UNIVERSIDADE FUMEC
FACULDADE DE CIÊNCIAS EMPRESARIAIS – FACE
PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO
E GESTÃO DO CONHECIMENTO

WILLIAM MACHADO BOTELHO ARABI

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

BELO HORIZONTE - MG
2024

WILLIAM MACHADO BOTELHO ARABI

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

Dissertação apresentada ao Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade Fumec, como parte dos requisitos para a obtenção do título de mestre em Sistemas de Informação e Gestão do Conhecimento.

Área de concentração: Gestão em Tecnologia da Informação.
Linhas de Pesquisa: Tecnologias de Informação e da Comunicação.
Orientadora: Prof.ª Dra. Adriane Maria Arantes de Carvalho.

BELO HORIZONTE - MG
2024

Dados Internacionais de Catalogação na Publicação (CIP)

A658a Arabi, William Machado Botelho, 1969 -

A adequação à Lei Geral de Proteção de Dados Pessoais em instituições de ensino superior: um estudo multicasos / William Machado Botelho Arabi. - Belo Horizonte, 2024.

152 f. : il.

Orientadora: Adriane Maria Arantes de Carvalho

Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento), Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2024.

1. [Lei geral de proteção de dados pessoais (2018)]. 2. Ensino superior. 3. Privacidade. 4. Proteção de dados. I. Título. II. Carvalho, Adriane Maria Arantes de. III. Universidade FUMEC, Faculdade de Ciências Empresariais.

CDU: 342.721

Ficha catalográfica elaborada pela Biblioteca Universitária-FUMEC

UNIVERSIDADE
FUMEC

Dissertação intitulada **"A adequação à Lei Geral de Proteção de Dados Pessoais em instituições de ensino superior: um estudo multicasos"** de autoria de **William Machado Botelho Arabi**, aprovada pela banca examinadora constituída pelos seguintes professores:

Profª. Drª. Adriane Maria Arantes de Carvalho – Universidade FUMEC
(Orientadora)

Prof. Dr. Luiz Claudio Gomes Maia – Universidade FUMEC;
(Examinador Interno)

Prof. Dr. Rodrigo Moreno Marques – UFMG.
(Examinador Externo)

Prof. Dr. Armando Sérgio de Aguiar Filho
Coordenador do Programa de Doutorado e Mestrado em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC.

Belo Horizonte, 26 de fevereiro de 2024.

DEDICATÓRIA

Dedico este trabalho a minha querida mãe, Magali Machado Botelho Arabi (*in memoriam*), exemplo de amor, sabedoria e fé.

Ao meu pai, Mohamad Wehbe Arabi, exemplo de força e persistência, que me matriculou no primeiro curso de informática (BASIC I), nos idos de 1985, quando iniciei meus estudos na fascinante área de Tecnologia da Informação.

Aos meus queridos filhos, Pedro (filósofo marombeiro), Mateus (mente brilhante) e Paulo (embaixador dos bichos), pelo amor, carinho, apoio e maturidade que foram indispensáveis para concluir esta missão.

A Jan, pela compreensão e apoio essenciais para a conclusão desta pesquisa.

Aos meus irmãos e irmãs, pelo apoio e incentivo.

Aos demais familiares que, direta ou indiretamente, me apoiaram nesta conquista.

A todos que, de alguma forma, contribuíram para a elaboração desse trabalho.

AGRADECIMENTOS

A Deus,

À Profª. Adriane M. A. de Carvalho, pelas infindáveis orientações, pelos valiosos ensinamentos e pela contribuição em minha formação acadêmica.

Aos professores Dr. Luiz Cláudio Gomes Maia e Dr. Rodrigo Moreno Marques, pelas excelentes contribuições dadas a esta pesquisa.

Aos professores do mestrado em Sistemas de Informação e Comunicação e Gestão do Conhecimento da Fumec. Aulas sensacionais! Impossível não gostar das exposições, aprendizados, trabalhos e ensinamentos...

À Face-Fumec, em especial ao Coordenador do curso, Prof. Dr. Armando Sérgio de Aguiar Filho e à Profª. Dra. Renata de Sousa da Silva Tollentino.

Ao time de apoio do Programa de Pós-Graduação (Secretaria acadêmica, Biblioteca, TI e aos demais colaboradores), por contribuir no funcionamento do curso e apoio aos alunos.

À Fundação de Amparo à Pesquisa do Estado de Minas Gerais – FAPEMIG, pelos recursos financeiros disponibilizados para a condução e conclusão desta pesquisa.

A todos que contribuíram, de variadas formas, para a elaboração deste trabalho.

“Eu tentei 99 vezes e falhei, mas na centésima tentativa eu consegui; nunca desista de seus objetivos mesmo que esses pareçam impossíveis: a próxima tentativa pode ser a vitoriosa.”

(Albert Einstein)

RESUMO

A presente pesquisa busca verificar como foi o processo de adequação das Instituições de Ensino Superior (IES) privadas, sem fins lucrativos, à Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. O trabalho de investigação visa entender como se deu esta adequação, quais instrumentos foram utilizados, se houve o emprego da Governança de Tecnologia da Informação (GTI) e da Governança de Dados (GD), bem como seus modelos e *frameworks*, e em que medida, como foi a participação dos colaboradores e parceiros e qual foi o resultado atingido pelas IES. O processo de adequação foi compulsório, logo após a sansão da Lei pela Presidência da República no ano de 2020. A LGPG foi utilizada como marco referencial primário e a TIC como secundário. Foram identificadas as normas antecedentes à promulgação da LGPD que abordam o acesso a dados pessoais, como a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet (MCI). Identificou-se os requisitos necessários para adequação da LGPD, bem como os conceitos de Governança de TI e de Dados, além de normativos consolidados no mercado corporativo, como as normas ISO 38.500 e 27.701 e *frameworks* como COBIT e ITIL, os quais foram abordados no decorrer da pesquisa. O estudo multicasos foi realizado em duas grandes universidades, Fumec e PUC Minas, sediadas em Belo Horizonte, Minas Gerais. Foi realizada uma pesquisa exploratória e descritiva, com abordagem qualitativa, conduzida por meio de entrevistas semiestruturadas com os responsáveis pela proteção de dados (*Data Protection Officer* – DPO) e o Gerente da GTI destas IES. Dessa forma, os dados coletados foram categorizados e analisados. A GTI, bem como normas/modelos e *frameworks* forneceram processos, além de uma base de conhecimento sólida para a adequação e operação do novo sistema legal nas IES pesquisadas. Identificou-se que a governança de dados (GD) é um processo inexistente em uma IES e, em outra, um processo incipiente, logo a sua implementação é recomendada para melhor gestão do volume informacional contidos nas instituições pesquisadas. Observou-se, em ambas as IES, que a adequação à LGPD ocorreu conforme cronograma estabelecido pelos DPOs e a adequação ocorreu de forma cadenciada devido à complexidade da legislação. Houve o envolvimento da alta direção das IES e demais parte interessadas de forma direta. O processo de comunicação é um ponto forte em uma Instituição, e realizado com frequência semanal, e na outra Instituição é realizado sob demanda ou periodicidade definida. Em ambas IES o tratamento de dados pessoais ocorre de forma requerida pela LGPD atendendo aos seus requisitos e determinações. É consenso entre os DPOs que a adequação da LGPD é um processo contínuo e requer atualizações e melhorias devido ao seu amadurecimento nas Instituições e/ou pela evolução da legislação sancionada. A pesquisa trouxe relevantes conclusões seja na esfera da LGPD seja na esfera dos demais recursos de apoio utilizado para a adequação das IES à lei. Foram encontradas dificuldades como a falta de recursos humanos e financeiros, bem como desafios que é a própria manutenção e evolução da LGPD. A governança de TI foi utilizada considerando-se o *framework* ITIL, porém não na sua totalidade. Outras normas e modelos não foram referenciadas pelos entrevistados como o COBIT e a NBR ISO 38.500. A governança de dados não é uma realidade nas IES. Em apenas uma delas, o DBA tem conhecimentos aprofundadados em LGPD, porém não foi constatado o uso de recursos básicos e nem avançados sobre este tipo de governança, o que leva a reflexões sobre a sua real necessidade ou sobre possível desconhecimento das IES quanto ao tema.

Palavras-Chave: Governança de tecnologia da informação; Instituição de ensino superior; Governança de dados; Proteção de dados; Privacidade de dados.

ABSTRACT

This research seeks to verify how the process of adapting private, non-profit Higher Education Institutions (HEIs) to the General Data Protection Law (LGPD), Law No. 13,709/2018. The research work aims to understand how this adaptation occurred, which instruments were used, how Information and Communication Technology (ICT) was involved, how the participation of employees and partners was and what was the result achieved by the HEIs. The ultimate reason for the research is to verify how the privacy of personal data, including sensitive ones, are treated and protected by HEIs. The adaptation process was compulsory, shortly after the Law was sanctioned by the Presidency of the Republic in 2020. LGPG was used as the primary reference framework and ICT as secondary. We sought to verify whether Information Technology Governance (ITG) and Data Governance (DG) were used in this adaptation process, as well as their models and frameworks, and to what extent. The regulations preceding the promulgation of the GDPL that address access to personal data were identified, such as the Access to Information Law (AIL) and the Marco Civil da Internet (IMC). The necessary requirements for adapting the GDPL were identified, as well as the concepts of IT and Data Governance, in addition to consolidated regulations in the corporate market, such as ISO standards 38,500 and 27,701 and frameworks such as COBIT and ITIL, which were addressed in the during the research. The multi-case study was carried out at two large universities: Fumec and PUC Minas, based in Belo Horizonte, Minas Gerais. An exploratory and descriptive research was carried out, with a qualitative approach, conducted through semi-structured interviews with those responsible for data protection (Data Protection Officer – DPO) and the ITG Manager of these HEIs. In this way, the collected data was ordered, processed and subsequently categorized into groups and analyzed. The ITG, as well as standards/models and frameworks provided processes, in addition to a solid knowledge base for the adaptation and operation of the new legal system in the HEIs researched. It was identified that data governance (DG) is a non-existent process in one HEI and, in another, an incipient process, so its implementation is recommended to better manage the information volume contained in the researched institutions. It was observed, in both HEIs, that the adaptation of the LGPD occurred according to the schedule established by the DPOs; adaptation occurred in a rhythmic manner due to the complexity of the legislation. Stakeholders were involved directly and indirectly. The communication process is a strong point in one Institution, and is carried out on a weekly basis, and in the other Institution it is carried out on demand or defined frequency. In both HEIs, personal data is processed in a manner required by the LGPD, meeting its requirements and determinations. There is a consensus among DPOs that adapting the LGPD is a continuous process and requires updates and improvements due to its maturity in the Institutions and/or the evolution of sanctioned legislation. The research brought relevant conclusions, whether in the sphere of the LGPD or in the sphere of other support resources used to adapt HEIs to the law. Difficulties were encountered such as the lack of human and financial resources, as well as challenges in the maintenance and evolution of the LGPD. IT governance was used considering the ITIL framework, but not in its entirety. Other standards and models were not referenced by interviewees, such as COBIT and NBR ISO 38,500. Data governance is not a reality in HEIs. In only one of them, the DBA has in-depth knowledge of LGPD, but the use of basic or advanced resources on this type of governance was not found, which leads to reflections on its real need or on possible lack of knowledge on the part of HEIs on the topic.

Keywords: Information technology governance; Higher education institution; Data governance; Data protection; Data privacy.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ABES	Associação Brasileira de Empresas de Software
ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
ANPD	Agência Nacional de Proteção de dados
BI	*Business Intelligence*
BIG DATA	Grande armazenamento de dados
BSC	*Balance Scorecard*
CF	Constituição Federal
CIO	*Chief Executive Officer*
CMM	*Capability Maturiry Model*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
DAMA	*Data Management Association*
DAMA-Brasil	*Data Management Association – Chapter Brasil*
DBA	*Data Base Administrator*
DGI	*Data Governance Institute*
DMBOK	*Data Management Body of Knowledge*
DPO	*Data Protection Officer*
EBSCO	*Academic Databases for Colleges and Universities*
EMERALD	*Scientific Electronic Library Online*
ERP	*Enterprise Resource Planning*
ESG	*Environmental, Social and Governance*
FAPEMIG	Fundação de Amparo à Pesquisa do Estado de Minas Gerais
FGV	Fundação Getúlio Vargas
GC	Governança Corporativa
GD	Governança de Dados
GDPR	*General Data Protection Regulation*
GTI	Governança da Tecnologia da Informação
IBGC	Instituto Brasileiro de Governança Corporativa
IBM	*International Business Machines Corporation*
IES	Instituição de Ensino Superior

ISACA	*Information System Audit and Control Association*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
ITIL	*Information Technology Infrastructure Library*
ITSM	*Information Technology Service Management*
ITSMF	*Information Technology Service Management Forum*
LGPD	Lei Geral de Proteção de Dados Pessoais
MEC	Ministério da Educação
NBR	Norma Técnica Brasileira
OCDE	Organização para Cooperação e Desenvolvimento Econômico
PDI	Plano Diretor de Informática
PDTI	Plano Diretor de Tecnologia da Informação
PMI	*Project Management Institute*
PRINCE2	*Project In Controlled Environments*
SciELO	*Scientific Electronic Library Online*
SOX	*Sarbanes-Oxley*
SPELL	*Scientific Periodicals Electronic Library*
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação
TOGAF	*The Open Group Architecture*
UE	União Europeia
WOS	*Web of Sciences*

SUMÁRIO

1 INTRODUÇÃO

A oferta de serviços educacionais, por Instituições de Ensino Superior (IES), tem crescido de forma significativa, principalmente na modalidade Educação a Distância (EAD). De acordo com o INEP (2021), tem aumentado a oferta[1] de cursos, na graduação ou na pós-graduação, na modalidade virtual (EAD síncrono ou assíncrono) (INEP, 2021, p.37). O aumento da demanda trouxe, a reboque, a necessidade de uma gestão mais eficaz e eficiente para o setor de Tecnologia da Informação (TI) dessas instituições. A gestão informacional corporativa tornou-se prioridade para elas, bem como a existência de uma sólida e ágil estrutura de TI que suporte a crescente demanda pelo ensino remoto.

As IES possuíam perspectivas de crescimento na modalidade de ensino EAD, previamente estimadas, conforme planejamento corporativo (anual e, ou, bienal), e uma das razões para isso deveu-se à busca exponencial dessa modalidade de ensino após o evento da COVID-19 (ABMES, 2023). Outras razões, que permitiram tal crescimento, traduzem-se em: entregar facilidade de acesso aos discentes, docentes e demais interessados; a praticidade de acessar as aulas em qualquer local; a possibilidade de assistir às aulas em dispositivos móveis (*smartphones* e *tablets*), dentre outros fatores (MEC, 2023). A pandemia do COVID-19 perdurou de janeiro de 2020 a maio de 2023 e levou diversos setores e ramos de negócio a reverem suas perspectivas de crescimento, e a se adequarem (em diversas áreas, inclusive as IES) para a continuidade dos negócios (IPEA, 2020).

No caso específico das IES, inclusive aquelas que já ofereciam cursos na modalidade EAD, tornou-se necessário rever/readequar a estrutura de TI para suportar a crescente demanda e manter seus sistemas de informação (*compliance*) adequados às exigências do novo arcabouço jurídico (SILVA, 2020). Estas estruturas técnicas e de serviços (prestados pela TI das IES) já exigiam, antes da COVID-19, uma eficaz estrutura para o seu bom funcionamento. Com o evento pandêmico, houve aumento expressivo nos volumes a serem armazenados nos bancos de dados e computadores das instituições/organizações (INEP, 2022). Nesse contexto, a Governança da Tecnologia da Informação assume uma posição de destaque dentro dessas instituições, por possibilitar a utilização de modelos e padrões para controle e gestão dos dados organizacionais, em conformidade com a legislação, e por suportar os processos administrativos e acadêmicos oferecidos pelas IES (Wu; Straub; Liang, 2015).

[1] O número de matrículas em cursos a distância aumentou 378,9%. Ingressantes em cursos de EaD correspondiam a 16,1% do total de calouros, em 2009. Em 2019, esse público representou 43,8% do total de estudantes que iniciam a educação superior (MEC-INEP, 2021).

Nesse cenário, sobrevém a Lei Geral de Proteção de Dados (LGPD), lei nº 13.709/2018, a qual estabelece normas para que dados e informações pessoais sejam tratados, armazenados, utilizados e, ou, excluídos pelas organizações, de forma a atenderem os preceitos legais, em conformidade com a LGPD (BRASIL, 2018).

A utilização de modelos de governança de tecnologia da informação e de governança dados, juntamente com a LGPD, pode oferecer às IES e às demais organizações públicas ou privadas, bem como aos demais interessados, um ambiente seguro para o uso dos dados pessoais e sensíveis (conforme exige a LGPD), para a própria prestação de serviços educacionais pelas IES. A GTI possibilita a utilização e integração de um cabedal de recursos, como políticas, normas, controles (modelos de gestão, sistemas e plataformas tecnológicas), dentre outros que, devidamente implementados, mantidos e controlados no seu ecossistema informacional, possibilitarão ganho de performance/desempenho e segurança nas operações físicas e, ou, lógicas das informações utilizadas e mantidas pelas organizações (Lunardi, p. 200, 2008).

O Instituto Brasileiro de Governança Corporativa (IBGC) define GC 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.

> As boas práticas de governança convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum (IBGC, 2019, p. 20).

A Governança Corporativa (GC) das empresas têm passado por grandes adaptações/atualizações, principalmente após a criação da Lei *Sarbanes-Oxlei* – SOX, em 2002, nos Estados Unidos da América (EUA). O propósito da lei era aprimorar os mecanismos de controle e gestão corporativa, com vistas a obter maior assertividade em suas operações. Em consequência, a TI das empresas precisou se rearranjar, técnica e logicamente, para que seus sistemas computacionais estivessem em conformidade com a nova lei (Borgerth, 2005, p. 18).

Segundo o ITGI (2007), a Governança de TI, "é uma responsabilidade do alto escalão executivo e uma parte integral da governança corporativa, consistindo em liderança, estruturas organizacionais e processos que garantem que a organização de TI sustenta e amplia suas estratégias e objetivos da organização" (ITGI, 2007, p. 3). Destarte, os *frameworks* de governança de tecnologia da informação existentes foram ajustados para que as organizações pudessem se adequar a esses novos controles no exercício das práticas comerciais existentes, e que atendessem a demanda da Governança Corporativa e a própria legislação *Sarbanes-Oxlei.*

Por sua vez, a Governança de Dados (GD) 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 (Barbieri, 2020).

As operações corporativas são sustentadas pela TI e, adicionalmente, pela Governança de Tecnologia da Informação e pela Governança de Dados (em organizações mais avançadas tecnologicamente), as quais podem ser consideradas um "braço" ou adendo/capítulo da GTI. Pode-se considerar que a falta de recursos tecnológicos avançados afeta diretamente o funcionamento dos negócios em todos os níveis organizacionais. Os processos de governança corporativa/TI favorecem a gestão e a segurança informacional, a qual pode ser prejudicada por incidentes de segurança (fraudes e sequestro de dados), podendo, inclusive, gerar impactos indesejados na privacidade de dados pessoais (Fernandes; Abreu, 2012).

A utilização da Governança de Dados, complementar à Governança de TI, somada às normas e procedimentos organizacionais e aos próprios recursos de TI, é um instrumento fundamental para o bom funcionamento das organizações, pois lida diretamente com estratégias de negócios, metas e objetivos organizacionais. A GTI favorece melhor gerenciamento do ambiente computacional, permite realizar o gerenciamento de riscos e contribui para atingir melhor desempenho na gestão e administração corporativa (Barata, 2015).

É importante ressaltar que a adequação da LGPD é um grande desafio para as organizações. A proteção e privacidade de dados (principalmente os dados sensíveis), não é, atualmente, uma opção para as organizações, mas um dever legal. A lei promulgada tem que ser rigorosamente cumprida pelas organizações. O propósito da LGPD é garantir a regulação no tratamento de dados, buscando a eliminação ou redução do risco (vazamento de dados, sequestro, ataques) no que se refere à segurança e privacidade dos dados pessoais armazenados nas bases de dados organizacionais (Luna, 2020).

O uso da GTI pelas organizações, portanto, contribui para evitar a insatisfação do usuário/cliente e pode interferir no processo de tomada de decisão pelas organizações, tornando-as mais eficientes (Furlan; Laurindo, 2019, p. 172). Por essa razão, e devido à própria dependência das Tecnologias da Informação e Comunicação (TICs) pelas organizações, a GTI assume papel expressivo nesse cenário, tornando o seu uso essencial, de forma a não comprometer a presença das organizações no acirrado e competitivo mercado corporativo (Furlan; Laurindo, 2019, p. 172).

