

# A ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES DE ENSINO SUPERIOR: UM ESTUDO MULTICASOS

William Machado Botelho Arabi  
 <http://lattes.cnpq.br/588222020780576> –  <https://orcid.org/0009-0007-7054-5240>  
[wiliamarabi@gmail.com](mailto:wiliamarabi@gmail.com)  
Universidade FUMEC  
Belo Horizonte, Minhas Gerais, Brasil

Adriane Maria Arantes de Carvalho  
 <http://lattes.cnpq.br/7121724013827539> –  <https://orcid.org/0000-0001-6754-8116>  
[adriane.arantescarvalho@gmail.com](mailto:adriane.arantescarvalho@gmail.com)  
Universidade FUMEC  
Belo Horizonte, Minhas Gerais, Brasil

## RESUMO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), definiu uma série de exigências para o tratamento de dados pessoais. A pesquisa investigou as iniciativas de duas instituições de ensino superior, privadas e sem fins lucrativos, a Universidade FUMEC e a Pontifícia Universidade Católica de Minas Gerais, sediadas em Belo Horizonte (Minas Gerais, Brasil), para se adequarem à LGPD. Especificamente analisou o emprego de normas ou frameworks de governança de tecnologia da informação e de governança de dados, e os resultados obtidos. A pesquisa é exploratória e descritiva, com abordagem qualitativa. Para o estudo multicasos, além da pesquisa documental, foram realizadas entrevistas semiestruturadas com os responsáveis pela proteção de dados (Data Protection Officer – DPO) e pela gerência de tecnologia da informação. Constatou-se o uso do framework ITIL que, mesmo aplicado de forma restrita, forneceu processo e uma base de conhecimento sólida para as operações da governança de tecnologia da informação. A governança de dados ainda é pouco utilizada, apontando a necessidade da sua implementação para melhor gestão do volume informacional. É consenso entre os DPOs que a adequação da LGPD é um processo contínuo e requer atualizações e melhorias.

**Palavras-chave:** Proteção de dados. Direito à privacidade. Universidades. Governança de dados. Governança de tecnologia da informação.

## COMPLIANCE WITH THE GENERAL LAW ON PERSONAL DATA PROTECTION IN HIGHER EDUCATION: A MULTI-CASE STUDY

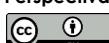
## ABSTRACT

The Law No. 13,709/2018, known as the General Data Protection Law (LGPD), defines a series of requirements for the processing of personal data. The research investigates the initiatives of two private, non-profit higher education institutions, Universidade FUMEC and Pontifícia Universidade Católica de Minas Gerais, based in Belo Horizonte (Minas Gerais, Brazil), to adapt to the LGPD. Specifically, it analyzes the use of information technology governance and data governance standards or frameworks, and the results obtained. The research is exploratory and descriptive, with a qualitative approach. For the multi-case study, in addition to documentary research, semi-structured interviews were carried out with the Data Protection Officer (DPO) and the Information Technology Manager. The ITIL framework was found to be used, but even when applied in a limited way, it provided a solid process and knowledge base for information technology governance operations. Data governance is still little used, pointing to the need to implement it in order to better manage the volume of information. There is consensus among the DPOs that compliance with the LGPD is an ongoing process and requires updates and improvements.

**Keywords:** Data protection. Right to privacy. Universities. Data governance. Information technology governance.

DOI <http://dx.doi.org/10.1590/1981-5344/54013>

Recebido em: 28/08/2024  
Aceito em: 06/10/2025





## 1 INTRODUÇÃO

Em 2018 ocorreu a promulgação da lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), a qual estabeleceu normas para que dados e informações pessoais sejam tratados, armazenados, utilizados e excluídos pelas organizações (Brasil, 2018). Stelzer et al. (2023) destacam que a LGPD trouxe fundamentos da proteção de dados pessoais, dispendo sobre direitos e garantias do titular de dados pessoais e teve como objetivo regulamentar o seu tratamento.

De acordo com os indicadores e dados estatísticos do Censo da Educação Superior de 2021, é evidente o aumento na oferta de cursos de graduação e pós-graduação, nas modalidades presencial e a distância no Brasil (INEP, 2021). A gestão informacional bem como a adequação à LGPD tornou-se uma prioridade para as Instituições de Ensino Superior (IES). A adequação à LGPD é um desafio dada a quantidade e abrangência de sistemas de informação e o volume e granularidade de dados (Luna, 2020), fomentando uma nova realidade para as IES que, até então, agiam com discricionariedade e poucas restrições normativas, mesmo com a proteção prevista na Constituição Federal de 1988 (Stelzer et al., 2023).

Destaca-se também a necessidade de uma sólida e ágil estrutura de Tecnologia da Informação (TI) que suporte a crescente oferta e que mantenha os sistemas de informação adequados (*compliance*) às exigências do arcabouço jurídico (Silva, 2020). A governança da TI utiliza modelos e padrões para controle e gestão dos dados e ativos organizacionais e fornece suporte aos processos organizacionais (Wu; Straub; Liang, 2015). Desta maneira, possibilita a utilização e integração de um cabedal de recursos que, devidamente implementados, mantidos e controlados no ecossistema informacional, permitem ganho de performance e segurança nas operações físicas e lógicas das informações utilizadas e mantidas pelas organizações, facilitam o gerenciamento de riscos e contribuem para atingir melhor desempenho na gestão e administração corporativa (Barata, 2015; Lunardi, 2008). De acordo com Gonçalves, Gaspar e Cardoso (2016), 99,1% das empresas declararam a dependência de seus negócios em relação à TI e quanto maior essa dependência, maior será o nível de maturidade da governança de TI na empresa.



Para o Instituto Brasileiro de Governança Corporativa (IBGC), a governança corporativa é como um sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (IBGC, 2019). A utilização de modelos de governança de TI e de governança de dados, alinhados aos requisitos da governança corporativa e da LGPD, pode oferecer às IES um ambiente seguro para o tratamento e uso dos dados pessoais e sensíveis.

A LGPD exige controles complexos para a sua efetiva utilização. Sua implementação requer uma adequação corporativa em diversos níveis organizacionais, seja em sistemas de informação, seja em processos de gestão administrativa e, ou, jurídicos, e até mesmo em processos operacionais e adjacentes estabelecidos. Pelo fato de manipularem alto volume de dados, relacionados à prestação de seus serviços educacionais (aulas presenciais, remotas, cursos avulsos, palestras e eventos), as IES necessitam de um alto grau de controle informacional.

Assim é importante esclarecer como as IES têm enfrentado o desafio de se adequarem à LGPD. De acordo com Souza, Belda e Arima (2022), nas IES existe a necessidade de implementação de um programa de privacidade de dados que vá ao encontro do plano institucional, de forma transparente, com controles técnicos, treinamentos e conscientizações. Nessa linha, Burkart (2021) afirma que o principal impacto da LGPD é a mudança de paradigma, trazendo a proatividade e a conscientização das organizações para respeitar os dados de clientes, fornecedores e parceiros.

Desta maneira, o objetivo geral da pesquisa é investigar quais foram as iniciativas utilizadas por duas IES, privadas e sem fins lucrativos, a Fundação Mineira de Educação e Cultura (Universidade FUMEC) e a Pontifícia Universidade Católica de Minas Gerais (PUC Minas), sediadas em Belo Horizonte (Minas Gerais), para se adequarem aos requisitos da Lei 13.709/2018 – LGPD (Brasil, 2018). São objetivos específicos: 1) mapear como foi o processo de adequação e adoção da LGPD nas IES; 2) identificar quais normas e, ou, frameworks de governança de TI e de governança de dados foram utilizados pelas IES; e, finalmente, 3) verificar quais os principais desafios encontrados na

adequação e no uso da LGPD, segundo os responsáveis institucionais por essa adequação.

O tripé IES, LGPD e governança de TI tem uma relação importante com a Ciência da Informação e a Arquivologia, pois remete a um exercício de gestão e curadoria de dados que dialoga diretamente com os fundamentos destas áreas (Conselho Nacional de Arquivos, 2022). Entende-se que a aplicação efetiva da governança de TI e da governança de dados envolve os profissionais de informação para os quais a mediação da informação perpassa e orienta a prática profissional (Almeida Júnior, 2008).

