VIII). Além destes, outro papel importante é o da **Autoridade nacional**, que é o “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional” (Brasil, 2018, Art. 5º, XIX).

Um outro conceito importante, tratado com uma das bases legais da LGPD, é o **Consentimento**, que também é definido em seu artigo 5º como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018, Art. 5º, XII). Barbieri (2020) traz ainda que o conceito de consentimento estabelece o direito legal ao processamento dos dados dentro de legítimos interesses explicitados, e, com isso, o consentimento deve ser um dos primeiros princípios éticos, centrado na concordância do uso de seus dados por alguém.

2.2.2 Fundamentos da Lei Geral de Proteção de Dados

Definidos os principais conceitos, a LGPD traz em seu artigo 2º os fundamentos que disciplinam a proteção de dados pessoais, elencando sete

pilares da lei, que ajudam a garantir que os dados sejam tratados de forma segura e respeitando a privacidade dos dados pessoais, como pode ser observado:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I – o respeito à privacidade;
> II – a autodeterminação informativa;
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
> IV – a inviolabilidade da intimidade, da honra e da imagem;
> V – o desenvolvimento econômico e tecnológico e a inovação;
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasil, 2018, Art. 2º)

De acordo com Garcia *et al*. (2020), é nesse artigo que se defende o ethos da lei, ou seja, o que não se pode perder de vista ao interpretar a lei. Ainda segundo o autor, qualquer interpretação que ferir esses fundamentos se torna inadequada.

Sobre o primeiro fundamento, Vainzof (2019) afirma que a preocupação com a proteção de dados pessoais está associada à própria noção de proteção da privacidade. O autor afirma ainda que a proteção da privacidade é elemento indissociável da dignidade da pessoa, razão pela qual qualquer ato capaz de afetar a intimidade do cidadão seria também um ato atentatório à experiência humana de uma vida digna.

A autodeterminação informativa, presente no segundo fundamento, de acordo com Teixeira e Guerreiro (2022), consiste no poder que o indivíduo tem de determinar como seus dados serão tratados mediante o recebimento de informações sobre como será esse tratamento. Ainda segundo Garcia *et al*. (2020):

> O segundo fundamento é o da autodeterminação informativa, cujo significado está em garantir que o Titular tenha o direito de decidir o que será feito com a sua informação, em saber quais dados as Organizações possuem, como elas os utilizam e se ele quer que seu dado esteja com elas, quer seja utilizado ou não. Em outras palavras, de acordo com esse fundamento, cada pessoa natural determina como sua informação pode (e se vai) ser utilizada. (Garcia *et al*., 2020, p.XVIII)

Nesse sentido, a autodeterminação dos titulares pode ser considerada um princípio-chave na LGPD, pois, de acordo com Teixeira e Guerreiro (2022), visa assegurar que os titulares dos dados tenham o controle sobre suas informações

pessoais e possam tomar decisões informadas sobre o uso e o compartilhamento desses dados. Com isso, as universidades públicas devem respeitar a autodeterminação dos titulares, garantindo que sejam fornecidas informações claras, precisas e acessíveis sobre o tratamento de dados pessoais, bem como possibilitando o exercício dos direitos dos titulares.

O terceiro fundamento traz a liberdade de expressão, de informação, de comunicação e de opinião, que também são direitos previstos na Constituição Brasileira onde, segundo Teixeira e Guerreiro (2022), decorrem diretamente do princípio constitucional da liberdade de expressão, princípio esse indissociável do princípio democrático, pilar do Estado brasileiro. Conforme Vainzof (2019), o terceiro fundamento da LGPD possibilita uma forma de garantir que o tratamento de dados pessoais seja considerado ilícito caso possa violar referidos direitos, como coleta de dados por órgão públicos ou entidades privadas.

Ainda em seu quarto fundamento, a LGPD traz a inviolabilidade da intimidade, da honra e da imagem, direitos igualmente fundamentais previstos no art. 5º, inc. X, da Constituição Federal:

> [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (Brasil, 1988, Art. 5º, Inc X)

Para Vainzof (2019), o quarto fundamento da LGPD é também uma referência à proteção de dados, onde, segundo o autor, condutas dolosas ou negligentes, imprudentes ou imperitas no tratamento de dados pessoais podem expor a intimidade dos titulares dos dados, assim como afetar diretamente sua honra e imagem.

O quinto fundamento trata do desenvolvimento econômico e tecnológico e da inovação, ao que se refere, de acordo com Vainzof (2019), com a capacidade de processamento de dados, onde a nova forma de economia de uma sociedade é pautada em dados pessoais. Nesse sentido, de acordo com Teixeira e Guerreiro (2022), o quinto fundamento é indispensável ao olhar de quem aplica a lei nos dias atuais, pois não há que se falar em progresso sem a utilização de dados, onde estes são a base de grandes conquistas tecnológicas, e a tendência é que cada vez mais o tratamento de dados seja a grande força motriz da economia.

Já o sexto fundamento, que trata da livre iniciativa, a livre concorrência e a defesa do consumidor, está preocupado, segundo Vainzof (2019), com a proteção de dados e os interesses de privacidade e dos direitos da personalidade dos indivíduos que são relevantes para qualquer avaliação de potencial abuso de poder por empresas públicas e privadas. Para Teixeira e Guerreiro (2022):

> [...] a proteção à livre iniciativa, livre concorrência e a defesa do consumidor se inserem no contexto dessa lei por serem os dados pessoais objeto de grande valia para a sociedade atual. Seria quase impossível grande parte das empresas funcionarem sem o tratamento de dados de seus clientes, fornecedores, empregados, dentre tantas outras pessoas com que se relaciona, sendo vital à sua sobrevivência. (Teixeira; Guerreiro, 2022, p.13)

E em seu último fundamento, a LGPD traz os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, onde, de acordo com Vainzof (2019), os dados, quando pessoais, estão contidos dentro das mais variadas possibilidades de representação da personalidade da pessoa. Dessa forma, os dados quando tratados podem passar a representar a identidade de determinado indivíduo, fazendo com que a proteção de dados tenha um papel fundamental para garantir os direitos da personalidade.

Assim, o artigo 2º da LGPD apresentou os fundamentos norteadores para a aplicação da lei, enquanto o artigo 6º, que será apresentado a seguir, fornece as diretrizes gerais que orientam o tratamento de dados pessoais. Essa relação entre os princípios e os fundamentos da LGPD é fundamental para compreender a abordagem adotada pela legislação em relação à proteção dos direitos e liberdades individuais no contexto do tratamento de dados pessoais.

2.2.3 Princípios da Lei Geral de Proteção de Dados Pessoais

Apresentados os fundamentos que disciplinam a proteção de dados, a LGPD traz em seu artigo 6º dez princípios, além da boa-fé, que devem ser observados e precisam ser atendidos na hora de tratar dados pessoais:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

> II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - **necessidade**: 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;
> IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018, Art. 6º, grifo nosso)

A LGPD é uma lei principiológica, desse modo, para Teixeira e Guerreiro (2022), seus princípios devem ser considerados em toda atividade de tratamento de dados, independentemente das mudanças que virão com o decorrer do tempo. De acordo com Pinheiro (2021), a garantia de proteção dos direitos dos titulares dos dados pessoais é pautada na indicação de princípios relativos ao tratamento de dados pessoais, cuja ação deve respeitar os limites dos direitos fundamentais. Assim, veremos cada um dos princípios e sua aplicação dentro do contexto das universidades públicas, que é tema desta pesquisa.

Segundo Tepedino, Frazão e Oliva (2020), o primeiro princípio, o princípio da finalidade exige que seja respeitada a correlação entre o tratamento dos dados e a finalidade informada. Souza, Magrani e Carneiro (2020) afirmam que o princípio da finalidade exige que o destino a ser conferido aos dados deve ser informado previamente ao titular dos dados, e os dados coletados só podem ser utilizados para fins legítimos, específicos e explícitos. Dessa forma, em relação às universidades públicas, os dados pessoais de estudantes, professores e de

funcionários devem ser coletados e processados com um propósito específico relacionado às atividades acadêmicas, administrativas ou de pesquisa.

Para Vainzof (2019), o princípio da finalidade apresenta estreita ligação com os princípios da adequação (II) e da necessidade (III), onde os três primeiros princípios são “umbilicalmente conexos” e, juntamente com o princípio da transparência (VI), são determinantes para o respeito da proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio da tutela dos dados pessoais.

No segundo princípio, o princípio da adequação, de acordo com Souza, Magrani e Carneiro (2020), os dados coletados devem ser usados apenas na medida que forem necessários para atingir a finalidade informada, sempre de acordo com o contexto do tratamento. Com isso, esse princípio se vincula ao princípio da finalidade, pois, conforme Vainzof (2019), prevê que o tratamento de dados pessoais somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular dos dados. Nesse sentido, as universidades públicas devem garantir que os dados pessoais sejam utilizados apenas para as finalidades estabelecidas, evitando o uso excessivo ou inadequado dessas informações.

O princípio da necessidade, de acordo com Tepedino, Frazão e Oliva (2020), restringe os dados coletados ao estritamente necessário para cumprimento da finalidade informada. Para Souza, Magrani e Carneiro (2020), somente o mínimo necessário para a realização das finalidades deve ser coletado, isso significa que as universidades devem coletar apenas os dados pessoais essenciais para a gestão acadêmica, administrativa, de pesquisa e prestação de serviços educacionais, evitando a coleta de informações desnecessárias.

Diante desse contexto, Teixeira e Guerreiro (2022) afirmam:

> A finalidade, adequação e a necessidade são princípios que somados resultam no que se chama de mínimo essencial, algo como saber qual a menor quantidade de dados pessoais necessária para que se chegue ao fim pretendido de forma adequada. No momento da coleta é primordial que se esteja atento à real necessidade de se obter determinado dado pessoal para se atingir a finalidade pretendida. (Teixeira; Guerreiro, 2022, p.19)

O princípio do livre acesso, de acordo com Souza, Magrani e Carneiro (2020), assegura que as pessoas possam ter acesso aos próprios dados no

momento em que desejarem. Para Vainzof (2019), esse princípio viabiliza que o titular dos dados possa acompanhar, constantemente, a utilização de seus dados pessoais junto ao controlador e, dessa forma, retificar informações incorretas, cancelar informações registradas indevidamente e, até mesmo, requerer o descarte de seus dados. Com isso, as universidades públicas devem fornecer meios para que os titulares dos dados possam acessar, corrigir e atualizar suas informações pessoais, quando necessário.

O quinto princípio, da qualidade dos dados, conforme Teixeira e Guerreiro (2022), “pressupõe que o titular de dados deve ter garantido que seus dados pessoais sejam coletados com exatidão, clareza e relevância e, caso isso não ocorra, poderá requerer a sua correção”. Nesse sentido, de acordo com Tepedino, Frazão e Oliva (2020), esse princípio se relaciona com os princípios da transparência e do livre acesso, na medida em que esses asseguram o conhecimento e os meios de correção de informações equivocadas. Em vista disso, as universidades públicas devem implementar procedimentos adequados para manter os dados atualizados e corrigir eventuais imprecisões.

O princípio da transparência, de acordo com Teixeira e Guerreiro (2022), pressupõe que o titular terá livre acesso às informações claras e precisas sobre o tratamento de seus dados pessoais. Para Vainzof (2019, p.150), “a transparência deve ser diretamente proporcional ao poder do tratamento dos dados pessoais e à capacidade de assimilação dos titulares dos novos e dinâmicos produtos e serviços apresentados para o seu uso”. Nesse contexto, as universidades públicas devem adotar práticas transparentes, informando de maneira clara, precisa e acessível sobre as suas políticas de privacidade e tratamento de dados pessoais.

Segundo Tepedino, Frazão e Oliva (2020), o princípio da segurança visa evitar situações ilícitas através de medidas técnicas e administrativas realizadas pelos agentes de tratamento de dados. Dessa forma, para Souza, Magrani e Carneiro (2020), pelo princípio da segurança, as medidas técnicas e administrativas devem estar sempre atualizadas e hábeis a proteger os dados pessoais de eventuais violações, como acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Assim, as universidades públicas devem adotar medidas de governança

adequadas para proteger os dados pessoais contra acesso não autorizado, destruição, perda, alteração ou divulgação indevida.

De acordo com o princípio da prevenção, segundo Souza, Magrani e Carneiro (2020), “métodos preventivos com as medidas técnicas cabíveis devem ser adotados para evitar danos decorrentes do tratamento de dados”. Assim, para Teixeira e Guerreiro (2022), as empresas, instituições e universidade públicas deverão, através de um projeto de adequação à LGPD, conhecer onde está o tratamento de dados, as suas vulnerabilidades e as prioridades de tratamento, prevenindo-se de possíveis incidentes.

O princípio da não discriminação, segundo Vainzof (2019), prevê a impossibilidade do tratamento de dados para fins discriminatórios, seja de forma automatizada ou não, propondo impor limites e permissões no processamento de dados. Conforme Teixeira e Guerreiro (2022), “a não discriminação encontra respaldo no princípio constitucional da igualdade, em que todos são iguais perante a lei e na lei, sendo vedado ao agente de tratamento qualquer tratamento de dados para fins discriminatórios, ilícitos ou abusivos”. Assim sendo, universidades públicas devem adotar medidas para prevenir a discriminação no tratamento dos dados pessoais dos estudantes, funcionários e demais partes interessadas.

Ainda, de acordo com Tepedino, Frazão e Oliva (2020):

> A não discriminação é um princípio que há tempos já tinha conquistado espaço nas legislações internacionais, com a identificação e o tratamento diferenciado da categoria dos dados sensíveis. Esses são identificados como os dados que contêm informações que podem levar à discriminação da pessoa, como origem étnica, religião, orientação sexual e posição política. (Tepedino; Frazão; Oliva, 2020, p. 168)

Por fim, o princípio da responsabilização e prestação de contas, de acordo com Souza, Magrani e Carneiro (2020), requer do agente que faz o tratamento dos dados a capacidade de demonstrar a eficácia das medidas adotadas para o cumprimento das normas de proteção de dados pessoais. Assim, para Vainzof (2019), os agentes deverão, durante todo o ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos. No âmbito das universidades públicas, estas têm a

responsabilidade de demonstrar a adoção de medidas eficazes para garantir o cumprimento da LGPD e proteger os dados pessoais sob sua responsabilidade.

Diante desse contexto, as universidades públicas têm uma responsabilidade crucial em cumprir os princípios estabelecidos na LGPD e devem adotar uma abordagem abrangente e pró-ativa para garantir sua implementação. Nesse sentido, as universidades devem tomar medidas efetivas para proteger os dados pessoais, sendo transparentes em relação ao tratamento dessas informações, coletando apenas os dados necessários, garantindo a segurança dos dados, promovendo a igualdade de acesso e oportunidades, além de demonstrar responsabilidade e prestar contas pelas suas práticas de tratamento de dados.

Assim, é essencial que as universidades públicas se empenhem em desenvolver políticas, diretrizes, procedimentos e controles adequados para garantir o cumprimento dos princípios da LGPD e garantir a proteção dos dados pessoais de seus estudantes, professores, funcionários e demais envolvidos. Essas ações ajudam a demonstrar o compromisso da instituição com a proteção dos dados pessoais e a assegurar a responsabilização por suas práticas de tratamento de dados.

2.2.4 Direitos e liberdades dos titulares dos dados

A LGPD trata dos direitos do titular dos dados em seu capítulo III – Dos Direitos do Titular, iniciando com o artigo 17: “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei” (Brasil, 2018, art. 17). De acordo com Pinheiro (2021), essa garantia da pessoa natural à titularidade de seus dados pode ser relacionada à inviolabilidade de sua vida privada, “pontuada por meio do art. 5, X, da Constituição Federal (CF) e do art. 21 do Código Civil, haja vista que as informações da pessoa fazem parte de sua privacidade, ainda mais no contexto digital”.

Da mesma forma, segundo Gomes (2020), os direitos dos titulares dos dados podem ser classificados em três:

> [...]
> (i) direitos fundamentais, previstos no art. 5° da Constituição Federal (CF);
> (ii) liberdades civis ou direitos civis, previstos no artigo 5° da CF;
> (iii) direito dos titulares de dados, previstos nos arts 18, 21 e 22 da LGPD. (Gomes, 2020, p. 271)

Assim, quando se fala em direitos dos titulares, não se pode limitar aos especificados no capítulo III da LGPD, os direitos fundamentais e liberdades civis previstos na CF também devem sempre ser levados em consideração nesses casos.

De acordo com Pinheiro (2021), “o direito dos titulares dos dados de livre acesso às informações relativas ao tratamento é reiterado de maneira enumerativa no art. 18”, onde o titular dos dados tem o direito a obter do controlador, a qualquer momento e mediante requisição:

> [...]
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (Brasil, 2018, Art. 18)

Para Silva (2020), os incisos I e II do artigo 18 decorrem do princípio da transparência e do livre acesso, respectivamente. Os mesmos incisos são complementados pelo artigo 19 da LGPD, que estabelece de que forma e em qual prazo os dados tratados serão fornecidos:

> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
> I – em formato simplificado, imediatamente; ou
> II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
> [...] (Brasil, 2018, Art. 19)

O artigo 20 trata da revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, assim, de acordo com Teixeira e Guerreiro (2022):

> A lei nesse artigo visou assegurar ao titular de dados que ele poderá pedir a revisão de decisão tomada única e exclusivamente de forma automatizada e que possam afetar seus interesses, seja para definir seu perfil pessoal, profissional, de consumo, de crédito e até mesmo perfis de sua personalidade. (Teixeira; Guerreiro, 2022, p.33)

Ainda para Silva (2020), “o artigo 20 busca oferecer mecanismos para minimizar os riscos do crescente uso de algoritmos para realização de julgamentos e avaliações das pessoas”, atendendo assim ao princípio da transparência.

No artigo 21 a Lei trata do uso indevido dos dados pessoais referentes ao exercício regular de direitos pelo titular, de modo a prejudicar o titular dos dados. Nesse sentido, de acordo com Teixeira e Guerreiro (2022), “não poderá qualquer pessoa física ou jurídica, pública ou privada, utilizar esses dados para prejudicar o titular, que somente os informou para exercer regularmente seu direito”.

Já o artigo 22 trata, segundo Maldonado (2019), “especificamente da possibilidade de que a defesa dos interesses e dos direitos dos titulares possa ser exercida em juízo, de forma individual ou coletiva”.

Com isso, segundo Pinheiro (2021), a preocupação da LGPD “é garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade”. Para Silva (2020), os artigos sobre os direitos do titular de dados conferem ao mesmo a capacidade de gerenciamento sobre seus próprios dados. Além disso, esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade.

2.2.5 Requisitos para o tratamento de dados

Os requisitos para o tratamento de dados pessoais estão regulados no artigo 7º da LGPD, em sua primeira seção que, de acordo com Garcia *et al*. (2020), indica as dez bases legais que legitimam e autorizam o início da atividade de tratamento de dados pessoais. Para Pinheiro (2021), a LGPD, em seu artigo 7º, destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir

finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares. Assim, de acordo com a lei:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019);
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (Brasil, 2018, Art. 7º)

Para Frajhof e Mangeth (2020), qualquer coleta de informações pessoais e seu consequente tratamento, de acordo com as ações descritas no artigo 5º, X, da LGPD, só podem ser iniciados se fundamentados em uma dessas hipóteses listadas pelo artigo 7º. Nesse mesmo sentido, Lima (2019) afirma que essas dez bases legais são taxativas, e, além disso, deve-se destacar que basta o atendimento de uma delas para o tratamento ser considerado legítimo (sendo possível cumular bases legais).

A primeira das dez hipóteses é considerada a principal base legal, contudo, como afirma Garcia *et al*. (2020), apesar de ser a mais comum, a obtenção de consentimento não é a única hipótese para coleta e tratamento de dados pessoais. Da mesma forma, Lima (2019) afirma que todas as demais bases mencionadas nos incisos II a X independem do consentimento para que sejam tidas como válidas.

O consentimento é definido no artigo 5º, inciso XII da LGPD, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018). Nesse contexto, Pinheiro (2021) afirma que, a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas.

Para que o consentimento seja válido, Lima (2019) afirma que, ele deve ser livre, informado e inequívoco, ou seja, o titular tem que ser informado sobre a finalidade do tratamento; tem que ter a possibilidade de concordar ou não, sem ser pressionado ou prejudicado em caso de negativa; e tem que dar o consentimento de forma expressa. Ainda segundo Tepedino e Teffé (2020, p.293), “o consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular”.