Conforme demonstrado por Gonçalves *et al*. (2016), 99,1% das empresas declararam a dependência de seus negócios em relação à TI. A pesquisa indica que quanto maior a

dependência dos negócios em relação à TI, maior será o nível de maturidade da GTI na empresa (Gonçalves *et al*., 2016, p. 65).

1.1 Problema de pesquisa

As IES devem atender aos requerimentos da LGPD, que 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 adjacentes, estabelecidos pelas IES. Conforme exposto, é importante compreender o cenário atual das IES, no que se refere à adoção de modelos de GTI, e à sua relação com a adequação da LGPD.

A adequação da LGPD, nas IES, é um desafio e um tema preocupante, conforme afirma Luna (2020, p.103): "A LGPD é um tema que preocupa bastante as IES, dada a quantidade de sistemas e granularidade de dados dos clientes". Este mesmo autor alerta que "a abrangência de sistemas das IES (e suas correlações) somada à quantidade de dados de aluno são fatores merecedores de atenção" LUNA (2020, p.117).

É importante esclarecer como as IES implementaram a LGPD. Elas utilizaram quais recursos/processos para atingir o cumprimento da norma federal? Empregam algum modelo de GTI? A GTI contribuiu para a adequação da LGPD? Houve a utilização de modelos de Governança de Dados?

As IES, pelo fato de manipularem alto volume de dados, por meio da prestação de seus serviços (aulas presenciais, remotas, cursos avulsos, palestras e eventos), necessitam possuir um arcabouço de controle informacional elevado. E as Governanças – Corporativa, de TI e de Dados – entre outros processos de gestão, podem auxiliar as IES em sua gestão administrativa e operacional. Somando-se a isso, é requerido pela LGPD o controle sobre a privacidade de dados pessoais, principalmente quanto aos dados sensíveis, o que se torna um grande desafio para elas. No mercado, existem diversos modelos de governança e *frameworks* muito eficazes, que podem contribuir consideravelmente para a prestação de serviços educacionais pelas IES.

Silva (2020) apresenta que, na adequação da LGPD, é importante mapear as dimensões do risco, como por exemplo:

- Tecnológico: Representa todo tratamento de dados pessoais realizado sobre interfaces tecnológicas: da coleta, armazenamento e transmissão à exclusão. Baliza, comumente, a relação entre Controladores e Operadores de Dados e os mecanismos de segurança

relacionados. Dimensão em que reside a Segurança da Informação, a ISO 27001 e a Governança de TI (COBIT).

- Jurídico: Representa a sólida compreensão da lei, em seus artigos, *caputs*, incisos e parágrafos, percorrendo os artefatos e princípios propostos e seus respectivos impactos sobre as organizações, principalmente sobre os titulares de dados e a garantia de preservação de seus diretos fundamentais. Dimensão hospedada nas leis 13.709/2018 - LGPD, 12.965/2014 - MCI e GPDR - EU.
- Operacional: Representa o uso do dado pessoal pela organização (*stakeholders*) em si, o posicionamento junto à atividade fim ou atividade meio e seu propósito. Refere-se aos processos que tratam dos dados pessoais e seu controle/*compliance*. Dimensão que abriga Governança Corporativa[1] (*Accountability, Responsibility, Transparency e Fairness*), Gestão de riscos (ISO31000), Controles Internos (COSO e COSO-ERM) (Silva, 2020, p. 86).

Cabe, na presente pesquisa, investigar quais foram as iniciativas utilizadas por duas instituições de ensino superior, privadas, sem fins lucrativos, sediadas em Belo Horizonte para adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018.

De acordo com Souza, Belda e Arima (2022), para a adequação da LGPD nas IES, existe a necessidade de implementação de um programa de privacidade que vá ao encontro do plano institucional, de forma transparente, com controles técnicos, treinamentos e conscientizações (Souza; Belda; Arima, 2022, p. 1870). Nessa linha, Burkart (2021) afirma que se pode considerar que o principal impacto da LGPD tenha sido a mudança de paradigma, trazendo a proatividade e a conscientização das organizações como ferramenta para combater as penalizações. Esta mesma autora afirma ainda que é importante que haja uma mudança dentro das organizações, de modo que comecem a respeitar os dados de clientes, fornecedores e parceiros.

Dessa forma, será necessária a criação de meios, não apenas para garantir a proteção de dados, mas também para produzir uma relação de confiança com os parceiros e cliente (Burkart, 2021, p. 59).

1.2 Objetivos

A presente pesquisa propõe, como objetivo geral, identificar quais foram as iniciativas utilizadas por duas IES privadas, sem fins lucrativos: a Fundação Mineira de Educação e

Cultura - Universidade Fumec e a Pontifícia Universidade Católica de Minas Gerais - PUC Minas, para adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD).

São objetivos específicos desta pesquisa:

a) Mapear como foi o processo de adequação e adoção da LGPD nas IES UNI1 e UNI2;
b) Identificar quais normas e, ou, *frameworks* de Governança de Tecnologia da Informação (GTI) foram utilizados pelas IES para a adequação da LGPD;
c) Identificar quais normas e, ou, *frameworks* de Governança de Dados (GD) foram utilizados pelas IES para a adequação da LGPD;
d) Verificar quais os principais desafios encontrados na adequação e no uso da LGPD, segundo os responsáveis institucionais por essa adequação.

1.3 Justificativa

A busca por cursos de graduação e pós-graduação, bem como por cursos extracurriculares e de extensão, nas modalidades presencial e EAD, tem crescido na última década, e, por via de consequência, ocasiona, nas IES, o aumento da demanda pelo setor de Tecnologia da Informação. A exigência computacional é ampliada para comportar o elevado volume de tratamento, armazenamento e transferência de dados desses estabelecimentos de ensino. Entende-se também que os processos de gestão e governança não são apenas necessários, mas fundamentais e prioritários para as IES, de forma a se obter um maior controle e eficiência em seus processos organizacionais, bem como uma rápida e eficaz resposta à comunidade acadêmica. Concomitante a isso, sobrevém a necessidade de cumprimento da LGPD. Portanto, as IES precisaram se adaptar aos novos conceitos e paradigmas, seja por exigência legal, seja para se manterem competitivas no mercado educacional.

A pesquisa é aderente ao programa de Pós-Graduação *Stricto Sensu* em Tecnologia da Informação e Comunicação e Gestão do Conhecimento da Universidade Fumec, linha de pesquisa Tecnologias de Informação e Comunicação. Essa afirmação baseia-se no fato de que, nas organizações, de um modo geral, inclusive nas IES, supõe-se inviável a sua adequação a esse novo aparato legal de lei (LGPD), sem o emprego das TICs, devido à sua complexidade, exigências e inúmeros controles e processos corporativos necessários ao seu bom funcionamento.

Nesse mesmo sentido, a Governança de Tecnologia da Informação, que é uma evolução da gestão da TI, surge devido às inúmeras necessidades de planejamento, administração, organização e gerenciamento de ativos/serviços de TI. Logo, ela assume importante papel nas organizações, principalmente na relação entre a governança corporativa e a governança de dados. A manipulação de dados pessoais nas IES é elevada (discentes por exemplo). Portanto, a GD é um recurso importante e facilitador na adequação a LGPD, pela sua essência e objeto (gestão/governança de dados, inclusive pessoais). E, somando-se a essas duas considerações, vale ressaltar que tais construtos estão ligados (por definição e origem) à informação, seja ela legal (LGPD) ou organizacional (GTI/GD).

Dessa forma, esses constructos, para uma boa aderência nas IES, precisam ser suportados pela TI (recursos de alta complexidade), com políticas de apoio, padrões operacionais, sistemas de informação orientados a este fim e especialização de recursos humanos, os quais servirão de base para a sustentação e operação do negócio de forma eficaz.

Dessa forma, acredita-se o presente estudo prestará o esclarecimento das perguntas elencadas nesta pesquisa, permitindo compreender o cenário atual das IES pesquisadas, no que se refere à adequação, implementação, uso e manutenção da LGPD, e a percepção de como o uso da GTI/GD auxiliou esse processo.

E, para aquelas IES e demais instituições que não implementaram a LGPD (estão em fase de análise ou em qualquer outra), os resultados a serem apresentados poderão servir como aprendizado, *benchmarking* ou "ponto de referência" para elas, bem como para outras organizações que possuam interesse nos constructos GTI e LGPD e em suas respectivas combinações. Espera-se que tais informações apresentadas facilitem o processo de implementação e eliminem/diminuam os percalços ou dificuldades encontradas pelas universidades ora analisadas.

Vale destacar que, para os pesquisadores no tema LGPD e GTI, os dados e informações trazidos nesta pesquisa poderão servir de referência para investigações ou esclarecimentos acerca do tema, bem como de referência para o estudo e aprofundamento dos constructos LGPD, GTI e GD.

Em pesquisas prévias, realizadas por este autor, no período de julho 2022 a junho 2023, nas bases de dados científicas - *WoS* (*Web of Science)*, *Spell* (*Scientific Periodicals Electronic Library*) e *SciELO* (*Scientific Electronic Library Online*), conforme palavras-chave especificadas no resumo, os resultados encontrados (teses, dissertações e artigos, derivados da

interseção LGPD e IES), foram pouco representativos numericamente. Tal fato reforça e justifica a realização da pesquisa proposta em razão de seu caráter de originalidade e ineditismo.

1.4 Estrutura de pesquisa da dissertação

O presente estudo está organizado em quatro capítulos. O segundo capítulo contém o referencial teórico, em que serão apresentados conceitos como os de Governança Corporativa, Governança de TI e seus *frameworks* e normas, Governança de Dados, Lei Geral de Proteção de Dados e Privacidade e Proteção de Dados.

O terceiro capítulo descreve a metodologia aplicada no desenvolvimento da pesquisa, a delimitação do escopo de estudo. Em seguida, são apresentados o estudo de caso e o procedimento para a coleta e análise de dados.

O quarto capítulo apresenta a discussão dos resultados. Nesta seção, serão apresentados os resultados, separadamente, por categorias de análise. Em primeiro lugar, foi apresentado o processo de implementação, seguido das pessoas (treinamentos e recursos envolvidos), a comunicação quanto ao processo de adaptação à nova lei, as questões pertinentes a Governança de TI e de Dados que foram utilizadas (ou não) na adequação das IES à LGPD, uma avaliação geral da adaptação (do processo de implementação e utilização da LGPD na IES) e a síntese dos resultados.

O quinto, e último capítulo, apresenta as considerações finais sobre toda a pesquisa realizada, com as impressões do pesquisador sobre o processo de adequação das duas IES à LGPD.

2 REFERENCIAL TEÓRICO

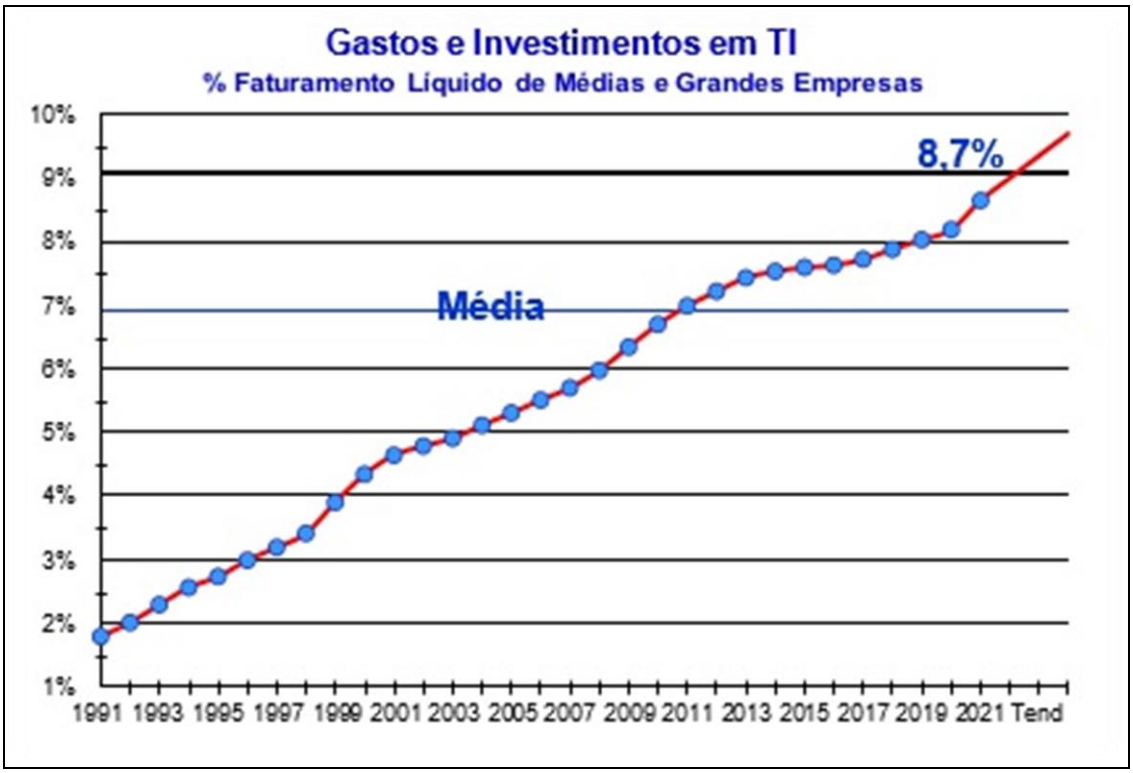
Um fato presente e marcante, principalmente após o evento da COVID-19, refere-se à forte presença da TI na vida cotidiana das pessoas, como formas de se relacionar, de se fazer negócios, de ensino-aprendizagem, algumas já conhecidas, mas com pouca ou relativa presença/utilização pela sociedade. Atualmente, a TI se tornou presente e permanente para a sociedade, de uma maneira geral.

Por outro lado, nas organizações, inclusive nas IES, novas formas de interações surgiram, as quais se fizeram necessárias para continuidade dos negócios, o que atribuiu um novo sentido à TI, nessas organizações. No caso da prestação de serviços realizada por elas (aulas virtuais no período pandêmico da COVID-19), tornou-se necessário o aumento na eficiência de seus processos, bem como ajustes na forma de gestão e, ou, governança. "Assume-se, então, que a TI é fundamental para a transformação da administração das organizações, migrando do *status* de um objeto de gestão para ser objeto de governança" (Moreira Neto *et al*., 2019, p. 16).

Stelzer *et al.* (2019) afirmam que a LGPD traz fundamentos da proteção de dados pessoais, dispondo sobre direitos e garantias do titular de dados pessoais e tem como objetivo regulamentar o tratamento, fomentando uma nova realidade para as IES que, até então, agiam com discricionariedade e poucas restrições normativas, mesmo com a proteção na Constituição Federal, de 1988 (Stelzer *et al*., 2019). As IES terão um grande desafio para a adequação, devido às cobranças e às especificidades da lei. A não conformidade a ela poderá acarretar sanções administrativas e pecuniárias (Stelzer *et al*. 2019, p. 11). Luna (2020) afirma que a LGPD preocupa as IES por sua abrangência, por uma arquitetura de sistemas (legado) muito ampla, pré-existente nas instituições, e pela quantidade de alunos (Luna, 2020, p. 117).

Conforme demonstrado na Figura 1, os gastos e investimentos com a tecnologia da informação, nas empresas, no período de 1991 a 2021, apresentaram crescimento exponencial, o qual deve permanecer ou se manter nos próximos anos. Em 2021, o setor demonstrou maturidade e importância para os negócios existentes (Figura 1). O índice 8,7% (acima da média) representa o gasto total destinado à TI, a soma de todos os investimentos, despesas e verbas alocadas em TI, incluindo: equipamento, instalações, suprimentos e materiais de consumo, *software*, serviços, comunicações e custo direto e indireto com pessoal próprio e de terceiros em TI, dividido pela receita da empresa (Meirelles, 2023).

Figura 1 - Gastos e investimentos com TI nas empresas de 1999 a 2021



Fonte: Meirelles (2023, p. 49).

A GTI é um embrião da Governança Corporativa e possui algumas de suas importantes características. O propósito da GTI é assegurar que a TI seja operacional e funcional, conforme as necessidades das organizações, obtendo-se o desempenho requerido pela alta gestão, e permitindo a gestão dos ativos de TI e o controle dos riscos (ITGI, 2007).

A Associação de Auditoria e Controle de Sistemas de Informação (*Information System Audit and Control Association* – ISACA), em 1988, estabeleceu o Instituto de Governança de TI (ITGI) para promover e difundir os padrões de controle e direção de TI (ISACA, 2019). Uma pesquisa conduzida em 2003, por este instituto, mostrou que a Governança de TI é considerada importante para mais de 80% dos executivos de TI, principalmente por contribuir para o alinhamento entre a TI e o negócio, bem como para reduzir os riscos operacionais da TI (ITGI, 2007).

Fernandes e Abreu (2012) apontam fatores que motivam a implantação da GTI nas organizações, qual sejam: ambiente de negócio mais competitivo e exigente, integração tecnológica mais abrangente dos processos, segurança da informação impactando a integridade do negócio, crescente dependência do negócio em relação à TI e marcos regulatórios.

2.1 A privacidade e a proteção de dados

A privacidade da pessoa humana é garantida no artigo 5º, inciso X, da Constituição Federal brasileira e abordada também em algumas leis adjacentes (Código Civil e Estatuto da Criança e do Adolescente), integrantes do ordenamento jurídico brasileiro (BRASIL, 1988). Ela é um direito personalíssimo do indivíduo de autodeterminar suas informações pessoais. É um Direito Fundamental garantido pela Carta Magna de 1988. A Constituição Federal do Brasil (CF) 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, recentemente publicada no Brasil, deixa claro que a privacidade de dados pessoais deve ser assegurada ao cidadão (BRASIL, 1988).

2.2 Normativos antecedentes à Lei Geral de Proteção de Dados no Brasil

Há, no Brasil, um conjunto de leis, de que fazem parte a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet, cujo objetivo precípuo é a proteção da vida privada e da intimidade de cada cidadão, tal como será abordado a seguir.

2.2.1 Lei de Acesso à Informação – LAI - Lei nº 12.527/2011

A Lei de Acesso à Informação (LAI) tem como principal objetivo garantir o direito fundamental de acesso à informação. Ela trata de assuntos de interesse da União, dos Estados, do Distrito Federal e também dos municípios. Como a própria Constituição Federal, de 1988, prevê, todos têm direito de receber, dos órgãos públicos, tanto informações de seu interesse particular, quanto de interesse coletivo ou geral, sempre lembrando-se de que algumas exceções existem para a própria segurança da sociedade e do Estado. É importante também lembrar que essa lei inclui toda a Administração Direta e Indireta, considerando também as entidades controladas direta ou indiretamente pelos municípios (BRASIL, 2011).

Ela também contribui para a garantia de outros direitos, pois as informações que podem ser obtidas dos órgãos públicos, como os dados sobre gastos do governo, políticas e serviços públicos, por exemplo, são importantes para garantir direitos referentes à educação, à saúde, à igualdade e outros.

Vale destacar que as disposições da LGPD são supervenientes à LAI e, até que aquela viesse a existir, o normativo legal em evidência (a título temporário) era a LAI. Após a promulgação da LGPD, a ANPD é o órgão central de interpretação dessa lei, com competência para o estabelecimento de normas e diretrizes para a sua implementação, conforme previsto em seu art. 55-K, parágrafo único, que estabeleceu novas formas de tratamento à privacidade dos dados pessoais (BRASIL, 2024).

A LAI, portanto, trata exclusivamente de critérios específicos de disponibilização de acesso ou de divulgação de informações públicas, não pessoais. Da mesma forma, não constitui objeto da presente pesquisa a análise sobre padrões e técnicas utilizados em processos de anonimização e pseudonimização de informações, embora relevantes para o tratamento de dados pessoais e para fins de estudos e pesquisas (BRASIL, 2024). Em suma, a LAI foi a primeira lei a regular o acesso à informação, tendo servido de referência ou embrião para futuras discussões sobre regulação de acesso a dados e informações.

Em sentido similar ao disposto na LGPD, o art. 61 do Decreto nº 7.724/2012, que regulamenta a LAI no âmbito do Poder Executivo federal, prevê que "a utilização de informação pessoal por terceiros vincula-se à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa", sob pena de responsabilização "por seu uso indevido, na forma da lei" (BRASIL, 2011). Analogamente à LGPD, o art. 31 da lei nº 7.724/2012 refere-se ao tratamento das informações pessoais da seguinte forma:

> [...] que deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal (BRASIL, 2011).

2.2.2 Marco Civil da Internet – MCI – Lei nº 12.965/2014

A proposição nasceu de uma iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas, no Rio de Janeiro. Estabeleceu-se um processo aberto, colaborativo e inédito para a formulação de um marco civil brasileiro para uso da Internet. Seu principal elemento de inspiração foi a Resolução, de 2009, do Comitê Gestor da Internet no Brasil (CGI.br) intitulada "Os princípios para a governança e uso da Internet" (Resolução CGI.br/RES/2009/003/P) (CGI.br., 2009).