O exercício ético da profissão demanda o conhecimento tanto dos aspectos legais associados ao manuseio e tratamento de dados pessoais, dentro os quais inclui-se a LGPD, quanto dos complexos dilemas relacionados ao acesso, sigilo e privacidade da informação (Bagatini; Guimarães; Santana, 2021; Brandão *et al.*, 2025; Coelho; Carvalho, 2025; Vignoli *et al.*, 2020). Desse modo, os profissionais da informação deparam-se com conflitos diários ao tentar equilibrar o acesso público a informações dos acervos com as exigências de privacidade da LGPD (Rockembach, 2020). Este dilema se manifesta também na gestão de dados pessoais sensíveis durante empréstimos, na mediação informacional em ambientes acadêmicos e na disseminação seletiva de informações em bibliotecas (Lemos; Passos, 2020; Souza Neto; Carvalho, 2020).

A análise dos frameworks de governança de TI e de governança de dados demonstra que a conformidade legal exige não apenas soluções técnicas, mas também políticas institucionais estabelecidas e processos informacionais que respeitem a privacidade sem comprometer o acesso e a transparência (Brasil, 2018; Zanon, 2022). Nesse sentido, a Arquivologia é chamada a oferecer metodologias de organização, classificação e preservação documental em sintonia com as exigências da LGPD, enquanto a Ciência da Informação fornece fundamentos para compreender a informação como recurso estratégico nas IES (Almeida; Soares, 2022). A integração entre LGPD, governança de TI e práticas arquivísticas reforça a necessidade de um profissional da informação crítico, capaz de transitar entre a legislação, a tecnologia e a gestão informacional no âmbito universitário (Pereira Júnior; Stakoviak Júnior, 2022).



## 2 REFERENCIAL TEÓRICO

A privacidade da pessoa humana é garantida no artigo 5º, inciso X, da Constituição Federal brasileira (Brasil, 1988) e abordada também em algumas leis complementares (Código Civil, Estatuto da Criança e do Adolescente, Lei de Acesso à Informação<sup>1</sup> e Marco Civil da Internet<sup>2</sup>), integrantes do ordenamento jurídico brasileiro. A privacidade é um direito personalíssimo do indivíduo de autodeterminar suas informações pessoais. A constituição brasileira protege a “intimidade” e a “vida privada” expressamente. Logo, visto que os dados pessoais privados são pertinentes à vida privada do sujeito e à sua intimidade, as informações correspondentes também devem ser protegidas e resguardadas. A LGPD deixou claro que a privacidade de dados pessoais deve ser assegurada ao cidadão (Brasil, 2018).

### 2.1 A Lei Geral de Proteção de Dados – Lei nº 13.709

A LGPD mudou a forma como as informações devem ser tratadas pelas organizações. Constrói-se, com ela, um novo paradigma na forma de tratamento da privacidade dos dados pessoais, independente do porte das organizações (Queiroz, 2021). Os requisitos necessários para a sua implementação são, principalmente: tratamento de dados pessoais, política de segurança da informação, política de proteção de dados pessoais, Relatório de Impacto à Proteção de Dados Pessoais (RIPD), política de privacidade, sistema de gestão de incidentes, controle de acesso em sistemas e utilização de criptografia (Brasil, 2018).

O dado pessoal é uma informação pertinente à pessoa natural identificada ou identificável e é fundamental identificar quais são os dados pessoais e quais devem ser anonimizados, para que seja possível realizar, de forma clara, a manutenção do registro das demais operações de tratamento de dados (Brasil, 2018). A política de segurança da informação é um dos principais elementos que compõem e asseguram que os dados corporativos, pertinentes aos indivíduos, estejam resguardados e até mesmo protegidos.

---

<sup>1</sup> A Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI) - tem como principal objetivo garantir o direito fundamental de acesso à informação pública (Brasil, 2011).

<sup>2</sup> A Lei nº 12.965/2014 – Marco Civil da Internet (MCI) – institui princípios e garantias, direitos e deveres para usuários e provedores de conteúdo e serviço de internet, e demais agentes envolvidos, isto é, estabelece princípios para a utilização e o desenvolvimento da Internet no Brasil (Brasil, 2014).

(ABNT, 2019). A política de proteção de dados pessoais deve estar em conformidade com a política de segurança da informação. Esta deve estar alinhada com o item 6.2.1.1 da norma NBR 27701 (ABNT, 2019) que fornece uma estrutura para gerenciamento de privacidade de dados, de forma que haja uniformidade e conformidade entre elas (ABNT, 2019). Mas devem existir outras políticas complementares que permeiem todo o ecossistema de informação das IES.

As IES devem entender e disseminar cada uma das políticas corporativas, bem como as suas finalidades. É comum que ocorra certa confusão entre a política de proteção de dados pessoais organizacional (direcionada ao público interno) e a política de privacidade organizacional, direcionada ao público externo (Fornasier; Knebel, 2021). Os itens 7.3.2 e 7.3.3 da NBR 27701(ABNT, 2019) sugerem que a organização estabeleça, documente e apresente aos titulares dos dados pessoais, de forma clara e facilmente acessível, informações que identifiquem o controlador de dados pessoais e que descrevam o tratamento destes dados. Outro requerimento é que a informação a ser fornecida seja feita em tempo hábil e de forma concisa, completa, transparente, inteligível e de fácil acesso, usando uma linguagem curta e clara, apropriada ao destinatário da mensagem (ABNT, 2019).

Para otimizar a gestão de incidentes, deve haver um sistema de informação que permita o registro dos incidentes de segurança da informação que envolvam violação de dados pessoais, assim como meios para registrar as ações adotadas para sua resolução (via RIPD). Os dados anonimizados, dados pessoais tratados e local de armazenamento são requerimentos relevantes e merecem especial atenção das IES (ABNT, 2019). O item 6.13.1.1 da NBR 27701destaca que devem ser estabelecidas responsabilidades e procedimentos para identificação, registro e tratamento de violações de dados pessoais (ABNT, 2019; Brasil, 2020).

O art. 48, § 3º, da LGPD, estabeleceu a utilização de sistemas de informação criptográficos, pois é uma medida técnica utilizada para tornar ininteligíveis os dados pessoais afetados em caso de incidente de segurança, o que impede que terceiros, não autorizados, consigam acessá-los (Brasil, 2018).



## 2.2 A adequação à LGPD nas IES

Para a adequação à LGPD nas IES, todo um arcabouço de processos, procedimentos, soluções tecnológicas e recursos (humanos, financeiros e administrativos) devem ser utilizados. Cabe, inicialmente, criar um plano de gestão, o qual perpassa por várias áreas de conhecimento (comunicação, qualidade, financeira e outras). A chance de êxito na adequação aumenta na medida em que as IES possuam bases de dados organizadas e gerenciáveis, e em conformidade com a legislação. Logo, o tratamento de dados pessoais nas IES deve anteceder à adequação da LGPD (Stelzer *et al.*, 2023).

De acordo com Silva (2020), as IES obtêm, de seus contratantes e alunos, dados pessoais sensíveis e não necessariamente imprescindíveis ao ato contratual (p. ex.: origem étnica/racial; crenças religiosas, dentre outros). Estes dados podem rotular ou tornar o aluno identificável. Tais dados, portanto, devem ser exclusivamente direcionados ao aluno e, ou, aos seus responsáveis legais (Silva, 2020). Neste contexto, “os processos e sistemas institucionais, bem como a cultura institucional de tratamento de dados pessoais precisarão ser revistos e adequados conforme o preconizado pela legislação em pauta” (Barbosa *et al.*, 2021, p. 6).

As organizações brasileiras podem utilizar ferramentas “como o mapa de dados pessoais e a avaliação de impacto sobre a proteção de dados, para mapear o fluxo de dados organizacionais” e verificar possíveis ajustes ou adequações que se farão necessários para a implementação da lei (Burkart, 2021, p. 85). Burkart (2021) reforça que o tratamento dos dados pessoais deve estar sujeito à compliance e os processos devem ser aderentes às normativas da LGPD.

Para Pereira Júnior e Stakoviak Júnior (2022) as IES devem realizar uma análise da conformidade de dados. Como atuam em diversas áreas além do ensino, tais como a pesquisa, a extensão e a consultoria técnica, “pode ser conveniente tratar, separadamente, o processo de adequação em cada uma dessas diferentes áreas” utilizando-se da criação de categorias de dados e informações para sanar eventuais problemas (Gomes; Cunha Filho; Luccas, 2023, p. 407). Logo, as IES devem possuir um arcabouço de soluções tecnológicas e procedimentais compatíveis com a LGPD, ou seja, “bancos de

dados e arquivos exigem políticas e documentos para proteção, preservação e arquivamento" (Pereira Júnior; Stakoviak Júnior, 2022, p.178).