As bases legais para o tratamento de dados pessoais em universidades públicas podem variar de acordo com a situação e o contexto específico do tratamento, sendo possível a dispensa do consentimento do titular do dado. Dessa forma, existem algumas bases legais comuns que podem ser aplicáveis, como apresentado no Quadro 3 a seguir.

Quadro 3 - Possíveis bases legais aplicáveis às universidades públicas

Base legal (Brasil, 2018, art. 7º)	**Contexto (Brasil, 2020 & Teixeira e Guerreiro, 2022).**	**Exemplo de aplicação (autora, 2023)**
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;	Se a universidade pública estiver sujeita a obrigações legais ou regulatórias que exijam o tratamento de dados pessoais, essa base legal pode ser aplicada. Essa hipótese dispensa o consentimento do titular do dado.	A universidade pode coletar e processar informações pessoais dos estudantes para cumprir obrigações estabelecidas pela legislação educacional, como a emissão de diplomas, geração de relatórios estatísticos ou a realização de processos seletivos
III - pela administração pública, para o tratamento e uso compartilhado de dados	As universidades públicas podem coletar, armazenar, processar e compartilhar dados pessoais quando essa atividade	Universidades públicas podem coletar e processar informações pessoais dos estudantes para a submissão

necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;	é necessária para o cumprimento de políticas públicas definidas em leis ou regulamentos. Essas políticas públicas podem envolver áreas como saúde, educação, segurança pública, previdência social, entre outras. Essa hipótese dispensa o consentimento do titular do dado.	dessas informações aos órgãos competentes, como o Ministério da Educação.
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	Universidades públicas têm o propósito de promover o ensino, a pesquisa e a extensão para o benefício da sociedade. Nesse sentido, o tratamento de dados pessoais pode ser justificado pelo interesse público ou pelo exercício de função pública. Essa hipótese dispensa o consentimento do titular do dado.	A coleta e o processamento de informações pessoais podem ser necessários para realizar pesquisas acadêmicas, gerar conhecimento científico ou fornecer serviços de extensão à comunidade
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;	O tratamento de dados pessoais pode ser justificado quando necessário para a execução de um contrato no qual o titular é parte, como a matrícula em um curso ou a prestação de serviços educacionais. Essa hipótese dispensa novo consentimento do titular, desde que: (a) o tratamento de dados em questão seja imprescindível para o devido cumprimento do contrato; e (b) o titular dos dados tenha previamente manifestado consentimento, na celebração do contrato.	Os dados coletados do titular podem ser utilizados para o pagamento de bolsas de estudo ou a contratação de serviços terceirizados

Fonte: elaborado pela autora (2023) com informações de Brasil (2018, Art. 7º); Brasil (2020); e Teixeira e Guerreiro (2022)

O amplo rol de princípios da LGPD e a referência à boa-fé, de acordo com Tepedino e Teffé (2020), revelam uma grande preocupação com as atividades de tratamento de dados pessoais. Em vista disso, é fundamental que as universidades públicas estejam em conformidade com a LGPD e identifiquem corretamente a base legal adequada para o tratamento de dados pessoais, garantindo assim que sejam respeitados os direitos dos titulares e adotando as medidas de segurança e privacidade necessárias para proteger as informações pessoais.

Diante desse contexto, os principais conceitos, fundamentos, princípios, bases legais e aplicações apresentados neste capítulo são fundamentais para a proteção dos dados pessoais e devem ser analisados e seguidos para o correto tratamento dos dados pessoais, de forma a atender aos requisitos de privacidade, aos padrões de boas práticas e de governança.

2.3 GOVERNANÇA DE DADOS E AS IMPLICAÇÕES ÉTICAS DE SEU USO

A governança e a ética no uso de dados são dois conceitos fundamentais na era da informação em que vivemos atualmente. A GD, de acordo com Ghavami (2020), refere-se às estruturas, políticas, processos e controles estabelecidos para garantir a qualidade, a segurança e a conformidade no uso dos dados. Enquanto a ética no uso de dados, de acordo com Magrani (2019), está relacionada aos princípios e valores que devem guiar o tratamento dos dados, envolvendo considerações morais, legais e sociais sobre como os dados são coletados, armazenados, processados e compartilhados, com respeito aos direitos e privacidade dos indivíduos envolvidos.

Nesse contexto, de acordo com Barbieri (2020), a ética de dados se inicia quando a governança e a gerência de dados são chamadas a interagir com aspectos de segurança e privacidade de dados, sendo potencializada com o crescimento acelerado no uso de TICs e ferramentas de inteligência artificial (IA) para a coleta e análise de grandes quantidades de dados. Da mesma forma, Marcovitcha e Rancourtb (2022) argumentam que as organizações precisam integrar sistematicamente a ética dos dados em suas práticas de governança para permitir confiança, responsabilidade e deliberação contínua sobre as regulamentações gerais.

Conforme Ladley (2019), a GD é importante para assegurar que os dados sejam utilizados de forma ética e eficiente. Nesse sentido, para entender melhor o contexto da GD e da ética no uso de dados, apresenta-se a seguir uma breve visão geral de algumas das principais abordagens da ética, com ênfase particular na ética normativa e na ética da informação, que são mais comumente aplicadas à tecnologia.

2.3.1 Ética na tecnologia

Estudos sobre a ética datam desde a Grécia antiga, sendo estudada e discutida por diferentes filósofos como Sócrates, Platão, Aristóteles e Kant. Com diferentes autores, a ética também se dividiu em diferentes teorias onde, segundo Stahl (2021), as teorias éticas são tentativas de encontrar uma resposta para a pergunta: o que torna uma ação eticamente melhor ou pior do que uma ação alternativa?

De acordo com Borges, Dall'Agnol e Dutra (2002, p.3), "a ética divide-se em três campos: meta-ética, ética normativa e ética aplicada". Ainda segundo os autores, a meta-ética investiga a natureza dos princípios e teorias morais (por exemplo, os padrões morais são universais ou culturalmente relativos? Os fatos morais existem? Existem verdades morais?); a ética normativa, de acordo com Tsou e Walsh (2023), aborda questões relativas ao que é moralmente bom ou certo (por exemplo, felicidade, equidade, liberdade); e a ética aplicada, também segundo os autores, é a aplicação de teorias éticas normativas a casos específicos (por exemplo, aborto, pena de morte).

Nesse sentido, de acordo com Tsou e Walsh (2023), as teorias éticas normativas podem ser muito bem aplicadas a casos particulares na ética da tecnologia, destacando-se a deontologia e o utilitarismo. Também segundo Stahl (2021), a deontologia e o utilitarismo não são as únicas teorias éticas que podem ser aplicadas à tecnologia, contudo, são as mais frequentemente discutidas no âmbito tecnológico, incluindo ainda a ética da informação, uma vez que a ética na tecnologia está em constante evolução devido ao surgimento de novas questões éticas relacionadas a IA, aprendizado de máquina, privacidade de dados, segurança e outros avanços tecnológicos.

Para Freire (2010):

> Vivemos em uma época que exige uma flexão ou uma plasticidade interativa da racionalidade a partir da qual possamos enfrentar o universo das novas questões éticas, políticas e legais que se acumulam diariamente nas práticas científicas, empresariais, sociais e governamentais, na vida pública e na vida privada (Freire, 2010, p. 6)

Robson e Tsou (2023) também abordam a ética normativa que, segundo os autores, aborda questões relativas ao que é moralmente bom ou certo e apresenta uma abordagem que fornece princípios e regras éticas para orientar

a conduta humana. Nesse contexto, de acordo com Dimmock e Fisher (2017), a ética normativa pode ser aplicada a casos específicos como a privacidade de dados e a disseminação de informações. Dessa forma, segundo Moraes (2019), no âmbito da privacidade de dados, a aplicação da ética normativa possibilita identificar as melhores práticas e políticas que protegem os dados pessoais dos indivíduos e que garantem que esses dados sejam usados de maneira ética e responsável.

Uma das teorias éticas normativas é a ética deontológica, que, segundo Magrani (2019), se enquadra no domínio das teorias morais que orientam e avaliam o que devemos fazer e que julgam a moralidade das escolhas individualmente, por um parâmetro não orientado pelos resultados. De acordo com Stahl (2021), a ética deontológica baseia-se no princípio de que a base da avaliação ética de uma ação é o dever do agente que a executa.

O filósofo Immanuel Kant (1788, 1797), é uma das figuras mais proeminentes na teoria ética deontológica e, conforme Tsou e Walsh (2023), Kant defendia o princípio moral do “Imperativo Categórico”, onde, segundo o autor, o princípio afirma que temos o dever de seguir regras morais que possam ser aplicadas universal e eficazmente por todas as pessoas no mesmo tipo de situação. Também segundo Stahl (2021), o aspecto interessante de tal posição para nossos propósitos é que essa visão da ética não presta atenção imediata às consequências de uma ação, mas concentra-se exclusivamente na motivação para empreendê-la.

Nesse contexto, com o avanço das novas tecnologias, a preocupação envolvendo a escolha em seguir determinações deontológicas se torna ainda mais importante. Tsou e Walsh (2023) ressaltam ainda que, as teorias éticas normativas oferecem diferentes razões filosóficas para pensar que uma determinada ação (ou regra) sobre tecnologia é moralmente boa ou má. Para O'Keefe e O Brien (2018), é a combinação das tecnologias e as decisões tomadas sobre quais dessas combinações serão disponibilizadas que podem dar origem a questões éticas de como são nossas relações com a tecnologia.

Assim, segundo Magrani (2019), a grande importância global atual em proteger os direitos humanos e evitar violações desses direitos, pode ser vista como uma prevalência da perspectiva deontológica, especialmente relacionada

à proibição de se usar uma pessoa como um meio e não como um fim em si mesma. Para Manteleroÿ (2018), os valores éticos e sociais são vistos pelas lentes dos direitos humanos e usados para ir além das limitações que a teoria legal ou a implementação prática de tais direitos podem implicar na abordagem efetiva das questões atuais relativas aos impactos sociais do uso de dados.

Dessa forma, enquanto a ética normativa e a ética deontológica abrangem um escopo mais amplo de questões morais, a ética da informação inclui o uso ético da informação em geral. Definida por Freire (2010):

> Uma ética da informação diz respeito aos dilemas deônticos ou conflitos morais que surgem na interação entre os seres humanos e as tecnologias e sistemas de comunicação e de informação a fim de refletir e, sobretudo, disciplinar a criação, a organização e o uso das informações. (Freire, 2010, p. 7)

As TICs e os sistemas de informação, segundo Porto (2016), dependem de premissas e de instruções que são colocadas pelos humanos e que devem ser regidas pela ética para definir prioridades e encaminhamentos. Essas interações entre humanos e sistemas de informação levantam a discussão entre o que é ético e o que pode resultar em problemas à segurança e privacidade das pessoas.

Também para Preisig, Rösch e Stückelberger (2014) os dilemas e conflitos éticos surgem, muitas vezes, porque os valores éticos entram em conflito entre si. Com isso, segundo os autores, o acesso irrestrito à informação não é compatível com a privacidade e proteção de dados; da mesma maneira que a liberdade ilimitada de expressão colide com a proteção contra difamação. Assim, fica evidente a necessidade de equilibrar valores conflitantes de forma cuidadosa e sensível.

Para o DAMA-DMBOK (2017), os princípios da ética da informação, geralmente, se concentram em ideias como justiça, respeito, responsabilidade, integridade, privacidade, qualidade, confiabilidade, transparência e confiança, e com o rápido avanço no uso de TICs para o tratamento automatizado e de grandes quantidades de dados, surgiram preocupações éticas sobre como esses dados são coletados, usados e protegidos, dando espaço para um novo ramo da ética da informação, mais específico, conhecido atualmente como a ética no uso de dados.

2.3.2 Ética no uso de dados

A ética no uso de dados, segundo Martin (2022), em muitos aspectos, não é diferente de qualquer esforço para encontrar a resposta “certa”. Para Van Dijk, Casiraghi e Gutwirth (2021), a ética no uso de dados é frequentemente invocada para proteger os indivíduos contra os efeitos disruptivos das tecnologias digitais em seus direitos e liberdades e para orientar o desenvolvimento de tais tecnologias em uma direção desejável.

De acordo com o DAMA-DMBOK (2017), a ética no uso de dados está preocupada com a forma de obter, armazenar, gerenciar, usar e descartar dados de maneira alinhada com os princípios éticos. Para Martin (2022), a ética no uso de dados inclui a ética de algoritmos, estatísticas, inteligência artificial, aprendizado de máquina e todos os outros tipos de ferramentas de análise de dados. Também para Canedo (2021), a ética no uso de dados está baseada no direito fundamental à privacidade e à proteção de dados pessoais, no uso da IA, visando combinar o uso de máquinas com os valores éticos e morais do ser humano.

Conforme Floridi e Taddeo (2016), a ética dos dados se concentra em problemas éticos colocados pela coleta e análise de grandes conjuntos de dados e em questões que vão desde o uso de big data em pesquisa biomédica e ciências sociais, até criação de perfis, publicidade e filantropia de dados, bem como dados abertos. Assim, para O'Keefe e O Brien (2023), questões éticas relacionadas à aplicação de tecnologias e práticas de gerenciamento e uso de dados estão ganhando mais destaque nas principais notícias e discussões políticas.

Para Barbieri (2020), a privacidade talvez seja uma das principais preocupações da ética no uso de dados, onde, com o crescente armazenamento e compartilhamento de dados pessoais, é fundamental garantir que os indivíduos tenham controle sobre suas informações e que sejam respeitados os princípios de consentimento informado, finalidade específica e minimização de dados.

Outra questão ética relevante no uso de dados, de acordo com Raab (2020), é a transparência. Dessa forma, os responsáveis pelo uso dos dados devem ser transparentes sobre como os dados são coletados, usados e

compartilhados, incluindo fornecer informações claras sobre as práticas de privacidade, políticas de segurança e os direitos dos indivíduos em relação aos seus dados.

Ainda segundo Barbieri (2020), a ética no uso de dados também aborda a equidade e a justiça, pois é importante garantir que o uso de dados não promova discriminação ou perpetue desigualdades sociais. Isso, ainda de acordo com o autor, envolve evitar viéses algorítmicos, garantir a igualdade de oportunidades e considerar os impactos sociais das decisões baseadas em dados.

Também, conforme o DAMA-DMBOK (2017), existe um imperativo ético não apenas para proteger os dados, mas também para gerenciar sua qualidade. Bertino, Kundu e Sura (2019), também fazem referência à ética dos dados como uma nova dimensão crítica da qualidade dos dados, pois aprimora a adequação dos dados para uso em operações, tomadas de decisão e planejamento. Assim, boas práticas de governança são determinantes para que a responsabilidade ética se estenda por todo o ciclo de vida dos dados, desde a criação até a destruição dos dados, ganhando destaque em alguns aspectos específicos do ciclo de vida e do tratamento dos dados.

Nesse contexto, Martin (2022) enfatiza que, questões de responsabilidade, privacidade, vigilância, preconceito e poder ampliam as discussões sobre se uma decisão é boa, ética ou justa. Com isso, Manteleroÿ (2018) afirma que a demanda por uso de dados ética e socialmente responsável revela a falta de uma estrutura regulatória que possa abordar as questões sociais levantadas por essas tecnologias intensivas em dados.

Segundo Raab (2020), a ética no uso de dados também está marcando sua presença na regulamentação de tecnologias e sua aplicação por meio de uma “virada” para uma ênfase em valores, estruturas e princípios éticos, incluindo a justiça, capacidade de prestação de contas e transparência e outros valores substantivos que podem fundamentar a regulamentação e a governança.

De acordo com Reynolds (2014), o crescimento da internet, a capacidade de capturar e armazenar grandes quantidades de dados pessoais e a maior dependência de sistemas de informação em todos os aspectos da vida aumentaram o risco de que a tecnologia da informação seja usada de forma

antiética. Em vista disso, para lidar com essas questões, são necessárias estruturas adicionais, como regulamentações, para entender o que está errado e o que poderia ser melhor.

2.3.3 Ética e a Lei Geral de Proteção de Dados

As leis, segundo Oliveira, Baldi e Rossetti (2019), são importantes meios de tentar regular o uso das informações, sendo geralmente baseadas nos códigos morais das sociedades para que servem, em especial em países democráticos e que possuem legisladores representantes da vontade dos cidadãos. Dessa forma, de acordo com os autores, é importante notar que “as leis e a ética são diretamente relacionadas”, conforme a teoria ética deontológica, onde a ética observa o código informal de condutas humanas que se baseiam no consenso sobre o bem e o mal e que ganham força pelo costume.

Diante disso, podemos observar como a ética está presente na construção de leis e normas que regulam a ação humana diante do acesso e uso de informações de terceiros. De acordo com Manteleroÿ (2018), os valores éticos e sociais são vistos pelas lentes dos direitos humanos e usados para ir além das limitações que a teoria legal ou a implementação prática de tais direitos podem implicar na abordagem efetiva das questões atuais relativas aos impactos sociais do uso de dados.

Entretanto, de acordo com o DAMA-DMBOK (2017), enquanto as leis codificam alguns princípios éticos, a legislação não consegue acompanhar os riscos associados à evolução do ambiente de dados, com isso, as organizações devem reconhecer e responder à sua obrigação ética de proteger os dados que lhes são confiados, promovendo e sustentando uma governança e cultura que valoriza o tratamento ético das informações. Também para Hasselbalch (2019), as implicações éticas das TICs e de uma infraestrutura de informações de dados em rápida evolução devem mediar os limites das regulamentações sobre proteção de dados.

Segundo Carvalho (2021), as regulamentações em torno do uso de dados pelas tecnologias mais recentes, como IA, não são apenas um problema tecnológico, o qual pode ser facilmente ajustado para atender as regras

pertinentes e previsíveis do mercado, envolve questões sociais e de ética. Da mesma forma, Ormay (2014), defende a importância da responsabilidade social do Estado e a participação da sociedade na criação de regulamentações referentes ao uso de informações pessoais.

Nesse sentido, conforme O'Keefe e O Brien (2023), em algumas jurisdições ao redor do mundo houve um movimento para formalizar e até mesmo regulamentar a ética de dados em alguma forma, tanto em níveis nacional e até supranacional, num esforço para ajudar os tecnólogos a lidarem com a complexidade das questões éticas levantadas no desenvolvimento de novas estruturas e abordagens éticas. Gacutan e Selvadurai (2020), também enfatizam que à medida que entidades governamentais e comerciais usam cada vez mais tecnologias para automatizar decisões, uma questão crítica a ser abordada é se deve haver uma regulamentação específica para tais decisões.

Assim, na União Europeia, que criou o Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*), Van Dijk, Casiraghi e Gutwirth (2021) observaram que várias iniciativas da Comissão Europeia têm vindo a recorrer à ética nos discursos políticos como forma de governar e regular as TICs. Os autores ainda destacam que o GDPR, que serviu de base para a criação da LGPD no Brasil, é considerado um termo imperfeito de referência, do ponto de vista de ser integrado pela ética, pois o documento não esclarece o que a ética acrescentaria na proteção de dados, nem como seria diferente do que já está firmado na lei. Ainda assim, de acordo com os autores, o GDPR apresenta uma estrutura regulatória sólida para tecnologias inovadoras, como IA, confiável e ética.

Nesse sentido, tornou-se essencial estabelecer diretrizes e regulamentações claras para o tratamento e uso responsável e ético dos dados. Por consequência, a LGPD, segundo Canedo (2021), impõe a utilização ética e transparente dos dados, o respeito à privacidade dos indivíduos quanto ao uso e o tratamento dessas informações, e visa garantir não só a proteção da privacidade dos dados, mas também que as instituições e o governo atuem de forma segura, transparente e adequada no manejo desses dados, o que irá gerar maior segurança jurídica na sociedade.

Ainda nesse mesmo sentido, o DAMA-DMBOK (2017) afirma ainda que a abordagem de ética de dados de uma organização deve estar alinhada com os requisitos de conformidade legais e regulamentares. Assim, de acordo com Canedo (2021):

> Só chegaremos a uma regulação jurídica adequada e democraticamente legítima nas questões relacionadas à utilização de dados, se nortearmos todo o aparato de novas tecnologias e avanço tecnológico à luz da governança ética e da proteção de dados pessoais nas instituições públicas e privadas, alinhada ao cumprimento do regramento estabelecido na LGPD. (Canedo, 2021, p.65)

Dessa forma, a GD e a ética devem atuar como base para uma conformidade da LGPD, onde uma GD eficaz considera a ética como um pilar fundamental, garantindo que as práticas de tratamento de dados sejam conduzidas de acordo com os princípios éticos, além de atender aos requisitos legais estabelecidos pela LGPD. Nesse sentido, para o DAMA-DMBOK (2017), as políticas públicas e as leis tentam codificar o certo e o errado com base em princípios éticos. Isso implica em adotar medidas técnicas, organizacionais e jurídicas para proteger os dados, obter consentimento adequado, garantir a transparência e assegurar que os direitos dos titulares dos dados sejam respeitados.