O "Marco Civil da Internet" é uma lei que 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. A iniciativa partiu da percepção de que o processo de expansão do uso da Internet por empresas, governos, organizações da sociedade civil, e por um crescente número de pessoas, colocou novas questões e desafios relativos à proteção dos direitos civis e políticos dos cidadãos. Nesse contexto, estabeleceram-se condições mínimas e essenciais não só para o futuro da Internet (baseado em seu uso livre e aberto), mas também para a inovação contínua, o desenvolvimento econômico, político e social (BRASIL, 2014).

2.3 A Lei Geral de Proteção de Dados – LGPD

A LGPD (Lei nº 13.709) foi criada no ano de 2018. Contudo, esse ordenamento jurídico passou a vigorar em setembro de 2020, após sanção do Presidente da República (BRASIL, 2018). Alguns passos importantes estão sendo tomados pelos legisladores. Nesse sentido, outros arcabouços jurídicos, normas legais e até mesmo a própria Constituição Federal estão sendo alterados para receber alguns dos requisitos da LGPD (BRASIL, 2018).

A emenda constitucional EC115/2022 incluiu a proteção de dados pessoais como um dos direitos e garantias fundamentais. O artigo 5º da Constituição Federal recebeu o inciso LXXIX, que diz: "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais" (BRASIL, 2022). Esta mesma emenda constitucional também incluiu alterações em outras leis, de forma a garantir a viabilidade da LGPD no ordenamento jurídico brasileiro (BRASIL, 2022).

Nas duas IES pesquisadas, o desafio consiste não apenas na adequação da LGPD, já que, após esta fase, as organizações devem se adequar também para a operação e funcionamento

deste sistema de proteção de dados pessoais, por meio de manutenção e ajustes que se fazem necessários com o desenvolvimento da própria lei. O descumprimento desse preceito legal pode acarretar sanções (ANEXO C), inclusive elevadas multas pecuniárias (BRASIL, 2018).

A LGPD mudou a forma como as informações eram tratadas pelas organizações. Constrói-se, com ela, um novo paradigma na forma de tratamento da privacidade dos dados pessoais, pelas organizações brasileiras, independente do porte (Queiroz, 2021, p. 41).

> No Brasil, a LGPD teve como referência para a sua criação o Regulamento Geral de Proteção de Dados (GDPR) da Comunidade Econômica Europeia (CEE). A criação dela representa um marco significativo para o Brasil, representa um avanço em nossa legislação devido ao tratamento e segurança oferecida por ela ao detentor dos dados privados. Cabe destacar que a referida lei aborda o tratamento e proteção de dados pessoais, e não (grifo nosso) se refere a tratamento dos dados organizacionais (Queiroz, 2021, p. 75).

A necessidade de adequação das organizações à LGPD é importante e necessária, pois, segundo o Núcleo de Informação e Coordenação do Ponto BR (NIC.BR), em um levantamento realizado pela Surfshark, empresa especializada em privacidade, o Brasil ocupou o 12º lugar entre os países que mais contabilizaram episódios de vazamento de dados no primeiro trimestre de 2022. A pesquisa também revelou que 286 mil brasileiros tiveram seus dados expostos através de informações na internet. Entre os vazamentos estão: *e-mail*, senhas, números de telefones, documentos pessoais (CPF e RG) e outras informações sensíveis (NICBR, 2023).

Corroborando tal necessidade, o Tribunal de Justiça do Distrito Federal e dos Territórios - TJDFT, em 2021, condenou as operadoras de telefonia Vivo e Claro a indenizar dois consumidores que tiveram os dados vazados e os aparelhos bloqueados por terceiro. Os desembargadores concluíram que as operadoras falharam no dever de segurança e preservação tanto dos dados pessoais dos clientes quanto das informações do sistema interno (TJDFT, 2021).

A seguir, são apresentados os principais requisitos impostos para a adequação e implantação da LGPD. As organizações, inclusive as IES, devem atender à conformidade estabelecida pela LGPD, bem como as próprias fiscalizações da Agência Nacional de Proteção de Dados (ANPD) - órgão controlador geral da LGPD no Brasil. Vale ressaltar que a fiscalização da ANPD pode ser executada a qualquer tempo ou mediante denúncia de violação de dados pessoais junto a este órgão federal (ANPD, 2022).

A Figura 2 apresenta a linha de tempo sobre o tema privacidade no Brasil. Conforme exposto anteriormente, a LAI foi criada em 2011 (etapa inicial) e, na outra extremidade da linha do tempo, ocorre a criação da LGPD (2018), com posterior promulgação em 2021.

Figura 2 - Linha do tempo sobre privacidade no Brasil

Fonte: SERPRO (2024).

2.4 Requisitos de adequação e implantação da LGPD

A LGPD possui requisitos indispensáveis para a sua implementação. Devido a sua complexidade, vale destacar que todos os requisitos não precisam ser implementados ao mesmo tempo, ou seja, a implementação pode ser realizada por fases ou capítulos (que podem conter

um ou mais requisitos), conforme desejar ou planejar a equipe de gestão/implementação. E, ao considerar que cada organização é única, as fases e seus respectivos processos não são necessariamente padronizados, por mais que a origem seja a mesma (BRASIL, 2018).

Os requisitos necessários para a implementação da LGPD são: Tratamento de Dados Pessoais, Política de Segurança da Informação, Política de Proteção de Dados Pessoais, Relatório de Impacto à Proteção de Dados Pessoais, Política de Privacidade, Sistema de Gestão de Incidentes, Controle de Acesso em Sistemas e Utilização de Criptografia (BRASIL, 2018), que serão abordados individualmente, conforme se segue:

a) Tratamento de Dados Pessoais

O dado pessoal é uma informação pertinente à pessoa natural identificada ou identificável segundo o art. 5º, inciso I, da LGPD. Exemplo de atributos da informação: nome, data de nascimento, CPF, RG, e endereço residencial (exemplo de dados pessoais e anonimizados)[2]. Tais elementos podem sofrer variação, pois dependem da forma como uma determinada organização trata seus dados, ou seja, o que pode ser tratado por uma organização, pode não ser por outra (BRASIL, 2018).

Conforme o art. 37 da LGPD, 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).

Além da identificação dos dados pessoais é muito importante saber em qual local eles se encontram (locais físicos e lógicos):

> Os dados pessoais podem ser armazenados em diferentes dispositivos, como: ativos de TI (e.g.: servidores de banco de dados, nuvem, dispositivo USB, *storage* e fita de *backup*) e arquivos físicos (armários e pastas). Ademais, é importante que as organizações identifiquem o endereço onde os dados se encontram. Essas informações são úteis para a análise de riscos (TCU, 2020, p. 53).

O Quadro 1 apresenta como os tipos de dados pessoais são classificados na LGPD, os conceitos relevantes e o foco especial da lei aos dados a serem obtidos, principalmente quanto aos dados sensíveis.

[2] Segundo a LGPD, dado anonimizado é o dado que, considerado os meios técnicos competentes no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Quadro 1 - Tipos de dados na LGPD

O que são dados pessoais?	A LGPD adota um conceito aberto de dado pessoal, definido como a informação relacionada a uma pessoa natural identificada ou identificável. Assim, além das informações básicas, relativas ao nome, Cadastro Nacional de Pessoas Físicas (CPF) e endereço residencial, são também considerados dados pessoais outros que estejam relacionados com uma pessoa, tais como seus hábitos de consumo, sua aparência e aspectos de sua personalidade. Segundo a LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa e que possa identificá-la.
O que são dados sensíveis?	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 (Art. 5º, inciso II).
O que é um dado anonimizado?	Dado anonimizado é qualquer dado pessoal que, submetido a meios técnicos razoáveis, passe a não mais identificar ou a proporcionar a identificação de uma pessoa natural, direta ou indiretamente, de maneira definitiva e irreversível.
O que são dados pseudonimizados?	Dados pseudonimizados são aqueles dados que, submetidos a tratamento, não oferecem a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente seguro.

Fonte: UFSC (2024).

O Quadro 2 apresenta a diferença entre dados pessoais e dados sensíveis. Fica evidente que a LGPD, portanto, é uma forma de garantir ao indivíduo, pessoa física, a proteção de suas informações pessoais, inclusive de dados sensíveis. Por meio dessa lei, um olhar ou atenção especial foi dado ao tipo de dado do indivíduo. Em suma, é a lei preservando um direito fundamental do indivíduo.

Quadro 2 – Principais atores no tratamento de dados pessoais

TITULAR	Pessoa física a quem se referem os dados pessoais
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da LGPD). O controlador pode exercer diretamente o tratamento dos dados, mas pode, também, designar um operador.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da LGPD). Ambos, controlador e operador, recebem a nomeação de "agentes de tratamento" (inciso IX do art. 5º da LGPD).
Encarregado	Corresponde a uma pessoa inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer – DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, assim como entre estes agentes e a ANPD (inciso VII do art. 5º da LGPD).
Autoridade Nacional De Proteção de Dados (ANPD)	Tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da LGPD.

Fonte: UFSC (2024).

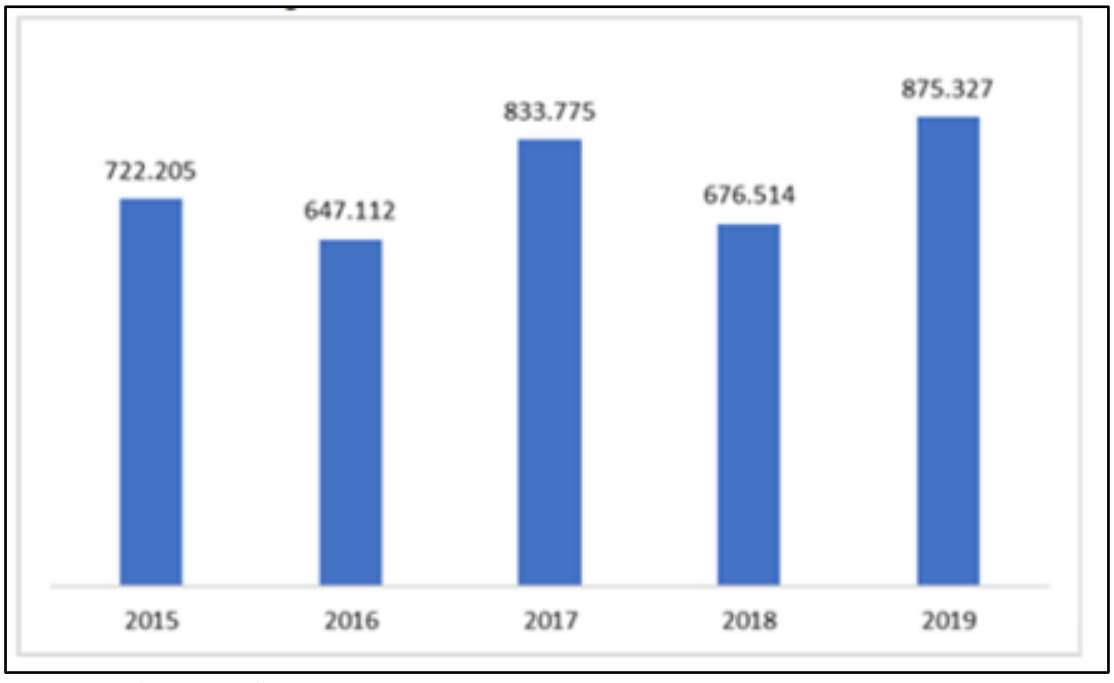
b) Política de Segurança da Informação

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 (ABNT, 2019). Não basta apenas uma política desta natureza: devem existir outras, complementares, que permeiem todo o sistema de informação da organização.

De acordo com a *ABNT NBR ISO/IEC 27701/2019*, item 6.2.1.1, uma Política de Segurança da Informação estabelece como a organização deve gerenciar os objetivos de segurança da informação. É de suma importância que a política seja aprovada pela alta direção e, obviamente, esteja de acordo com os requisitos de negócio e com os demais ordenamentos jurídicos aplicáveis (ABNT, 2019).

O Gráfico 1 demonstra o número de incidentes de segurança da informação identificados, no período de 2015 a 2019, pelo CERT.br em empresas públicas. Observa-se que, neste período, especificamente em 2019, o número de incidentes foi superior, em aproximadamente 25%, ao número de incidentes do ano anterior, 2018.

Gráfico 1 - Número de incidentes de segurança da informação identificados pelo CERT.br



Fonte: TCU (2020, p.54).

c) Política de Proteção de Dados Pessoais

Ainda de acordo com a LGPD, a política de proteção de dados pessoais deve estar *pari passu*, ou seja, em total sintonia com a política de segurança da informação, como, por exemplo, a de classificação da informação, a de *compliance*, a de matriz de riscos (BRASIL, 2018). Ela deve estar alinhada com a *ABNT NBR ISO/IEC 27701/2019*, item 6.2.1.1 (Norma que fornece uma estrutura para gerenciamento de privacidade de dados), de forma que haja uniformidade e conformidade entre elas (ABNT, 2019).

É importante que a organização, como um todo, entenda e compreenda cada uma das políticas corporativas, bem como as suas finalidades. É comum que ocorra certa confusão entre a Política de Proteção de Dados Pessoais, da organização, e a Política de Privacidade, da organização, a qual é direcionada ao público externo. Já aquela é direcionada ao público interno da organização (Fornasier; Knebel, 2020, p. 1032).

d) Relatório de Impacto à Proteção de Dados Pessoais

O relatório de impacto à proteção de dados pessoais possui função extremamente relevante no processo de implementação e uso da LGPD. Esta situação é evidenciada no item 7.2.5. da *ABNT NBR ISO/IEC 27701/2019*, que recomenda que os riscos gerados pelo tratamento de dados sejam, obrigatoriamente, analisados por um processo de avaliação de impacto de privacidade. Alguns dados são extremamente importantes, como, por exemplo, os dados anonimizados, dados pessoais tratados, local de armazenamento dos dados, além do local para o qual eles serão inseridos. Esses são requerimentos relevantes, merecendo especial atenção das organizações (ABNT, 2019).

e) Política de Privacidade

É importante compreender a diferença entre as políticas corporativas, principalmente aquelas relativas a dados organizacionais. A política de privacidade atende ao público externo da organização, diferente da política de proteção de dados pessoais, que é direcionada ao público interno da organização. O item 7.3.2 e 7.3.3 da *ABNT NBR ISO/IEC 27701/2019* sugere 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 de seus dados pessoais. 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).

f) Sistema de gestão de incidentes

Para a adequação da LGPD em uma organização, será necessária a implementação de um sistema de informação, com o objetivo de registrar os incidentes de segurança da informação que envolvam violação de dados pessoais. Para otimizar a gestão, é importante que esse sistema também possua meios para registrar as ações adotadas para resolução dos incidentes registrados.

> O item 6.13.1.1 da ABNT NBR ISO/IEC 27701/2019 ressalta que um processo de gestão de incidentes de segurança da informação abrangente deve estabelecer responsabilidades e procedimentos para identificação, registro e tratamento de violações de dados pessoais. Ademais, o item 6.13.1.5, da mesma norma, descreve que um incidente que envolva dados pessoais pode desencadear uma análise crítica para verificar se uma resposta adequada foi tomada quando necessária. Contudo, um evento de segurança da informação nem sempre desencadeia tal análise, pois pode não apresentar probabilidade significativa de acesso não autorizado a dado pessoal ou a qualquer instalação ou equipamento que armazene esse tipo de dado (TCU, 2020).

O tratamento de incidentes deve promover solução alternativa de imediato. Deve-se inicialmente identificar o incidente (por exemplo a interrupção de um serviço), registrar em sistema específico com o devido detalhamento e prioridade no seu tratamento e solucioná-lo. As causas do incidente devem ser tratadas a posteriori à solução tomada (análise crítica para eliminar a causa raiz). A gestão de incidentes, que envolvam a violação de dados pessoais, deve ser observada e, em sua solução, a equipe da Proteção de Dados/DPO deve atuar em pares (TJDFT, 2021).

g) Controle de acesso em sistemas

Além das medidas supracitadas, que envolvem a proteção de dados pessoais, o art. 46 da LGPD requer a gestão de controle de acesso de usuários. O item 6.6.2.1, da *ABNT NBR ISO/IEC 27701/2019*, sugere que a organização defina um processo formal para registro e cancelamento de usuários dos sistemas que realizam tratamento de dados pessoais, bem como para conceder ou revogar os direitos de acesso dos usuários a esses sistemas. Somando-se a isso, a norma também recomenda que a organização mantenha um registro atualizado dos usuários que tenham sido autorizados a acessar os sistemas de informação e os dados pessoais neles contidos (BRASIL, 2018).

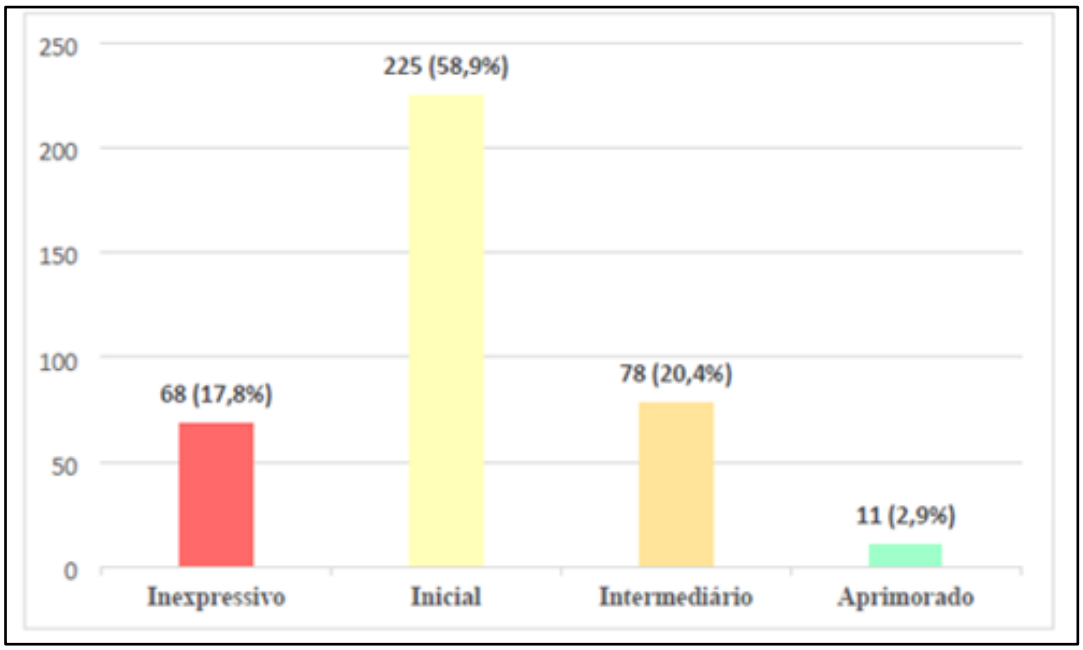
h) Utilização de criptografia

O art. 48, § 3º, da LGPD, estabelece, como um processo de relevante importância, 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).

O Gráfico 2 demonstra o índice percentual da distribuição das organizações públicas por níveis de adequação à LGPD, em 2020, conforme o TCU. Empresas em fase avançada de implementação (nível aprimorado) representam apenas 2,9% do total. Um outro ponto relevante é o número de empresas em fase inicial de implementação: 58,9% do total. Pode-se perceber que, nos próprios órgãos governamentais, o nível de maturidade de implementação e uso da LGPD é incipiente (TCU, 2020, p. 62).

A título de ilustração, conforme a pesquisa realizada pelo TCU (2020), foram avaliados 382 órgãos da administração pública federal em 2020, e identificados os dados pertinentes ao nível de adequação da LGPD.

Gráfico 2 - Distribuição das organizações públicas por níveis de adequação à LGPD



Fonte: TCU (2020, p. 52.).

A auditoria realizada pelo TCU apresenta que,

> A sensibilidade dos dados pessoais deve ser considerada na implementação de um programa de governança em privacidade (LGPD, art. 50, § 2º, inciso I, alínea ‘c’). Por exemplo, o uso de criptografia pode proteger tipos específicos de dados pessoais, como dados sobre saúde, endereço, número de passaporte e número de licença de motorista (TCU, 2020, p. 70).