Queiroz (2021) apresenta algumas dificuldades práticas enfrentadas pelos Encarregados da Proteção de Dados pessoais (*Data Protection Officer - DPOs*) em exercício no Brasil, dentre as quais destacam-se a: dificuldade relacionada aos conhecimentos específicos necessários para o exercício da função de DPO bem como o acúmulo com outras funções designadas ao profissional.

Silva (2020) traçou uma trajetória de adequação à LGPD nas IES que pesquisou, a qual compreende três etapas: planejamento e avaliação, execução e auditoria. Em geral, as IES estabeleceram um comitê de estudos prévio, para realização do planejamento e avaliação do projeto e definição de planos de ação. Na fase de execução, houve a gestão de processos requeridos pela LGPD (gestão da privacidade) com envolvimento dos setores Jurídico, TI, Alta Direção, e outros e, em seguida, estabeleceram um programa de implantação e de treinamento para os envolvidos. Por fim, após a implantação, o projeto é continuamente avaliado por meio de auditorias internas.

### **2.3 Governança de Tecnologia da Informação e Governança de Dados**

É necessário que as IES se adequem a aspectos de gestão, de processos, de pessoas e tecnológicos, sendo que este último se configura um alicerce (Gomes; Cunha Filho; Luccas, 2023). Mas, os processos de governança são essenciais pois amparam os processos organizacionais, atribuindo-lhes padrões e rigor.

A governança de TI refere-se a uma relação estruturada de um conjunto de diretrizes, responsabilidades, competências e habilidades, compartilhadas e assumidas dentro das organizações por executivos, gestores, técnicos e usuários de TI, com o objetivo de controlar os processos, garantir a segurança das informações, otimizar a aplicação de recursos e dar suporte para a tomada de decisões, de forma alinhada com a missão, visão e metas estratégicas das organizações (ITGI, 2007). Ela tem como principal objetivo estabelecer o vínculo entre as organizações e a TI, auxiliando na tomada de melhores decisões pelos gestores (Albertin; Albertin, 2010; Fernandes; Abreu, 2014). Para o seu funcionamento, tanto a estratégia de TI quanto a de negócios devem estar



alinhadas e sincronizadas, facilitando que as organizações atinjam seus objetivos de negócio (ITGI, 2007). Para Queiroz (2021, p. 99):

Quanto à proteção dos dados pessoais, mostrou-se que o avanço da tecnologia potencializa o tratamento dos dados pessoais, em especial com o uso da inteligência artificial. Com isso, atualmente, há muito maior exposição do indivíduo, e o tratamento dos dados pessoais, quando realizado de modo indiscriminado, pode culminar no prejuízo do livre desenvolvimento da personalidade. Assim, indispensável se faz a legislação da proteção dos dados pessoais.

A governança de TI possui diversos frameworks e normas. As normas são publicadas por organismos nacionais e internacionais e são padrões definidos por entidades (normalmente) reconhecidas pelos Governos. Os frameworks são modelos definidos por empresas privadas e largamente utilizados no mercado corporativo (são práticas usuais e consolidadas pelo mercado corporativo).

A norma NBR 27701/2019 – Sistema de Gestão da Privacidade da Informação – especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI), na forma de uma extensão das normas série NBR 27000: NBR 27001 e NBR 27002 (ABNT, 2018, 2022<sup>a</sup>, 2022b). A norma NBR 27701/2019 especifica as boas práticas, além de fornecer diretrizes e requisitos para que os controladores e operadores de dados pessoais<sup>3</sup> possam assumir responsabilidade direta pelo seu tratamento.

O framework *Control Objectives for Information and Related Technologies* (COBIT) foi criado, em 1994, pelo *Information System Audit and Control Association* (ISACA), uma organização independente e sem fins lucrativos, com o propósito específico de fornecer boas práticas de controle de TI, bem como otimizar os investimentos nessa área, além de propiciar a entrega de serviços conforme planejado. Em síntese, é um modelo corporativo de boas práticas para governança e gestão de TI facilitando o seu alinhamento aos objetivos organizacionais (ISACA, 2019). O framework COBIT 2019 possui seis princípios: fornecer valor às partes interessadas, a adoção de uma abordagem holística, um sistema dinâmico de governança, o uso de abordagens distintas para governança e gerenciamento, a adaptação às necessidades corporativas e um sistema de governança de ponta a ponta. O seu diferencial reside na

<sup>3</sup> O termo *Personally Identifiable Information* (PII), expresso no guia DAMA-DMBOK2 (Dama International, 2015), foi traduzido para a expressão dados pessoais (DP) que é de uso corrente e, no Brasil, e sua adoção foi feita pela LGPD.

adaptação (customização) da solução junto à organização, bem como na utilização em conjunto com a governança corporativa (ISACA, 2019).

A Biblioteca de Infraestrutura de Tecnologia da Informação (*Information Technology Infrastructure Library* – ITIL) foi criada pelo Governo do Reino Unido (Axelos, 2019). A versão quatro do ITIL reúne as melhores práticas de Gestão de Serviços de TI por meio de um conjunto de procedimentos documentados, padronizados e organizados, possibilitando otimizar estes serviços para criar valor para as organizações e impulsionar a estratégia de negócios (Axelos, 2019).

A governança de dados é um conceito em evolução que envolve o cruzamento de várias disciplinas, com foco central em qualidade de dados (Barbieri, 2020). De acordo com o autor, a governança de dados retrata a busca de maturidade da empresa em: gerência de 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. O modelo de referência é o DAMA-DMBOK2 (Dama International, 2015), um guia de referência no mercado nacional e internacional, que define a gestão de dados como:

O gerenciamento de dados é um processo complexo. Os dados são gerenciados em diferentes lugares dentro uma organização, por equipes que têm responsabilidade por diferentes fases dos dados vida útil. O gerenciamento de dados requer habilidades de design para planejar sistemas e altas habilidades técnicas para administrar hardware e construir software, habilidades de análise de dados para entender questões e problemas, habilidades analíticas para interpretar dados, habilidades de linguagem para trazer consenso para definições e modelos, bem como pensamento estratégico para servir os clientes e cumprir metas (Dama International, 2015).

O guia DAMA-DMBOK2 propõe uma divisão bidimensional da governança de dados em visão regulatória e executiva, a serem desempenhadas, respectivamente, pelo diretor de dados (função estratégica) e pelo diretor de informações (função executiva) (Dama International, 2015). Se, por um lado, a governança corporativa possui uma visão ampla da estratégia da empresa, por outro lado a governança de dados procura “assegurar que os controles de gerenciamento formal – processos, sistemas e



pessoas responsáveis pela custódia dos dados, estejam implementados de forma a governar os ativos de dados e a aprimorar a qualidade dos dados" (Assis, 2011, p. 81).

### 3 PROCEDIMENTOS METODOLÓGICOS

Este trabalho é resultante de uma pesquisa de mestrado que pode ser caracterizada como exploratória e descritiva. Segundo Pozzebon e Freitas (1998), os estudos exploratórios permitem ao investigador aumentar sua experiência em torno de determinado problema. Por sua vez, uma pesquisa descritiva descreve os fatos e fenômenos de uma determinada realidade (Triviños, 1987). Adotou-se uma abordagem qualitativa por permitir uma investigação mais próxima da realidade das organizações (validação do *status quo*).

O método escolhido foi o de estudo de casos múltiplos, que permite "lidar com uma ampla variedade de evidências – documentos, artefatos, entrevistas e observações" (Yin, 2009, p. 101). A unidade de análise adotada foi a organizacional. Especificamente foram escolhidas duas universidades mineiras, sem fins lucrativos: a Universidade FUMEC e a PUC Minas, ambas sediadas em Belo Horizonte.

A PUC Minas, denominada UNI1, caracteriza-se por ser uma universidade comunitária, confessional, filantrópica e privada, de caráter público não estatal, mantida pela Sociedade Mineira de Cultura. Ela está presente em sete campi localizados nas cidades de Belo Horizonte, Betim, Contagem, Arcos, Poços de Caldas, Serro e Uberlândia (PUC Minas, 2023a). A Universidade FUMEC, denominada UNI2, é uma instituição de ensino superior sediada no município de Belo Horizonte e sua mantenedora é a Universidade FUMEC, pessoa jurídica de direito privado, sem fins lucrativos, criada e gerida por professores (Universidade FUMEC, 2023). Elas possuem, respectivamente 120 e 64 cursos de graduação e diversos cursos de pós-graduação (*stricto* e *lato sensu*).