3 PROCEDIMENTOS METODOLÓGICOS

Quanto aos aspectos metodológicos, além da pesquisa bibliográfica a ser realizada, esta é uma pesquisa de natureza aplicada, pois, segundo Prodanov e Freitas (2013), a pesquisa aplicada tem por objetivo gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Quanto aos objetivos esta é uma pesquisa descritiva, onde, para Prodanov e Freitas (2013), esta tem o objetivo de observar, registrar, analisar e ordenar os dados, sem manipulá-los.

O método de pesquisa adotado foi o *Design Science Research* (DSR). O termo *Design Science* (DS), de acordo com Rodrigues (2018), surgiu na década de sessenta, onde os primeiros autores a utilizá-lo, Fuller (1965) e Gregory (1966), concordavam a respeito da necessidade de buscar uma forma mais sistemática para projetar artefatos ou melhoramentos em suas pesquisas, surgindo assim a *Design Science Research* (DSR). Segundo Wieringa (2009), as primeiras ideias que mais tarde inspirariam a DSR, teriam iniciado com o artigo de Simon (1996) e March & Smith (1995, p.253), onde estes autores introduziram a ciência do design como tentativas de criar soluções que servem aos propósitos humanos.

Para Hevner *et al*. (2004), o princípio fundamental da pesquisa em DS é que o conhecimento e a compreensão de um problema de design e sua solução são adquiridos na construção e aplicação de um artefato. Dessa forma, ao evoluir seu conceito ao longo dos anos, passando por diferentes autores e linhas de pesquisa, Bax (2015), traz a DSR como um tipo de metateoria que auxilia o pesquisador a criar conhecimento teórico durante os processos de concepção de artefatos, justificando como tais processos podem representar pesquisa de caráter científico.

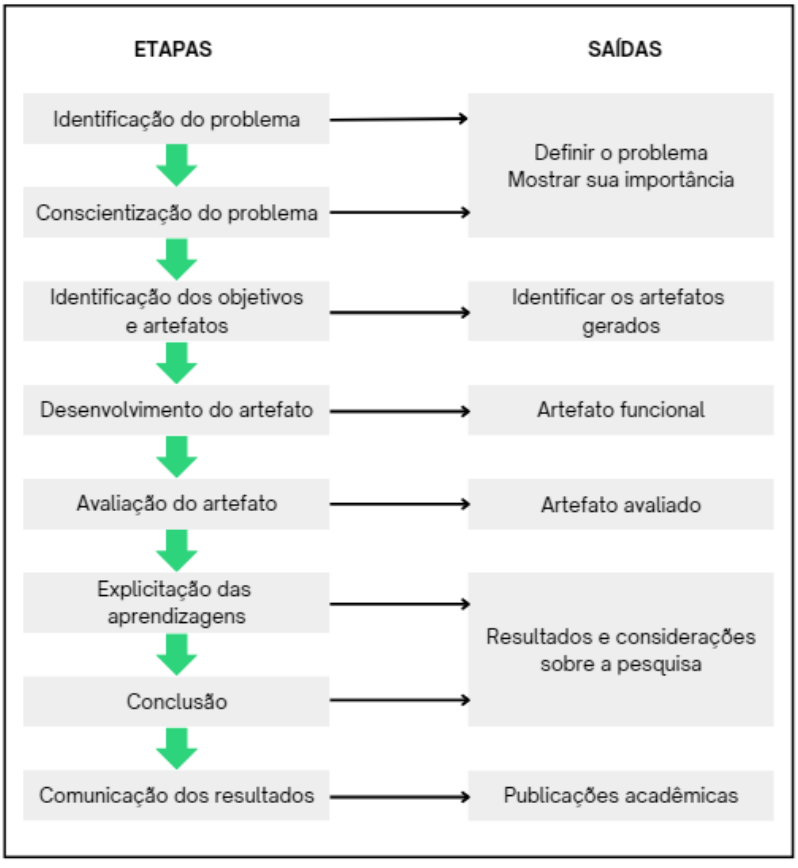
Conforme Dresch, Lacerda e Antunes Júnior (2015, p.125) “a DSR também contribui para aumentar a relevância dos trabalhos realizados, diminuindo a distância entre o que se desenvolve na academia e o que é aplicado nas organizações”. Para Bax (2015), a DSR envolve construir, investigar, validar e avaliar artefatos, tais como construtos, arcabouços, modelos, métodos e

instâncias de sistema de informações, a fim de resolver novos problemas práticos.

Com isso, o objetivo da pesquisa irá resultar em um modelo para a implementação de requisitos de acesso à dados transacionais, conforme a LGPD. Esse modelo é considerado um artefato, que é definido por Hevner *et al* (2004), citado por Bax e Barbosa (2017), como uma representação simbólica ou uma instanciação física, e também pode ser um modelo, construtos, métodos, instanciações e sistemas de informações.

Dessa forma, o roteiro de aplicação do método DSR será baseado na proposta de Dresch, Lacerda e Antunes Júnior (2015), representado pelas etapas ilustradas na primeira coluna da Figura 2.

Figura 2 - Roteiro para aplicação do *Design Science Research*



Fonte: elaborada pela autora, com base em Dresch, Lacerda e Antunes Júnior (2015)

O roteiro apresentado, que foi adaptado de Dresch, Lacerda e Antunes Júnior (2015), inicia com a identificação do problema e sua conscientização, que traz como saída os itens apresentados no capítulo 1, itens 1.1 e 1.4 desta

pesquisa. Após a identificação e conscientização do problema, foram definidos os objetivos específicos (item 1.3) e com isso, foram identificados os métodos necessários para realizar cada um desses objetivos, a fim de criar um artefato adequado para representar cada um deles.

Nesse sentido, quanto aos materiais e métodos, esta pesquisa utilizará cenários de estudo, com o objetivo de coletar, analisar os dados que serão catalogados, a fim de estabelecer uma base conceitual lógica que permitirá produzir uma matriz de risco, que é definida, segundo Guagliard *et al*. (2016), como uma ferramenta de gerenciamento voltada para assessorar os processos decisórios, e que será utilizada para analisar os riscos do atual acesso aos dados que serão catalogados, permitindo assim identificar e determinar o tamanho dos riscos.

Também será utilizado o método DSR (*Design Science Research*), que irá permitir definir um conjunto de requisitos de acesso aos dados catalogados. Assim sendo, os materiais e métodos adotados para esta pesquisa estão representados pelo quadro abaixo (Quadro 4), onde é possível identificar qual o método utilizado para atender cada um dos objetivos estipulados pela pesquisa.

Quadro 4 - Procedimentos metodológicos utilizados na pesquisa e seus artefatos

Objetivo	Método utilizado	Artefato
a) Catalogar a fonte de dados, apontando aqueles considerados sensíveis, conforme a LGPD	Cenários de estudo	Catálogo de dados
b) Analisar os riscos de acesso aos dados catalogados e considerados sensíveis, produzindo uma matriz com riscos mitigados, utilizando parâmetros escalares para a classificação dos riscos	Cenários de estudo	Matriz de risco
c) Definir um conjunto de requisitos de acesso aos dados catalogados	DSR	Documento de requisitos

Fonte: Elaborada pela autora (2023)

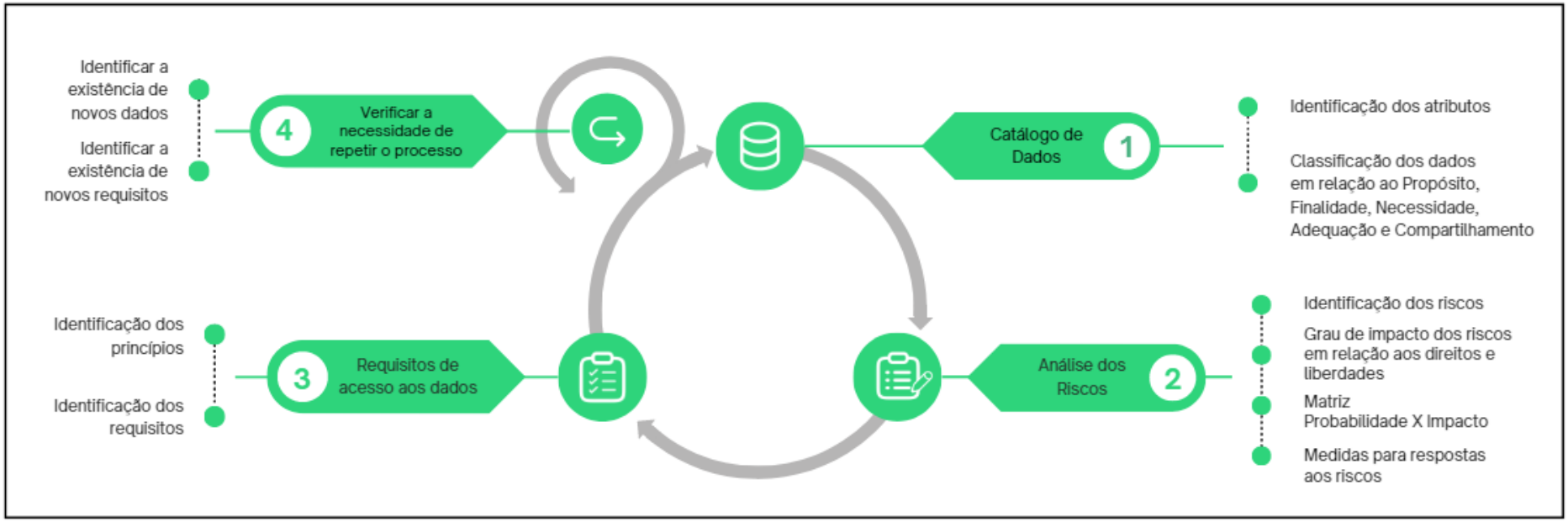
Na sequência, após definidor os objetivos e seus respectivos métodos, o DSR adaptado para esta pesquisa (Figura 2) irá criar os artefatos, resultados de cada objetivo, que serão demonstrados com foco nos dados de usuários da UDESC. A etapa de avaliação será apresentada com a análise dos resultados dos artefatos gerados, em conjunto com as explicitações das aprendizagens e a

conclusão. Já a etapa de comunicação dos resultados, esta se dará ao longo e ao final do desenvolvimento da pesquisa com a publicação da mesma.

4 MODELO PROPOSTO

O modelo proposto por esta pesquisa para implementação de requisitos de acesso à dados transacionais, em Instituições de Ensino Superior, em conformidade com os preceitos da LGPD, é apresentado pela Figura 3 a seguir.

Figura 3 - Modelo para implementação dos requisitos



Fonte: elaborada pela autora (2023)

Conforme apresentado na Figura 3, o modelo é cíclico e iterativo, onde a primeira etapa inicia com a catalogação dos dados da fonte de dados escolhida. Esse primeiro método consiste em identificar e classificar cada campo da base de dados, informando seu nome, sua classificação (pessoal, pessoal sensível ou não pessoal), seu propósito, ou seja, qual a finalidade de acordo com a LGPD e seus princípios. Esse método permite também identificar qual a necessidade do dado, qual sua adequação, e identificar ainda se existe compartilhamento, e qual o órgão e a justificativa para esse compartilhamento.

Esta classificação dos dados é importante para atender aos princípios da LGPD quanto à finalidade, necessidade e adequação, além de identificar o tipo do dado para dar a ele o tratamento adequado. Também é possível verificar se o dado é anonimizado ou pseudoanonimizado, qual o tempo de permanência do mesmo na base informada, e quem é o responsável pelo dado. O Quadro 5, a seguir, é o modelo (artefato) que pode ser utilizado para a catalogação dos dados.

Quadro 5 – Modelo de referência para catalogação dos dados

Dado	**Classificação do Dado**	**Propósito / Finalidade**	**Adequação / Necessidade**	**Compartilhamento / Órgão e Justificativa**

Fonte: elaborada pela autora (2023)

Através da catalogação dos dados é possível identificar gargalos no tratamento dos dados, como a permanência além do necessário do dado, a falta de anonimização, ou mesmo quando dados irrelevantes são armazenados, sem propósito ou finalidade adequada. Esta é a etapa mais exaustiva do modelo, por exigir maior atenção na identificação correta dos dados, porém é a etapa que dará o direcionamento correto para o modelo na execução dos demais métodos.

Ao final da catalogação, o segundo método do modelo permitirá identificar os potenciais riscos que podem afetar os dados catalogados. Assim, o método inicia com a criação de uma lista dos potenciais riscos identificados, sendo possível relacioná-los com os direitos e liberdades dos titulares que podem ser impactados, além de definir um grau e urgência para a mitigação daquele risco.

Esse processo inicial é representado através do Quadro 6, a seguir, possibilitando um melhor entendimento da gravidade dos riscos identificados.

Quadro 6 – Modelo de referência para análise dos riscos

Id	Risco	Direito potencialmente impactado	Grau/Urgência

Fonte: elaborado pela autora (2023)

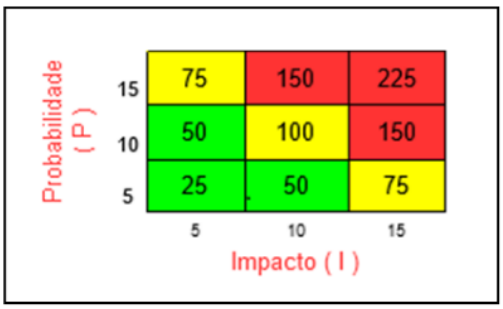
Depois de identificados os riscos, segue-se para a criação da Matriz Probabilidade X Impacto, que foi desenvolvida utilizando como base o modelo de implementação do RIPD, de acordo com o Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD) – Brasil (2020). Para a criação da matriz, primeiramente, são definidos parâmetros escalares (Tabela 1) para representar os níveis de probabilidade e impacto, que, ao serem multiplicados, resultarão nos níveis de risco, representados pela Figura 4, que direcionarão a aplicação de medidas de segurança.

Tabela 1 - Parâmetros escalares para a classificação dos riscos

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Fonte: Brasil (2020)

Figura 4 - Matriz Probabilidade X Impacto



Fonte: Brasil (2020)

O artefato final do segundo método será a Matriz Probabilidade x Impacto, representada pela Tabela 2 a seguir, onde será possível visualizar com maior clareza os níveis de probabilidade e impacto dos riscos identificados, podendo assim tomar-se as medidas corretas para a resolução e prevenção dos riscos.

Tabela 2 – Modelo referência para os riscos referentes ao tratamento de dados pessoais

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)

Fonte: elaborada pela autora com base em Brasil (2020)

O segundo método ainda oferece um artefato que auxilia a tomada de decisão pela instituição, onde é possível, através dos riscos definidos e seus potenciais de ocorrência, identificar possíveis meios de reduzir, evitar, compartilhar ou aceitar os efeitos dos eventos de risco identificados. Representado pelo Quadro 7, a seguir, esse artefato pode direcionar a equipe técnica para os melhores resultados envolvendo mitigar os riscos identificados.

Quadro 7 – Modelo de referência para medidas de resposta aos riscos

Id	Risco	Medida(s)	Efeito sobre o risco

Fonte: elaborada pela autora (2023)

O terceiro método do modelo desenvolvido consiste em identificar os princípios e requisitos que são atendidos pelo sistema, e os que ainda faltam ser atendidos, gerando assim um documento de requisitos possíveis de serem implementados.

Para ajudar na identificação dos requisitos é utilizado o artefato representado pelo Quadro 8, onde deve-se preencher com os requisitos

previstos na LGPD e que são passíveis de serem atendidos pela instituição analisada. Também são preenchidos a aplicação desse requisito dentro do sistema analisado, e se ele atende ou não o requisito, podendo referenciar se existe alguma observação para o não atendimento do mesmo.

Quadro 8 – Modelo de referência para os requisitos de acesso aos dados

Requisito	Aplicação	Atende

Fonte: elaborada pela autora (2023)

Esse artefato permite visualizar com clareza os requisitos necessários para o cumprimento da legislação, dando apoio aos operadores para as ações a serem tomadas em favor da instituição, garantindo assim a legitimidade do tratamento dos dados pessoais.

Dessa forma, por ser um modelo cíclico e iterativo, após a aplicação do terceiro método, o modelo deve ser revisado periodicamente para cumprir as exigências da Lei e novas demandas que possam surgir, conforme apontado pela Etapa 4 do modelo. Da mesma forma, as recomendações resultantes dos métodos devem ser efetivamente aplicadas, para garantir que o modelo adotado cumpra seu propósito.

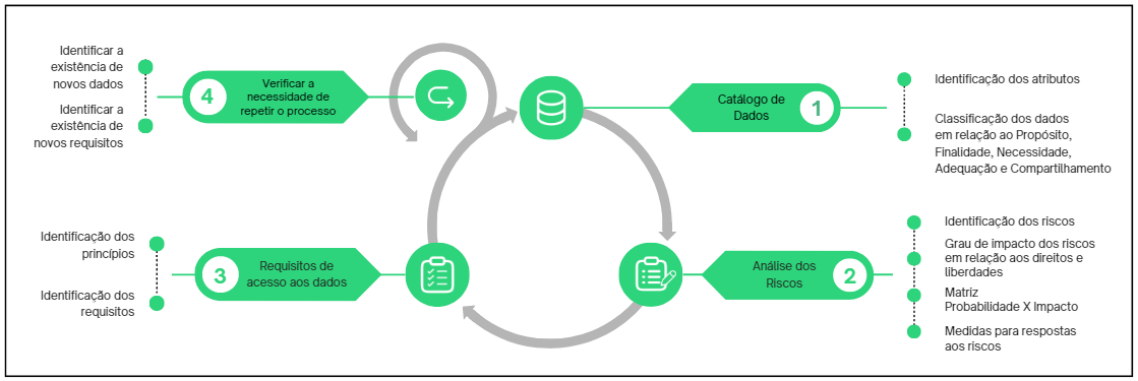
Assim, é possível avaliar que o modelo desenvolvido, com seus artefatos resultantes, representa um conjunto de melhores práticas, de acordo com as disciplinas basilares indicadas na literatura estudada através da fundamentação teórica apresentada.

5 ANÁLISE DOS DADOS E RESULTADOS

Neste capítulo são apresentados os cenários de estudo que resultaram na catalogação da fonte de dados, com a classificação e análise dos dados considerados sensíveis, conforme a LGPD, além da matriz de risco elaborada com base nos dados catalogados. Será apresentado, ainda, o relatório de requisitos de acesso aos dados catalogados, elaborado segundo o método DSR, e, por fim, a análise do modelo criado para implementar esses requisitos, também elaborado através do método DSR.

Conforme o modelo apresentado na seção anterior, representado pela Figura 5, o modelo proposto é composto de quatro fases cíclicas e iterativas, que serão apresentadas e detalhadas na sequência.

Figura 5 - Modelo para implementação dos requisitos



Fonte: elaborada pela autora (2023)

5.1 LEVANTAMENTO DOS DADOS

Para o desenvolvimento desta pesquisa foi selecionado o Sistema de Gestão de Identidades e Acessos (GIA) da UDESC, que é um sistema que realiza a gestão dos usuários e permite a administração centralizada dos acessos que os usuários possuem aos sistemas da UDESC.