2.5 Adequação da LGPD nas IES

Para a adequação à LGPD todo um arcabouço de processos, procedimentos, soluções tecnológicas e recursos (humanos, financeiros e administrativos) devem ser utilizados. Isto é, para realizar a adequação, cabe inicialmente, criar um plano de gestão ou plano de gerenciamento do projeto, o qual perpassa por várias areas de conhecimento, como por exemplo: a comunicação, a qualidade, a financeira (custo), tempo (prazo), enfim, todo um aparato de gestão deve ser previamente considerado, planjeado, adotado e gerido antes da adequação propriamente dita. Somado a estas questões, a chance de êxito na adequação aumenta na medidada em que as IES possuam bases de dados (tecnológicas) gerenciáveis e em conformidade com a legislação (aderente às regras de proteção de dados pessoais). Entende-de, portanto que o tratamento de dados pessoais nas IES deve anteceder à adequação da LGPD, (como exemplo, os dados pessoais sensíveis devem estar protegidos e com acesso restrito mesmo sem a adequação à nova legislação), conforme constatado por Valentim (2002):

> As IES lidam com considerável quantidade de dados pessoais e podem ser classificados em: estruturados – já se encontram sistematizados, com tratamento e estão disponíveis para acesso; estruturáveis – produzidos, porém sem tratamento; e, não estruturados – produzidos fora da IES, sem identificação e nenhum tratamento (Valentim, 2002).

De acordo Stelzer *et al.* (2019), “Um exemplo de tratamento de dados é o currículo do aluno: que contém dados pessoais do acadêmico, que educadores compartilham e que é gerado e alterado na medida da progressão ao longo da carreira acadêmica” (Stelzer *et al.,* 2019). Outros dados pessoais, que são tratados pelas IES, dizem respeito ao corpo docente e aos demais membros da comunidade acadêmica, o que representa o grande desafio na implementação da LGPD (Stelzer *et al.,* 2019).

Segundo aqueles autores, “as mudanças organizacionais geralmente envolvem a transformação de processos de negócios, mudanças nas cadeias hierárquicas de comando e controle, novas formas de acesso a informações e reformulação nas formas tradicionais de operação” (Stelzer *et al.,* 2019). Portanto, as IES devem observar as inovações organizacionais e tecnológicas, atentando para a introdução de novas formas de gestão que atendam às mudanças corporativas, legais, bem como às crescentes pressões competitivas e do cumprimento da legislação de proteção de dados (Stelzer *et al.,* 2019).

> A LGPD não torna impossível gerir dados, tampouco oferece riscos à inovação, pelo contrário, ela promove e determina mecanismos de controle e proteção do núcleo duro dos direitos fundamentais dos indivíduos. As providências da LGPD são incisivas e merecedoras de todo o zelo por parte das IES, pois existe um grande desafio e um impacto para as IES em prol da adequação à emergente proteção. A LGPD é um reflexo do cuidado que se deve ter com a dignidade da pessoa humana e seu respectivo direito, seja de natureza material, moral, espiritual, seja, mesmo, informacional (Stelzer, 2019).

Stelzer *et al*. (2019) sugerem que as IES terão que se adequar jurídica, metodológica e tecnologicamente para sustentar os direitos dos titulares dos dados:

> As IES poderão sofrer sanções se não estiverem em conformidade com a LGPD, tanto sanções administrativas – aplicadas pela Autoridade Nacional de Proteção de Dados, que pode se limitar à simples advertência – quanto a uma multa de até 2% do faturamento anual (BRASIL, 2019). Diante disso, as IES deverão focar seus esforços no mapeamento dos dados pessoais, verificando os riscos de maior grau de impacto e possibilidade de ocorrência de incidentes, para os de menores riscos, sucessivamente (Stelzer *et al.*, 2019).

A LGPD define a forma de tratamento de dados organizacionais, assim como destaca Silva (2020): "o tratamento de dados pessoais e as normas dispostas à LGPD estão diretamente atrelados às atividades das instituições de ensino, assim como de qualquer empresa, e devem ser objeto de adequação" (Silva, 2020, p. 44).

De acordo com Silva (2020), as instituições de ensino obtêm, de seus contratantes, dados pessoais e sensíveis, não necessariamente imprescindíveis ao ato contratual (p. ex.: origem étnica/racial de seus alunos; crenças religiosas, dentre outras informações) que relacionam o resultado de avaliações com o desempenho acadêmico do aluno, relatórios que podem rotular, identificar o aluno ou torná-lo identificável. Tais dados, portanto, devem ser exclusivamente direcionados ao aluno e aos seus responsáveis legais (Silva, 2020, p. 41).

Silva (2020, p.61) recomenda que para propriciar um processo de adequação mais eficiente é importante que as IES identifiquem, na análise inicial do ambiente, se há falhas ou deficiências em processos organizacionais; se a organização está aderente à lei (*compliance)*; ou ainda, e se a TI está aderente ao negócio e em que medida.

Para solucionar possíveis problemas, como os descritos acima, Silva (2020) sugere maior grau de adesão da IES à Governança de TI e propõe um *framework* orientado por Governança de TI, Controles Internos, Gestão de Riscos e a própria LGPD, com o objetivo de auxiliar no processo de entendimento e adequação à legislação que se impõe e, ainda, de contribuir para a melhoria dos níveis atuais de Governança de TI (Silva, 2020, p. 61).

A pesquisa de Queiroz (2021) apresentou as dificuldades práticas enfrentadas pelos encarregados de proteção de dados pessoais em exercício no Brasil, as quais podem

ser amenizadas ou, até mesmo sanadas, com a regulamentação da profissão:

- Eles acumulam a função de DPO às demais e não há equipe específica para o exercício da função. As razões para a contratação de terceiros para essa função é a inexistência de funcionários para atuar nesse cargo.
- Dificuldade relacionada aos conhecimentos específicos necessários para o exercício da função. A legislação não aponta quais são os requisitos necessários para atuar nessa função. Os encarregados nomeados não possuem conhecimento específico no tema, o que, inclusive, é o outro argumento que motiva a contratação externa e, ou, treinamentos especializados para capacitação de colaboradores.
- Todos os entrevistados possuem tarefas adicionais, entre as quais se destacam o monitoramento das conformidades das atividades de tratamento de dados pessoais com a regulamentação e normas vigentes, bem como editar diretrizes dos planos de adequação.
- Há pontos indispensáveis a serem trabalhados na regulamentação, como por exemplo, aqueles relacionados ao melhor esclarecimento das tarefas a serem exercidas pelos DPO's e aos conhecimentos específicos necessários (Queiroz, 2021, p. 85).

Neste contexto, Barbosa *et al.* (2021, p. 6), aduzem que

> Evidencia-se que a LGPD confere especial atenção e importância ao tratamento de dados pelo Poder Público. Desse modo, evidentemente, as instituições públicas de ensino não estão isentas de adequar-se ao regramento posto. 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.

As organizações brasileiras buscam a adaptação à LGPD, utilizando-se de 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 (conformidade). Isto é, o tratamento dos dados pessoais deve estar sujeito à *compliance* e os processos devem ser aderentes às normativas que a LGPD dispõe (Burkart, 2021).

> Para garantir o cumprimento e conformidade ao regramento vigente, as instituições públicas de ensino precisarão realizar adequações jurídicas e, de igual modo imprescindíveis, adaptações tecnológicas, uma vez que os dados devem permanecer, em sua maioria, armazenados em meio digital. A LGPD preocupou-se em garantir que o tratamento dos dados prime pela segurança, evitando invasões, acidentes, acessos criminosos que ocasionem a exclusão, perda, modificação, comunicação ou outra ação de tratamento indevido ou ilegal. As organizações, obrigatoriamente, deverão adotar medidas técnicas e administrativas capazes de proteger os dados pessoais, procedendo à análise e à revisão dos sistemas informacionais de tratamento de dados, objetivando robustecer os mecanismos de proteção e mitigar possíveis riscos. Outro desafio consiste na definição de um grupo responsável pelo trabalho de adequação da

> instituição à LGPD. Esta equipe deverá gerir todo o processo de adequação, partindo, a priori, do mapeamento dos processos e sistemas que operam e armazenam os dados pessoais e, ou, dados pessoais sensíveis. Reafirma-se que, sem tal mapeamento, torna-se impossível decidir acerca dos critérios a serem adotados para proteção dos dados pessoais manipulados pela instituição de ensino (Barbosa *et al.*, 2021).

Nessa mesma linha, Pereira e Stakoviak (2022) afirmam que, no processo de implementação da LGPD nas IES, deve-se realizar uma análise da conformidade de dados pessoais acadêmicos e outros dados pessoais de natureza diversa, pois eles não estão necessariamente relacionados somente com as atividades acadêmicas (Pereira; Stakoviak, 2022, p. 177).

Pereira e Stakoviak (2022) afirmam que "todos os dados pessoais sensíveis relacionados a dados acadêmicos devem ser analisados para separá-los e estabelecer um tratamento adequado para que as instituições de ensino não tenham problemas com o uso desses dados." 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; Stakoviak, 2022, p. 178).

Dessa maneira, Gomes, Cunha e Luccas (2023) afirmam que as IES podem atuar em diversas áreas além do Ensino, como Pesquisa e Consultoria Técnica. "Desse modo, pode ser conveniente tratar, separadamente, o processo de adequação em cada uma dessas diferentes áreas". Esses autores propõem a criação de categorias de dados e informações para sanar problemas durante o processo de adequação à LGPD (Gomes; Cunha; Luccas, 2023, p. 407).

> Em primeiro lugar, uma vez realizado o mapeamento, há a preocupação de determinar quais processos de tratamento serão considerados como pertinentes à área de Ensino. Pode-se dizer que os tratamentos pertinentes à área de Ensino são aqueles realizados pela IES como preliminares à prestação de serviços acadêmicos, como forma de prestar os serviços propriamente ou, ainda, como decorrência, jurídica ou não, de tal prestação. A criação das categorias serviu para operacionalizar a aplicação dessa definição a operações de tratamento concretas. [...]
>
> Em segundo lugar, uma vez identificados os processos de tratamento relevantes para a área de Ensino, deve-se organizar a apresentação das recomendações de adequação, de modo que as operações de tratamento de dados possam ser agrupadas e que se identifiquem às recomendações cabíveis (Gomes; Cunha; Luccas, 2023, p. 9).

Gomes, Cunha e Luccas (2023) apresentam, no Quadro 3, uma proposta de modelo de segmentação de dados (classificação) a ser utilizado na implementação da LGPD a das IES. O modelo é simples, porém funcional. O que merece atenção neste modelo refere-se à coleta de dados do aluno ser realizada conforme a sua finalidade, isto é, a coleta do dado

é orientada ao uso e com um fim específico.

Quadro 3 - Exemplo de classificação de dados para implementação

	Interessados	Inscritos	Matriculados	Ex-alunos
Dados coletados	Endereço de *e-mail*, nome.	Dados de identificação pessoal (RG, CPF etc.), dados de contato (endereço residencial, endereço de *e-mail*, número de telefone), dados acadêmicos (currículos, comprovantes de estudos, históricos escolares, cartas de recomendação).	Dados de identificação pessoal (RG, CPF), dados de contato (endereço residencial, endereço de *e-mail*, número de telefone), dados acadêmicos (notas em provas, provas, trabalhos).	Dados de identificação pessoal (RG, CPF), dados de contato (endereço residencial, endereço de e-mail, número de telefone), dados acadêmicos (histórico escolar na instituição, prontuário do aluno), dados sobre desempenho profissional
Finalidade(s)	Propaganda de serviços da IES (cursos, disciplinas).	Organização e realização de exame de seleção. .	Cumprimento de contrato de prestação de serviços educacionais; cumprimento de obrigações legais ou regulatórias. .	Propaganda de serviços da IES; cumprimento de obrigações legais ou regulatórias; fortalecimento de laços institucionais.

Fonte: Gomes, Cunha e Luccas (2023, p. 10).

Destarte, cabe salientar que, para a implementação da LGPD, torna-se necessário que as IES se adequem em sentidos diversos, não apenas tecnológicos, mas, principalmente, em governança, gestão, processos, controles, pessoas. O aparato tecnológico é um alicerce para a adequação da LGPD, tal como foi destacado por Gomes, Cunha e Luccas (2023), além de outros autores e pesquisadores citados ao longo do texto.

Observa-se que o processo da adequação da LGPD, nas IES, é uma atividade em desenvolvimento, possivelmente pelas seguintes razões: - entrada em vigor da LGPD há apenas três anos, os quais foram ocupados por uma pandemia severa e interruptiva; - a própria complexidade da lei e seus inúmeros controles; - a dimensão corporativa que ela atinge, ou seja, o todo organizacional; - a ausência de profissionais especializados (técnicos e administrativos), com domínio sobre a lei, dentre outros ferramentais para alavancar e acelerar a adequação da LGPD

Diante deste cenário, vale destacar que os processos de governança são tão essenciais quanto os demais. A governança ampara os processos organizacionais,

atribuindo-lhes padrões e rigor, que, por sua vez, contribuem sobremaneira para o processo de recepção da LGPD nas IES.

2.6 Governança corporativa

No cenário internacional, a discussão sobre governança corporativa iniciou-se na década de trinta, com os clássicos Berle e Means, que publicaram em 1932, porém, na década de oitenta, o tema ganha relevância perante as organizações (Gonçalves, 2012, p. 1-13). Na academia científica, somente a partir de 1980 é que tal abordagem passou a ser estudada com maior intensidade, ou seja, o tema é relativamente recente num contexto geral (Sirqueira, 2007, p. 14).

Segundo o Banco Mundial (1992), a governança corporativa (GC) é "o exercício da autoridade, controle, administração e poder de governo". De acordo com a Fundação Dom Cabral - FDC (2021), *apud* Gonçalves *et al.* (2016, p. 56), GC é "o 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" (Gonçalves *et al.*, 2016, p. 56).

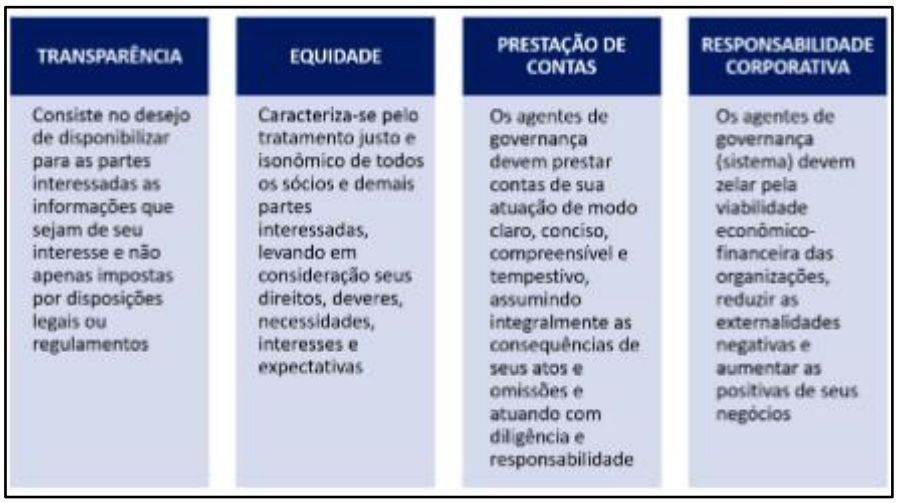
A Figura 3 apresenta os quatro princípios da governança corporativa, conforme definição do Instituto Brasileiro de Governança Corporativa. Os quatro pilares são: Transparência, Equidade, Prestação de Contas e Responsabilidade Corporativa.

Transparência significa que as informações corporativas devem ser disponibilizadas de forma clara e objetiva aos *stakeholders* (reservado o sigilo das informações confidenciais) e demais interessados. A Equidade deve ser buscada pelas organizações no sentido de atribuir um tratamento igualitário a todos, colaboradores, *stakeholders*, e outros interessados.

Quanto à Prestação de Contas (termo também utilizado na literatura como *Accontability*), ela se refere à responsabilidade da organização no cumprimento legal de seus deveres e obrigações, não se eximindo da veracidade e responsabilidade junto aos seus *stakeholders* e a comunidade em geral.

O quarto e último princípio é a Responsabilidade Corporativa, indicando que as organizações devem atuar de forma colaborativa e responsável para com os demais agentes e ambientes intra- e extraorganizacionais. Na literatura atual, utiliza-se o termo *Environmental, Social and Governance* - ESG, ou seja, as organizações devem estar com consonância com o meio-ambiente, com as questões sociais e as de governança (IBGC, 2019).

Figura 3 - Princípios da Governança Corporativa



Fonte: IBGC (2021, p. 21).

Organizações, como IBM e Gartner, possuem modelos de governança que geram benefícios diretos, como qualidade e segurança das informações, conforme afirmam Sonza e Kloeckner (2014). Nesse sentido, pode-se compreender que a boa governança é um ambiente no qual as pessoas procuram cumprir com as regras estabelecidas, por meio da tomada de decisões no melhor interesse coletivo, em conformidade com a ética e os princípios organizacionais (IBGC, 2019).

A GC, em conjunto com a GTI, possibilita que o gestor de TI possa maximizar o uso da TI, aumentando a eficiência, reduzindo custos e riscos associados ao seu uso, propiciando o cumprimento de suas obrigações organizacionais de maneira transparente e contribuindo, portanto, para o bom desempenho das organizações (ABNT, 2009).

Existem diversos modelos de GC consolidados no mercado (COSO, BSC, ISO 9001, TOGAF, dentre outros)[3] que podem auxiliar as organizações em seu processo de gestão. Cabe ao gestor verificar qual(is) modelo(s) e, ou, norma(s) é(são) apropriado(s) a ela. A adoção de um único modelo ou de alguns modelos, em conjunto, de forma concomitante e, ou, combinada entre eles, é uma decisão que compete à alta gestão da organização, conforme as suas necessidades e prioridades. Vale destacar que os modelos não são excludentes entre si, mas complementares (Giampaoli, 2010, p.14).

[3] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Balance Scorecard (BSC), International Organization for Standardization (ISO) 9001, The Open Group Architecture Framework (TOGAF).

2.7 Governança em Tecnologia da Informação – normas e *frameworks*

A Governança de Tecnologia da Informação 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).

> Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e a utilizam para direcionar os valores das partes interessadas no negócio. Essas organizações também entendem e gerenciam os riscos associados, tais como as crescentes demandas regulatórias e a dependência crítica de muitos processos de negócios da TI (Gonçalves *et al.*, 2016, p. 58).

Weill e Ross (2006) definem a Governança da TI como "o estabelecimento dos direitos de decisão e da matriz de responsabilidades para encorajar comportamentos desejáveis no uso da TI" (Weill; Ross, 2006, p. 14). Estes autores, em 2006, defendem um modelo de GTI com objetivo de tornar o processo de gestão e administração dos ativos de TI uma forma estratégica, integrada aos negócios e aos próprios objetivos da empresa (Weill; Ross, 2006).

O Quadro 4 apresenta uma relação de definições sobre GTI, segmentado por áreas de foco, com as respectivas referências bibliográficas. São conceitos afins a um dos principais constructos desta pesquisa, "governança de tecnologia da informação – GTI". Os autores ali referenciados, em seu entendimento, apresentam variações na definição, apesar das semelhanças entre si. Às vezes, em algumas, há uma diferença apresentada na forma de escrever ou de se definir o conceito; em outras, há acréscimo ou decréscimo de atividades/responsabilidades da GTI.

A GTI tem, como principal objetivo, estabelecer o vínculo entre as organizações e a TI. Para o seu bom funcionamento, tanto a estratégia de TI quanto a de negócios devem estar muito bem alinhadas e sincronizadas, facilitando, assim, que as organizações atinjam seus objetivos de negócio. O seu uso torna-se vital para que as organizações obtenham um desempenho satisfatório, impactando de forma positiva a consecução dos objetivos, metas e estratégias organizacionais (ITGI, 2007).