Com base na LGPD, foram selecionados três perfis distintos: (1) o DPO, que possui domínio da lei e tem como atribuição garantir que as IES estejam em conformidade com a LGPD, estabelecendo padrões de forma a proteger as informações dos usuários e demais interessados; (2) o gerente de TI / governança de TI, que é responsável pelo apoio a todas as atividades

relacionadas à tecnologia, governança de TI e facilitador da comunicação entre stakeholders — principalmente conselho e diretoria; e (3) o Gerente de governança de dados que é responsável por garantir a segurança dos dados e informações. Nas duas IES, foram entrevistados dois profissionais, o DPO e o gerente de TI, perfazendo um total de quatro entrevistados.

Os roteiros de entrevista semiestruturada foram elaborados com questões abertas. Este tipo de entrevista favorece “a exploração dos saberes dos entrevistados em profundidade, bem como de suas representações, crenças e valores” (Laville; Dionne, 1999, p. 196). Para a área de TI, o roteiro foi dividido nas áreas de governança de TI e de governança de dados. As questões foram elaboradas com base nos frameworks e normas da área e em diversos trabalhos (Quadro 1), especialmente nos de Barata (2015), Assis (2011) e Moreira e Vieira Neto (2014).

**Quadro 1** - Relação entre os objetivos da pesquisa versus autores

Objetivos específicos	Referências
Identificar quais áreas de negócios e sistemas de Informação existentes nas IES passaram por adaptações para apoiar a implementação, uso e gestão da LGPD.	Barbosa et al. (2021), Brasil (2018), Stelzer et al. (2023)
Verificar quais iniciativas/ações relacionadas à Governança de TI têm sido adotadas pelas IES. Verificar quais disposições expressas nos capítulos da LGPD foram implementadas pelas IES.	ABNT (2018; 2019; 2022), Albertin e Albertin (2010), Assis (2011), Barata (2015), Brasil (2018), Fernandes e Abreu (2014), ITGI (2007), Lunardi (2008), Moreira e Vieira Neto (2014), Pereira Júnior e Stakoviak Júnior (2022), Weill e Ross (2006).
Identificar os modelos específicos de governança de TI e de governança de dados utilizados nas IES.	Axelos (2019), Cavalcanti Filho (2011), ISACA (2019), Dama International (2015), Weill e Ross (2006)

**Fonte:** Elaborado pelos autores (2024).

O projeto de pesquisa foi aprovado pelo Comitê de Ética em Pesquisa da Universidade FUMEC porque envolve seres humanos, no caso as pessoas responsáveis pela implantação da LGPD nas IES estudadas. As entrevistas foram agendadas por e-mail e realizadas de forma on-line, por meio de plataformas digitais, utilizando-se softwares de videoconferência como Teams e Google Meeting. Em seguida, houve a transcrição das entrevistas (75 páginas) e seu encaminhamento aos entrevistados para validação do seu conteúdo. O Quadro 2 apresenta a relação de entrevistados por IES. As entrevistas ocorreram entre outubro e dezembro de 2023.



**Quadro 2 - Relação de entrevistados**

<b>Participantes</b>	<b>IES</b>	<b>Cargo / Função</b>
Entrevistado 1	IES1	DPO
Entrevistado 2		Gerente de TI (Governança de TI / Dados)
Entrevistado 3	IES2	DPO
Entrevistado 4		Gerente de TI (Governança de TI / Dados)

**Fonte:** Elaborado pelos autores (2024).

Foram consultados documentos<sup>4</sup> produzidos pelas IES no processo de adequação à LGPD, o que possibilitou a triangulação de dados e análise crítica mais aprofundada de todo o processo.

Após as entrevistas, realizou-se a análise de conteúdo. Bardin (2011) afirma que a análise de conteúdo é um conjunto de instrumentos de cunho metodológico em constante aperfeiçoamento. O Quadro 3 apresenta as categorias utilizadas na pesquisa.

**Quadro 3 - Categorias de análise**

<b>Categorias</b>	<b>Subcategorias</b>
Processo de adequação	Escopo / Relação com o negócio / Papel Alta Direção
	Histórico
	Instituição de Comitê e Política de Privacidade
Pessoas	Equipe
	Capacitação
Comunicação	Público-alvo/periodicidade
	Meios (Website e outros)
Governança de TI e governança de dados	Papel (Plano Diretor de Informática)
	Frameworks / Normas
	Interface com outros órgãos/parceiros
Tratamento de Dados Pessoais	Políticas de segurança (RIPD/Riscos)
	Incidentes (Ameaças, denúncias, vazamento)
Avaliação	Resultados
	Dificuldades/desafios
	Perspectivas Futuras (Pontos relevantes/diferenciais)

**Fonte:** Elaborado pelos autores (2024).

O agrupamento por categorias visa uma melhor significação e compreensão dos dados (Bardin, 2011).

<sup>4</sup> **UNI1** – Boletim de privacidade, Boletim de segurança da informação, Páginas do sítio eletrônico sobre Comunicação com o cliente, política de Privacidade e Política de Segurança da Informação, Formulário para reportar incidente de segurança da informação ou privacidade e Formulário para acesso a informações pessoais.

**UNI2** – Comitê de privacidade e proteção de dados pessoais, Evento de conscientização sobre proteção de dados pessoais, Páginas do sítio eletrônico sobre Canal LGPD e Cookies, Formulário para contato com a Ouvidoria e Diretiva de Privacidade (proteção de dados).

**Agência Nacional de Proteção de Dados (ANPD)** – Fluxo de processos para aplicação do RIPD.

## 4 DISCUSSÃO DOS RESULTADOS

### 4.1 O processo de adequação à LGPD: histórico e avaliação

A adequação à LGPD nas IES pesquisadas teve início no período de 2019/2020, logo após a entrada em vigor da lei. O processo ocorreu em conformidade aos requerimentos da legislação, contudo ainda está em andamento devido, dentre outros fatores, aos desdobramentos da lei.

A designação de um DPO para o exercício da função (requerimento legal obrigatório) revelou que foram escolhidos profissionais experientes, com forte conhecimento em gestão corporativa, LGPD e know-how sobre o negócio das instituições (prestação de serviços educacionais). Os DPO entrevistados foram nomeados formalmente pela alta gestão das instituições.

[...] O projeto iniciou aqui na universidade, em 2019. E eu fui coordenador do comitê de proteção de privacidade e proteção de dados durante um pouco mais de um ano. E, logo depois, eu fui nomeado como DPO então, antes de assumir o cargo, porque agora é cargo mesmo [...] (Entrevistado 1 / UNI1).

Porém, eles ainda acumulam cargos, isto é, acumulam a sua função original com a função de DPO. Eles também ocupam posição nos comitês gestores da LGPD, em suas respectivas instituições. Destaca-se que o DPO da UNI2 possui a certificação DPO pela EXIN (entidade certificadora).

As IES pesquisadas criaram comitês para os trabalhos de adequação da LGPD e eles estão subordinados à alta gestão.

Nós temos um comitê de privacidade e proteção de dados, que é basicamente para atender questões pontuais que envolvem um impacto mais amplo. Eu, basicamente, eu tenho autonomia para tomar várias decisões, mas, quando eu entendo que determinada adequação, alguma medida que vai gerar um impacto maior dentro da IES, aí sim, eu envolvo o comitê, mas ele não tem, assim, ele não tem uma atuação tão frequente como o DPO (Entrevistado 1 / UNI1).

Há semelhança na composição desses comitês que são formados pelo DPO, por membros da área jurídica, da área de TI e da alta gestão. Os encontros são regulares (mensais). Outra característica comum refere-se à competência consultiva e não deliberativa dos comitês.

Tanto na UNI1 quanto na UNI2 o processo se iniciou com um diagnóstico prévio, com diversos stakeholders, e, posteriormente, prosseguiu com a estruturação e planejamento do programa de adequação à LGPD. Depois



ocorreu o levantamento de dados (*datamaping*), com posterior análise e classificação dos dados em todas as unidades das instituições pesquisadas, inclusive determinado a sensibilidade do dado. Esta etapa foi denominada diagnóstico institucional. Depois partiu-se para a criação de plano de comunicação, capacitação de colaboradores, estabelecimento de medidas corretivas e preventivas, gestão do consentimento, gestão das bases legais e RPID, conforme requerido pela lei e observado por Silva (2020) em outras IES.

#### **4.2 Pessoas envolvidas**

Nas duas IES as equipes responsáveis pela LGPD são reduzidas e contam com um DPO e um auxiliar administrativo. De forma semelhante, adotou-se a estratégia de escolher uma pessoa (colaborador-chave) como ponto focal da LGPD no setor. Esta pessoa tornou-se o “embaixador” da LGPD em seu setor, com o compromisso de atuar não apenas como um interlocutor, mas como um parceiro. Quando surgem questões pertinentes à TI, o gerente de TI é acionado para auxiliar na resolução do problema/demandas.