A seleção desse sistema se deu por este concentrar a coleta de dados de fontes distintas para fazer o controle de usuários, onde é realizada uma extração diária das fontes com dados pessoais e dados pessoais sensíveis; por já possuir alguns processos de tratamento desses dados coletados, que atendem alguns

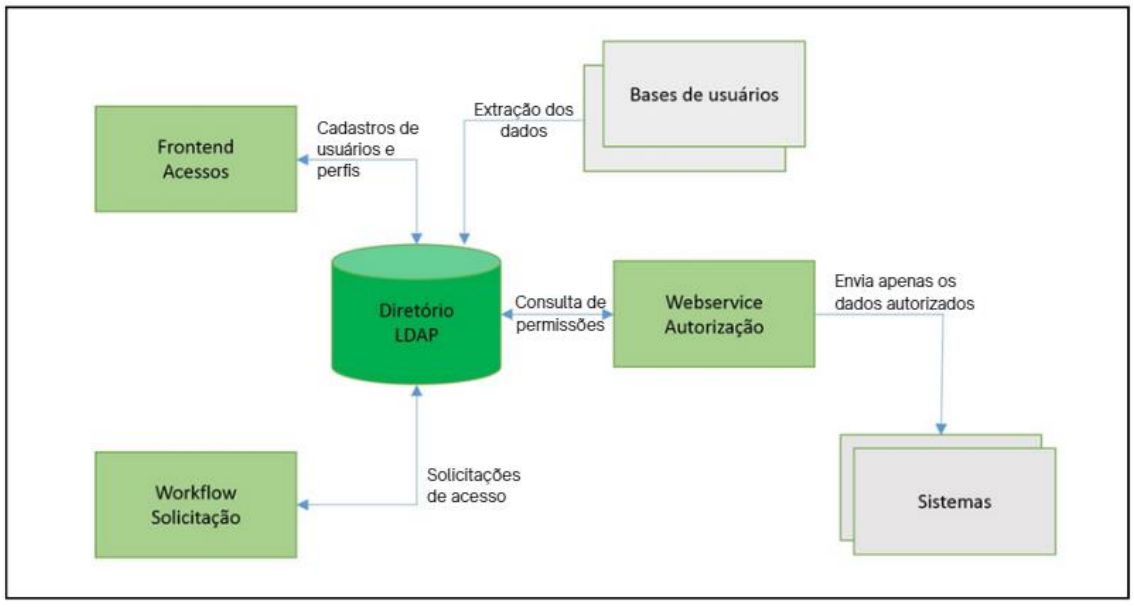
dos princípios da LGPD, como guardar dados consideráveis sensíveis para que sejam usados apenas nos respectivos sistemas da UDESC com finalidade e adequação devidamente justificados; e também por ter um webservice que permite aos demais sistemas acessarem os dados coletados.

Atualmente, o GIA trabalha com a extração automática diária em duas fontes de dados: 1) o Sistema de Recursos Humanos do Estado de Santa Catarina (SIGRH), fonte dos dados ocupacionais dos servidores da UDESC; e 2) o banco de dados do Sistema de Gestão Educacional (SIGA), fonte dos dados dos estudantes e professores e seus respectivos vínculos com a UDESC.

5.2 FLUXO DO TRATAMENTO DOS DADOS

Para entender o fluxo do tratamento dos dados do Sistema GIA, é importante conhecer a estrutura dos componentes que fazem parte desse sistema, sendo apresentados pela Figura 6.

Figura 6 - Componentes do Sistema GIA



Fonte: elaborada pela autora, adaptado da UDESC (2023)

Conforme representado pela Figura 6, as bases de usuários são aquelas que possuem informações de usuários com algum tipo de vínculo com a UDESC. Assim, a base do SIGRH representa a carga dos vínculos de professores,

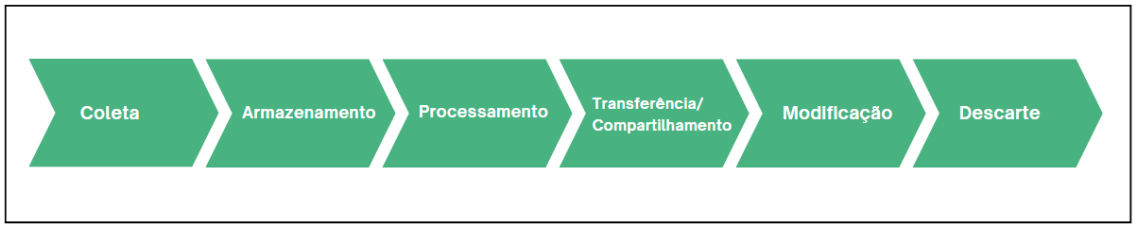
técnicos, bolsistas e estagiários, incluindo também uma interface que faz a carga de todas as informações das lotações e dos afastamentos. Já a base do SIGA representa a carga dos vínculos de alunos regulares e de extensão e dos tutores EAD, além da carga dos cursos cadastrados.

Ainda representado pela Figura 6, o “Diretório LDAP” é a base principal do sistema GIA, ela recebe os dados pessoais e funcionais dos usuários e grava os acessos que cada usuário possui aos sistemas da UDESC. Na sequência é apresentado o “*Frontend* de acessos”, que é uma interface web que permite cadastrar os usuários que não são carregados pelas fontes de dados SIGRH e SIGA, além de cadastrar contas de serviços, associar transações, acessos e os perfis, além de permitir administrar a interface do GIA com os outros sistemas da UDESC.

A estrutura do GIA conta ainda com o “*Webservice* de autorização”, que é a parte que recebe as solicitações dos sistemas da UDESC com a chave do usuário que irá acessar, retornando quais são os acessos que o usuário está autorizado a realizar. Já o “*Workflow* de solicitação” representa a parte que registra as solicitações de acesso aos sistemas da UDESC, onde somente após um fluxo de aprovação dessa solicitação o acesso pode ser concedido no GIA. Por fim, a parte dos “Sistemas” representa todos os sistemas da UDESC que utilizam o GIA para fazer seu controle de acesso.

Definidos os componentes do GIA, passamos a identificar, através da Figura 7 como se dá o fluxo dos dados no sistema.

Figura 7 - Fluxo dos dados no Sistema GIA



Fonte: elaborada pela autora (2023)

No diagrama apresentado é possível perceber como se dá a entrada das informações no Sistema GIA, a fase de transformação dos dados, e posterior uso e compartilhamento dos mesmos, de acordo com os webservices dos

sistemas que se alimentam desses dados. Assim, considerando o artigo 5º, inciso X[3] da LGPD, seguem abaixo discriminadas todas as operações de tratamento realizadas pelo Sistema GIA:

- **Coleta**: os dados são coletados por rotina automática diária, que faz a extração dos dados das bases de usuários (SIGRH e SIGA);
- **Armazenamento**: o GIA armazena os dados pessoais dos titulares no Diretório LDAP (Figura 6), que serve como base centralizadora dos dados dos usuários;
- **Processamento**: os dados pessoais coletados são filtrados de acordo com as necessidades e funcionalidades exigidas pelos sistemas da UDESC que irão utilizar esses dados. Esta etapa atende à tríade dos princípios da finalidade, da adequação e da necessidade de acordo com a LGPD[4];
- **Transferência/Compartilhamento**: o GIA permite a transferência e o compartilhamento dos dados pessoais com os demais sistemas da UDESC, os quais são integrados através dos webservices, permitindo a consulta por esses sistemas, que podem gerar relatórios com informações variadas;
- **Modificação**: os dados pessoais dos titulares, que necessitam modificação, são acessados através da interface web (*Frontend* de Acessos – Figura 6), apenas por usuários com os papéis específicos para a atividade, através de login e senha exclusivos;
- **Descarte**: a forma que ocorre o processo de eliminação dos dados pessoais dos titulares não foi especificada para nenhum dos bancos de dados informados.

O sistema GIA, por ter iniciado seu desenvolvimento em meados de 2016, ou seja, antes da criação da LGPD, não descreve em seus documentos os meios

[3] [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (Brasil, 2018, Art.5º, X)

[4] A finalidade, adequação e a necessidade são princípios que somados resultam no que se chama de mínimo essencial, algo como saber qual a menor quantidade de dados pessoais necessária para que se chegue ao fim pretendido de forma adequada. (Teixeira; Guerreiro, 2022, p.19)

de proteção de dados adotados, nem as medidas de segurança à proteção dos dados pessoais. Porém, sua documentação indica a proteção do acesso ao sistema por meio de área restrita, com a utilização de senha e login intransferíveis, e com a definição e uso de papéis específicos para os acessos.

Os dados especificados são armazenados em uma base de dados local, dentro do Datacenter da SETIC, que diariamente realiza o backup integral do banco de dados em Disco (*Onsite* em um *appliance* de backup) e em Fita (Backup em fita LTO movida para *offsite* semanalmente).

Não foi descrito o período mínimo e máximo para o armazenamento dos dados no banco de dados do GIA que, atualmente, os armazena por período indeterminado. Já os backups realizados pela SETIC ficam disponíveis por um período de noventa (90) dias em Disco, e cento e oitenta (180) dias em Fita.

Atualmente, o GIA não realiza a anonimização dos dados pessoais, mas o sistema filtra os dados de acordo com as necessidades dos sistemas da UDESC que irão utilizá-los. Ainda nesse contexto, os usuários que acessam o sistema possuem acesso restrito por papéis (administrador, editor, visualizador), onde apenas alguns papéis possuem o acesso completo aos dados inseridos no sistema.

5.3 CATALOGAÇÃO DA FONTE DE DADOS

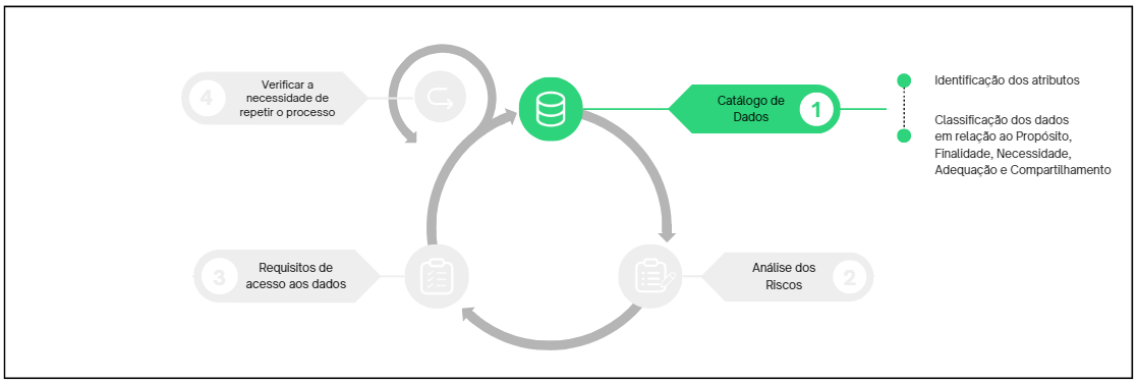
Depois de descrito o fluxo do tratamento de dados realizado pelo GIA, foi realizada a catalogação da fonte de dados. Nesse cenário de estudo foi identificado o processo inicial do tratamento de dados realizado pela GIA, a coleta de dados, com foco nos dados dos estudantes.

Assim, foram analisadas as telas da plataforma do Sistema SIGA (ANEXO A), no cadastro de pessoa física, que trazem todos os dados dos estudantes que podem ser extraídos pelo GIA. Para esta análise foi criada uma tabela com a identificação de cada atributo, a sua classificação quanto ao tipo de dado, se é um dado pessoal, pessoal sensível ou um dado não pessoal. Também foram identificados o propósito e a finalidade do uso daquele dado, de acordo com a LGPD, além da sua necessidade e adequação, para mostrar que o dado atingiu a finalidade pretendida. E, por fim, foi possível identificar se ocorre ou não o

compartilhamento do dado, com qual órgão do setor público e a sua correspondente justificativa para o compartilhamento.

Esta etapa dá início ao modelo proposto por esta pesquisa, de implementar requisitos de acesso aos dados catalogados, representado pela Figura 8.

Figura 8 – Etapa 1 – Catálogo de Dados



Fonte: elaborada pela autora (2023)

Já a extração e análise dos dados resultou na catalogação dos dados representados pelo Quadro 9.

Quadro 9 – Catálogo de dados referentes a estudantes

	Dado	Classificação do Dado	Propósito / Finalidade	Adequação / Necessidade	Compartilhamento / Órgão e justificativa
	Nome	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação dos estudantes para utilização do sistema e serviços	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
Documentos	CPF	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação dos estudantes para utilização do sistema e serviços	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	RG/R.N.E	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação dos estudantes	Não compartilhado
	Passaporte	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação dos estudantes estrangeiros para utilização do sistema e serviços	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Data de emissão do RG/Passaporte	Pessoal	Artigo 7°, Inciso II da LGPD	Data de emissão para identificação do RG/Passaporte dos estudantes	Não compartilhado
	Órgão emissor RG/passaporte	Pessoal	Artigo 7°, Inciso II da LGPD	Órgão emissor para identificação do RG/Passaporte dos estudantes	Não compartilhado
	Número do PIS	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação dos estudantes junto a Previdência Social	Não compartilhado
	Curriculum lattes	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do Curriculum lattes dos estudantes e professores	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
Título de eleitor	Número	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação dos estudantes	Não compartilhado
	Seção	Pessoal	Artigo 7°, Inciso II da LGPD	Seção eleitoral para identificação do eleitor	Não compartilhado
	Zona eleitoral	Pessoal	Artigo 7°, Inciso II da LGPD	Zona eleitoral para identificação do eleitor	Não compartilhado
	Município	Pessoal	Artigo 7°, Inciso II da LGPD	Município eleitoral para identificação do eleitor	Não compartilhado
	Data de expedição	Pessoal	Artigo 7°, Inciso II da LGPD	Data de expedição do título eleitoral para identificação do eleitor	Não compartilhado

Documento militar	Número	Pessoal	Artigo 7°, Inciso II da LGPD	Número do documento militar de identificação dos estudantes	Não compartilhado
	Categoria	Pessoal	Artigo 7°, Inciso II da LGPD	Categoria do documento militar para identificação dos estudantes	Não compartilhado
	Orgão expedidor	Pessoal	Artigo 7°, Inciso II da LGPD	Órgão expedidor do documento militar para identificação dos estudantes	Não compartilhado
	Município	Pessoal	Artigo 7°, Inciso II da LGPD	Município do documento militar para identificação dos estudantes	Não compartilhado
	Data de expedição	Pessoal	Artigo 7°, Inciso II da LGPD	Data de expedição do documento militar para identificação dos estudantes	Não compartilhado
Endereço	CEP	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do CEP do endereço dos estudantes	Não compartilhado
	Endereço	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do endereço dos estudantes	Não compartilhado
	Número	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação número do endereço dos estudantes	Não compartilhado
	Bairro	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do bairro do endereço dos estudantes	Não compartilhado
	Município	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do município do endereço dos estudantes	Não compartilhado
	Complemento do Endereço	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do complemento do endereço dos estudantes	Não compartilhado
	Zona de residência	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da zona de residência do endereço dos estudantes	Não compartilhado
	Localização diferenciada	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da localização do endereço dos estudantes	Não compartilhado
	Tipo de endereço de correspondência	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do tipo de endereço de correspondência dos estudantes	Não compartilhado
	Não utilizar Endereço Familiar	Pessoal	Artigo 7°, Inciso II da LGPD	Identificador para utilização de endereço familiar dos estudantes	Não compartilhado
	Fone residencial	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato com o estudante, para demandas administrativas diversas, após tentativas por e-mail não tiverem sucesso	Não compartilhado
	Fone celular	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato com o estudante, para demandas	Não compartilhado

				administrativas diversas, após tentativas por e-mail não tiverem sucesso	
	Fone comercial	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato com o estudante, para demandas administrativas diversas, após tentativas por e-mail não tiverem sucesso	Não compartilhado
	Ramal	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato com o estudante, para demandas administrativas diversas, após tentativas por e-mail não tiverem sucesso	Não compartilhado
	E-mail Pessoal (para recuperação de senha)	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato e envio de procedimento para recuperação de senha dos estudantes	Não compartilhado
	E-mail institucional (@udesc.br)	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato para comunicação de recebimento de resposta ou para comunicação administrativa, e acessos do estudante a serviços e sistemas da universidade	Não compartilhado
	E-mail com domínio da instituição	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato para comunicação de recebimento de resposta ou para comunicação administrativa, e acessos do estudante a serviços e sistemas da universidade	Não compartilhado
	Unidade atual	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da unidade de lotação dos estudantes	Não compartilhado
	Home page	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação dos estudantes	Não compartilhado
	Outros contatos	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para realizar o contato com os estudantes, caso os demais não tenham retorno	Não compartilhado
Dados Complementares	Tipo de nacionalidade	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do tipo de nacionalidade dos estudantes	Não compartilhado
	Nacionalidade	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação da nacionalidade dos estudantes	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição

	Município de nascimento	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do município de nascimento dos estudantes	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Data de nascimento	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação dos estudantes para utilização do sistema e serviços	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Sexo/Gênero	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do sexo/gênero dos estudantes	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Estado civil	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do estado civil dos estudantes	Não compartilhado
	Religião	**Sensível**	Artigo 11, Inciso II alínea “a” da LGPD	Identificação da religião dos estudantes	Não compartilhado
	Cor/Raça/Etnia (autodeclarado)	**Sensível**	Artigo 11, Inciso II, alíneas “a” e “b” da LGPD	Identificação da declaração de cor/raça/etnia dos estudantes	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Cônjuge	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do nome do cônjuge	Não compartilhado
	Nome do pai	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da filiação dos estudantes	Não compartilhado
	Nome da mãe	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da filiação dos estudantes	Não compartilhado
	Responsável	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do responsável pelo estudante, quando menor de idade	Não compartilhado
	Parentesco do Responsável	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do parentesco do responsável pelo estudante	Não compartilhado
	Data de falecimento	Pessoal	Artigo 7°, Inciso II da LGPD	Data de falecimento do estudante	Não compartilhado
	Emancipado	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da emancipação ou não do estudante	Não compartilhado

	Possui pendências de multa na biblioteca	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação se o estudante possui pendências de multa na biblioteca	Não compartilhado
	Possui pendências de material na biblioteca	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação se o estudante possui pendências de material na biblioteca	Não compartilhado
	Bloquear por pendência financeira	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação para bloqueio ou não do estudante por pendência financeira na biblioteca	Não compartilhado
	Permite a instituição mandar e-mail	Pessoal	Artigo 7°, Inciso II da LGPD	Consentimento do estudante para comunicação da instituição via e-mail	Não compartilhado
	Permite a instituição mandar mensagens pelo celular	Pessoal	Artigo 7°, Inciso II da LGPD	Consentimento do estudante para comunicação da instituição via mensagens pelo celular	Não compartilhado
	Observações gerais	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para adicionar informações faltantes no cadastro	Não compartilhado
	Código de integração	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do código de integração dos estudantes	Não compartilhado
	Bloquear acesso as centrais	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do bloqueio ou não de acesso do estudante as centrais	Não compartilhado
	Ano de realização da prova do ENEM	Pessoal	Artigo 7°, Inciso II da LGPD	Ano em que o estudante realizou a prova do ENEM	Não compartilhado
	Código de inscrição do ENEM	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do código de inscrição do estudante no ENEM	Não compartilhado
	Código do INEP	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do código do INEP da instituição	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Data da última integração com a biblioteca	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da data da última integração do estudante com a biblioteca	Não compartilhado
	Assinatura	Pessoal	Artigo 7°, Inciso III da LGPD	Documento contendo assinatura digital do estudante	Dado utilizado para autenticação de documentos

Estudante	Observação	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para adicionar informações faltantes no cadastro	Não compartilhado
Servidor	Conta bancária	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da conta bancária para estudantes, professores, servidores e terceirizados	Não compartilhado
	Vínculo de Professor	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do vínculo de professor	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Data de bloqueio do professor na biblioteca	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação da data de bloquei do professor na biblioteca	Não compartilhado
	Registro do professor no Estado	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação do registro do professor no estado	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Credenciado para ministrar na Pós-graduação	Pessoal	Artigo 7°, Inciso III da LGPD	Identificação se é professor credenciado para ministrar na Pós-graduação	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Departamento	Pessoal	Artigo 7°, Inciso II da LGPD	Identificação do departamento de lotação do professor ou servidor	Não compartilhado
	Observação	Pessoal	Artigo 7°, Inciso II da LGPD	Necessário para adicionar informações faltantes no cadastro	Não compartilhado
Informações profissionais	Empresa que trabalha	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da empresa em que trabalha	Não compartilhado
	Ocupação profissional	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da ocupação profissional	Não compartilhado
	Ocupação atual	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da ocupação atual	Não compartilhado
	CTPS	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da Carteira de Trabalho e Previdência Social	Não compartilhado