Quadro 4 - Definições sobre GTI

Definição	Foco	Referência

As organizações de Governança representam padrões de autoridade relacionados à TI de uma organização, para direcionar, controlar e coordenar a gestão da infraestrutura da TI, gerenciamento do uso da TI e gerenciamento dos projetos. São os padrões de autoridade para atividades-chave da TI em empresas de negócio, incluindo a infraestrutura de TI, seu uso e o gerenciamento dos projetos.	• Estrutura de decisão • Padrões de autoridade sobre os principais recursos da TI • Ênfase nos recursos da TI	Sambamurthy; Zmud (1999, p. 261)
São as estruturas ou arquiteturas relacionadas à TI, associadas a padrões de autoridade, implementadas para viabilizar com sucesso (os imperativos de TI) as atividades em resposta a imperativos estratégicos e ambientais de umaempresa.	• Estrutura de decisão	Sambamurthy; Zmud (1999, p. 261)
É o sistema pelo qual o portfólio de TI de uma organização é direcionado e controlado. A Governança de TI descreve: i) a distribuição de direitos e responsabilidades na tomada de decisões de TI entre os diferentes envolvidos na organização; e ii) as regras e procedimentos para a execução e monitoramento das decisões dos interesses estratégicos da TI.	• Estrutura de decisão • Conjunto de processos • Ênfase em controle	Peterson (2004, p. 41)
É a capacidade organizacional exercida pelo alto escalão, gestores de negócios e gestores de TI, para controlar a formulação e a implantação da estratégia de TI, garantindo a fusão entre o negócio e a TI.	• Estrutura de decisão • Conjunto de processos • Competência organizacional	Van Grembergen *et al*. (2004, p. 5)
É o termo utilizado para descrever como as pessoas encarregadas da governança de uma organização consideram a TI nas suas atribuições de supervisionar, monitorar, controlar e dirigir a empresa.	• Conjunto de processos	Roussey (*apud* Information Technology Governance Institute (2003))
É o sistema pelo qual a TI nas empresas é dirigida e controlada. A estrutura de Governança de TI especifica a distribuição de direitos e responsabilidades entre diferentes participantes, como o alto escalão, o negócio e os gestores de TI, e dita as regras e procedimentos para a tomada de decisões em TI. Por meio disso, também provê a estrutura para definir os objetivos da TI, os meios para alcançar estes objetivos e para monitorar seu desempenho.	• Estrutura de decisão • Conjunto de processos • Relacionamento entre diversos atores	Brand; Boonen (2004, p. 16)
Tem tudo a ver com políticas e procedimentos que determinam como uma organização direciona e controla o uso de seus recursos tecnológicos, de forma que esses recursos possam facilitar, de forma adequada, a realização dos objetivos de negócio.	• Conjunto de processos • Ênfase nos recursos da TI	Posthumusa; Solms (2004)
É responsabilidade do alto escalão executivo e uma parte integral da Governança Corporativa. Consiste em liderança, estruturas organizacionais e processos que garantam que a organização de TI sustente e amplie sua	• Estrutura de decisão • Conjunto de processos • Visão estratégica da Governança de TI	Information Technology Governance Institute (2003, p. 10)

estratégia e os objetivos da organização.		
É como a empresa governa a TI para garantir desempenho satisfatório.	• Visão estratégica da Governança de TI	Rau (2004)
É o estabelecimento dos direitos de decisão e da matriz de responsabilidades para encorajar comportamentos desejáveis no uso da TI.	• Estrutura de decisão • Relação com a cultura organizacional	Weill; Woodham (2002, p. 1); Weill; Ross (2004a, p. 1)
A definição está relacionada ao processo de decisão em TI sobre certos ativos: *hardware,software*, processos, pessoal e objetivos estratégicos.	• Estrutura de decisão • Ênfase nos recursos da TI	Simonsson; Johnson (2006, p.)
Governança Corporativa de Tecnologias da Informação e Comunicação (TIC) é o sistema pelo qual o uso atual e futuro das TIC's é dirigido e controlado. Trata-se de avaliar e orientar os planos de utilização das TIC's para apoiar a organização e acompanhar este uso para atingir planos. Inclui a estratégia e as políticas para o uso das TIC dentro de uma organização.	• Conjunto de processos • Visão estratégicada Governança de TI	Australian Standard (2010)

Fonte: Assis (2011, p. 46).

A Governança de TI auxilia a tomada de melhores decisões por parte das organizações e contribui para a própria alavancagem dos negócios (Albertin; Albertin, 2010). Permite maior agilidade nas transações e maior precisão nas operações e, somado a isso, oferece ao cliente/consumidor processos mais transparentes, ágeis e íntegros, segundo Albertin e Albertin (2010). Por outro lado, a governança de TI é um processo lento e caro, pois necessita de um aparato tecnológico (infraestrutura de *hardware* e *software*) e recursos humanos especializados (Albertin; Albertin, 2010).

A GTI promove inúmeros benefícios e, entre eles, um importante atrativo é a vantagem competitiva para a organização, desde que os recursos (financeiros e humanos) sejam geridos de forma eficiente (Schiavon *et al*., 2010). Dessa forma, ela deve: a) agregar valor; b) ajudar a empresa na proteção de integridade de um produto raro que ela venha a comercializar; c) auxiliar a empresa na proteção da integridade das informações de um produto difícil de ser imitado; d) auxiliar a empresa na proteção da integridade das informações de um produto insubstituível (Schiavon *et al*., 2010).

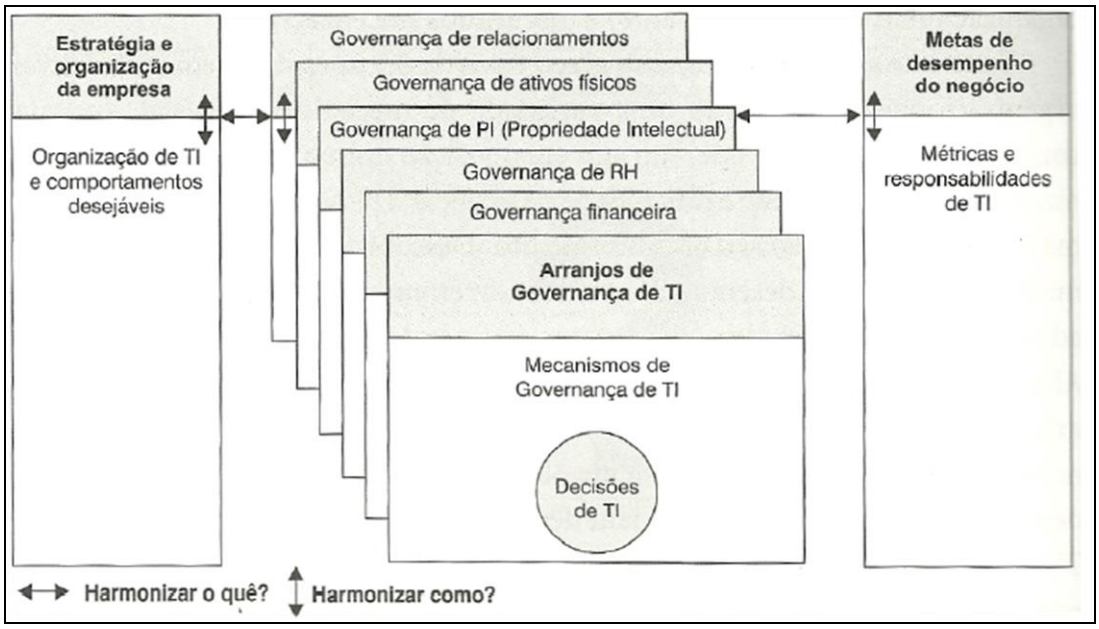
A norma *ABNT NBR ISO/IEC 38.500/2018* fornece princípios, definições e um modelo para estruturas de governança utilizarem ao avaliarem, direcionarem e monitorarem o uso de tecnologia da informação (TI) em suas organizações. Fornece também uma ampla orientação

sobre o papel de uma estrutura de governança. A norma fornece princípios, definições e um modelo para a boa governança da TI, de forma a ajudar as organizações a entenderem e cumprirem suas obrigações legais, regulamentares e éticas em relação ao uso de TI (ABNT, 2018).

Considerando que os custos de TI são elevados, além de a mão de obra especializada ser concorrida, e até mesmo escassa, sobreveio a necessidade de gerir tais recursos e custos de forma racional e otimizada. Carr (2003) questiona o papel da TI, ao afirmar que a relação custo x benefício não é proporcional (Carr, 2003).

A Figura 4 apresenta o esquema de GTI proposto por Weill e Ross (2006). Nela é possível perceber a divisão da governança em três grandes grupos: a) Estratégia e organização da empresa; b) Governança em camadas; c) Metas de desempenho do negócio. Vale salientar que o foco do modelo centra-se nas camadas de governança estabelecidas pelos autores e que esses elementos são uma proposta. Cada organização deve avaliar quais serão as camadas a serem adotadas em sua organização, conforme o seu modelo de negócio. Um dos pontos principais propostos por eles referem-se à harmonização da TI aos negócios, mensurados por meio de metas e de métricas estabelecidas para avaliar o desempenho. Em resumo, eles propõem a GTI como um mecanismo de integração das atividades organizacionais para obtenção de estratégias corporativas.

Figura 4 - Framework de GTI



Fonte: Weill e Ross (2006, p. 10).

Um desafio importante para gestores é

> Gerenciar a informatização da organização de forma consistente e coerente, garantindo o alinhamento com a estratégia empresarial e a evolução conjunta dos modelos de organização e gestão. A construção do futuro da tecnologia não é apenas fruto do avanço da tecnologia, mas de seu emprego como agente de transformação dos negócios (Meirelles, 2004, p.11).

A implementação da GTI, para as organizações, é um grande desafio, de grande importância, pois facilita que as estratégias de negócio sejam mais facilmente atendidas (suportados pelas TICs), de forma a gerar valor e ser um diferencial competitivo para elas. A entrega de valor da TI deve estar em conformidade e sintonia com a estratégia corporativa. O meio para se alcançar este resultado é o emprego da GTI (ITGI, 2007).

Weill e Ross (2006) apresentam os seguintes objetivos para avaliar a eficácia da GTI dentro da organização:

- Uso da TI com boa relação custo/benefício;
- Uso eficaz da TI para utilização de ativos;
- Uso eficaz da TI para o crescimento;
- Uso eficaz da TI para a flexibilidade dos negócios.

Fernandes e Abreu (2012) ensinam que são necessárias medições e indicadores de desempenho para verificar o nível de maturidade da GTI. Deve-se avaliar a governança por dois aspectos: primeiro, pelo resultado da TI, em que se medem os indicadores de gerenciamento de processos e serviços; segundo, verifica-se o resultado da TI para o negócio (agregação de valor) (Fernandes; Abreu, 2012). Conforme Cavalcanti Filho (2011), a GTI tem um papel contributivo para o crescimento dos negócios, de uma forma estruturada, nas organizações, e, por via de consequência, para o alcance de melhores resultados. Entende-se que “as TICs têm papel fundamental para alavancar a expansão estruturada da educação superior no Brasil” (Cavalcanti Filho, 2011, p. 17).

O Quadro 5 apresenta as estruturas (Normas, modelos e *frameworks)* de GTI mais utilizadas pelas empresas, segundo o *Information Technology Service Management Forum* – ITSMF (ITSMF, 2023). Nele, está elencada também a lista de tipo, fonte e objetivo. Na coluna tipo, encontramos os termos *Framework* e Norma. A diferença reside em que as normas são publicadas por organismos nacionais e internacionais e são, em tese, um padrão definido por entidades reconhecidas pelos Governos. *Frameworks* são modelos definidos por empresas e largamente utilizados no mercado corporativo sem aval ou respaldo legal. Eles são práticas de mercado testadas e consolidadas.

Quadro 5 - Normas e Frameworks mais utilizados para a governança de TI no Brasil

#	Descrição	Tipo	Fonte	Objetivo
1	COBIT (*Control Objetives for Information and Related Technology*)	*Framework*	ISACA	Direcionada ao controle do negócio. Alinhamento dos serviços de TI aos negócios
2	ITIL V4 (*Information Technology Infraestructure Library*)	*Framework*	CCTA / AXELOS (Atual)	Gerenciamento de serviços e ativos de TI
3	ABNT NBR ISO/IEC 38.500	Norma	NBR-ISO	Governança de TI
4	ABNT NBR ISO/IEC 20.000	Norma	NBR-ISO	Gerenciamento de Serviços de TI
5	ABNT NBR ISO/IEC 27.000	Norma	NBR-ISO	Segurança da Informação
6	ABNT NBR ISO/IEC 31.000	Norma	NBR-ISO	Gerenciamento de Riscos
7	Val-IT (*Entreprise Value – Governance of IT Investiments*)	*Framework*	*IT Governance Institute*	Gestão de portifólio de investimentos em TI
8	Risk-IT (*Enterprise Risk Identify – Govern and IT risks*)	*Framework*	ISACA	Gerenciamento de riscos em TI
9	Seis Sigma	*Framework*	Motorola	Melhorar a qualidade de gerenciamento de processos
10	TOGAF (*The Open Group Archtitecture Framework*)	*Framework*	The Open Group	Gestão de arquitetura de TI
11	CMMI (*Capability Maturity Model Integration*)	*Framework*	Software Engineering Institute	Utilizado para desenvolvimento de software

Fonte: Adaptado do ITSMF (2023).

Há outros modelos, *frameworks* e normas de GTI, além daqueles apresentados no Quadro 3, inclusive modelos proprietários (desenvolvidos e customizados para uma determinada organização). Por razão de delimitação de escopo, apenas os *frameworks* COBIT, ITIL e a norma *ABNT NBR ISO/IEC 38.500/2018* serão explorados com maior profundidade.

Vale destacar que os modelos relacionados no Quadro 3 podem ser utilizados em conjunto ou não. Com a combinação entre eles, pode-se obter maior segurança e resultados assertivos na governança e gestão da TI corporativa. Porém, o custo será mais elevado, o que pode inviabilizar a adoção de mais de um modelo, concomitantemente.

No tocante ao uso da GTI e as tecnologias associadas a ela, bem como a sua relação com a LGPD, Queiroz (2021) aponta, em sua tese de doutoramento, que

> 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, com a transformação do indivíduo em mercadoria. Assim, indispensável se faz a legislação da proteção dos dados pessoais (Queiroz, 2021).

2.7.1 Norma ABNT NBR ISO/IEC 38.500/2018 – Governança de TI

A *NBR ISO/IEC 38500/2018 – Governança de TI* fornece princípios com o objetivo de orientar os membros das organizações responsáveis pela governança de TI (que pode incluir os proprietários, diretores, sócios, gerentes executivos, ou similares) sobre o uso eficaz, eficiente e aceitável de tecnologia da informação em suas organizações (ABNT, 2018).

A NBR ISO/IEC 38500:2018 aplica-se ao uso atual e futuro da organização de TI, incluindo processos e decisões relacionadas com o uso atual e futuro do gerenciamento de TI. Estes processos podem ser controlados por especialistas de TI da organização, prestadores de serviços externos, ou unidades de negócios da organização e definem a governança de TI como um subconjunto ou domínio da governança organizacional ou corporativa (ABNT, 2018).

Segundo a NBR ISO/IEC 38500:2018, a norma se aplica a todas as organizações, empresas públicas ou privadas de todos os tamanhos, independente da extensão do uso da TI, com o principal objetivo de avaliar, orientar e monitorar o emprego da TI nas organizações, para promover o uso eficaz, eficiente e aceitável da TI, buscando assegurar que as partes interessadas tenham conhecimento se os princípios e práticas propostas pelo padrão são seguidos, para assim obterem confiança na governança de TI da organização (ABNT, 2018).

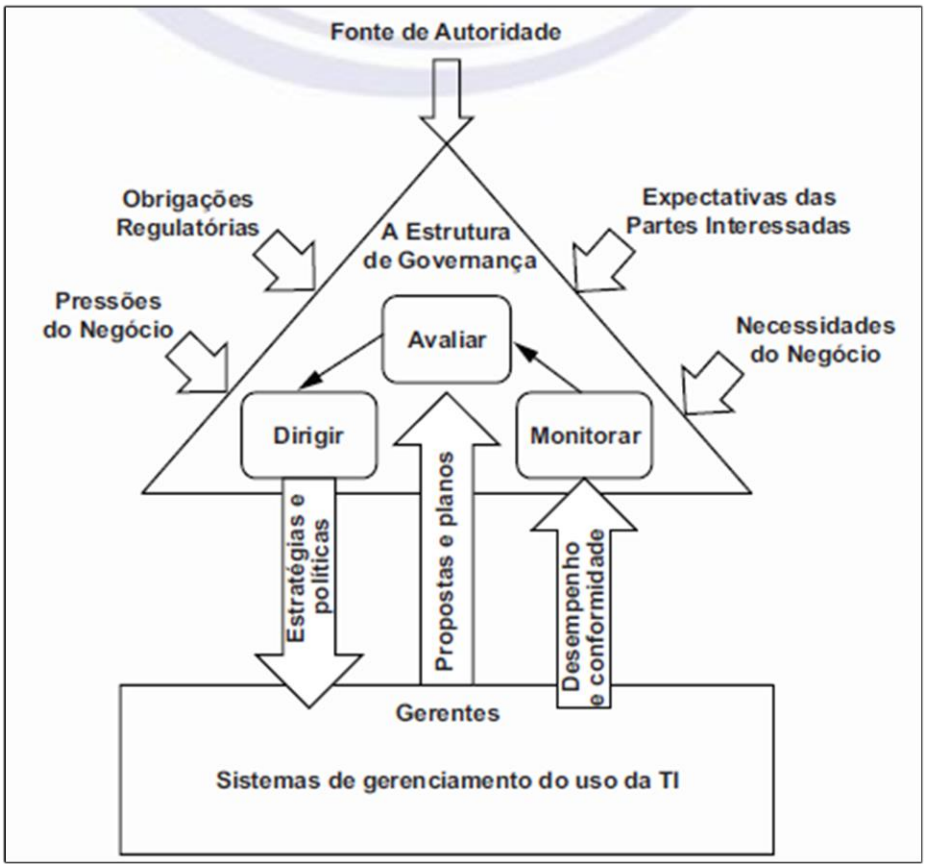
A *NBR ISO/IEC 38500/2018* recomenda seis princípios característicos para uma boa governança de TI:

- Princípio 1 – Responsabilidade: Indivíduos e grupos dentro da organização compreendem e aceitam suas responsabilidades em relação ao fornecimento de e demanda por TI. Aqueles com responsabilidade por ações também têm autoridade para realizar essas ações.
- Princípio 2 – Estratégia: A estratégia de negócios da organização leva em consideração as capacidades atuais e futuras das TI; os planos para o uso da TI atendem às necessidades atuais e contínuas da estratégia de negócios da organização.
- Princípio 3 – Aquisição: As aquisições de TI são feitas por razões válidas, com base em constantes análises apropriadas, com uma tomada de decisão clara e transparente. Existe um equilíbrio adequado entre benefícios, oportunidades, custos e riscos, tanto no curto quanto no longo prazo.
- Princípio 4 – Desempenho: A TI é adequada para apoiar a organização, fornecendo os serviços, os níveis de serviço e a qualidade de serviço necessários para atender aos requisitos atuais e futuros do negócio.

- Princípio 5 – Conformidade: O uso da TI atende a todas as leis e regulamentos obrigatórios. Políticas e práticas são claramente definidas, implementadas e aplicadas.
- Princípio 6 – Comportamento humano – As políticas, práticas e decisões de TI demonstram respeito pelo Comportamento Humano, incluindo as necessidades atuais e necessidades em evolução de todas as "pessoas no processo" (ABNT, 2018).

A Figura 5 demonstra o modelo de governança de TI, segundo a norma ABNT ISO/EIC 38500:2018. De acordo com essa norma, a governança de TI deve ser implementada com base em três tarefas: avaliar, dirigir e monitorar. Para avaliar, os dirigentes responsáveis pela implantação da governança de TI devem examinar o estado atual e futuro da TI, com base nas estratégias definidas pelo negócio. Para dirigir a governança de TI, é importante que os papéis e responsabilidades estejam claros e definidos pelos dirigentes, a fim de que seja estabelecido o direcionamento dos investimentos para implementação dos planos e políticas da governança de TI.

Figura 5 - Modelo de Governança NBR para TI



Fonte: ABNT NBR ISO/IEC 38500/2018 (2018, p. 7).

O monitoramento deve ser realizado pelos dirigentes, verificando se o desempenho da TI está alinhado com os objetivos do negócio e em conformidade com a legislação e regulamentos obrigatórios (Fernandes; Abreu, 2012).

2.7.2 Norma ABNT NBR ISO/IEC 27701:2019 – Sistema de Gestão da Privacidade da Informação

A norma ABNT NBR ISO/IEC 27701/2019 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 ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

Entende-se que essa norma é complementar às normas ISO/Série 27.000 “Segurança da Informação”, que fornecem diretrizes e requisitos para que os controladores e operadores de

dados pessoais[4] (DP), possam assumir responsabilidade direta pelo tratamento de DP da organização. Ela, por ser específica para proteção de dados, fornece uma estrutura que auxilia na implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação - SGPI (ABNT, 2019).