No que se refere ao desenvolvimento de competências relacionadas à LGPD, à governança de TI e à governança de dados, inicialmente a capacitação dos colaboradores ocorreu sob demanda, principalmente durante a pandemia do Coronavirus Disease (COVID-19). Houve um esforço de conscientização sistemática e contínua (palestras, workshops, *folders*), e a realização de treinamentos constantes, inclusive de colaboradores das áreas indiretas, fortalecendo assim o processo de adequação e promoção da LGPD.

Nós tivemos uma conscientização institucional para todo o público, do Presidente à área de conservação e limpeza. Foi dado um overview para todo mundo. Em março de 2020, foi contratada uma empresa para fazer isso. E depois, quando começaram as entrevistas de *datamaping*. Antes das entrevistas, eu fazia essa conscientização individualizada, tirava dúvidas, esclarecia, antes da gente caminhar para de fato eles começarem a responder; então, assim, somente com a alta administração e com a gestão, como tudo, né, e agora no segundo momento a gente faz workshops (Entrevistado 1 / UNI1).

“[...] Nós tivemos palestras, seminários, nós aplicamos alguns testes de conhecimento em três níveis nos setores, e a gente tem trabalhado nesse

sentido. É de atualização das práticas. É no sentido da aplicação da lei [...]” (Entrevistado 2 / UNI1).

#### **4.3 Comunicação**

O processo de comunicação é relevante em toda organização. Quando se abordam processos corporativos (implementação de sistemas, rotinas, processos, leis e normas), eles devem ser muito bem definidos, orientados, direcionados e amplamente difundidos (Rocha; Luz, 2020). Segundo Barros e Brondani (2016), para ter uma comunicação considerada eficiente a empresa precisa manter o público interno bem-informado, compartilhando dados, resultados e utilizando os recursos da comunicação corporativa como estratégia de gestão. Nas IES estudadas, ele se mostrou não menos importante, e é realizado com frequência.

Na UNI1, a gerência de tecnologia emite, semanalmente, boletins de segurança da informação intercalados com boletins sobre a LGPD, ou seja, é um processo de comunicação recorrente com o público interno e externo. Podem ser percebidas diversas ações neste sentido, pois “[...] (quanto ao) plano de comunicação, a gente também tem essa preocupação de trabalhar a comunicação interna e externa com relação à aplicação da LGPD. [...]” (Entrevistado 3 / UNI2). No caso da UNI2 foi realizado um trabalho de conscientização e divulgação da adequação à LGPD, tanto para o público interno quanto externo, porém as comunicações são *ad hoc*, sem periodicidade definida.

Em conformidade com as exigências da LGPD, as IES disponibilizam em seu sítio eletrônico um formulário específico para recebimento de comunicação externa referente a incidentes de segurança (vazamento/violação de dados).

[...] no nosso sítio eletrônico tem o link do nosso canal de comunicação com os titulares, os dados com que eles podem fazer o registro desse possível incidente. Porque envolve a questão investigativa (procedimento), inclusive. Mas também nós temos a ouvidoria da instituição, que pode também receber essa demanda e eles já receberam as devidas orientações no sentido de direcionar para o DPO demandas que envolvem tratamento de dados pessoais [...] (Entrevistado 1 / UNI1).

#### **4.4 Governança de TI e de Dados**

Possibilitar às organizações a tomada de decisões estratégicas por meio de técnicas e ferramentas apropriadas para alinhar os negócios e a TI



(frameworks) é fortemente desejável, visto que tais elementos são práticas consolidadas no mercado (Weill; Ross, 2006; Wu; Straub; Liang, 2015). A UNI1 utiliza parcialmente o framework ITIL e, de forma incipiente, a parte financeira de orçamento e custos gerenciados (processo APO06) da estrutura do COBIT, mas alinhada com a alta direção por meio dos orçamentos anuais e plurianuais. Sugere-se a utilização do framework COBIT em sua totalidade, visto que sua utilização pode trazer benefícios diretos no processo de adequação à LGPD, como na gestão de incidentes, na gestão de atendimento aos usuários, no monitoramento do ambiente, e outros.

Na UNI1 não há política definida ou um setor específico para a governança de dados. O tratamento de dados está restrito aos sistemas de banco de dados e, quando se trata de assuntos relacionados à LGPD, um Analista de Banco de Dados (DBA) possui a chancela para outorgar ou não dados pertinentes àquele conteúdo, ou seja, o tratamento de dados passa por sua avaliação antes de adentrar em qualquer sistema informatizado daquela instituição. Ocorre, de certa forma, um tratamento analítico de dados prévio, sob a ótica de um DBA com expertise em LGPD. Mas não há plano de governança de dados estabelecido e nem framework destinado a este fim. A Política de Segurança da Informação da UNI1 contempla os requisitos elencados na NBR ISO 27.701 (ABNT, 2019) de Segurança da Informação (PUC Minas, 2023b).

Quanto aos frameworks de governança de TI, a UNI2 os utiliza de forma empírica. Parte das operações está de acordo com os frameworks mais conhecidos, como COBIT, ITIL e há o interesse na implementação completa destes e, também, da NBR 38500 por parte da IES (porém os estudos estão em fase embrionária). A governança de dados é praticamente inexistente e não é utilizado nenhum tipo de framework específico. O DBA não possui formação em LGPD ou em governança de dados, porém para o gerenciamento do banco de dados corporativo a informação deve passar, pela sua análise. A gerência de TI na UNI2 está desenvolvendo um plano geral para medição de serviços/atividades de TI, por meio de KPIs (indicadores de performance), em conformidade com a ITIL.

Outro ponto a ser destacado refere-se ao tratamento da violação de dados. Nas duas IES pesquisadas não foram relatados registros de incidentes

relevantes dessa natureza. E, em caso de ocorrência, as IES possuem plano de contingência para tratamento de riscos. Porém eles ainda não foram colocados em prática, o que impede de verificar sua eficiência. Um ponto negativo, neste caso, refere-se à não realização de testes de incidente como, por exemplo, intrusão, sequestro, ransomware e outros, o que pode comprometer a eficácia do procedimento. Em caso incidente de segurança ou violação de dados pessoais, por força de lei, a instituição deve, obrigatoriamente, comunicar o fato à Agência Nacional de Proteção de Dados (ANPD) (Brasil, 2018).

Assim, apesar de não haverem sido criadas políticas específicas para a gestão de riscos envolvendo dados nas IES, há o procedimento definido pela ANPD, que é o RYPD, para relatar incidentes com dados organizacionais:

Nós utilizamos um modelo da própria ANPD; nós temos aqui essa prática. A gente preenche o formulário e debruçamos sobre esse incidente, para ver se realmente é uma questão que se faz necessário comunicar à ANPD ou pode ser trabalhado internamente e não vai gerar nenhum dano a nenhum titular (Entrevistado 3 / UNI2).

[...] agora o RYPD é um relatório mais específico, mais analítico, que a própria ANPD está regulamentando melhor ainda. Ela falou que vai ter mais, mas não especificou exatamente como vai ser. [...] estamos fazendo esta atividade somente para aquelas (situações) que tratam do legítimo interesse. Uma vez que conseguirmos automatizar, faremos para todas (Entrevistado 2 / UNI1).

Apesar de cada instituição ter autonomia para determinar os processos e formas de relato dos incidentes, a diretiva da ANPD auxilia neste ponto. De acordo com o guia DAMA-DMBOK2, é essencial a criação de uma política específica para esse fim e ela que deve conter elementos que abordem a coleta, o processamento, o armazenamento, o tratamento e o descarte dos dados de uma forma segura e eficaz (Dama International, 2015).

#### **4.5 Tratamento de Dados Pessoais**

O processo de tratamento de dados pessoais está formalmente estabelecido nas IES pesquisadas. Existem canais específicos para o tratamento de demandas pertinentes à LGPD de forma a atender aos seus requisitos primários (políticas específicas). Em seus sítios e em suas políticas de privacidade de dados existem espaços apropriados para comunicação direta com o DPO. Vale destacar que, para uma melhor gestão dos dados pessoais, o uso da governança de dados é recomendado, o que não ocorre em ambas IES como citado anteriormente.



No caso da UNI1, inicialmente foi utilizado o conceito de *Privacy by Default*<sup>5</sup>. Porém, à medida que alguns processos são revisitados, avalia-se o dado e o processo de tratamento que está sendo utilizado. Quanto aos novos processos, busca-se utilizar o conceito *Privacy By Design*<sup>6</sup>, isto é, a implementação da proteção de dados é estabelecida desde a sua concepção, e não mais por um padrão previamente estabelecido.