	Série CTPS	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da série da Carteira de Trabalho e Previdência Social	Não compartilhado
	Data de emissão do CTPS	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da data de emissão da Carteira de Trabalho e Previdência Social	Não compartilhado
	UF CTPS	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação do estado de emissão da Carteira de Trabalho e Previdência Social	Não compartilhado
	Qualificação profissional	Pessoal	Artigo 7°, Inciso V da LGPD	Identificação da qualificação profissional	Não compartilhado
Dados socioeconômicos	Renda	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação da renda do estudante	Não compartilhado
	Recebe benefício governamental	Pessoal	Artigo 7°, Incisos III e IV da LGPD	Identificação se recebe benefício governamental	Ministério da Educação: para fins de relatório de comprovação de realização / uso do recurso público e classificação da instituição
	Nº de passes recebidos	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do número de passes recebidos pelo estudante	Não compartilhado
	Frequência do recebimento de passes	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação da frequência do recebimento de passes pelo estudante	Não compartilhado
	Transporte escolar público	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do transporte público utilizado pelo estudante	Não compartilhado
	Poder público responsável pelo transporte escolar	Não é dado pessoal	Artigo 7°, Inciso IV da LGPD	Identificação se o poder público é o responsável pelo transporte escolar do estudante	Não compartilhado
	Faz refeição na instituição	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação se o estudante faz refeições na instituição	Não compartilhado
	Turno da refeição na instituição	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do turno da refeição realizada pelo estudante na instituição	Não compartilhado
	Ocupação de moradia	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do tipo de moradia do estudante	Não compartilhado
	Número de Cômodos	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do número de cômodos que contém a moradia do estudante	Não compartilhado
	Com quem mora	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação das pessoas que moram com o estudante	Não compartilhado

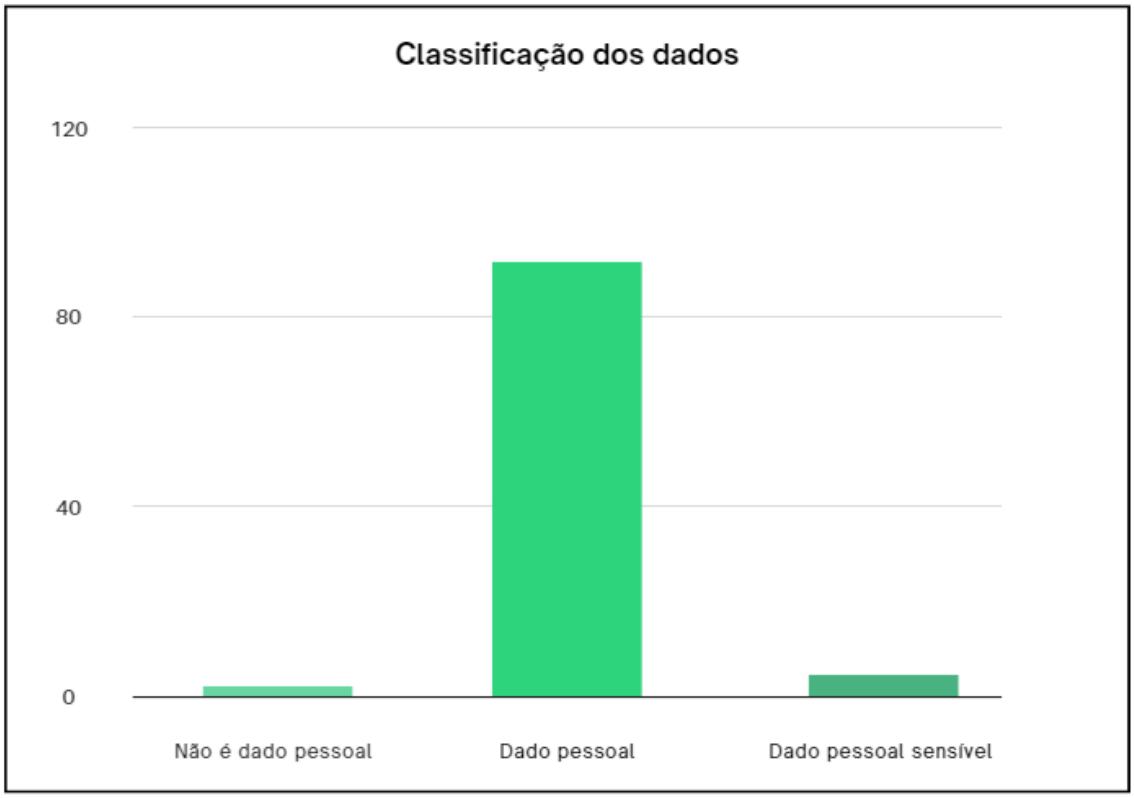
	Talento do aluno	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação do talento do estudante	Não compartilhado
	Possui veículo automotor	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação se o estudante possui veículo automotor	Não compartilhado
	Possui outro imóvel	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação se o estudante possui outro imóvel	Não compartilhado
	Possui outros bens	Pessoal	Artigo 7°, Inciso IV da LGPD	Identificação se o estudante possui outros bens	Não compartilhado

Fonte: elaborada pela autora (2023)

Dessa forma, o Quadro 9 representa todos os dados disponíveis no sistema SIGA, os quais podem ser extraídos pelo sistema GIA. Vale destacar que todos os dados apresentados não possuem um prazo de armazenamento e/ou eliminação definido, sendo que seu armazenamento hoje não possui um procedimento de eliminação de dados, exceto a pedido do titular e com base legal definida pela LGPD. Além disso, nenhum dado é anonimizado ou pseudoanonimizado, contudo, como informado anteriormente, apenas os dados necessários são extraídos pelo GIA, a fim de atender a tríade dos princípios da finalidade, necessidade e adequação da LGPD.

Assim, a partir do Quadro 9, foi possível identificar 96 dados pessoais, ou seja, as informações relacionadas a pessoa natural; também foram identificados 2 dados pessoais sensíveis (Religião e Cor/Raça/Etnia), informações que podem descriminalizar a pessoa natural; além de 1 dado não pessoal, informação que não está relacionada a pessoa natural. Estas informações foram elencadas pelo Gráfico 1.

Gráfico 1 - Proporção dos dados pessoais e dados pessoais sensíveis



Fonte: elaborado pela autora (2023)

Com isso, a catalogação dos dados coletados pela UDESC permitiu apontar os dados pessoais e os dados pessoais sensíveis, conforme estipulado pela LGPD, atendendo o primeiro objetivo da pesquisa. Além disso, foi possível afirmar que o tratamento de dados inicial é realizado de forma proporcional com as finalidades informadas, também observando os aspectos que envolvem o acesso ao direito social e fundamental à educação (artigo 6° e 205 da Constituição Federal[5]).

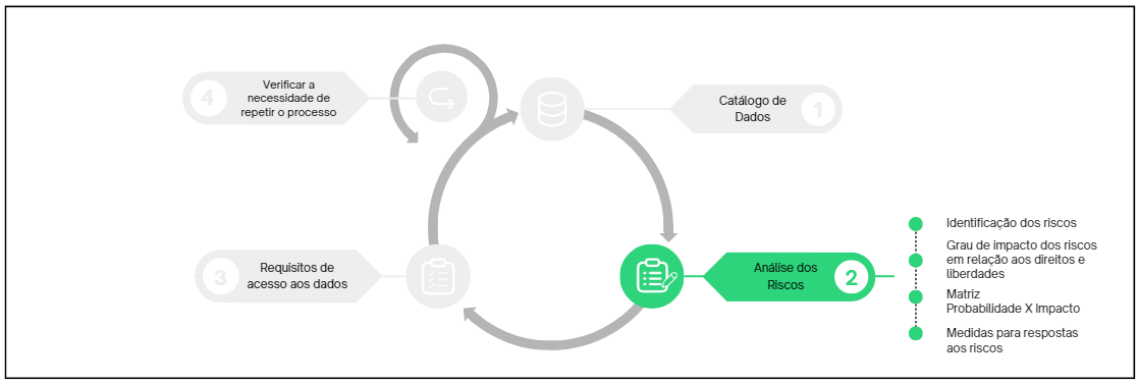
5.4 AVALIAÇÃO DOS RISCOS PARA OS DIREITOS E LIBERDADES

Com os dados devidamente catalogados, foi realizada a análise dos riscos em relação aos mesmos, iniciando a Etapa 2 do modelo proposto da pesquisa, representado pela Figura 9. Como a LGPD não conceitua risco, os agentes de

[5] Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. (Brasil, 1988)

tratamento podem, de acordo com as especificidades do tratamento de dados realizado, estabelecer a sua própria metodologia na análise de riscos aos direitos dos titulares.

Figura 9 – Etapa 2 – Análise dos Riscos



Fonte: elaborada pela autora (2023)

De acordo com o art. 5º, XVII da LGPD, o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco”, assim, a metodologia que será adotada pelos agentes de tratamento deve servir como elemento orientador para a verificação de potenciais eventos prejudiciais aos direitos dos titulares de dados. Além disso, essa metodologia poderá ser alterada sempre que necessário, principalmente quando ocorrerem mudanças no cenário tecnológico, no contexto da gestão e governança dos dados, e nas demais mudanças de estado e ambiente.

Contudo, antes de definir uma metodologia, os riscos que geram impacto potencial sobre os direitos e liberdades do titular dos dados devem ser identificados. Assim, de acordo com Brasil (2020), para cada risco identificado faz-se necessário definir qual a probabilidade de ocorrência do evento de risco e qual o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Tendo como base o modelo de implementação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), de acordo com o Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD) – Brasil (2020), os possíveis riscos identificados para os dados catalogados foram:

1. **Acesso não autorizado**: o acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais;
2. **Modificação não autorizada**: modificação de dados pessoais sem a anuência do titular, onde este risco viola o princípio da segurança;
3. **Perda**: destruição ou extravio de dados pessoais, o que viola os princípios da segurança e da prevenção;
4. **Remoção não autorizada**: retirada de dados pessoais sem autorização do titular;
5. **Coleta excessiva**: extração de mais dados além do necessário para a realização do trabalho ou do que é previsto em Lei ou autorizado pelo usuário;
6. **Informação insuficiente sobre a finalidade do tratamento**: ausência de informações claras acerca do tratamento de dados que devem ser disponibilizadas desde a coleta;
7. **Tratamento sem consentimento do titular dos dados pessoais**: caso o tratamento não esteja previsto em legislação ou regulação pertinente;
8. **Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais**: quando os dados pessoais são utilizados em outros sistemas sem a devida informação e anuência do titular dos dados;
9. **Retenção prolongada de dados pessoais sem necessidade**: manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado;
10. **Falha/erro de processamento**: processamento dos dados de forma imperfeita ou equivocada, o que viola o princípio da qualidade dos dados;
11. **Reidentificação de dados pseudoanonimizados**: anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão;

12. **Inacessibilidade de informações**: ausência de instrumentos, fluxos e canais de atendimento que disponibilizem informações sobre o tratamento de dados ou mesmo sobre os dados ao titular;

13. **Inércia perante incidentes de privacidade**: ausência de protocolos definidos em caso de eventual vazamento acidental ou intencional de dados dos titulares;

14. **Incompatibilidade com a conjuntura tecnológica**: ausência de análise da conjuntura tecnológica e de uma política de atualização tecnológica definida, tornando os sistemas suscetíveis a incidentes de privacidade;

15. **Apropriação ou uso indevido de dados pessoais:** possibilidades de fraude e vazamento intencional de dados.

Com a identificação e classificação dos riscos, faz-se necessária uma análise acerca dos possíveis impactos aos direitos dos titulares.

5.4.1 Grau de impacto dos riscos em relação aos direitos e liberdades

A análise dos possíveis impactos aos direitos dos titulares foi realizada através da comparação entre o tratamento de dados descrito nos itens anteriores e o rol de direitos elencados na LGPD e na Constituição Federal, conforme quadro resumo apresentado a seguir (Quadro 10).

Quadro 10 - Resumo da análise de riscos

ID	Risco	Direito potencialmente impactado	Grau/Urgência
R01	Acesso não autorizado	Artigo 5°, inciso X da CF Artigo 17° e 18° da LGPD	alto/ não urgente
R02	Modificação não autorizada	Artigo 5°, inciso X da CF Artigo 17° e 18°, inciso III, da LGPD	alto/ não urgente
R03	Perda	Artigo 5°, inciso X da CF Artigo 17° e 18°, incisos, II e III, da LGPD	alto/ não urgente
R04	Remoção não autorizada	Artigo 18°, incisos, II e III, da LGPD	alto/ não urgente
R05	Coleta excessiva	Decorrente do artigo 6°, Inciso III, da LGPD	baixo/ não urgente

R06	Informação insuficiente sobre a finalidade do tratamento	Artigo 18°, incisos I, II e VII da LGPD	alto/urgente
R07	Tratamento sem consentimento do titular dos dados pessoais	Artigo 5°, inciso X da CF Artigo 17° e 18° da LGPD	alto/urgente
R08	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Artigo 5°, inciso X da CF Artigo 17° e 18°, incisos, II e III, da LGPD	alto/urgente
R09	Retenção prolongada de dados pessoais sem necessidade	Decorrente do artigo 6°, Inciso III, e artigo 18°, inciso VI da LGPD	alto/urgente
R10	Falha ou erro de processamento	Decorrente do artigo 6°, Inciso V, da LGPD	alto/urgente
R11	Reidentificação de dados pseudonimizados	Artigo 18°, inciso IV, da LGPD	alto/urgente
R12	Inacessibilidade de Informações	Artigo 18°, incisos I, II e VII, e artigo 19° da LGPD	alto/urgente
R13	Inércia Perante a Incidentes de Privacidade	Artigo 5°, inciso X da CF Artigo 17° da LGPD	alto/urgente
R14	Incompatibilidade com a Conjuntura Tecnológica	Artigo 5°, inciso X da CF Artigo 17° e 18° da LGPD	alto/urgente
R15	Apropriação ou uso indevido de dados pessoais	Artigo 5°, inciso X da CF Artigo 17° e 18° da LGPD	alto/ não urgente

Fonte: elaborado pela autora (2023)

Após a identificação e análise dos riscos e seus possíveis impactos aos direitos dos titulares, foram definidos parâmetros escalares para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

Assim, os parâmetros escalares adotados nesta pesquisa são apresentados na Tabela 3.

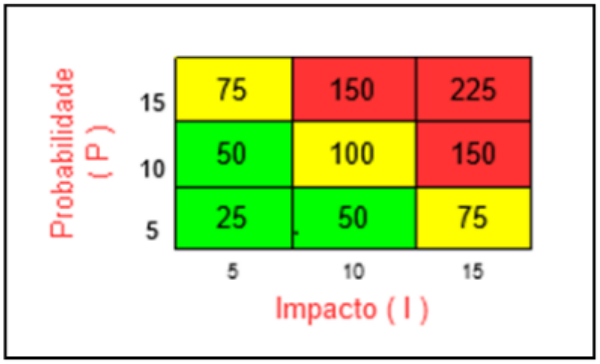
Tabela 3 – Parâmetros escalares para a classificação dos riscos

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Fonte: Brasil (2020)

Para construir a matriz de risco, foi utilizada a Matriz Probabilidade x Impacto, representada pela Figura 10, que, de acordo com Brasil (2020), é um instrumento de apoio para a definição dos critérios de classificação do nível de risco. Nesta matriz, o produto da probabilidade pelo impacto de cada risco identificado deve se enquadrar em uma das regiões da matriz (Figura 10).

Figura 10 - Matriz Probabilidade X Impacto



Fonte: Brasil (2020)

Na representação da matriz, segundo Brasil (2020, p.40), um “risco enquadrado na região:

• Verde, é entendido como baixo;

• Amarelo, representa risco moderado; e

• Vermelho, indica risco alto.”

Dessa forma, conforme Brasil (2020), as definições e os conceitos de riscos adotados nesta pesquisa, que seguem o modelo de implementação do RIPD, serão utilizados como forma de ilustrar a identificação e a avaliação dos riscos para esta pesquisa. Contudo, é importante destacar que o gerenciamento de riscos, relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com as políticas de gestão de risco adotados pela instituição.

Assim, depois de identificados os riscos há a necessidade de se apontar a probabilidade de ocorrência do evento de risco e o seu possível impacto, caso o risco ocorra, avaliando o nível potencial de risco para cada evento, conforme apresentado na Tabela 4 abaixo.

Tabela 4 - Riscos referentes ao tratamento de dados pessoais

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado	10	15	150
R02	Modificação não autorizada	10	15	150
R03	Perda	5	15	75
R04	Remoção não autorizada	5	15	75
R05	Coleta excessiva	10	10	100
R06	Informação insuficiente sobre a finalidade do tratamento	10	15	150
R07	Tratamento sem consentimento do titular dos dados pessoais	10	15	150
R08	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	10	15	150
R09	Retenção prolongada de dados pessoais sem necessidade	10	5	50
R10	Falha/erro de processamento	5	15	75
R11	Reidentificação de dados pseudoanonimizados.	5	15	75
R12	Inacessibilidade de Informações	5	15	75
R13	Inércia Perante a Incidentes de Privacidade	5	15	75
R14	Incompatibilidade com a Conjuntura Tecnológica	10	15	150
R15	Apropriação ou uso indevido de dados pessoais	10	15	150

Fonte: elaborada pela autora com base em Brasil (2020).

Com isso, a Matriz Probabilidade x Impacto elaborada permitiu ilustrar os riscos levantados nesta etapa da pesquisa e, a partir da multiplicação, foram identificados os níveis dos riscos identificados, sendo possível assim priorizar os riscos, afim de mitigar os que apresentam maior criticidade. Dessa forma, foi possível atender ao segundo objetivo da pesquisa.

5.4.2 Medidas para resposta aos riscos

Após a análise dos eventuais riscos aos direitos dos titulares de dados, faz-se necessária a adoção de medidas para mitigar esses riscos. Assim, de acordo com a LGPD:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Brasil, 2018, art. 46)

As medidas apresentadas pelo Quadro 11 a seguir foram elaboradas de acordo com a classificação dos riscos, apresentando os possíveis efeitos resultantes do tratamento do risco com a aplicação das medidas descritas na Tabela 4.

Quadro 11 - Medidas para resposta aos riscos

Id	Risco	Medida(s)	Efeito sobre o risco
R01	Acesso não autorizado	• Submeter os sistemas a testes periódicos de vulnerabilidade • Registro e documentação dos testes de vulnerabilidade	Reduzir
R02	Modificação não autorizada	• Submeter os sistemas a testes periódicos de vulnerabilidade • Registro e documentação dos testes de vulnerabilidade	Reduzir
R03	Perda	• Submeter os sistemas a testes periódicos de vulnerabilidade • Registro e documentação dos testes de vulnerabilidade	Reduzir
R04	Remoção não autorizada	• Submeter os sistemas a testes periódicos de vulnerabilidade • Registro e documentação dos testes de vulnerabilidade	Reduzir
R05	Coleta excessiva	• Revisão periódica dos dados pessoais e dados pessoais sensíveis a serem coletados, relacionando estes com a finalidade, adequação e necessidade do tratamento	Evitar
R06	Informação insuficiente sobre a finalidade do tratamento	• Elaboração da Política de Privacidade da UDESC • Capacitação dos colaboradores que atuem no tratamento de dados • Publicação dos fluxos de tratamento de dados incluindo compartilhamento com órgãos/entidades parceiros	Reduzir
R07	Tratamento sem consentimento do titular dos dados pessoais	• Disponibilizar informações aos titulares de dados acerca do tratamento de dados realizado pelo sistema	Evitar
R08	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	• Disponibilizar informações aos titulares de dados acerca do compartilhamento de dados no momento da coleta	Evitar
R09	Retenção prolongada de dados pessoais sem necessidade	• Elaborar e publicizar uma política de armazenamento e eliminação de dados pessoais e dados pessoais sensíveis	Evitar

R10	Falha ou erro de processamento	• Submeter os sistemas a testes de vulnerabilidade • Atualização contínua dos sistemas de acordo com a Conjuntura Tecnológica Atual	Reduzir
R11	Reidentificação de dados pseudonimizados	• Revisão dos processos de anonimização e pseudonimização de dados • Ampliação dos referidos processos • Análise da Conjuntura Tecnológica	Evitar
R12	Inacessibilidade de Informações	• Criação e estruturação de setor (Encarregado de Dados) • Publicação dos fluxos de tratamento de dados incluindo compartilhamento com órgãos/entidades parceiros	Evitar
R13	Inércia Perante a Incidentes de Privacidade	• Elaboração de um Protocolo de Segurança em caso de incidentes • Capacitação dos colaboradores que atuem no tratamento de dados • Atualização contínua dos termos de confidencialidade	Evitar
R14	Incompatibilidade com a Conjuntura Tecnológica	• Análise e revisão dos sistemas utilizados em relação a Conjuntura Tecnológica Atual • Análise dos sistemas utilizados por operadores e órgãos/ entidades com os quais são compartilhados dados • Política de atualização dos sistemas • Registro e documentação das referidas atividades	Reduzir
R15	Apropriação ou uso indevido de dados pessoais	• Submeter os sistemas a testes periódicos de vulnerabilidade • Registro e documentação dos testes de vulnerabilidade	Reduzir

Fonte: elaborada pela autora (2023)

De acordo com Brasil (2020), os efeitos sobre o risco podem ser: Reduzir, Evitar, Compartilhar e Aceitar, onde a instituição nem sempre precisa eliminar todos os riscos, podendo decidir que alguns riscos são aceitáveis (até mesmo um risco de nível alto), devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação.