2.7.3 Framework COBIT

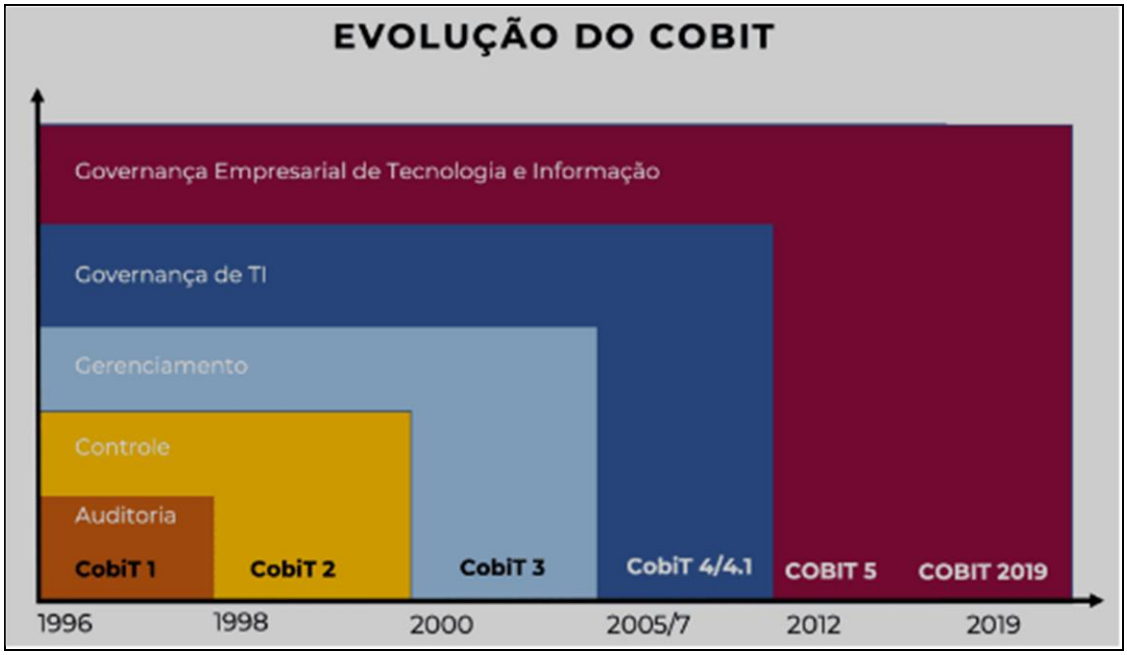
O *framework* COBIT foi criado, em 1994, pelo ISACA (uma organização independente e sem fins lucrativos), com o propósito específico de fornecer boas práticas de controle de TI, bem como otimizar os investimentos nessa área, além de propiciar a entrega de serviços conforme planejado. Este *framework*, de forma geral, auxilia o processo de governança de TI, facilitando o alinhamento dela aos objetivos organizacionais. Em síntese, o *framework* COBIT é um modelo corporativo de boas práticas, para governança e gestão de TI de uma organização (ISACA, 2019).

A Figura 6 apresenta a evolução do *framework* COBIT ao longo do tempo. Os modelos são aprimorados pelas suas entidades mantenedoras, conforme evolução do mercado. Não há um prazo ou ciclo de tempo estabelecido para que ocorram modificações. O *framework* é utilizado pelas organizações ao redor do mundo, as quais podem se relacionar com a mantenedora do modelo, fornecendo propostas de melhorias e adaptações por diversas razões (legais e, ou, tecnológicas) (ITGI, 2007).

Nesta figura 6 é possível perceber que o modelo (*framework*) COBIT possui quase trinta anos de existência e já passou por seis atualizações, sendo a versão atual a de 2019. O objetivo desse modelo foi crescente ao longo do tempo, assim como as necessidades de controle organizacionais. Em 1996, o foco era a Auditoria; em 1998, Controle; em 2000, Gerenciamento; em 2005 e 2007, Governança de TI; em 2012, e até o momento, o foco deste modelo é a Governança Empresarial de TI.

[4] O termo "*Personally Identifiable Information* (PII)" foi traduzido para dados pessoais (DP) na literatura. A expressão *dados pessoais* é de uso corrente, no Brasil, e sua adoção foi feita pela lei brasileira que trata de privacidade e proteção de dados pessoais (Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD).

Figura 6 - Evolução do COBIT no período de 1996 a 2019



Fonte: Moreira Neto *et al.* (2019, p. 29).

A Figura 7 apresenta os princípios fundamentais do *framework* COBIT 2019 (versão do *framework* em vigência). Percebe-se, através dos seis princípios (círculos), que o modelo possibilita tratar pontos relevantes e inerentes a uma grande parte das organizações, como a integração de suas estruturas de negócio, o envolvimento das partes, abordagem distinta entre governança e gerenciamento, enfoque nas necessidades de a corporação possuir uma visão do todo organizacional. Além dos fundamentos apresentados na Figura 7, o diferencial desse modelo reside na possibilidade de adaptação (customização) da solução junto à organização, bem como na utilização em conjunto com a governança corporativa (COBIT, 2019).

Figura 7 - Sistema de Governança do COBIT 19

Fonte: Isaca (2019. p.10).

O COBIT possui uma estrutura bem definida e estruturada (dividida em princípio, processos, objetivos de controle, mapas e ferramentas), para que as organizações consigam

estabelecer controles na TI, de forma que ela possa gerar valor para aquelas organizações (ISACA, 2019). Devido à complexidade e extensão deste *framework*, a presente pesquisa não foi direcionada para a exploração da totalidade dos *frameworks* e modelos de GTI. Assim, será apresentado, a seguir, o Sistema de Governança do COBIT com seus princípios fundamentais:

I) Fornecer valor às partes interessadas (*stakeholders*)

Organizações existem para criar valor para suas partes interessadas, mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 19 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor, para a organização, com o uso de TI. Como cada organização tem objetivos diferentes, o COBIT 19 pode ser personalizado, de forma a adequá-lo ao seu próprio contexto, por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos (ISACA, 2019).

II) Sistema de governança de ponta a ponta

O COBIT 19 faz a integração da GTI da organização à governança corporativa:

- Cobre todas as funções e processos corporativos; O COBIT 19 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização.
- Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização (ISACA, 2019).

III) Sistema dinâmico de governança

Há muitas normas e boas práticas relacionadas a TI, cada qual provendo orientações para um conjunto específico de atividades de TI. O COBIT 19 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como um modelo unificado para a governança e gestão de TI da organização (ISACA, 2019).

IV) Possibilitar uma abordagem holística

A governança e gestão eficiente e eficaz da TI de uma organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 (versão anterior, porém utilizada em algumas organizações) define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos. O modelo do COBIT 5 definia sete categorias de habilitadores:

- Princípios, políticas e modelos são recursos utilizados para orientar e direcionar os comportamentos dos colaboradores da organização, bem como seus parceiros de negócio e demais *stakeholders*.
- Processos (conjunto de atividades e práticas) são documentos e ações documentadas com objetivo de padronizar as operações e ações corporativas, visando a atingir os objetivos determinados pela alta gestão da organização.
- Estruturas organizacionais (variáveis conforme o modelo organizacional) são as unidades de negócios da organização. Nelas são realizadas as atividades corporativas, conforme objetivos e metas estabelecidos pela gestão.
- Cultura, ética e comportamento: estes elementos são a essência da organização, a sua forma de atuar e agir para com os seus colaboradores, parceiros e demais *stakeholders* envolvidos em alguma relação com ela. Pressupõe-se um comportamento apropriado e justo no comportamento de seu todo, núcleo e partes.
- Informação são os dados com sentido para a organização. São dados coletados, processados e atribuídos a um elemento informacional. É um recurso-chave para as organizações em que se exigem formas de tratamento diferenciadas para o sucesso organizacional.
- Serviços, infraestrutura e aplicações são o suporte para a operação da organização, como sistemas de informação ou aplicações para um determinado fim; são a estrutura computacional que suporta determinadas aplicações e, por fim, a prestação de serviços da organização.
- Pessoas, habilidades e competências, que são pertencentes aos colaboradores e demais envolvidos nos negócios corporativos. São, em última análise, a materialização da organização, pois, através destes elementos, pode-se atingir o propósito e os objetivos finais da organização (ISACA, 2019).

O modelo do COBIT 19 refere-se a esses habilitadores como Fatores de Desenho e Área de Foco, os quais permitem a personalização do Sistema de Governança para a realidade da organização. Os fatores de desenho são: estratégia corporativa, objetivos corporativos, porte da organização, papel da TI, modelo de prestação de serviços da TI, requisitos de *compliance*, entre outros. A Área de Foco tem, como objetivo, definir o componente principal do seu sistema de Governança: se é risco, segurança; DevOps, se é uma pequena ou média empresa (ISACA, 2019).

V) Separar Governança da Gestão

O modelo do COBIT 19 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciados e servem a propósitos diferentes. A visão do COBIT 19 sobre essa importante distinção entre governança e gestão é:

- Governança: A governança garante que as necessidades, as condições e as opções das partes interessadas sejam avaliadas, a fim de determinar os objetivos corporativos acordados e equilibrados; define a direção por meio de priorizações e tomadas de decisão; e fornece monitoramento de desempenho e conformidade com relação aos objetivos estabelecidos.
- Gestão: A gestão é responsável pelas ações de planejar, construir, executar e monitorar as atividades, de acordo com a direção corporativa e definidas pela governança, visando a atingir os objetivos corporativos (ISACA, 2019).

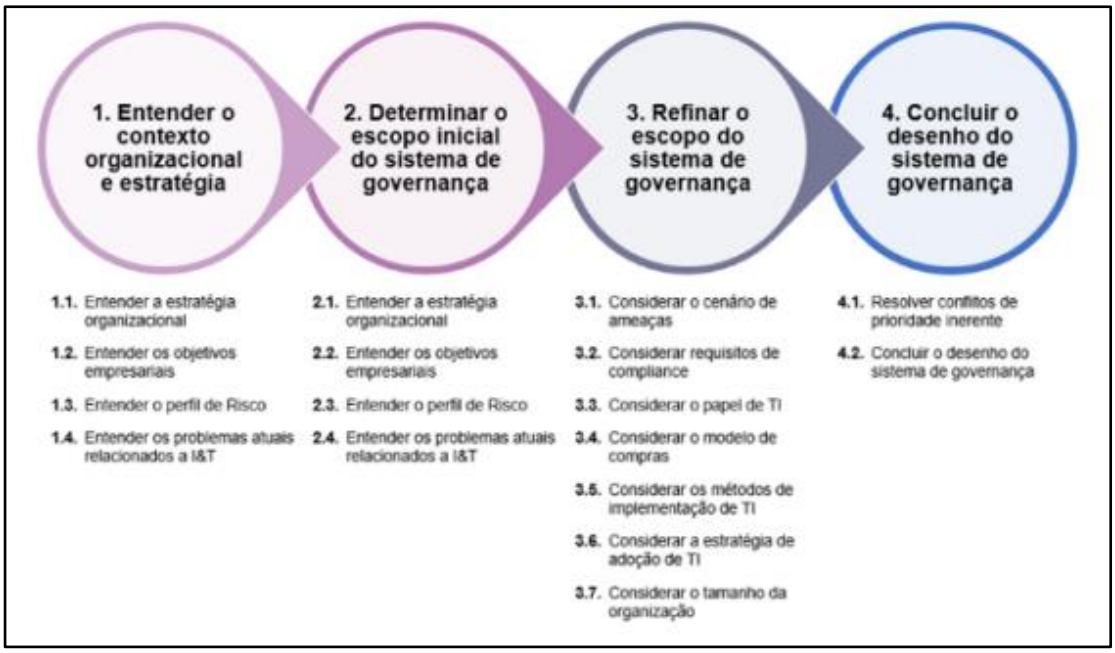
VI) Adaptado às necessidades corporativas

O modelo do COBIT 19 possui flexibilidade na sua estrutura em relação à versão anterior. A organização seleciona os objetivos de gestão antes de sua implementação. Define as necessidades de áreas de foco de forma específica, ou seja, o modelo faz-se adaptável à necessidade da organização. Os contextos, como cenário de ameaças, riscos específicos e a configuração da infraestrutura, são considerados na aplicação do modelo (ISACA, 2019).

A Figura 8 apresenta o fluxo para desenhar um sistema de governança, sob medida, no *framework* COBIT 2019, de forma detalhada. Esta proposta trata-se de uma evolução em relação à versão anterior do COBIT 19. A nova versão é dividida em quatro principais seções: a) Entender o contexto organizacional e a estratégia da organização, b) Determinar o escopo

inicial do sistema de governança, c) Refinar o escopo do sistema de governança, d) Concluir o desenho do sistema de governança. O modelo apresenta, em detalhes, os passos a serem utilizados (1.1 a 4.2) (ISACA, 2019).

Figura 8 - Fluxo para desenhar um sistema de governança sob medida



Fonte: Isaca (2019, p. 25).

2.7.4 Framework ITIL

A Biblioteca de Infraestrutura de Tecnologia da Informação – ITIL (*Information Technology Infrastructure Library)* foi criada pelo governo do Reino Unido a partir da década de oitenta, pelo departamento governamental (CCTA), que, posteriormente, passou a chamar-se Gabinete de Governo do Reino Unido - OGC (Axelos, 2019).

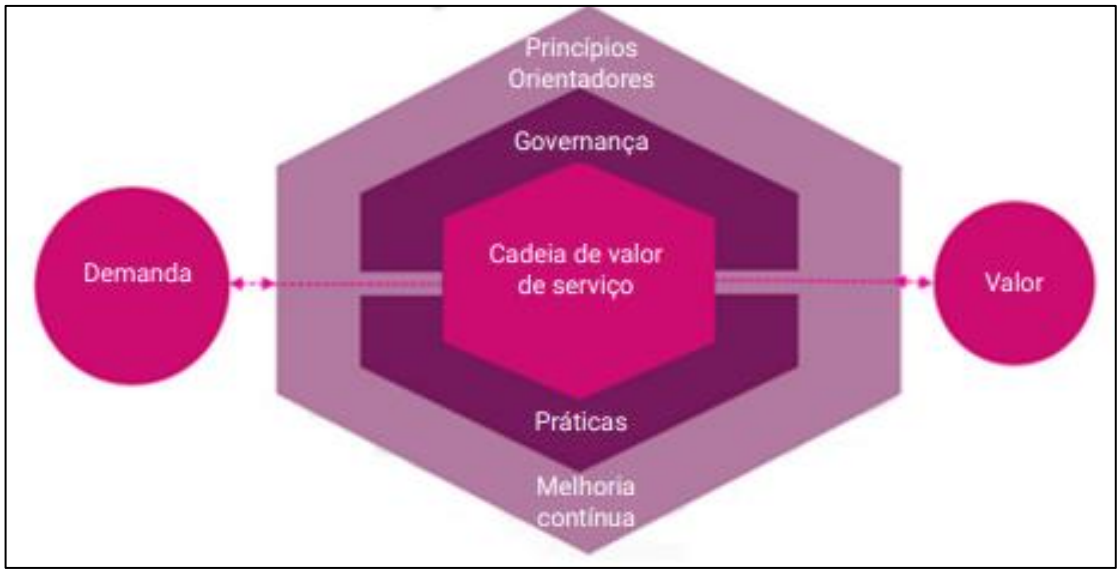
O ITIL 4 é uma estrutura adaptável para gerenciamento de serviços de TI. Por meio de módulos de melhores práticas, o ITIL 4 possibilita otimizar os serviços de TI para cocriar valor para as organizações e impulsionar a estratégia de negócios (Axelos, 2019). O ITIL 4 é uma biblioteca que reúne as melhores práticas de Gestão de Serviços de Tecnologia da Informação (TI). É um conjunto de procedimentos (composto por livros) documentados e padronizados, que permite às organizações gerirem os serviços fornecidos pela TI (Axelos, 2019).

Vale destacar que o ITIL não se refere apenas à infraestrutura especificamente, pois ela aborda também a gestão da TI (como apoio à governança de tecnologia da informação). Ele busca construir, em uma única base de conhecimento, um senso comum sobre boas práticas de

gestão de serviços, que podem ser usadas para auxiliar na administração e gestão da TI de forma eficaz e segura (Axelos, 2023).

A Figura 9 representa as quatro dimensões essenciais no processo de cocriação de valor para clientes e outras partes interessadas do ITIL V4. O objetivo central é a criação de valor (ao centro) para os *stakeholders*, conforme a demanda/oportunidade de negócio. Este *framework* é muito utilizado pelas organizações cujo ramo de negócio é voltado para a prestação de serviços. Ele permite a integração com a governança de TI e corporativa, e possui inúmeros controles que podem gerar aferição da qualidade do serviço prestado, além de promoção da melhoria contínua por meio de suas práticas ou princípios orientadores (Axelos, 2019).

Figura 9 - Estrutura ITIL V4



Fonte: Axelos (2019, p. 18).

As quatro dimensões do ITIL V4 são:

a) Organizações e Pessoas

Determina as funções e responsabilidades dos colaboradores. São essenciais para estabelecer uma organização estruturada, o que influencia a entrega de serviços. Os serviços prestados pela organização devem estar alinhados com as estratégias corporativas, isto é, apoiar seus objetivos e metas. E a sua estrutura funcional é composta por pessoas (funcionários técnicos, não técnicos, equipe administrativa, funcionários de gestão de instalações e segurança), que são os recursos mais importantes de qualquer organização. Logo, para a entrega de serviços contratados, tais colaboradores devem estar alinhados com os propósitos e metas da organização para o bom funcionamento do negócio (Axelos, 2019).

b) Informação e Tecnologia

A dimensão de informação e tecnologia abrange as tecnologias que dão suporte à gestão de serviços, sistemas de gestão de fluxo de trabalho, inventários, bibliotecas, ferramentas analíticas e sistemas de comunicação em uma organização. Além disso, inclui todas as informações criadas, armazenadas, gerenciadas e usadas pela organização durante a entrega de um serviço de TI. Dessa forma, este *framework* contribui para a GTI de forma relevante (Axelos, 2019).

c) Parceiros e Fornecedores

Nenhum ecossistema de gestão de serviços está completo sem os parceiros e fornecedores. Cada organização depende de seus parceiros e fornecedores para a entrega de seus serviços. Essa dimensão da ITIL 4 inclui os relacionamentos de uma organização com outras organizações ou indivíduos que estiverem envolvidos no projeto, desenvolvimento, entrega e suporte de serviços. Essa dependência pode ocorrer em diferentes níveis (Axelos, 2019).

Assim, algumas organizações podem se concentrar no desenvolvimento de competências essenciais, internamente, e contar com parceiros e fornecedores para outras necessidades. Outras também podem depender de seus parceiros o mínimo possível. Um método que as organizações usam para abordar essa dimensão é a integração e gestão de serviços (SIAM), em que há um "integrador" para garantir que os relacionamentos de serviço sejam coordenados de maneira adequada (Axelos, 2019).

Seja qual for o caso, os parceiros e fornecedores devem se alinhar aos valores essenciais e aos objetivos de negócio da organização, a fim de garantir a entrega do serviço, conforme contratado e dentro da qualidade esperada (Axelos, 2019).

d) Fluxos de valor e Processos

O ITIL V4 descreve esta dimensão da seguinte forma: envolve a definição das atividades, fluxos de trabalho, processos e procedimentos necessários para atingir os objetivos empresariais acordados, além de determinar como os diferentes componentes da organização se unem e trabalham em uníssono para permitir a criação de valor através de produtos e serviços (Axelos, 2019).

Segundo a definição de ITIL 4, um fluxo de valor é uma série de etapas que uma organização concretiza para criar e fornecer produtos e serviços aos consumidores. Esses fluxos

de valor são, por sua vez, ativados por processos que transformam contribuições em resultados. Essa dimensão ajuda a definir o modelo de entrega de serviço e a identificar processos que não auxiliam na criação de valor para o negócio (Axelos, 2019).

2.7.5 Implantação da Governança de TI

Para a implantação da GTI, são considerados diversos fatores organizacionais, como o porte da organização, o modelo de mercado escolhido, a disponibilidade de investimento, o prazo, a disponibilidade de recursos humanos. Independentemente do *framework* escolhido, o objetivo principal é o promover o alinhamento estratégico dos objetivos do negócio, bem como atender às legislações pertinentes, marcos regulatórios e às estratégias organizacionais (Fernandes; Abreu, 2012). Estes autores também propuseram as seguintes etapas para a implementação da GTI: a) Alinhamento estratégico e conformidade; b) Decisão, compromisso, priorização e alocação de recursos; c) Estrutura, processos, operações e gestão e d) Medição de desempenho (Fernandes; Abreu, 2012).

A Figura 10 apresenta as áreas de foco da GTI, conforme COBIT. De acordo com este *framework*, a GTI, para entregar benefícios e valor para a organização, precisa realizar os seguintes passos: Entregar valor para a organização; Gerir os Recursos Humanos; Mensurar o desempenho organizacional; Alinhar os princípios da GTI com a estratégia organizacional.

Figura 10 - Áreas foco GTI

Fonte: Axelos (2019).

A organização, após a decisão da alta gestão, de implementar a GTI, precisa elaborar um Plano Estratégico de TI (PETI) e, ou, Plano Diretor de TI (PDTI). Nesse documento, será detalhado todo o processo de implementação da GTI. Nesse caso, os modelos (COBIT, ISO e outros) possuem uma estrutura definida, com requisitos mínimos para a sua implantação e utilização (Axelos, 2019).