Segundo os DPOs entrevistados, estabeleceu-se uma cultura de proteção de dados pessoais nas IES, passo relevante para o êxito da adequação à lei. Na UNI1 há formas e processos estabelecidos, como é o caso da comunicação com as partes interessadas (interna e/ou externa), bem como como o canal de denúncias. Logo, diante destes recursos comunicacionais, o tratamento de questões pertinentes à LGPD pode ser direcionado e tratado pelos responsáveis pelos dados e até mesmo diretamente pelo DPO.

#### 4.6 Síntese dos casos analisados

É possível perceber que a LGPD está incorporada à rotina das instituições pesquisadas e em processo de melhoria contínua. E ainda que

[...] nós estamos assim trabalhando no sentido de criar e fortalecer o tripé para ter um programa efetivo de privacidade e proteção de dados, que é basicamente a governança, o jurídico e a cibersegurança (Entrevistado 3 / UNI2).

O Quadro 4 apresenta uma síntese das categorias e subcategorias analisadas. Percebe-se que há certa similaridade nos resultados, visto que o processo de adequação à LGPD foi conduzido de forma semelhante pelos DPOs. A adequação realizada atende aos requisitos da legislação em vigor, e, parcialmente, às normas e frameworks de boas práticas de governança de TI.

---

<sup>5</sup> Privacy by Default (privacidade por padrão): para preservar a privacidade todas as ferramentas devem ser acionadas como padrão, isto é a configuração padrão já confere a maior expectativa de privacidade possível ao titular de dados pessoais (Brasil, 2024). Os agentes de tratamento devem, desde o esboço até a execução de produtos, projetos ou serviços, implementar medidas técnicas, administrativas e de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações accidentais ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A partir da sua vigência, todos os procedimentos criados ou programas implementados para o desempenho da atividade deverão estar adequados à LGPD, conforme o art. 46, § 2º (Brasil, 2018).

<sup>6</sup> Privacy By Design (privacidade pelo desenho ou por concepção): Diz respeito ao emprego de meios para se preservar a privacidade durante todo o ciclo de vida dos dados pessoais (Brasil, 2024). No caso, a privacidade é base para a arquitetura dos sistemas e processos desenvolvidos, de modo a possibilitar, pelo formato disponibilizado e pelo serviço prestado, condições que permitam ao titular de dados pessoais preservar a sua privacidade e o formato em que ocorre o tratamento dos seus dados (Brasil, 2018).

**Quadro 4 - Síntese da análise**

Categorias	Subcategorias	UNI1	UNI2
<b>Processo de adequação</b>	Escopo	Definido	Definido
	Relação com o negócio	Existente	Existente
	Alta Direção	Participa	Participa
	Instituição de comitê e política de privacidade	Sim	Sim
<b>Pessoas</b>	Equipe	DPO/Assistente/DBA	DPO/Assistente
	Capacitação (seminário, palestras, treinamentos)	Sim, frequente	Sim, sob demanda
<b>Comunicação</b>	Público-alvo	Interno/Externo	Interno/Externo
	Periodicidade	Semanal	Eventual / esporádico
	Meios	Palestras, e-mail, website, folders e outros	E-mail, website WhatsApp, e outros
<b>Governança de TI e governança de dados</b>	Papel (plano de diretor de informática constituído)	Não	Não
	Normas <sup>7</sup>	Uso conceitos - parcial	Uso conceitos - parcial
	Frameworks	ITIL parcial	ITIL incipiente
	Interface com outros órgãos/parceiros	Sim	Sim
	Riscos <sup>8</sup>	Procedimento operacional. Sem política formal definida para tratamento de riscos.	Procedimento operacional. Sem política formal definida para tratamento de riscos.
<b>Tratamento de dados pessoais</b>	Incidentes (ameaças, denúncias, vazamentos) <sup>9</sup>	Sim	Sim
	Resultados obtidos	Positivo	Positivo
	Dificuldades	Recursos financeiros e humanos	Recursos financeiros e humanos
	Desafios	- Manutenção das diretivas estabelecidas pelo DPO - Capital humano qualificado - Adequação às novas orientações da ANPD - Implementação / evolução Legislação	- Manutenção das diretivas estabelecidas pelo DPO - Capital humano qualificado - Adequação às novas orientações da ANPD - Implementação / evolução da legislação
<b>Avaliação da adequação</b>	Perspectivas futuras (pontos relevantes / diferenciais)	- Implementar governança de TI	- Ampliação programa LGPD - Implementar cultura de dados - Implementar governança de dados

<sup>7</sup> Referência à ISO 27.000 (27.001 e 27.002) – Segurança da Informação.

<sup>8</sup> Há o tratamento conforme política de segurança da informação, contudo não há mapeamento prévio de riscos definidos em política específica.

<sup>9</sup> Possuem recursos técnicos para tratamento e procedimentos padrões na política de segurança da informação, porém cabe melhoria nos processos existentes bem como integração com softwares de governança.



Categorias	Subcategorias	UNI1	UNI2
		<ul style="list-style-type: none"> <li>- Implementar governança de dados e evoluir a cultura/dados</li> </ul>	<ul style="list-style-type: none"> <li>- Melhorar controles de TI</li> <li>- Implementar governança de TI</li> <li>- Melhorar processo de comunicação</li> <li>- Desenvolvimento de políticas de governança de TI</li> </ul>

**Fonte:** Elaborado pelos autores (2024).

A adequação é um processo contínuo, visto que a ANPD e o próprio Congresso Nacional realizam ajustes e melhoria na legislação sobre privacidade de dados, podendo criar regras novas, ajustar mecanismos de controle, sugerir modelos de relatórios e outros. A própria agência de controle governamental (ANPD) realiza atualizações nas formas de controle e fiscalização de seus instrumentos, o que afeta diretamente as IES. Identificou-se que as IES possuem mais de uma base legal<sup>10</sup> atendida, a saber: Consentimento; Cumprimento de obrigação legal ou regulatória, execução ou criação de contrato, dentre outros. Logo, a aderência do programa de adequação à LGPD tem sido relevante e adequada ao propósito estabelecido.

## 5 CONSIDERAÇÕES FINAIS

A proteção de dados no Brasil é tratada por legislações gerais e específicas. Com a promulgação da LGPD, em 2018, e sua vigência a partir de 2020, a proteção de dados tem sido debatida nas esferas pública e privada, e diversas questões têm sido levantadas quanto às formas de adoção (compulsória) e de operacionalização. As IES também tiveram que se adequar às regras da LGPD.

Esta pesquisa teve como objetivo identificar as ações e iniciativas utilizadas por duas IES privadas, sem fins lucrativos, a Universidade FUMEC e a PUC Minas, para adequação aos requisitos da LGPD. Embasada na revisão da literatura e em um estudo multicasos, e amparada nas informações obtidas junto aos entrevistados e nos documentos das IES pesquisadas, os objetivos foram atingidos.

---

<sup>10</sup> No Art. 7º, a LGPD determina 10 hipóteses ou bases legais que devem justificar o tratamento de dados pessoais (Brasil, 2018). Estas bases são fundamentais para garantir que a empresa esteja em conformidade com a lei.

Em consonância com o primeiro objetivo específico, identificou-se como a privacidade dos dados pessoais é tratada pelas IES. A LGPD está implementada e os DPO estão atentos em relação às novas necessidades que podem surgir. O segundo objetivo específico buscou identificar quais normas e frameworks de governança de TI e de governança de dados foram utilizados pelas IES. O framework ITIL foi eleito por ambas, que o utilizaram como referência, mas não na sua totalidade. Não foram identificadas normas/modelos/frameworks para o tratamento e gerenciamento da governança de dados. Há boas práticas sendo aplicadas na gestão de banco de dados, contudo sem o viés de governança de dados. Espera-se que, no futuro, as IES reconheçam a importância e os benefícios que possam ter com a adoção da governança de dados e que desenvolvam a estrutura técnica e humana para atuar com esta disciplina.

Finalmente com o terceiro objetivo específico buscou-se verificar quais os principais desafios encontrados na adequação e no uso da LGPD. As IES tiveram dificuldade em conseguir recursos humanos e financeiros, e vivenciaram desafios, como o de manter todo o aparato legal da LGPD em funcionamento e atualizado, de realizar comunicações frequentes para disseminar o conteúdo e importância da proteção de dados pessoais. Destaca-se a solução utilizada pela UNI1 de criar “embaixadores” da LGPD em cada setor.