Dessa forma, segundo Brasil (2020):

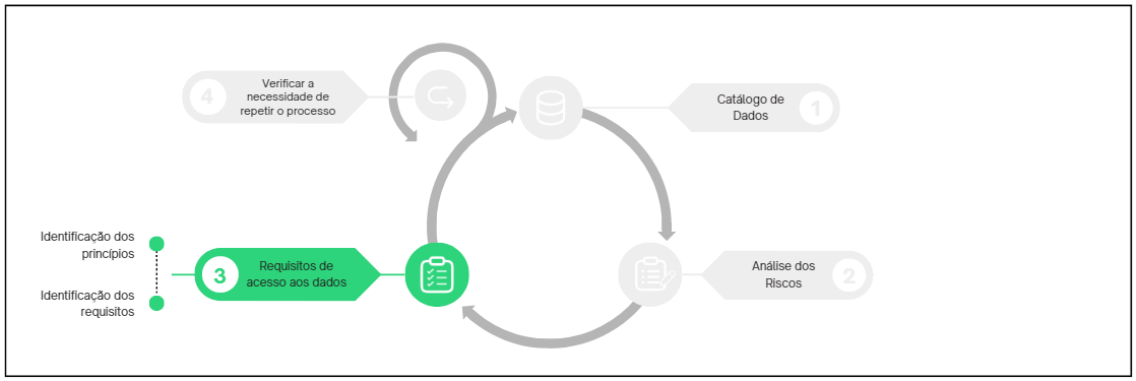
> A instituição deve manter revisão do RIPD a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional. (BRASIL, 2020)

Com isso, o relatório de impacto deve ser revisto e atualizado periodicamente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

5.5 REQUISITOS DE ACESSO AOS DADOS CATALOGADOS

Com a descrição do tratamento de dados, os riscos devidamente definidos e suas métricas analisadas, foi utilizado o método DSR para definir um conjunto de requisitos de acesso aos dados catalogados, representando a terceira etapa do modelo proposto desta pesquisa (Figura 11). Assim, na primeira etapa do método, na investigação do problema, foi identificada a situação atual do acesso aos dados transacionais pelo sistema GIA.

Figura 11 – Etapa 3 – Requisitos de acesso aos dados



Fonte: elaborada pela autora (2023)

Pode-se observar que o GIA possui um controle de acesso através de autenticação com login e senha intransferíveis, o que garante que apenas pessoas autorizadas possam acessar o sistema. Além disso, depois de autenticados, os usuários só devem ter acesso aos dados para os quais têm permissão, isso envolve a definição de papéis, funções e permissões de acesso que são cadastradas no sistema. Essas medidas já adotadas pelo GIA atendem ao princípio da **segurança** da LGPD.

Quanto a carga dos dados no sistema, o GIA faz a extração das bases de dados diariamente, a fim de garantir a integridade e a **qualidade dos dados**, e o sistema de backup garante a disponibilidade dos dados em caso de falhas no sistema, atendendo ao princípio da **prevenção** da LGPD.

A extração dos dados é realizada de forma a filtrar os dados, de acordo com as necessidades dos sistemas que irão utilizá-los, atendendo aos princípios da **finalidade**, **necessidade** e **adequação** da LGPD. Ainda nesse contexto, os

filtros realizados na coleta de dados permitem atender também ao princípio da **não discriminação**, pois os dados sensíveis, que podem ser utilizados para fins discriminatórios ilícitos ou abusivos não são extraídos.

Já os princípios do **livre acesso** e da **transparência** não são ainda atendidos pelo GIA, pois os titulares dos dados, não tem informações claras sobre como seus dados são tratados pelo sistema, nem sobre a duração do tratamento. Da mesma forma, a ausência de uma política de privacidade ou mesmo de documentação apropriada sobre o tratamento dos dados, impossibilita atender ao princípio da **responsabilização e prestação de contas**.

Nesse contexto, percebeu-se que o sistema GIA efetivou o seu tratamento de dados de forma incremental, mesmo tendo iniciado seu desenvolvimento antes da promulgação da LGPD. Assim, alguns princípios ainda precisam ser trabalhados para serem atendidos em sua plenitude.

Além dos princípios analisados acima, que são estipulados pela LGPD em seu artigo 6º, o GIA precisa atender aos requisitos estipulados pela LGPD em seu artigo 7º. Nesta sequência, fez-se a análise dos requisitos conforme destacado pelo Quadro 12.

Quadro 12 - Requisitos para acesso aos dados catalogados

Requisito (art. 7º LGPD)	**Aplicação**	**Sistema GIA**
I – mediante o fornecimento de consentimento pelo titular	Atualmente a UDESC não solicita consentimento do titular dos dados, salvo ações isoladas	Não atende
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;	A UDESC trata as informações pessoais dos estudantes para cumprir obrigações estabelecidas pela legislação educacional na emissão de diplomas, geração de relatórios estatísticos e, quando necessário para a realização de processos seletivos	Atende
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;	A UDESC, como instituição pública, pode coletar e processar informações pessoais dos estudantes para a submissão dessas informações aos órgãos competentes, como o Ministério da Educação. A UDESC pode realizar a transferência internacional de dados para outras instituições de ensino, a fim de promover o intercâmbio de estudantes e mesmo o processo de pós-graduação de alunos e professores (também atendendo ao artigo 5º, inciso XVI da	Não atende (atualmente não é da competência do sistema GIA o compartilhamento de dados com terceiros)

	LGPD[6]).	
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	Na UDESC, a coleta e o processamento de informações pessoais podem ser necessários para realizar pesquisas acadêmicas, gerar conhecimento científico ou fornecer serviços de extensão à comunidade.	Atende
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;	Na UDESC, os dados coletados do titular podem ser utilizados para o pagamento de bolsas de estudo ou para a contratação de serviços terceirizados.	Atende

Fonte: elaborada pela autora (2023)

Conforme apresentado no Quadro 12, o consentimento é um requisito que não é atendido em sua plenitude, tanto pela UDESC como instituição, e mesmo pelo sistema GIA. Apesar de ser dispensável quando atendido outros requisitos, o consentimento, de acordo com Teixeira e Guerreiro (2022), “facilita a obrigação do agente de tratamento em demonstrar que o tratamento foi feito dentro de uma hipótese legal, ante o princípio da *accountability* (prestação de contas)”. Nesse caso, o consentimento poderia ser solicitado aos estudantes diante da matrícula dos mesmos, informando o tratamento que será realizado com seus dados, e apresentando os dispositivos legais para os mesmos.

No caso do segundo requisito apresentado, inciso II do art. 7º, segundo Frajhof e Mangeth (2020), “os dados pessoais poderão ser tratados sem a necessidade de consentimento por parte do titular quando a relação jurídica em questão exigir que o controlador cumpra determinada obrigação legal ou regulatória”. Ainda segundo o autor, nesses casos o titular não poderá se opor ao tratamento. Contudo, Teixeira e Guerreiro (2022) propõe que, mesmo sem a necessidade do consentimento, o controlador informe dentro de quais possibilidades os dados do titular poderão ser tratados, atendendo-se assim ao princípio da transparência.

[6] XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; (Brasil, 2018, artigo 5º, XVI)

Em seu inciso III, sobre o compartilhamento de dados pelas instituições públicas, apesar da UDESC atender as prerrogativas da Lei, atualmente não é da competência do sistema GIA realizar o compartilhamento de dados com terceiros. Contudo, como o sistema consegue extrair os dados das fontes base, poderia ser implementada uma API para a realização desse compartilhamento, atendendo os princípios de segurança, adequação, necessidade e finalidade, a fim de manter um único ponto de controle de dados pela instituição.

Frajhof e Mangeth (2020) ainda destaca que:

> Apesar de o titular de dados estar dispensado de consentimento, o art. 23, I, da LGPD impõe que o mesmo seja informado sobre a realização do tratamento, devendo fornecer informações claras e atualizadas, em veículo de fácil acesso aos usuários, previstos, em especial, nos *sites* da administração pública. Devem estar disponíveis para acesso as informações sobre a previsão legal que autoriza o tratamento de dados, a existência de compartilhamento de dados, a finalidade para a qual se destina o uso das informações e a forma como o tratamento será realizado. (Frajhof e Mangeth, 2020, p.69-70)

O quarto requisito, inciso IV, refere-se ao uso dos dados do titular para estudo por órgãos de pesquisa, desde que garantida, sempre que possível, a anonimização dos dados. Atualmente o sistema GIA não realiza a anonimização dos dados conforme previsto pela LGPD, contudo é possível realizar a implementação dessa técnica para atender por completo esse requisito. Ainda assim, nesses casos, apesar da Lei permitir a discricionariedade do controlador em anonimizar os dados pessoais, ou seja, fazê-lo “sempre que possível”, de acordo com Frajhof e Mangeth (2020), “a sua dispensa em assim não fazer deverá ser justificada, em atenção ao que determina os princípios da segurança, prevenção, responsabilização e prestação de contas (art. 5, VII, VIII e X)”.

Quanto ao quinto requisito, presente no inciso V, Frajhof e Mangeth (2020) destaca que devem ser observados os princípios da necessidade e da finalidade para atender essa base legal, além do fundamento e objetivo final do contrato. Nesse sentido, o GIA atende a esse requisito ao trazer os dados envolvidos em contrato para que sejam tratados pelos sistemas com os devidos fins.

Assim, ficou evidente que o sistema GIA, bem como a própria instituição UDESC, atendem os requisitos necessários diante das situações impostas, e, quando necessário, o GIA poderá ser ajustado para o pleno cumprimento do específico requisito. Vale ressaltar que o consentimento que hoje não é atendido

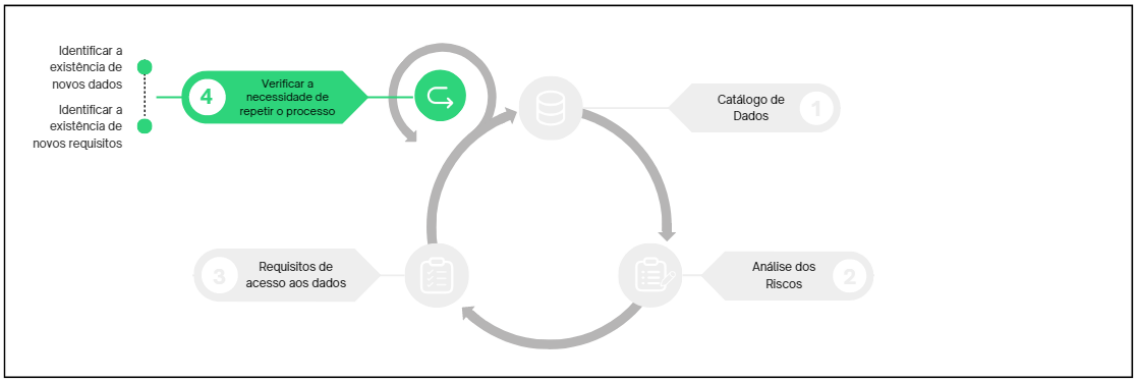
pelo GIA, poderia ser aplicado e adaptado conforme o tratamento realizado nos dados, a fim de atender a base legal da Lei, sem precisar depender dos demais requisitos impostos.

Assim, definidos os requisitos necessários para o acesso aos dados catalogados, o que atende ao terceiro objetivo da pesquisa, passamos a análise do modelo aqui desenvolvido para a implementação do acesso aos dados catalogados.

5.6 VERIFICAR A NECESSIDADE DE REPETIR O PROCESSO

Assim, finalizadas as etapas 1, 2 e 3, descritas acima, segue-se para a etapa 4 do modelo proposto, que consiste em verificar a necessidade de repetir os processos. A etapa 4 é representada pela Figura 12.

Figura 12 – Etapa 4 – Verificar a necessidade de repetir o processo



Fonte: elaborada pela autora (2023)

Nesta etapa é preciso verificar se novos dados foram inseridos na base analisada inicialmente. Assim, quando novos dados são inseridos na base, eles também devem ser catalogados, iniciando a etapa 1 novamente.

Da mesma forma, é preciso verificar se as regulamentações (Leis, PLs, etc.) que são utilizadas nas avaliações dos dados e dos requisitos de acesso foram promulgadas, editadas ou extintas. Com isso, o processo também se reinicia a partir da etapa 1.

6 CONCLUSÃO

Em um mundo cada vez mais digital e orientado por dados, percebe-se que a Governança de Dados e a LGPD se tornaram requisitos essenciais para aumentar a privacidade, a segurança e a transparência no tratamento dos dados pessoais dos indivíduos. Juntas, a GD e a LGPD desempenham um papel fundamental na proteção e no acesso adequado aos dados pessoais.

Nesse sentido, no início desta pesquisa, foram definidos os seguintes objetivos específicos: a) Catalogar a fonte de dados, apontando aqueles considerados sensíveis, conforme a LGPD; b) Analisar os riscos de acesso aos dados catalogados e considerados sensíveis, produzindo uma matriz com riscos mitigados; e c) Definir um conjunto de requisitos de acesso aos dados catalogados.

Dessa forma, foi criado o artefato do “Modelo de Implementação” e nele descreveu-se todos os métodos utilizados para chegar aos artefatos finais. Foi necessário estabelecer no modelo um ciclo de vida iterativo, reforçando a noção da aplicação desse modelo ser repetida periodicamente para atender as possíveis mudanças no escopo dos dados e nas legislações vigentes.

Assim, para o alcance do objetivo específico de “Catalogar a fonte de dados, apontando aqueles considerados sensíveis, conforme a LGPD” – foi realizado um cenário de estudo, selecionando o Sistema de Gestão de Identidades e Acessos (GIA) da UDESC, onde foi possível extrair das fontes de dados os dados dos alunos para sua catalogação, identificando e classificando cada um dos dados extraídos pelo sistema. Esta catalogação utilizou-se de uma classificação dos atributos de dados considerados sensíveis, definindo as finalidades, necessidades e adequação, conforme os princípios da LGPD, além de identificar a existência ou não, e o tipo de compartilhamento que está se dando com cada um dos dados, resultando no artefato do “Catálogo de Dados”.

Para atingir o objetivo específico de “Analisar os riscos de acesso aos dados catalogados e considerados sensíveis, produzindo uma matriz com riscos mitigados” – foram realizados processos encadeados, iniciando com a identificação dos possíveis riscos aos dados catalogados; após foram definidos o grau de impacto dos riscos em relação aos direitos e liberdades do titular dos

dados, conforme a LGPD e demais Leis envolvidas. A seguir foi gerado o artefato final do objetivo, que foi a “Matriz Probabilidade X Impacto”, e ainda foi possível gerar um artefato com medidas para respostas aos riscos identificados.

Para o alcance do objetivo específico de “Definir um conjunto de requisitos de acesso aos dados catalogados” – foram adotados os princípios e os requisitos presentes na LGPD, em seus respectivos artigos 6 e 7, onde foi possível identificar aqueles já alcançados pelo sistema e, da mesma forma, os requisitos que ainda podem ser contemplados por uma Instituição de Ensino Pública. Com isso, esta análise resultou no artefato do “Documento de Requisitos”.

Diante desse contexto, no que se refere ao problema definido para nortear esta pesquisa – Como implementar requisitos de acesso à dados, em conformidade com a LGPD, em bases de dados transacionais de Instituições de Ensino Superior? – este é respondido ao se apresentar um modelo para implementação de requisitos que segue as diretrizes da LGPD e, com base em métodos e processos já utilizados em outras literaturas, demonstra que é possível sua adequação em bases de dados transacionais de uma Instituição de Ensino Superior. O modelo apresentado permite ainda a adequação da instituição em um, ou até mais de um, dos requisitos propostos pela LGPD, dependendo da finalidade do uso do dado analisado.

Além da LGPD, normas e legislações internacionais também sugerem o uso de metodologias e políticas de governança para garantir o adequado tratamento dos dados pessoais, como é o caso da GDPR em seu artigo 40[7]. Assim, conforme Palmeira (2020), tanto na lei brasileira quanto na lei europeia, “as organizações são estimuladas a trabalhar na linha da corregulação, em uma associação entre a legislação e um conjunto de instrumentos capaz de auxiliá-las na aplicação e na eventual comprovação da correta aplicação da Lei” (Palmeira, 2020, p.300).

A segurança dos dados também é um fator que se destacou nesta pesquisa, uma vez que vários riscos foram identificados no tratamento dos

[7] Art. 40,1: “Os Estados-Membros, as autoridades de controle, o Comitê e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.” (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho)

dados. O compartilhamento de dados entre órgãos públicos e mesmo entre a instituição e empresas terceirizadas, quando necessário, reforça a necessidade de uma análise mais reflexiva sobre o tratamento de dados realizado, para sua consequente conformidade com a LGPD, principalmente, no que tange às boas práticas e segurança.

Outro fator importante a se considerar na estrutura para o desenvolvimento da metodologia analisada é a ética no uso dos dados, uma vez que, de acordo com Marcovitcha e Rancourtb (2022), é importante ter um método para que as organizações descrevam, avaliem a qualidade, melhorem continuamente e divulguem suas práticas relacionadas à ética de dados.

Assim sendo, o uso adequado da governança de dados e a conformidade com a LGPD mostraram-se essenciais para assegurar que o acesso a dados pessoais seja realizado de maneira ética, legal e segura. Esses requisitos não apenas protegem os indivíduos, mas também fortalecem a integridade das instituições em um ambiente de dados cada vez mais complexo e interconectado.

Com isso, espera-se que esta pesquisa possa contribuir para a adequação do tratamento de dados no sistema estudado, conforme as indicações levantadas, além de contribuir para os demais sistemas da UDESC como um todo, e ainda servir de modelo para demais instituições públicas de ensino, que também realizam tratamento de dados de seus alunos.

6.1 TRABALHOS FUTUROS

Como proposta para trabalhos futuros, sugere-se que o modelo desenvolvido seja validado em outros sistemas, inclusive em empresas e instituições além do contexto educacional, para que os demais requisitos presentes na LGPD possam ser verificados.

Além disso, esta pesquisa pode evoluir com o uso massivo de dados, ou *big data*, melhorando e adaptando o modelo desenvolvido para trabalhar com sistemas que usam processos automatizados de inteligência artificial no tratamento dos dados.

Outra sugestão para trabalhos futuros seria a validação do modelo com sistemas que já possuem implementação de anonimização ou pseudoanonimização, prevendo se estas implementações estão corretas de acordo com a LGPD e atendem aos requisitos da Lei.

REFERÊNCIAS

ARTESE, Gustavo. Compliance digital e privacidade. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otavio (coord.). **Manual de Compliance**. [*s. l.*]: Grupo GEN, 2021. cap. 24, p. 501-526. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 23 ago. 2022.

BARBIERI, Carlos. **Governança de dados**: práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2020.

BAX, Marcello Peixoto. Design science: filosofia da pesquisa em ciência da informação e tecnologia. **Ciência da Informação**, [*s. l.*], v. 42, n. 2, 2015. Disponível em: http://revista.ibict.br/ciinf/article/view/1388. Acesso em: 16 nov. 2021.

BAX, Marcello Peixoto; BARBOSA, Daniel Mendes. A Design Science como metodologia para a criação de um modelo de Gestão da Informação para o contexto da avaliação de cursos de graduação. **Revista Ibero-Americana De Ciência Da Informação**, [*s. l.*], v. 10, n. 1, 2017. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/2471. Acesso em: 16 nov. 2021.

BERTINO, Elisa; KUNDU, Ahish; SURA, Zehra. Data Transparency with Blockchain and AI Ethics. **Journal of Data and Information Quality**, [*s. l.*], v. 11, n. 16, ed. 4, 2019. Disponível em: https://doi.org/10.1145/3312750. Acesso em: 12 jan. 2023.

BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Thiago Cripa; VENTURINI, Otavio (coord.). **Manual de Compliance**: Da estratégia à Gestão de Processos e Serviços. 3. ed. [*s. l.*]: Grupo GEN, 2021. cap. 26, p. 549-562. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 23 ago. 2022.

BORGES, Maria de Lourdes; DALL'AGNOL, Darlei; DUTRA, Delamar Volpato. **O que você precisa saber sobre Ética**. Rio de Janeiro: DP&A, 2002.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 12-39. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jan. 2023.

BRASIL. Ministério da Gestão e Inovação em Serviços Públicos. Equipe Técnica de Elaboração. **Guia de Boas Práticas**: Lei Geral de Proteção de Dados Pessoais (LGPD). 2.0. [Brasília], 18 ago. 2020. Disponível em:https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf . Acesso em: 18 fev. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 fev. 2021.

BUCKLAND, M. K. Information as thing. **Journal of the American Society for Information Science** (1986-1998), v.42, n. 05, p. 351-360, 1991. Disponível em: https://ppggoc.eci.ufmg.br/downloads/bibliografia/Buckland1991.pdf. Acesso em: 04 jan. 2021.

CANEDO, Fabiolla Labelle Ornelas. Privacidade e ética na Sociedade de Dados: Uma reflexão filosófica sobre a Lei Geral de Proteção de Dados brasileira. **Pontifícia Universidade Católica de São Paulo**, São Paulo, 2021. Disponível em: https://repositorio.pucsp.br/handle/handle/24533. Acesso em: 16 jan. 2023.

CARVALHO, André Carlos Ponce de Leon Ferreira de. Inteligência Artificial: riscos, benefícios e uso responsável. **Estudos Avançados**, São Paulo, 2021. DOI https://doi.org/10.1590/s0103-4014.2021.35101.003. Disponível em: https://www.scielo.br/j/ea/a/ZnKyrcrLVqzhZbXGgXTwDtn/. Acesso em: 14 jan. 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados comentada**. 3. ed. rev. atual. e aum. São Paulo: Thomson Reuters Brasil, 2019.

DAMA-DMBOK: **Data Management Body of Knowledge**. 2. ed. Basking Ridge, New Jersey: Technics Publications, 2017. Disponível em: https://doceru.com/doc/nxcx5nc. Acesso em: 10 ago. de 2022.

DENNEDY, Michelle Finneran; FOX, Jonathan; FINNERAN, Thomas R. Data and Privacy Governance Concepts. *In*: DENNEDY, Michelle Finneran; FOX, Jonathan; FINNERAN, Thomas R. **The Privacy Engineer's Manifesto**: Getting from Policy to Code to QA to Value. 1. ed. [*s. l.*]: Apress Berkeley, CA, 2014. cap. Getting Your Head Around Privacy, p. 51–72. Disponível em: https://doi.org/10.1007/978-1-4302-6356-2_3. Acesso em: 20 jan. 2023.

DIMMOCK, Mark; FISHER, Andrew. **Ethics for A-Level**. [*s. l.*]: Open Book Publishers, 2017. Disponível em: https://doi.org/10.11647/OBP.0125. Acesso em: 12 jan. 2022.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES JÚNIOR, José Antonio Valle. **Design Science Research**: Método de Pesquisa para Avanço da Ciência e Tecnologia. Porto Alegre: Bookman, 2015.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI**: da estratégia à Gestão de Processos e Serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

FERNANDES, Aguinaldo Aragon; DINIZ, Jose Luis; ABREU, Vladimir Ferraz de. **Governança digital 4.0.** Rio de Janeiro: Brasport, 2019.

FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics?. **Philosophical Transactions of the Royal Society A**, [*s. l.*], 2016. Disponível em: https://doi.org/10.1098/rsta.2016.0360. Acesso em: 12 jan. 2023.

FRAJHOF, Isabella Z.; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 62-95. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

FREIRE, Gustavo Henrique de Araújo. **Ética da informação**: conceitos, abordagens, aplicações. João Pessoa: Ideia, 2010. Disponível em: https://lti.pro.br/uploads/posts_files/148/5174bcdc63b1722a7b0a923f3f8fe63f.pdf. Acesso em: 12 out. 2021.

FULLER, R. 1965. World design science decade, 1965-1975. **World Resources Inventory**. Illinois: Southern Illinois University, 1965.

GACUTAN, Joshua; SELVADURAI, Niloufer. A statutory right to explanation for decisions generated using artificial intelligence. **International Journal of Law and Information Technology**, [*s. l.*], v. 28, ed. 3, 2020. Disponível em: https://doi.org/10.1093/ijlit/eaaa016. Acesso em: 9 jan. 2023.

GARBACCIO, Grace Ladeira; VADELL, Lorenzo-Mateo Bujosa; TORCHIA, Bruno. Principais disposições da governança em privacidade à luz da Lei Geral de Proteção de Dados no Brasil. [*s. l.*]: **Revista Justiça Do Direito**, v. 36, n. 1, 2022. DOI https://doi.org/10.5335/rjd.v36i1.13379. Disponível em: http://seer.upf.br/index.php/rjd/article/view/13379. Acesso em: 22 ago. 2022.

GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; GONÇALVES, Rafael Augusto Moreno; PEREIRA-BARRETTO, Marcos Ribeiro. **Lei Geral de Proteção de Dados (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

GHAVAMI, Peter. **Big Data Management**: Data Governance Principles for Big Data Analytics. [*s. l.*]: Walter de Gruyter GmbH & Co KG, 2020.

GIOVANNINI JUNIOR, Josmar Lenine. Fase 4: governança de dados pessoais. *In*: MALDONADO, Viviane Nóbrega. **LGPD**: Lei Geral de Proteção de Dados pessoais: manual de implementação. São Paulo: Thomson Reuters Brasil, 2019. cap. 4, p. 167-188.

GOMES, Maria Cecília Oliveira. **Entre o método e a complexidade**: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (coord.).

Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

GREGORY, S.A. **The design method**. Nova Iorque: Springer Science + Business Media, 1966.

GUAGLIARD, José Augusto; SILVA, Nelson Ricardo Fernandes da; CHAIA FILHO, Alfredo; RAMOS JUNIOR, Lázaro. **Análise de risco parametrizada**: manual prático de gestão de riscos e seguros. São Paulo: All Print Editora, 2016.

HASSELBALCH, Gry. Making sense of data ethics: The powers behind the data ethics debate in European policymaking. **Internet Policy Review**, [*s. l.*], v. 8, n. 2, 2019. Disponível em: https://doi.org/10.14763/2019.2.1401. Acesso em: 12 set. 2022.

HEINRICH, Bernd; HRISTOVA, Diana; KLIER, Mathias; SCHILLER, Alexander; SZUBARTOWICZ, Michael. Requirements for Data Quality Metrics. **Journal of Data and Information Quality**, [*s. l.*], v. 9, ed. 2, 2018. Disponível em: https://doi.org/10.1145/3148238. Acesso em: 24 jan. 2023.

HEVNER, Alan R.; MARCH, Salvatore T.; PARK, Jinsoo; RAM, Sudha. Design Science in Information Systems Research. [*s. l.*]: **Management Information Systems Research Center**, 2004. v. 28, ed. 1. Disponível em: https://doi.org/10.2307/25148625. Acesso em: 16 nov. 2021.

LADLEY, John. **Data Governance**: How to Design, Deploy, and Sustain an Effective Data Governance Program. [s*. l.*]: Academic Press, 2019.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral De Proteção De Dados - Comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. cap. II, p. 179-213.

LOSHIN, David. **The Practitioner's Guide to Data Quality Improvement**. [*s. l.*]: Elsevier, 2010.

MAGRANI, Eduardo. **Entre dados e robôs**: Ética e privacidade na era da hiperconectividade. [s*. l.*]: Arquipélago Editorial, 2019.

MAHANTI, Rupa. **Data Governance and Data Management**: Contextualizing Data Governance Drivers, Technologies, and Tools. [s*. l.*]: Springer Nature, 2021.

MALDONADO, Viviane Nóbrega. Dos Direitos do Titular. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral De Proteção De Dados - Comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. cap. III, p. 215-242.

MANTELEROŸ, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. **Computer Law and Security Review**,

[*s. l.*], v. 34, ed. 4, 2018. Disponível em: https://doi.org/10.1016/j.clsr.2018.05.017. Acesso em: 10 nov. 2022.

MARCH, S.T.; SMITH, G.F. **Design and natural science research on information technology**. [*s. l.*]: Decision Support Systems, 1995. v.15, n.4, p.251-266.

MARCOVITCHA, Inbal; RANCOURTB, Eric. A data ethics framework for responsible responsive organizations in the digital world. **Statistical Journal of the IAOS**, [*s. l.*], v. 38, ed. 4, 2022. Disponível em: https://doi.org/10.3233/SJI-220067. Acesso em: 10 jan. 2023.

MARTIN, Kirsten. **Ethics of Data and Analytics**: Concepts and Cases. New York: CRC Press, 2022. Disponível em: https://doi.org/10.1201/9781003278290. Acesso em: 20 ago. 2022.

MENDES, Anderson. **Governança digital**. São Paulo: Senac, 2022.

MORAES, João Antonio de. **O Paradigma da Complexidade e a Ética Informacional**. Campinas: Coleção CLE, 2019. 85 p. Disponível em: https://www.cle.unicamp.br/ebooks/index.php/publicacoes/catalog/download/7/6/23?inline=1. Acesso em: 12 jan. 2023.

MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

OLIVEIRA, Eliza Ribeiro de; BALDI, Vania; ROSSETTI, Êmili Adami. Questionando a atuação do Regulamento Geral de Proteção de Dados: a ética da privacidade entre controladores e negócios. In: CHRISTOFOLETTI, Rogério (org.). **Privacidad, transparencia y éticas renovadas**. [*s. l.*]: Ediciones Egregius, 2019. cap. II, p. 33-48. Disponível em: https://books.google.com.br/books?id=FEHHDwAAQBAJ. Acesso em: 12 out. 2021.

O'KEEFE, Katherine; O BRIEN, Daragh. **Data Ethics**: Practical Strategies for Implementing Ethical Information Management and Governance. 2. ed. [*s. l.*]: Kogan Page Publishers, 2023.

O'KEEFE, Katherine; O BRIEN, Daragh. **Ethical Data and Information Management**: Concepts, Tools and Methods. [*s. l.*]: Kogan Page Publishers, 2018.

ORMAY, Larissa Santiago. Inteligência artificial e controle social da ct&i: uma relação pertinente à ciência da informação. **XV Encontro Nacional de Pesquisa em Ciência da Informação - ENANCIB 2014**, Belo Horizonte, 2014. Disponível em: http://enancib2014.eci.ufmg.br/documentos/anais/anais-gt5/view. Acesso em: 1 fev. 2022.

PALMEIRA, Mariana de Morais. A segurança e as boas práticas no tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**: Da estratégia à Gestão de Processos e Serviços. Porto Alegre: Arquipélago Editorial, 2020. p. 292-308. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

PEFFERS, Ken; TUUNANEN, Tuure; ROTHENBERGER, Marcus A.; CHATTERJEE, Samir. A design science research methodology for information systems research. **Journal of Management Information Systems**, [*s. l.*], v. 24, ed. 3, 2007. Disponível em: https://www.researchgate.net/publication/284503626. Acesso em: 20 jul. 2023.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**. 3ª Edição. São Paulo: Saraiva Educação S.A., 2021.

PORTO, Renata Maria Abrantes Baracho. **Questões éticas no campo científico da informação**. Portugual: Prisma.com, 2016. n. 32, p. 46-61. Disponível em: http://hdl.handle.net/20.500.11959/brapci/61420. Acesso em: 24 nov. 2021.

PREISIG, Amélie Vallotton; RÖSCH, Hermann; STÜCKELBERGER, Christoph. Ethical Dilemmas in the Information Society: how codes of ethics help to find ethical solutions. In: PREISIG, Amélie Vallotton; RÖSCH, Hermann; STÜCKELBERGER, Christoph. **Ethical Dilemmas in the Information Society**: Codes of Ethics for Librarians and Archivists. Geneva: Globethics.net, 2014. cap. 1, p. 11-18. Disponível em: https://www.researchgate.net/profile/Rachel-Spacey/publication/283485452_Filtering_Access_to_the_Internet_in_Public_Libraries_an_Ethical_Dilemma/links/5639e97208ae4624b7608194/Filtering-Access-to-the-Internet-in-Public-Libraries-an-Ethical-Dilemma.pdf. Acesso em: 18 ago. 2022.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico - 2. ed. Novo Hamburgo: FEEVALE, 2013.

RAAB, Charles D. Information privacy, impact assessment, and the place of ethics. **Computer Law & Security Review**, [*s. l.*], v. 37, 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105404. Acesso em: 4 jan. 2023.

REDMAN, Thomas C. **Getting in Front on Data**: Who Does What. [*s. l.*]: Technics Publications, 2016.

RÊGO, Bergson Lopes. **Simplificando a governança de dados**: governe os dados de forma objetiva e inovadora. Rio de Janeiro: Brasport, 2020.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504. Acesso em: 27 jan. 2023.

REYNOLDS, George. **Ethics in Information Technology**. [*s. l.*]: Cengage Learning, 2014.

ROBSON, Gregory; TSOU, Jonathan Y. Technology Ethics: A Philosophical Introduction and Readings. **Routledge**, New York, NY, USA, 2023. Disponível em: https://philarchive.org/rec/ROBTEA-16. Acesso em: 10 jan. 2023.

RODRIGUES, Diogo Duarte. Design Science Research como caminho metodológico para disciplinas e projetos de Design da Informação. **Infodesign**, [*s. l.*], v. 15, n. 1, 2018. Disponível em: https://infodesign.emnuvens.com.br/infodesign/article/view/564. Acesso em: 16 nov. 2021.

SEINER, Robert S. **Non-Invasive Data Governance**: The Path of Least Resistance and Greatest Success. [*s. l.*]: Technics Publications, 2014.

SEMELER, Alexandre Ribas; PINTO, Adilson Luiz. Os diferentes conceitos de dados de pesquisa na abordagem da biblioteconomia de dados. **Ciência da Informação**, Brasília, v. 48, n. 1, 2019. Disponível em: https://revista.ibict.br/ciinf/article/view/4461. Acesso em: 7 jun. 2022.

SERPRO, Serviço Federal de Processamento de Dados. **Objetivo e abrangência da LGPD**. [*s. l.*], 2019. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/linha-do-tempo/view. Acesso em: 18 fev. 2021.

SHINTAKU, Milton; SOUSA, Rosilene Paiva Marinho de; COSTA, Lucas Rodrigues; MOURA, Rebeca dos Santos de; MACEDO, Diego José. Discussões sobre política de privacidade de dados em um sistema de informação governamental. **Em Questão**, [*s. l.*], v. 27, n. 4, p. 39-60, 2021. Disponível em: https://www.redalyc.org/journal/4656/465668631003/html/. Acesso em: 22 ago. 2022.

SILVA, Priscilla Regina. Os direitos dos titulares dos dados. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 182-202. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

SIMON, H. **The sciences of artificial**. Cambridge: MIT Press, 1996.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 40-61. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

STAHL, Bernd Carsten. **Artificial Intelligence for a Better Future**: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies.

[*s. l.*]: Springer Cham, 2021. Disponível em: https://doi.org/10.1007/978-3-030-69978-9. Acesso em: 7 out. 2022.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: comentada artigo por artigo. 4. ed. [*s. l.*]: Saraiva, 2022. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 14 mar. 2023.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters, 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. cap. 10, p. 281-318.

TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do Poder Público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 213-541. Disponível em: https://play.google.com/store/books/details?id=IDjnDwAAQBAJ. Acesso em: 10 maio 2022.

TSOU, Jonathan Y.; WALSH, Kate Padgett. Ethical Theory and Technology. In: ROBSON, Gregory J.; TSOU, Jonathan Y. **Technology Ethics**: A Philosophical Introduction and Readings. New York: Routledge, 2023. p. 62-72. Disponível em: https://philarchive.org/rec/TSOETA. Acesso em: 10 jan. 2023.

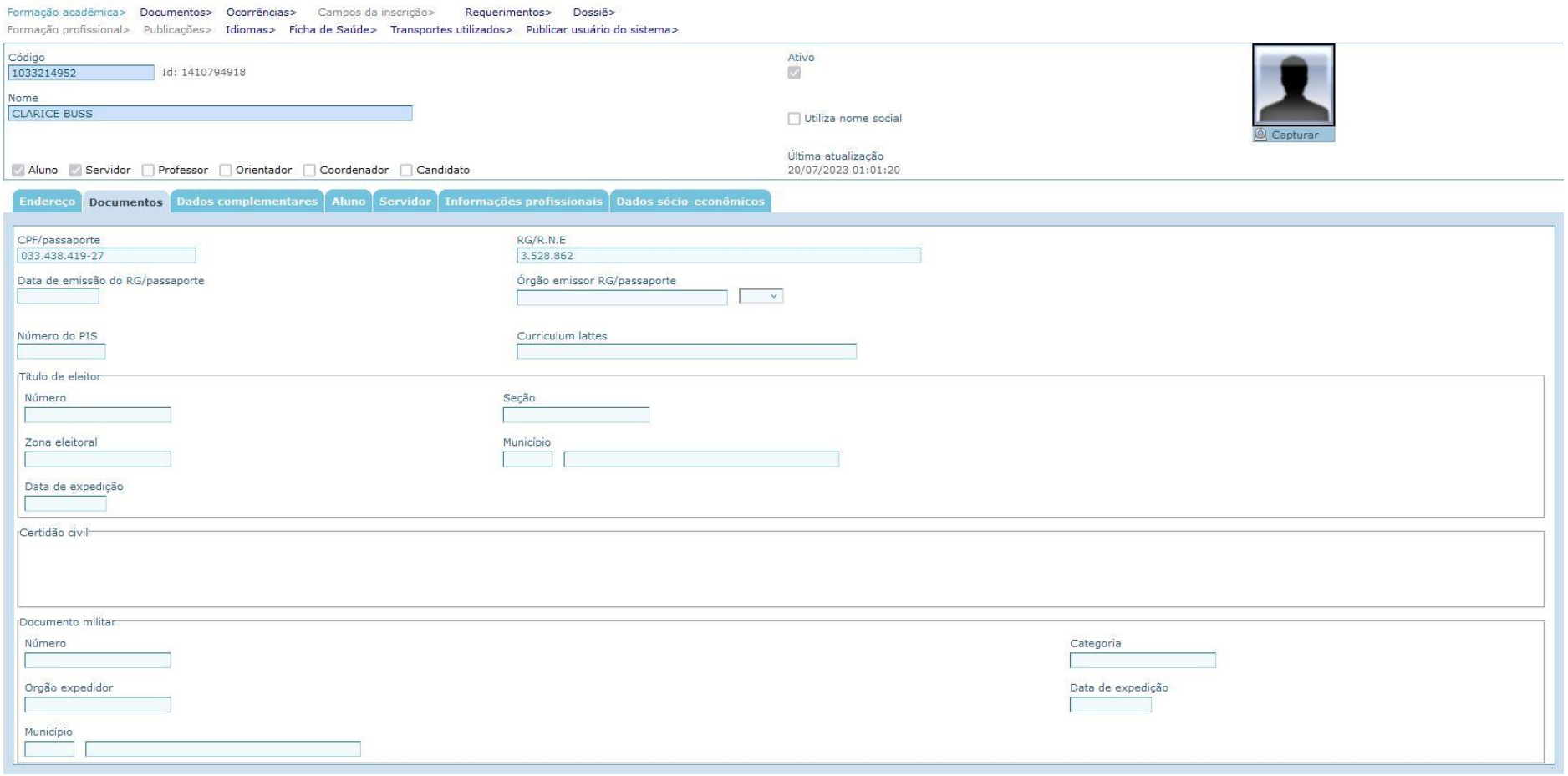
TURBAN, Efraim; SHARDA, Ramesh; E. ARONSON, Jay; KING, David. **Business Intelligence**: um enfoque gerencial para a inteligência do negócio. Porto Alegre: BookMan, 2009.

VAINZOF, Rony. Disposições Preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral De Proteção De Dados - Comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. cap. I, p. 19-135.

VAN DIJK, Niels; CASIRAGHI, Simone; GUTWIRTH, Serge. The ‘Ethification’ of ICT Governance. Artificial Intelligence and Data Protection in the European Union. **Computer Law & Security Review**, [*s. l.*], v. 43, 2021. Disponível em: https://doi.org/10.1016/j.clsr.2021.105597. Acesso em: 12 jan. 2023.