O objetivo principal da GTI é garantir o alinhamento de TI com o negócio e gerar valor agregado em seus produtos e, ou, serviços. Os modelos existentes, além de favorecer este alinhamento, colaboram para que o uso dos recursos de TI seja maximizado e os riscos sejam minimizados, de forma otimizar os benefícios e oportunidades identificados (ITGI, 2007).

O Quadro 6 apresenta os motivadores para a implantação da governança de TI, possíveis causas/origens e riscos que podem estar associados à sua adoção.

Quadro 6 - Motivadores para adoção da Governança de TI

Motivador	Possíveis causas	Riscos
Gastos altos com TI	Desvalorização e desatualização muito rápida de recursos de TI. Dificuldade de gestão de bens de TI. Alocação inadequada dos recursos de TI. Demora no processo de escolha,aquisição e entrega de soluções de TI insuficiente.	Diminuir lucratividade da organização. Perda de desempenho das funções de TI e dos negócios da organização.
Desalinhamento entre as necessidades de negócio e a infraestrutura de TI da organização	Infraestrutura de TI superestimada ou subestimada. Tempo de implementação das soluções de TI não atinge a expectativa dos usuários das áreas de negócios da organização.	Fluxo de informação truncado devido a processos não implementados por TI. Falta de alinhamento entre a área de TI e de negócios, proporcionando baixa eficiência operacional.
Decisões de TI tomadas de forma isolada	Área de TI não encarada na organização como estratégica. Falta de integração entre as áreas denegócio e a área de TI.	Serviços entregues sem a qualidade desejada. Desconhecimento das necessidades de novos serviços de TI para atendimento adequado ao negócio.
A segurança da informação não existe ou não é difundida adequadamente naorganização.	Indisponibilidade de informação sobre os proprietários dos dados dos sistemas e permissões necessárias para a manipulação dos dados. Indefinição de uma política desegurança.	Informações podem não ser confiáveis e íntegras, pois não existe controle sobre elas, gerando perdas significativas para a organização. Perda de credibilidade.
A contratação de serviços de terceiros não atende às necessidades de TI	Os contratos com terceiros não são firmados de forma adequada, acarretando dificuldade norelacionamento. Estratégia para a terceirização dos serviços de TI não atende àsnecessidades dos clientes e aos objetivos de negócio.	Quebra de contrato pode causar interrupção de serviços de TI. Serviços de TI estratégicos estão sob o controle de terceiros, ocasionando problemasde continuidade dos serviços de TI. Perda do controle dos serviços de TI.

Fonte: Moreira Neto *et al.* (2019, p. 15).

2.8 Governança de Dados

Governança de Dados (GD) 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 (Barbieri, 2020). Ele passa pela 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. 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, mas um ativo organizacional (Barbieri, 2020, p. 42).

A GD é responsável por diferentes tipos de dados, conforme o negócio da organização. É comum que exista um Conselho/Comitê de Governança de Dados com seus subcomitês de trabalho. O Comitê monitora a aplicação das políticas de GD e soluciona questões controversas relacionadas aos dados corporativos (Furlan; Laurindo, 2019). O Quadro 7 apresenta uma relação de definições sobre GD, segmentado por áreas de foco, com as respectivas referências bibliográficas. São conceitos afins ao constructo GD, conforme o entendimento dos autores, com variações no enfoque que cada um deu ao seu trabalho.

Quadro 7 - Definições sobre GD

Definição	Foco	Referência
O modelo de direitos de decisão e responsabilidades para estimular comportamentos adequados no uso dos dados.	• Estrutura de decisão • Cultura organizacional	Weber *et al*. (2009)
É uma parte da Governança de TI e envolve processos e controles para garantir que as informações no nível de dados sejam confiáveis e únicas (não redundantes).	• Processos • Parte da GTI • Necessidade de confiabilidade e unicidade	Smallwood (2014)
Governança de Dados busca assegurar os controles de gerenciamento formal.	• Estrutura de decisão • Processos • Importância da qualidade de dadosna cadeia de valor	Smallwood (2014)
Governança de Dados é o exercício de tomar decisões e a autoridade sobre os assuntos relacionados a dados.	• Estrutura de decisão	Thomas (2016)
O sistema de direitos de decisão e responsabilidades pelos processos relacionados às informações, executados de acordo com	• Estrutura de decisão • Processos	Thomas (2016)

modelos acordados e que descrevem quem pode tomar quais ações com base em quais informações e também quando, sob quais circunstâncias, e utilizando quais métodos.	• Métodos sobre "quem pode fazer o quê, com base em que, quando e como"	

Fonte: Assis (2011, p. 55).

Chapple (2013) relata o valor de uma GD estruturada com boas práticas e processos bem definidos. Porém, destaca que existem problemas, dificuldades e obstáculos, perante as organizações, para a criação e implementação de modelo de GD (Chapple, 2013, p.17).

O *Data Management Association* (DAMA) é uma organização internacional sem fins lucrativos. Ela possui o capítulo Brasil (DAMA-BRASIL), composto por profissionais que promovem as melhores práticas de GD. Ela é responsável pela definição de padrões e métodos que proporcionem uma melhor gestão dos dados corporativos. É um guia de referência no mercado nacional e internacional (DAMA-BRASIL, 2012).

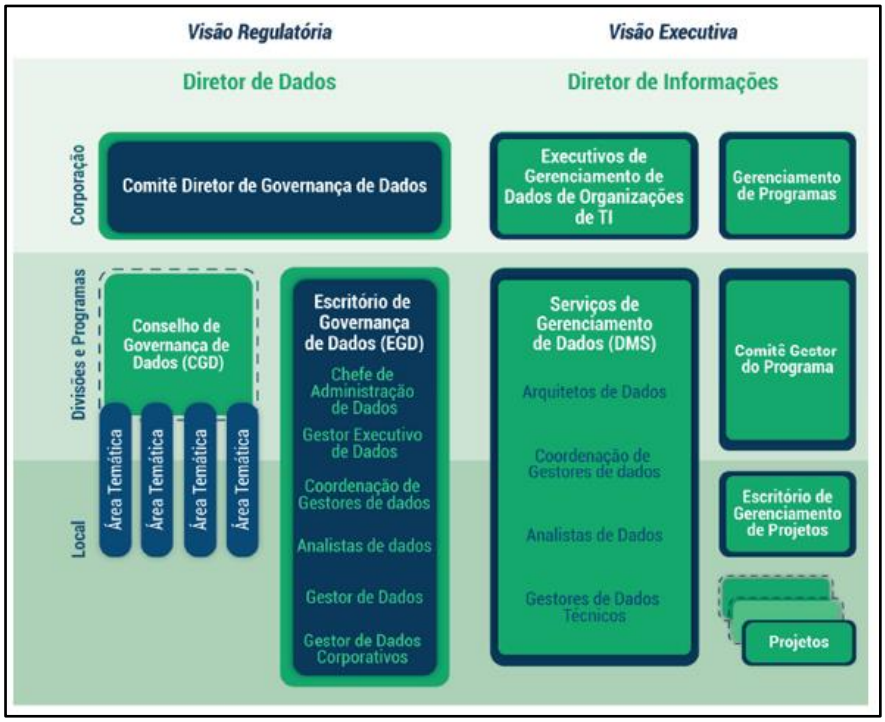
O modelo de referência, quando se aborda a GD, é o DAMABOK, cujo conteúdo será brevemente explanado nesta pesquisa. Outros modelos de GD existem no mercado corporativo, como, por exemplo, o modelo do GARTNER, da IBM, dentre outros. Porém, por questões de limitação da pesquisa, eles não serão abordados (DAMA-BRASIL, 2012).

O guia DAMA-DMBOK define a gestão de dados da seguinte forma:

> 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-BRASIL, 2012, p. 50).

A Figura 11 apresenta um esquema proposto pelo guia DAMA-DMBOK, onde é possível perceber a divisão bidimensional da governança de dados (DAMA-BRASIL, 2012). Há três pilares na horizontal, que representam o local, as divisões e programas da corporação. Outros dois pilares, na vertical, representam a visão regulatória e executiva. Percebe-se que existe uma divisão de funções, sendo que o lado esquerdo da figura representa as funções e atividades a serem desempenhadas pelo Diretor de Dados (função estratégica); ao lado direito da figura estão representadas as funções e atividades a serem desempenhadas pelo Diretor de Informações (função executiva). Este modelo pode ser aplicado a grandes organizações. No caso de pequenas e médias empresas, o modelo proposto pode ser adequado à estrutura organizacional.

Figura 11 - Componentes de Governança de Dados organizacional



Fonte: DMBOK2 (2022, p. 114).

Entre os mais diversos modelos existentes para a governança de dados, termos comuns são citados na literatura, quando se trata de manipulação de dados eletrônicos, como *Big Data* e *Data Analytics.* Essas expressões referem-se à tecnologia capaz de tratar grandes quantidades de dados, normalmente, de diferentes origens e formatos, em fluxo contínuo. Esses conceitos surgiram em meados dos anos noventa, quando o aumento das transações eletrônicas produziu uma base de dados gigantesca. O *Analytics* tem, como função, auxiliar as organizações a explorarem os seus dados de uma maneira orientada e maximizada (via gestão analítica de dados e suas inter-relações com outras bases de dados e informações sistêmicas), a fim de criar oportunidades de negócios (IBM, 2022).

O Quadro 8 apresenta a matriz dos tipos de Governança atualmente aceitos e empregados nas organizações, conforme define Assis (2011). Essa composição, em que podem ser estabelecidos Objetivos, Contexto, Foco, Escopo e Responsabilidade aos tipos de governança, possui um caráter inovador, e irá contribuir como referência norteadora para as organizações.

Quadro 8 - Matriz de comparação entre governanças

Quesito	Governança Corporativa	Governança de TI	Governança de Dados	Referencial Teórico
Conceito	É uma visão mais ampla da estratégia da empresa, considerando inclusive os relacionamentos com a comunidade, e visa a criar um conjunto eficiente de mecanismos, incentivos e de monitoramento para assegurar o alinhamento entre os comportamentos dos executivos e os dos Acionistas.	- É como a empresa governa a TI para garantir desempenho satisfatório; - É um sistema de direitos e responsabilidades, que envolve vários participantes na organização: alto escalão, gestores de negócio e gestores de TI; - É um conjunto de sistemas, processos e procedimentos modelados para harmonizá-los aos da organização, garantindo o bom uso dos recursos de TI.	Governança de Dados busca 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, a aprimorar a qualidade dos dados e a evitar os efeitos de dados de baixa qualidade na cadeia de valor das organizações.	Sambamurthy; Zmud (1999); Roussey *apud* Information Technology Governance Corporativa (2009); Kooper *et al*. (2011, p. 10); Smallwood (2014). Sambamurthy;
Objetivos	- Zelar pela continuidade e perenidade da organização, acoplando visão de longo prazo e sustentabilidade; - Preocupar-se com o equilíbrio entre as metas econômicas e sociais, e entre as metas individuais e comuns.	Controlar e prover transparência das decisões em Tecnologia da Informação, sem desconsiderar mecanismos e processos para incrementar a eficácia da TI.	Garantir que as informações no nível de dados sejam confiáveis e únicas (não redundantes).	Coombes; Watson (2000); Iskander; Chamlou (2000); Peterson (2004); Riotto (2008); Instituto Brasileiro de Governança Corporativa (2009); Smallwood (2014).

Contexto	É o nível mais alto de governança na organização.	Governança Corporativa.	Governança de TI.	Khatri; Brown (2010); Smallwood (2014).
Foco	Elevação do valor das corporações.	Estratégia e otimização da TI.	Qualidade de dados.	Smallwood (2014).
Públicos	- Alto escalão da organização; - Investidores, empregados e credores; - Autoridades, legisladores e órgãos reguladores; - Comitês de apoio aos órgãos da administração; Relações com Investidores e Conselhos Fiscais; Assembléia geral de Acionistas.	Alto escalão da organização; Gestores de negócio; Gestores de TI.	Gestores de negócio; Gestores de TI.	Comissão de Valores Mobiliários (2002).
Responsabili-dade	- Órgãos máximos da administração ; - Executivos de cargos mais altos nos negócios: presidências, superintendências e diretorias Executivas.	- Autoridades da TI: CIO.	- Gestores da TI.	Weill; Ross (2004b); Australian Standard (2010).
Escopo	- Incorpora a "função social" da empresa, visando à criação de riqueza, a geração de oportunidades de emprego, o estímulo ao desenvolvimento científico e a melhoria da qualidade de vida; - Inclui as questões ambientais e a defesa do meio ambiente.	- Deve ser apta para apoiar a organização, a prestação dos serviços, os níveis de serviço e a qualidade de serviço necessária para atender os requisitos de negócio, atuais e futuros.	- Relacionada a áreas específicas nas organizações, responsáveis pela qualidade dos dados; as regras aplicáveis aos dados, como políticas, padrões, protocolos e regras de negócios; direitos de decisão e responsabilidades; e métodos e processos para orientar o comportamento das pessoas e o funcionamento dos sistemas de informação; É parte da Gov. De TI.	Weber *et al*.(2009); Smallwood (2014); Thomas 2016)

Princípio datransparência	- É o "desejo de informar", para além da "obrigação de informar"; - Deve ir além da legislação específica e expandir-se para assuntos e fatores que possam interessar aos públicos da organização, como valores e ações estratégicas.	- Transparência e educação caminham juntas em Governança de TI; - Processos devem ser divulgados nos portais internos da empresa, bem como ações de comunicação pelos gestores, representando oportunidades para melhor entendimento GTI.	- Os processos de governança e custódia de dados exporão transparência. - Deve ficar claro a todos como e quando as decisões e controles relacionados aos dados foram introduzidas nos processos.	Weill; Ross (2004b); Australian Standard (2010);IBGC (2009); Arma International (2014); Smallwood (2014); Thomas (2016).
Princípio daprestação de contas	- Atribuir aos devidos encarregados a responsabilidade integral por atos praticados no decorrer de seus mandatos; - Todos os responsáveis pela Governança devem prestar contas a quem os colocou no posto ou lhes atribuiu as responsabilidades.	Indivíduos e grupos concordam e aceitam suas responsabilidades acerca da demanda e do fornecimento da TI. Os indivíduos responsabilizados por ações também têm autoridade para desempenhar essas ações;	- A Governança de Dados definirá responsabilidades para as decisões multifuncionais de processose controles relacionadas aos dados; - Também definirá as responsabilidades para as atividades de custódia dos contribuintes individuais, bem como as responsabilidades para os grupos de custodiantes de dados.	Standards Australia (2005); Instituto Brasileiro de Governança Corporativa (2009); Arma International (2014); Thomas (2016).
Princípio da Equidade (relacionamento humano)	Erradicar atitudes ou práticas discriminatórias, consideradas como inaceitáveis, e prover tratamento justo e igualitário aos grupos minoritários.	As políticas, práticas e decisões da TI devem demonstrar respeito pelo comportamento humano, incluindo as necessidades atuais e nascentes de todas as "pessoas no processo".	Os participantes da Governança de Dados devem praticar integridade em suas relações uns com os outros, ser verdadeiros e trabalhar de forma próxima ao discutir *drivers*, restrições, opções e impactos para as decisões relacionadas a dados.	Smallwood (2014)

incípios específicos	- Responsabilidade corporativa: zelar pela continuidade e perenidade da organização, acoplando uma visão de longo prazo e de sustentabilidade,	- Estratégia: a estratégia do negócio deve levar em conta as capacidades atuais e futuras da TI e os planos estratégicos para que a TI atenda às necessidades da estratégia organizacional; - Aquisição: as compras da TI devem ser feitas de acordo com razões específicas e válidas, baseadas em análises e em processos claros e transparentes de tomada de decisão; - Desempenho: a TI deve ser apta a apoiar a organização, a prestação dos serviços, os níveis deserviço e a qualidade de serviço necessária para atender aos requisitos de negócio atuais e futuros; - Conformidade: a TI deve estar de acordo com toda a legislação e regulamentos obrigatórios.	- Auditabilidade: decisões, processos e controles devem ser passíveis de auditoria, e acompanhados por documentação para suportar os requisitos de conformidadeà auditoria operacional; - Verificação: mecanismos de verificação entre as equipes de negócios e tecnologia, bem como entre aqueles quecriam e, ou, coletam informações, aqueles que usam, e aqueles que implantam padrões e requisitos de conformidade; - Padronização: padronizaçãodos dados da empresa; - Gestão de mudança: atividades proativas e reativasde Gerenciamento de Mudanças para dados de referência e a estrutura e, ou, uso de metadados e dados corporativos	Australian Standard (2010); Instituto Brasileiro de Governança Corporativa (2009); Arma International (2014); Thomas (2016).

Fonte: Assis (2011, p. 81).

3 METODOLOGIA

Nesta pesquisa, pretende-se verificar o processo de adequação da LGPD de duas IES (elemento comparativo) e a utilização da GTI no suporte a essa adequação.

3.1 Caracterização da pesquisa

A pesquisa é do tipo exploratória e descritiva, porque tem o propósito de ambientar-se com o tema ora estudado e esclarecer o objeto pesquisado (LGPD). Segundo Pozzebon e Freitas (1998), os estudos exploratórios permitem ao investigador aumentar sua experiência em torno de determinado problema. A realização de um estudo exploratório, embora possa parecer simples, não elimina o cuidadoso tratamento científico necessário em qualquer trabalho de pesquisa (Pozzebon; Freitas, 1988, p. 156-157).

Conforme Merlugo, Carraro e Pinheiro (2021, p. 186) apresentam, por meio da pesquisa exploratória, é possível obter respostas comparáveis de diferentes indivíduos de uma mesma amostra. Adotou-se uma abordagem qualitativa, permitindo uma investigação mais próxima da realidade das organizações (validação do *status quo).*

De acordo com Oliveira (2007)

> Um processo de reflexão e análise da realidade através da utilização de métodos e técnicas para compreensão detalhada do objeto de estudo em seu contexto histórico e/ou segundo sua estruturação. Esse processo implica em estudo segundo a literatura pertinente ao tema, observações, aplicações de questionários, entrevistas e análise de dados, que deve ser apresentada de forma descritiva. (Oliveira, 2007, p.37).

O estudo de caso é uma categoria de pesquisa cujo objeto é uma unidade que se analisa profundamente. Esta definição determina suas características, dadas por duas circunstâncias (natureza e abrangência da unidade), principalmente (Triviños, 1987, p.134).

Segundo Triviños (1987) para a realização de uma pesquisa descritiva o investigador/pesquisador necessita de uma série de informações sobre o que se deseja pesquisar. Esse tipo de estudo descreve os fatos e fenômenos de uma determinada realidade (Triviños, 1987).

De acordo com Triviños (1987), no estudo de caso qualitativo, a complexidade do exame aumenta à medida que se aprofunda no assunto. Ele possibilita estabelecer comparações entre dois ou mais enfoques específicos (estudos comparativos de casos). O enfoque comparativo enriquece a pesquisa qualitativa, especialmente se ele se realiza na perspectiva

histórico-estrutural. Em geral, essa linha de investigação segue os passos do método comparativo, descrevendo, explicando e comparando, por justaposição, os fenômenos. Pode-se ter a possibilidade de estudar dois ou mais sujeitos e, ou, organizações. Trata-se, então, de estudos multicasos (Triviños, 1987, p. 136).

Segundo Yin (2004), "o estudo de caso é uma investigação empírica de um fenômeno contemporâneo, dentro de um contexto da vida real, sendo que os limites entre o fenômeno e o contexto não estão claramente definidos" (Yin, 2004). Este autor afirma também que é preciso analisar as questões objeto de investigação por meio de uma compreensão ampla, holística, utilizando-se uma lógica indutiva (do específico para o geral). O estudo de caso "reside em sua capacidade de lidar com uma ampla variedade de evidências – documentos, artefatos, entrevistas e observações" (Yin, 2004). Nesta pesquisa, será utilizado o estudo de caso múltiplo, pois, conforme ensina Yin (2004), a pesquisa de casos múltiplos reflete situações de projetos diferentes, ou seja, é possível realizar múltiplas análises sobre o objeto investigado.

> A investigação de estudo de caso enfrenta uma situação tecnicamente única, em que haverá muito mais variáveis de interesse do que pontos de dados, e, como resultado, baseia-se em várias fontes de evidências, com os dados precisando convergir em um formato de triângulo, e, como outro resultado, beneficia-se do desenvolvimento prévio de proposições teóricas para conduzir a coleta e a análise de dados (Yin, 2004).

Triviños (1987) afirma que o grande valor do estudo de caso é "fornecer o conhecimento aprofundado de uma realidade delimitada, que os resultados atingidos podem permitir, e formular hipóteses para o encaminhamento de outras pesquisas" (Triviños, 1987, p. 111). Por sua vez, Laville e Dionne (1999, p. 156) argumentam que

> A vantagem mais marcante dessa estratégia de pesquisa (estudo de caso) repousa, é claro, na possibilidade de aprofundamento que oferece, pois os recursos se veem concentrados no caso visado, não estando o estudo submetido às restrições ligadas à comparação do caso com outros casos.