Finalmente, apesar das IES estarem em conformidade com a LGPD, segundo os entrevistados, elas estão sujeitas a melhorias em relação à governança de TI e à governança de dados. O processo de governança apoiou a adequação à LGPD e parte do êxito deve-se à atuação dos DPOs, pela condução do processo, empenho e conhecimento sobre práticas de governança, gestão e LGPD. Esses profissionais conseguiram, como afirmam Wu, Straub e Liang (2015), realizar o alinhamento entre o negócio e a tecnologia por meio da associação positiva do desempenho da governança de TI. Assim, apesar do estudo ter trabalhado com um grupo pequeno de entrevistados, estes eram representantes das principais áreas envolvidas: DPO e TI. Além disso, os entrevistados ocupam cargos hierárquicos relevantes e, portanto, possuem uma visão estratégica de suas instituições.

Espera-se que os resultados obtidos contribuam para a adequação de IES que não implementaram a LGPD ou estão em fase de implementação, bem



como demonstrar a elas a importância e uso dos conceitos de governança de TI e governança de dados.

## REFERÊNCIAS

ALBERTIN, A. L.; ALBERTIN, R. M. M. **Estratégias de Governança de Tecnologia da Informação:** estruturas e práticas. Rio de Janeiro: Elsevier, 2010.

ALMEIDA JÚNIOR, O. F. Mediação da informação e múltiplas linguagens. In: ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÉNCIA DA INFORMAÇÃO, 9., 2008, São Paulo. **Anais** [...]. São Paulo: USP. 2008. Disponível em:

<http://enancib.ibict.br/index.php/enancib/ixenancib/paper/viewFile/3037/2163>. Acesso em: 0 abr. 2025.

ALMEIDA, S. C. D.; SOARES, T. A. Os impactos da LGPD no cenário digital: uma revisão integrativa. **Perspectivas em Ciéncia da Informação**, Belo Horizonte, v. 27, n. 3, p. 26–45, jul./set. 2022. Disponível em:  
<https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?lang=pt>. Acesso em: 28 set. 2025.

ASSIS, C. B. **Governança e gestão da Tecnologia da Informação:** diferenças na aplicação em empresas brasileiras. 2011. Dissertação (Mestrado em Engenharia de Produção) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2011. Disponível em:  
[https://www.teses.usp.br/teses/disponiveis/3/3136/tde-05082011-155506/publico/Dissertacao\\_Celia\\_Barbosa\\_Assis.pdf](https://www.teses.usp.br/teses/disponiveis/3/3136/tde-05082011-155506/publico/Dissertacao_Celia_Barbosa_Assis.pdf). Acesso em: 10 fev. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS [ABNT]. **Norma Brasileira ABNT NBR ISO/IEC 38.500:2018** – Tecnologia da informação – Governança de TI para a organização. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS [ABNT]. **Norma Brasileira ABNT NBR ISO/IEC 27701:2019** – Técnicas de Segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS [ABNT]. **Norma Brasileira ABNT NBR ISO/IEC 27001:2022** – Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão e segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2022a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS [ABNT]. **Norma Brasileira ABNT NBR ISO/IEC 27002:2022** – Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

AXELOS. **ITIL Foundation**. 4. ed. Londres: TSO, 2019. v. 1, p. 19-310,

BAGATINI, J. A.; GUIMARÃES, J. A. C.; SANTANA, R. C. G. Gerenciamento dos dados pessoais em arquivos: uma perspectiva centrada no indivíduo com base na LGPD. **Acervo Revista do Arquivo Nacional**, Rio de Janeiro, v. 34, n. 3, p. 1-20, 2021. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/168258>. Acesso em: 16 maio 2022.

BARATA, A. M. **Governança de dados em organizações brasileiras**: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistemas de Informação) – Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo, 2015. DOI 10.11606/D.100.2015.tde-28072015-215618.

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

BARBOSA, T. S. et al. Lei Geral de Proteção de Dados (LGPD) nas instituições públicas de ensino: possíveis impactos e desafios. In: ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL, 7, 2021, Aracaju. **Anais** [...]. Aracaju: 2021. Disponível em:  
<https://api.org.br/conferences/index.php?conference=ENPI2021&schedConf=ENPI2021&page=paper&op=view&path%5B%5D=1455>. Acesso em: 27 mar. 2024.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARROS, K. L.; BRONDANI, R. F. Comunicação Corporativa: A Importância da Comunicação na gestão das Empresas. **REGRAD – Revista Eletrônica de Graduação do UNIVEM**, [S.I.], v. 9, n. 1, p. 85-100, ago. 2016. Disponível em: <https://revista.univem.edu.br/REGRAD/article/view/1095>. Acesso em: 22 abr. 2024.

BRANDÃO, G. et al. Perspectivas acerca do perfil do Mediador da Informação. **Informação & Informação**, Londrina, v. 30, n. 2, p. 159–187, 2025. DOI 10.5433/1981-8920.2025v30n2p159.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: [http://www.Planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm](http://www.Planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm). Acesso em: 01 ago. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em:  
[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acesso em: 15 fev. 2023.



BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 15 fev. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 15 fev. 2023.

BRASIL. Tribunal de Contas da União [TCU]. (Plenário). **TC Auditoria: 039.606/2020-1.** Auditoria do TCU mostrou que é alto o risco à privacidade dos cidadãos que têm dados pessoais coletados e tratados pela Administração Pública Federal. Brasília, DF: TCU, 2020. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo>. Acesso em: 03 mar. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia sobre privacidade desde a concepção e por padrão:** Programa de Privacidade e Segurança da Informação (PPSI). Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2024. Disponível em: [https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia\\_privacidade\\_concepcao.pdf](https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf). Acesso em: 14 abr. 2024.

BURKART, D. V. V. **Proteção de dados e o estudo da LGPD.** 2021. Dissertação (Mestrado em Mídia e Tecnologia) – Faculdade de Artes, Arquitetura e Comunicação, Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, 2021. Disponível em: <https://repositorio.unesp.br/server/api/core/bitstreams/bd12b4d0-87b7-4705-9e5d-423cd938a42a/content>. Acesso em: 22 set. 2023.

CAVALCANTI FILHO, J. H. **Investigação da influência da governança de TI nas instituições federais de ensino superior:** estudo de caso. 2011. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011. Disponível em: <https://repositorio.ufpe.br/handle/123456789/2823>. Acesso em: 22 jun. 2023.

COELHO, F.C.; CARVALHO, A. M. A. A Ciência da Informação e a Lei Geral de Proteção de Dados Pessoais (LGPD): uma revisão sistemática de literatura. **Informação & Informação**, Londrina, v. 30, n. 1, p. 24–54, 2025. DOI 10.5433/1981-8920.2025v30n1p24.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **e-ARQ Brasil:** Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Brasília, DF: Arquivo Nacional : CONARQ, 2022. (Versão 2). Disponível em: <https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV203MAI2022.pdf>. Acesso em: 2 set. 2025.



DAMA INTERNATIONAL. **DAMA-DMBOK2:** Data Management Body of Knowledge. 2. ed. Basking Ridge: Tecnics Publications, 2015. Disponível em: <https://pdfcoffee.com/dama-dmbok-2nd-edition-data-management-body-of-knowledge-pdfdrivecom-pdf-2-pdf-free.html>. Acesso em: 20 nov. 2023.

FERNANDES, A. A.; ABREU V. F. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. 4. ed. Rio de Janeiro. 2014.

FORNASIER M. O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Rev. Direito e Práx.**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021.

GOMES, V., F.; CUNHA FILHO, M. C.; LUCCAS, V. N. Proteção de dados e instituições de ensino: o que fazer com dados de alunos? **Revista Brasileira de Políticas Públicas**, [S.I.], v. 13, n. 1, p. 402-420, 2023.

GONÇALVES, A. P.; GASPAR, M. A.; CARDOSO, M. V. Governança de Tecnologia da Informação: uma análise do nível de maturidade em empresas atuantes no Brasil. **Revista de Gestão e Projetos**, [S.I.], v. 7, n. 1, p. 56-69. 2016. Disponível em: <https://periodicos.uninove.br/gep/article/view/9636>. Acesso em: 28 set. 2025.

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION [ISACA]. **COBIT 2019:** Modelo corporativo para governança e gestão de TI da organização. [S.I.]: ISACA, 2019.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA [IBGC]. **Código das melhores práticas de Governança Corporativa:** Código de boas práticas. São Paulo: IBCG, 2019.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA [INEP]. **Censo da Educação Superior.** 2021. Disponível em: <https://www.gov.br/inep/pt-br/areas-de-atuacao/pesquisas-estatisticas-e-indicadores/censo-da-educacao-superior/resultados/2021>. Acesso em: 17 jul. 2024.