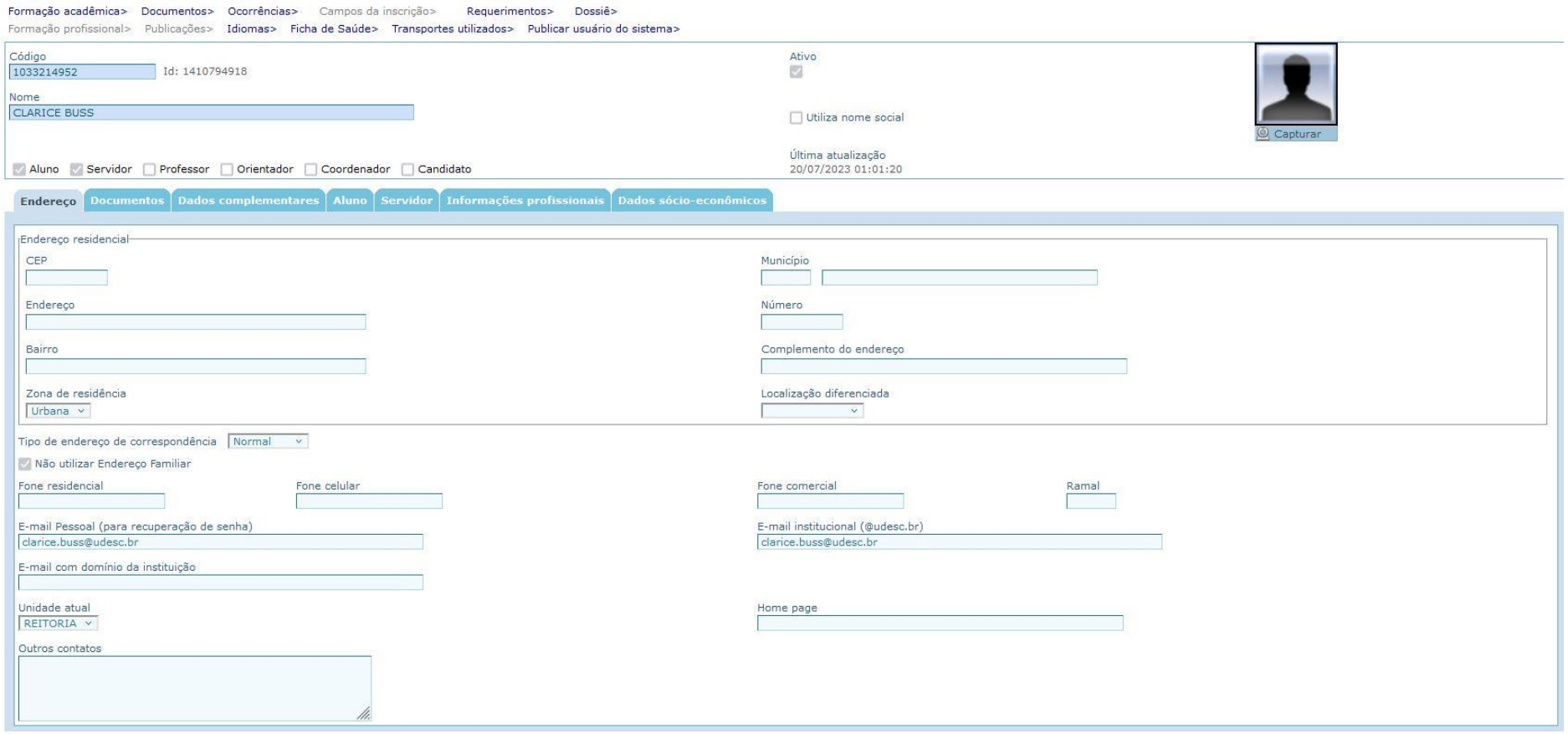
WIERINGA, Roel. Design science as nested problem solving. New York: **ACM**, 2009. Disponível em: https://dl.acm.org/doi/10.1145/1555619.1555630. Acesso em: 16 nov. 2021.

ANEXO A – INTERFACE DO SISTEMA COM OS DADOS DE DOCUMENTOS



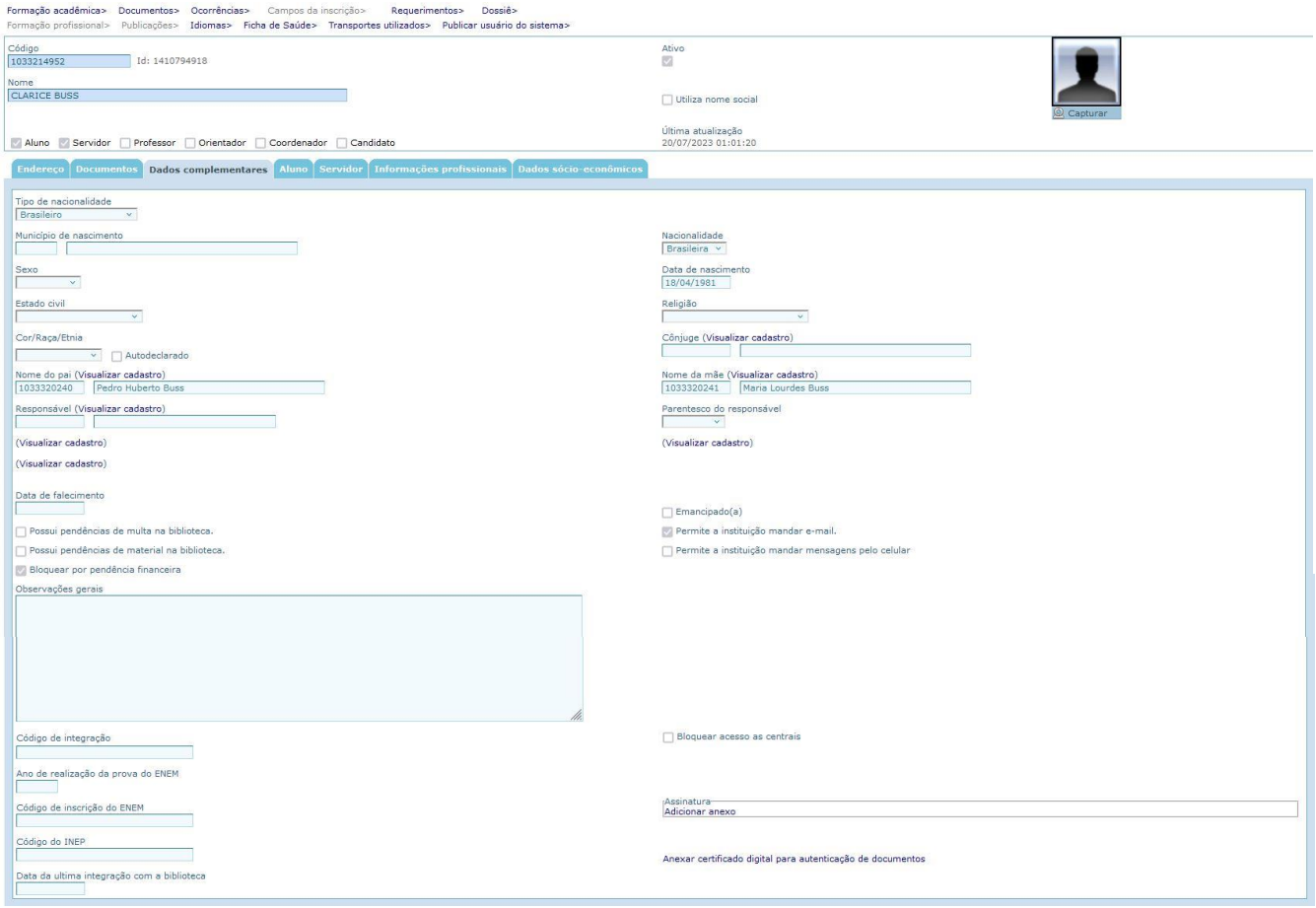
Fonte: Sistema SIGA (2023)

ANEXO B – INTERFACE DO SISTEMA COM OS DADOS DE ENDEREÇO



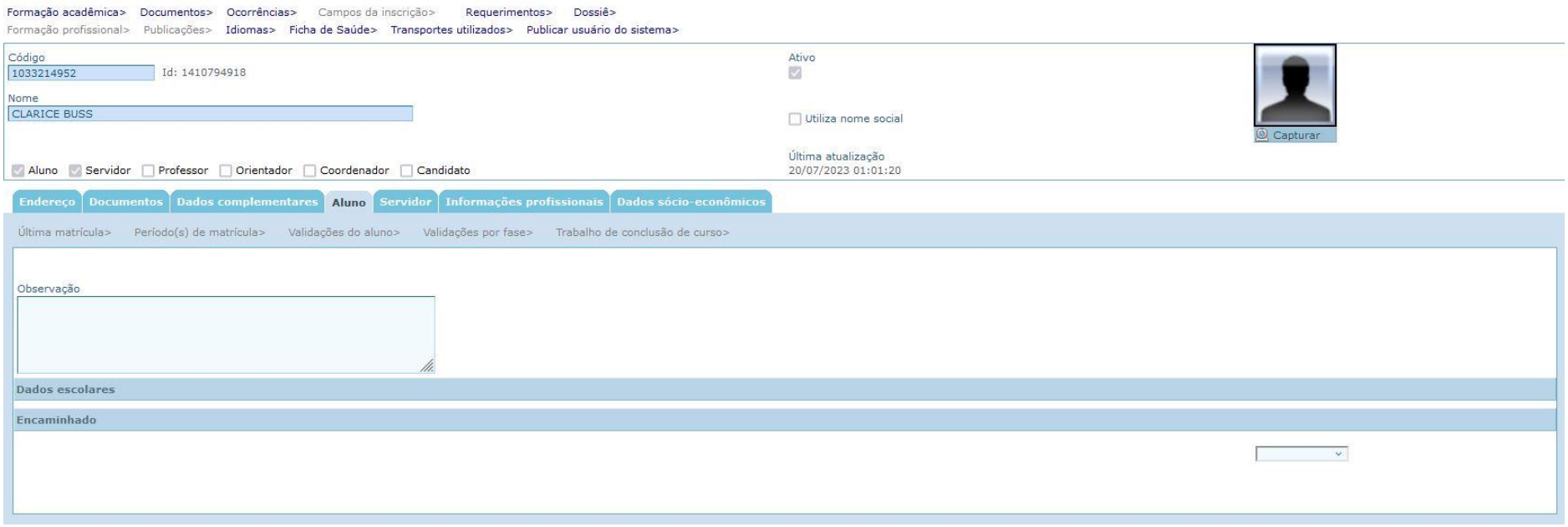
Fonte: Sistema SIGA (2023)

ANEXO C – INTERFACE DO SISTEMA COM OS DADOS COMPLEMENTARES



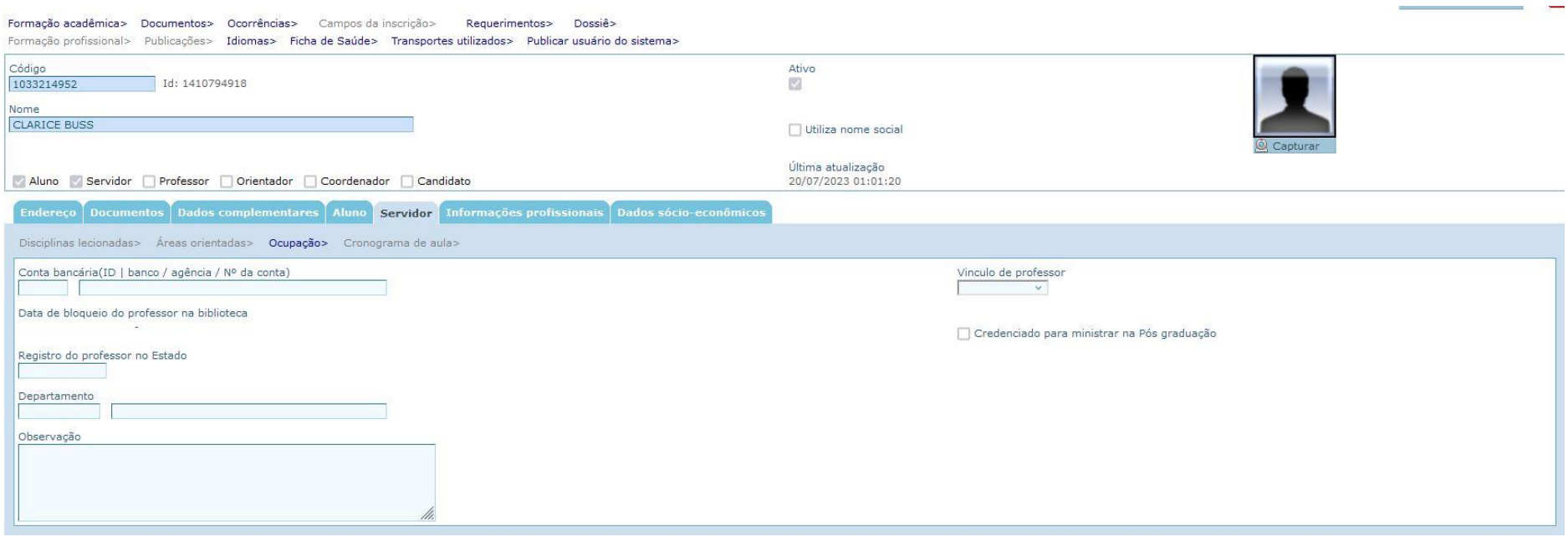
Fonte: Sistema SIGA (2023)

ANEXO D – INTERFACE DO SISTEMA COM OS DADOS DE ALUNO



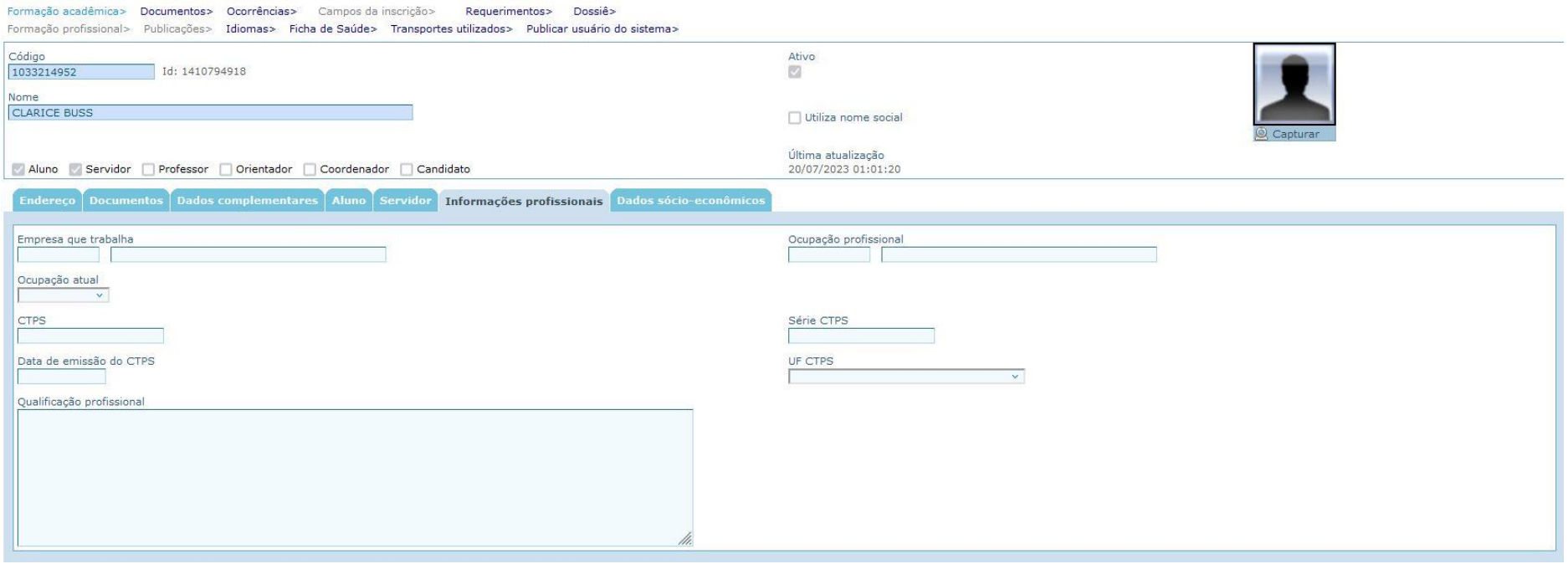
Fonte: Sistema SIGA (2023)

ANEXO E – INTERFACE DO SISTEMA COM OS DADOS DE SERVIDOR



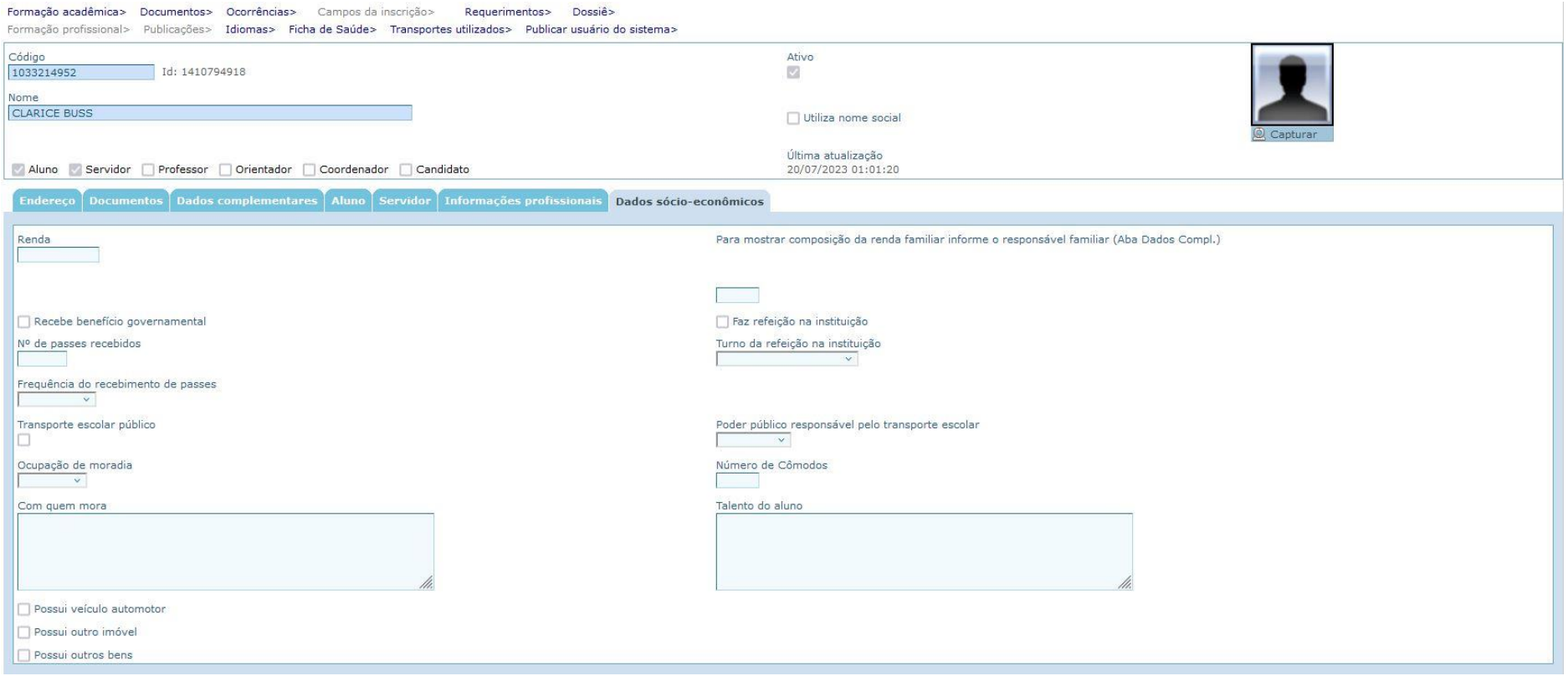
Fonte: Sistema SIGA (2023)

ANEXO F – INTERFACE DO SISTEMA COM OS DADOS DE INFORMAÇÕES PROFISSIONAIS



Fonte: Sistema SIGA (2023)

ANEXO G – INTERFACE DO SISTEMA COM OS DADOS SOCIOECONÔMICOS



Fonte: Sistema SIGA (2023)