IT GOVERNANCE INSTITUTE [ITGI]. **COBIT 4.1:** Modelo, Objetivos de Controle, Diretrizes de Gerenciamento e Modelos de Maturidade. Illinois: ITGI, 2007. Disponível em: <https://drive.google.com/file/d/0B7TPEf35oSMiZGU5MDMyZjktZGYwMi00ZDgwLTlhZDUtMTImNDI3NTg1MDg0/view?resourcekey=0-YoNFpf-zbW8Kcak-CK-TUw>. Acesso em: 14 maio 2024.

LAVILLE, C.; DIONNE, J. **A construção do saber:** manual de metodologia da pesquisa em ciências humanas. Porto Alegre; Belo Horizonte: Artmed : Editora UFMG, 1999.



LEMOS, A. N. L. E.; PASSOS, E. A adequação das bibliotecas à lei geral de proteção de dados. **CAJUR - Caderno de Informações Jurídicas**, Brasília (DF), v. 7, n. 1, p. 85-103, 2020. Disponível em: <https://cip.brappci.inf.br/download/145226>. Acesso em: 16 set. 2022.

LUNA, F. D. S. **Instituições de ensino superior brasileiras e sua jornada para a transformação digital**. 2020. Dissertação (Mestrado em Empreendedorismo) – Universidade de São Paulo, São Paulo, 2020. Disponível em: DOI [10.11606/D.12.2020.tde-15102020-154313](https://doi.org/10.11606/D.12.2020.tde-15102020-154313).

LUNARDI, G. L. **Um estudo empírico e analítico do impacto da Governança de TI no desempenho organizacional**. 2008. Tese (Doutorado em Administração) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/13248/000642838.pdf?Sequence=1&isAllowed=y>. Acesso em: 15 out. 2023.

MOREIRA, A. W.; VIEIRA NETO, J. Diferenças entre gestão de TI e governança de TI: Uma breve comparação. In: CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO, 10, 2014, Rio de Janeiro. **Anais** [...]. Rio de Janeiro, UFF, 2014. Disponível em: [https://cneg.org/anais/download.php?acao=anais&evento=CNEG2014&codigo=T14\\_0075.pdf](https://cneg.org/anais/download.php?acao=anais&evento=CNEG2014&codigo=T14_0075.pdf). Acesso em: 22 nov. 2023.

PEREIRA JÚNIOR, M. A.; STAKOVIAK JÚNIOR, P. B. M. A lei geral de proteção de dados no ensino superior. **Revista Humanidades e Inovação**, Palmas, v. 9, n. 20, 2022.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS [PUC Minas] **A PUC Minas**. Belo Horizonte: PUC Minas, 2023a. Disponível em: <https://www.pucminas.br/institucional/Paginas/a-puc-minas.aspx>. Acesso em: 11 jun. 2024.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS [PUC Minas] **Política de Segurança da Informação**. Belo Horizonte: PUC Minas, 2023b. Disponível em: <https://smcgtpucminas.sharepoint.com/:b/s/psi/EQwqOPyJGOBPITX0ibr8PoBeHKKhZFZEPR92KX0FS-H3w?e=EulOR0&download=1>. Acesso em: 17 ago. 2024.

POZZEBON M.; FREITAS M. R. H. Pela Aplicabilidade com um maior Rigor Científico dos Estudos de Caso em Sistemas de Informação. **Revista de Administração Contemporânea RAC**, [S.I.], v.2, n. 2, p. 143-170, maio/ago. 1998.

QUEIROZ, R. C. Z. **A proteção de dados pessoais**: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Tese (Doutorado em Administração) – Universidade de São Paulo, São Paulo, 2021. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-085834/publico/11550929DIO.pdf>. Acesso em: 19 out. 2023.

ROCHA, M. M. S.; LUZ, C. N. M. A Importância da Comunicação nas Organizações. **Revista Multidebates**, Palmas, v. 4, n. 3, p. 10-23, 2020.



ROCKEMBACH, M. Estudos de usuários de arquivo e os desafios da lei geral de proteção de dados. **Acervo – Revista do Arquivo Nacional**, Rio de Janeiro, v. 33, n. 3, p. 102-115, 2020. Disponível em:  
<http://hdl.handle.net/20.500.11959/brapci/145798>. Acesso em: 17 maio 2022.

SILVA, R. G. P. **Gestão de Riscos e Controles Internos no Ensino Superior**: Uma Proposta de Framework para Uso e Proteção de Dados Pessoais em Uma Instituição de Ensino. 2020. Dissertação (Mestrado em Ciências Contábeis) - Fundação Escola de Comércio Álvares Penteado, São Paulo, 2020. Disponível em: [https://www.fecap.br/wp-content/uploads/2021/08/DISSERTACAO\\_vDEFESA\\_final-REV.pdf](https://www.fecap.br/wp-content/uploads/2021/08/DISSERTACAO_vDEFESA_final-REV.pdf). Acesso em: 13 fev. 2024.

SOUZA, J. G. S.; BELDA, F. R.; ARIMA, C. H. Análise de aplicação da LGPD numa instituição pública de ensino: um estudo de caso. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1856-1872, 2022. DOI <https://doi.org/10.21723/riaee.v17i3.16789>.

SOUZA NETO, J.; CARVALHO, L. E. M. A avaliação da governança de TI da administração pública sob a ótica dos princípios da governança corporativa. **Revista do Serviço Público**, Brasília, DF, v. 71, [ed. esp.], p. 345–374, 2020. DOI <https://doi.org/10.21874/rsp.v71ic.4426>.

STELZER, J et al. A Lei Geral de Proteção de Dados Pessoais e os desafios para adequação das contratações públicas das instituições de ensino superior federais. In: COLOQUIO INTERNACIONAL DE GESTIÓN UNIVERSITARIA, 22, 2023, Ciudad de Asunción, Paraguai. **Anais** [...]. Florianópolis: INPEAU, 2023. Disponível em:  
<https://repositorio.ufsc.br/bitstream/handle/123456789/253838/1230126.pdf?sequence=3&isAllowed=y>. Acesso em: 14 abr. 2023.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais**. São Paulo: Atlas, 1987.

UNIVERSIDADE FUMEC. **Nossa História**. Disponível em: <https://www.fumec.br/afumec/nossa-historia/>. Acesso em: 16 ago. 2023.

VIGNOLI, R. G. et al. Mediação da informação e a proteção da privacidade e de dados sensíveis por bibliotecários. **Informação & Informação**, Londrina, v. 25, n. 4, p. 280-305, 2020. DOI <https://doi.org/10.5433/1981-8920.2020v25n4p280>.

WEILL, P.; ROSS, J. W. **Governança de TI**: Tecnologia da Informação. São Paulo: M. Books do Brasil Editora, 2006.

WU, S. P. J.; STRAUB, D. W.; LIANG, T. P. How information technology governance mechanisms and strategic alignment influence organizational performance. **MIS Quarterly**, (S.I.), v. 39, n. 2, p. 497-518, 2015.

YIN, Robert K. **Case Study Research**: Design and Methods. 4. ed. Thousand Oaks: SAGE Publications, 2009. p. 101.



ZANON, S. B. Arquivos públicos: proteção de dados frente o acesso à informação. **Revista Ibero-Americana De Ciência Da Informação**, [S.I.], n. 15, v. 2, p. 416–435, 2022. DOI 10.26512/rici.v15.n2.2022.40678.



## CONTRIBUIÇÕES DAS AUTORIAS

Informa-se nesta seção as funções de cada pessoa autora, de acordo com a [taxonomia CRedit](#), conforme orientado na página da revista PCI:

Função	Definição
Conceituação	William Botelho Arabi; Adriane Maria Arantes de Carvalho.
Curadoria de dados	—
Análise Formal	—
Obtenção de financiamento	—
Investigaçāo	William Botelho Arabi.
Metodologia	William Botelho Arabi; Adriane Maria Arantes de Carvalho.
Administração do projeto	William Botelho Arabi.
Recursos	—
Software	—
Supervisão	Adriane Maria Arantes de Carvalho.
Validaçāo	—
Visualização [de dados (infográfico, fluxograma, tabela, gráfico)]	—
Escrita – primeira redação	William Botelho Arabi.
Escrita – revisão e edição	William Botelho Arabi; Adriane Maria Arantes de Carvalho.

**DECLARAÇÃO DE DISPONIBILIDADE DE DADOS** data-available-upon-request – Os dados de pesquisa só estão disponíveis mediante solicitação.

**Editora Chefe:** Lorena Tavares de Paula  