Pozzebon e Freitas (1998, p. 145) afirmam que

> O estudo de caso é definido como aquele que examina um fenômeno em seu ambiente natural, pela aplicação de diversos métodos de coleta de dados, visando a obter informações de uma ou mais entidades. Essa estratégia de pesquisa possui caráter exploratório, sem nenhum controle experimental ou de manipulação. Além disso, as fronteiras do fenômeno não são evidentes.

Diante dessas considerações, cabe ressaltar que a metodologia escolhida para esta pesquisa deve-se à necessidade de explorar os ambientes e fenômenos ocorridos nas IES escolhidas, de forma que se possa identificar (o mais próximo possível) as informações relevantes daqueles ambientes. Ou seja, observar quais são as circunstâncias, condições, configurações, ambientes e outras características e fatos relevantes para o processo de

adequação da LGPD. A proximidade e interação do pesquisador e entrevistado é favorecida por tal metodologia. Logo, a obtenção de dados e informações, nestas circunstâncias, é bastante profícua para o fim que se pretende nesta pesquisa.

E, como afirmam Pozzebon e Freitas (1998, p. 146): “Os resultados do estudo dependem fortemente do poder de integração do pesquisador, de sua habilidade na seleção do local e dos métodos de coleta de dados, bem como de sua capacidade de fazer mudanças no desenho de pesquisa de forma oportuna”.

O Quadro 9 criado por Benbasat, Goldstein e Mead (1987), *apud* Pozzebon (1998), corrobora a definição da metodologia escolhida para esta pesquisa, pois permite a síntese de questões relevantes para este pesquisador/pesquisa.

Quadro 9 - Questões sobre a adequação do Estudo de Caso

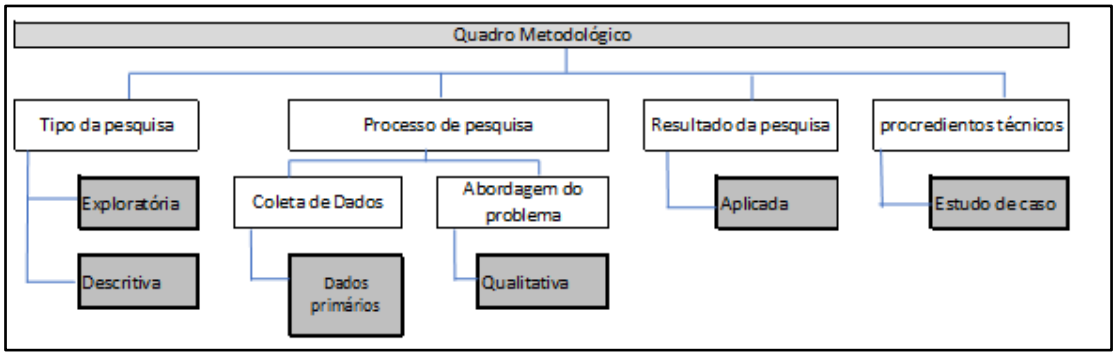
Pergunta	Resposta
• O fenômeno de interesse pode ser estudado fora de seu ambiente natural?	⇒ Não. Um ambiente natural rico é considerado fértil para a geração de teorias.
• O estudo focaliza eventos contemporâneos?	⇒ Sim. A metodologia *case* é claramente útil quando o ambiente natural é necessário e quando foca evento contemporâneo.
• O controle ou a manipulação dos sujeitos ou eventos é necessária?	⇒ Não. Quando pessoas ou eventos devem ser controlados ou manipulados no curso de um projeto de pesquisa, o estudo de caso não é recomendável.
• O fenômeno de interesse tem uma base teórica estabelecida?	⇒ Não. O fenômeno estudado, não apoiado por forte base teórica, deve ser verdadeiramente perseguido pela pesquisa.

Fonte: Benbasat, Goldstein e Mead (1987)

A unidade de análise escolhida foi a Organização. Especificamente, nesta pesquisa, optou-se por duas universidades mineiras, sem fins lucrativos: a Universidade Fumec e a Pontifícia Universidade Católica de Minas Gerais (PUC Minas).

O Figura 12 apresenta, de forma gráfica, a caracterização do tipo de pesquisa adotada nesta pesquisa. As imagens destacadas em cinza representam a síntese do percurso metodológico.

Figura 12 - Caracterização da pesquisa



Fonte: Elaborado pelo autor (2023).

3.2 Apresentação dos casos selecionados

Nesta seção, será realizada uma breve descrição das duas IES selecionadas para a realização do estudo de caso.

3.2.1 Caso UNI1

A Pontifícia Universidade Católica de Minas Gerais - PUC Minas caracteriza-se por ser uma universidade comunitária, confessional, filantrópica e privada, de caráter público não estatal. A sua mantenedora é a Sociedade Mineira de Cultura, através do Decreto-Lei n.º 45.046, de 12 de dezembro de 1958. A PUC Minas está presente em Minas Gerais em sete *campi* localizados nas cidades de Belo Horizonte, Betim, Contagem, Arcos, Poços de Caldas, Serro e Uberlândia. Além da sede, no bairro Coração Eucarístico, tem mais três unidades localizadas em Belo Horizonte – Barreiro, Praça da Liberdade e São Gabriel. Na graduação, são ofertados 120 cursos de bacharelado, 21 de graduação tecnológica e 12 cursos de licenciatura (PUC Minas, 2023).

A Universidade PUC Minas possui uma estrutura administrativo-acadêmico ampla, dividida em setores: pró-Reitorias, coordenações e setores. A Reitoria é comum todos os *campi*. Contudo, as demais estruturas administrativas podem variar de um para outro *campus*. Pretende-se, inicialmente, nesta pesquisa, que a coleta de informações seja direcionada para o responsável pela LGPD e, em seguida, ao setor de Tecnologia da Informação. Consultas realizadas permitiram perceber que as variações estruturais ocorrem, com maior frequência, na esfera administrativa onde a TI está alocada. Vale destacar que a área de TI está vinculada a sua mantenedora, a Sociedade Mineira de Cultura (SMC), atendendo tanto à universidade

quando à rede de colégios dentre outras (Mitra, Rádio América, Fumarc). A parte acadêmica, de certa forma, é semelhante entre os *campi* e as variações ocorrem em relação aos cursos ofertados por instituição, em suas respectivas unidades (PUC Minas, 2023).

3.2.2 Caso UNI2

A Universidade Fumec é uma instituição de ensino superior sediada no município de Belo Horizonte, capital do estado de Minas Gerais. Sua mantenedora é a Fundação Mineira de Educação e Cultura, pessoa jurídica de direito privado, sem fins lucrativos. Criada e gerida por professores, completou sessenta anos de existência em 2023. As atividades de Ensino começaram com as Faculdades de Ciências Empresariais – FACE e de Engenharia e Arquitetura – FEA. Posteriormente, ampliou sua área de atuação com a criação da Faculdade de Ciências Humanas – FCH. Em 2004, conquistou o título de Universidade e, ao longo dessas seis décadas, passou por diversas transformações, construiu uma reputação sólida e contribuiu para a formação e o desenvolvimento de muitas pessoas, por meio de sua oferta de cursos superiores, especializações e pós-graduações (Fumec, 2023).

A Universidade Fumec também possui uma estrutura acadêmico-administrativa complexa. A estrutura da alta gestão é composta por Reitoria e diretorias. As demais estruturas administrativas e operacionais são dispostas conforme as unidades de negócios e os *campi*. Pretende-se, inicialmente, nesta pesquisa, que a coleta de informações seja direcionada ao responsável pela adequação da LGPD e, em seguida, ao setor de Tecnologia da Informação. Consultas realizadas permitiram perceber que as variações estruturais ocorrem, com maior frequência, assim como na PUC Minas, na esfera administrativa de TI. Quanto à parte acadêmica, cada *campi* possui a sua própria estrutura (Fumec, 2023).

3.2.3 Perfil dos Entrevistados

O Quadro 10 apresenta a relação cargo/função com relação à LGPD aplicada nesta pesquisa. Isto é, o pesquisador estabeleceu este critério de agrupamento com base nas definições de papéis da LGPD e nos contructos componentes desta pesquisa. A proposta foi identificar, dentro das instituições, pessoas que, com seus respectivos cargos e funções, possuem relação estreita com a LGPD.

Nas duas IES, foram entrevistados dois profissionais, o DPO e o gerente de Tecnologia da Informação, perfazendo um total de quatro Entrevistados. Devido à limitação de tempo. não foi possível a realização de entrevistas adicionais.

Quadro 10 - Relação de cargo/função com a LGPD

Tema	Cargo/Função	Relação com a LGPD
LGPD	Encarregado da Proteção de Dados DPO (*Data Protection Officer*)	Trabalha para garantir que as organizações estejam em conformidade com os regulamentos de privacidade de dados, estabelecendo padrões para proteger as informações pertinentes aos usuários por meio de práticas e padrões éticos.
Tecnologia da Informação	Gerente de TI (Governança TI)	Responsável pelo apoio direto a todas as atividades relacionadas ao funcionamento do sistema de governança, como facilitar a comunicação entre os agentes e os órgãos — principalmente conselho e diretoria — e identificar previamente conflitos de interesse.
	Gerente de Governança de Dados	Este profissional é o responsável por controlar os processos internos e garantir a segurança das informações. É ele quem faz a gestão de riscos, capaz de identificar e antecipar possíveis problemas para a empresa, no que se refere à segurança dos dados.

Fonte: Elaborado pelo autor (2023).

3.3 Procedimentos para a coleta e análise de dados

Os procedimentos para a coleta e análise de dados serão descritos a seguir, de acordo com os objetivos da pesquisa.

3.3.1 Coleta de dados

A coleta de dados ocorreu em quatro fases: levantamento bibliográfico e revisão de literatura; elaboração e aplicação dos instrumentos de coleta de dados (entrevistas e coleta de documentos).

A primeira fase consistiu no levantamento bibliográfico e revisão de literatura, para a obtenção de informações sobre o tema de pesquisa em artigos, dissertações e teses, dentre outros. Para questões específicas da LGPD, foram consultadas legislações específicas, como a Constituição Federal de 1988, o Marco Civil da Internet, a Lei de Acesso à Informação, além de sites governamentais (Governo Federal, Câmara dos Deputados, Presidência da República e TCU, dentre outros).

Adicionalmente, foram realizadas pesquisas eletrônicas relacionadas ao tema proposto em sites científicos, especificamente nos constructos “Privacidade de Dados”, “LGPD”, “Governança de TI”, “Governança de Dados” e “Instituição de Ensino Superior” e a combinação entre eles. As buscas foram realizadas nas seguintes bases de dados científicas:

Web of Sciences (WOS), *Academic Databases for Colleges and Universities* (EBSCO), *Scientific Electronic Library Online* (SCIELO) e *Scientific Periodicals Electronic Library (*SPELL).

Na segunda fase, foram elaborados roteiros de entrevistas, com questões abertas, a serem respondidas pelos Entrevistados. Quanto à entrevista semiestruturada, Laville e Dionne (1999), afirmam que

> A entrevista semiestruturada oferece maior amplitude na coleta dos dados, bem como uma maior organização: esta, por sua vez, não estando mais irremediavelmente presa a um documento entregue a cada um dos interrogados. Por essa via, a flexibilidade possibilita um contato mais íntimo entre o Entrevistador e o Entrevistado, favorecendo assim a exploração em profundidade de seus saberes, bem como de suas representações, de suas crenças e valores (Laville; Dionne, 1999).

A divisão apresentada no Quadro 10 tornou-se necessária devido à própria natureza das informações e da estrutura requerida para a adequação e operação da LGPD. O DPO possui domínio da lei e o gerente de TI possui domínio das tecnologias e do tratamento de dados (governança de dados). Logo, justifica-se a entrevista de forma apartada, pois os constructos, na sua essência são distintos, apesar de relacionados. Ou seja, convivem e precisam de coesão e harmonia entre eles.

Assim, foram elaboradas entrevistas específicas para grupos de participantes específicos, conforme funções desempenhadas por eles nas respectivas IES. No caso da GTI, que aborda temas diversos dentro da sua área de conhecimento (tecnologia), a entrevista foi dividida nas áreas de Governança de TI e de Governança de Dados. Foram utilizados, como referência para esta pesquisa, os *frameworks* COBIT, ITIL e a norma ABNT/NBR ISO 38.500. E, no caso da LGPD, foi elaborado um modelo único de entrevista, em conformidade com a Lei 13.709/2018. Nesta etapa, a parte de Identificação do participante, comum a todos os Entrevistados, contém dados como: nome, *e-mail*, cargo e função, dentre outros, conforme Apêndice A.

O roteiro da entrevista está dividido da seguinte forma: a) Identificação do Entrevistado; b) Seção LGPD, a qual possui questões pertinentes à Lei Geral de Proteção de Dados Pessoais; c) Seção de Governança da Tecnologia da Informação, com questões pertinentes às pessoas, processos e tecnologias envolvidos na adequação da LGPD nas IES e, por fim; d) Seção Governança de Dados (Apêndices A, B e C).

O primeiro bloco da entrevista é comum aos dois grupos Entrevistados, que é a parte de identificação do participante. O segundo bloco da entrevista, que será aplicado para o grupo de participantes específicos LGPD e GTI/GD, contém questões abertas, porém, com um viés

técnico. O Entrevistado responderá as questões com suas palavras, de forma descritiva, conforme julgar conveniente.

Os roteiros para elaboração da entrevista foram feitos com base nos trabalhos dos seguintes autores: Barata (2015), Assis (2011) e Moreira (2019). Vale destacar que algumas questões foram incorporadas literalmente no roteiro de entrevista e outras foram adequadas para melhor se ajustarem ao tema de pesquisa.

O Quadro 11 apresenta os modelos de entrevistas que foram aplicados, segmentados por cargo e, ou, função. Os roteiros encontram-se nos Apêndices A, B e C.

Quadro 11 - Quadro esquemático de entrevista por função

ID	Área	Cargo/Função	Modelo entrevista
1	LGPD	Oficial - (Encarregado) da Proteção de Dados – DPO (*Data Protection Officer*)[5]	EA
2	GTI	Gerente de TI - Governança de TI	EB
3	GD	Gerente de TI - Governança de Dados (Ciência de Dados)	EC

Fonte: Elaborado pelo autor (2023).

O Quadro 12 apresenta a relação entre as questões elaboradas, os autores de base e os objetivos da pesquisa.

[5] Responsável pela proteção de dados dentro de uma organização, ele garante a comunicação entre o controlador, os titulares dos dados e a ANPD, assegurando a segurança das informações de clientes, fornecedores e da própria empresa. De acordo com a Lei 13.853/2019 - LGPD, artigo 5º, inciso VIII, a definição de Encarregado é: "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).

Quadro 12 - Relação entre os objetivos específicos x autores x entrevista

Objetivos específicos	Autores	Questões (do roteiro) Entrevista seção / questões
Identificar quais áreas de negócios e sistemas de Informação existentes nas IES passaram por adaptações para apoiar a implementação, uso e gestão da LGPD.	• Lei Geral de Proteção de Dados – Lei nº 13.709/18 • BARBOSA, T. *et al*. (2021) • STELZER, Joana *et al*.(2019)	EA EB EC
Verificar quais disposições expressas nos capítulos da LGPD foram implementadas pelas IES.	• Lei Geral de Proteção de Dados - Lei nº 13.709/18 • PEREIRA JR, M.A. (2020) • STAKOVIAK JR, P. B. M. (2020) • ABNT ISO 38.500 (2018) • IT Governance Institute. ITGI (2007) • ALBERTIN; ALBERTIN (2010) • FERNANDES, A. A.; ABREU, V. F. (2012) • WEILL, Peter; ROSS, Jeanne (2006) • LUNARDI *et al.* (2008)	EA EB
Verificar quais iniciativas/ações relacionadas à Governança de Tecnologia da Informação têm sido adotadas pelas IES.		EB
Identificar os modelos específicos de GTI e de GD utilizados nas IES.	• AXELOS. 2019. • ISACA. 2019. COBIT 5. • DAMA – Data Management Association (2014) • CAVALCANTI FILHO, Hermano *et al.* (2011) • WEILL, Peter; ROSS, Jeanne (2006)	EB EC

Fonte: Elaborado pelo autor (2023).

Cabe ressaltar que as etapas da pesquisa que envolvem instrumentos de interação do pesquisador com qualquer pessoa (sujeito de direito), requerem, obrigatoriamente, que tais instrumentos sejam submetidos e aprovados, antecipadamente, pelo Comitê de Ética e Pesquisa da Universidade Face-Fumec (Protocolo de aprovação número: 72831123.2.0000.5155). Dessa forma, este projeto de pesquisa e seus roteiros de entrevista foram aprovados e estão em conformidade com os requisitos daquele Comitê de Ética e Pesquisa.

Na terceira fase, foram realizadas as entrevistas com os participantes junto às universidades selecionadas. Nas entrevistas, foi possível que os participantes apresentassem uma visão geral de sua instituição e os aspectos pertinentes aos constructos específicos, objeto de estudo desta pesquisa, conforme suas percepções.

A realização da entrevista foi agendada por meio de convite enviado por *e-mail* aos participantes, previamente determinados pelas IES selecionadas. Elas foram realizadas de forma *on-line,* por meio de plataformas digitais, utilizando-se os softwares de videoconferência como *Teams* e *Google Classroom,* além de contatos via telefonia celular.

O Quadro 13 apresenta a relação de entrevistados por IES e, além do cargo/função, a data da entrevista. Destaca-se que as entrevistas ocorrem, em sua maioria, em outubro de 2023, exceto a do Entrevistado 2, que ocorreu em dezembro de 2023.

Quadro 13 - Relação das entrevistas x Cargo/Função x IES

Participantes	IES	Cargo / Função	Data da entrevista	Apêndice
Entrevistado 1	IES1	DPO	09/10/2023	E
Entrevistado 2		Gerente de TI (Governança de TI / Dados)	04/12/2023	F
Entrevistado 3	IES2	DPO	19/10/2023	G
Entrevistado 4		Gerente de TI (Governança de TI / Dados)	19/10/2023	H

Fonte: Elaborado pelo autor (2023).

Em seguida, houve a transcrição das entrevistas (que gerou 75 páginas de conteúdo), cujos dados foram analisados frente ao referencial teórico. A técnica utilizada para a interpretação dos resultados foi a análise de conteúdo.

Após a transcrição das entrevistas, que ocorreu no período de 10/10/23 a 08/12/23, o seu conteúdo foi encaminhado aos entrevistados por *e-mail*, para aferição e validação do seu conteúdo. A devolução das transcrições foi realizada também via *e-mail*, o que permitiu ao pesquisador realizar a análise e discussão dos resultados, apresentada a seguir.

Vale destacar que, além das entrevistas realizadas junto aos DPO's e Gerentes de TI, foram coletados os seguintes documentos (de forma eletrônica, via *website* e *e-mail*) produzidos pelas IES no processo de adequação da LGPD.

- Comitê de privacidade e proteção de dados pessoais – UNI2
- Evento de conscientização sobre proteção de dados pessoais – UNI2
- Boletim de privacidade – UNI1
- Boletim de segurança da informação – UNI1
- Tela do sítio UNI1 – Comunicação com o cliente
- Tela do sítio da UNI1 – Política de Privacidade
- Tela do sítio UNI2 – Canal LGPD
- Tela do sítio UNI2 – Canal LGPD – Cookies
- Formulário para contato com a Ouvidoria da Fumec

- Índice da Política de Segurança da Informação da UNI1
- Fluxo de processo sugerido pela ANPD para aplicação do RIPD
- Formulário para reportar incidente de segurança da informação ou privacidade UNI1
- Diretiva de Privacidade (proteção de dados) da UNI2
- Categoria de informações para coleta de dados da UNI2
- Formulário para acesso a informações pessoais - UNI1

A análise destes materiais (formulários, telas, fluxos e boletins) contribuíram para a realização de uma análise crítica mais aprofundada de todo o processo de adequação da LGPD nas instituições pesquisadas.

3.3.2 Análise de dados

Após as entrevistas, com que se obteve o aprofundamento necessário em pontos chave, pertinentes ao objeto de pesquisa (obtenção da compreensão do cenário de cada uma das IES selecionadas), foram realizadas análises de conteúdo com vistas a atingir os objetivos propostos nesta pesquisa. Bardin (2011) afirma que a análise de conteúdo é um conjunto de instrumentos de cunho metodológico em constante aperfeiçoamento, que se aplicam a discursos extremamente diversificados. Segundo esta autora, a função primeira da análise de conteúdo é desvendar o crítico (Bardin, 2011, p.15).

Dessa forma, podemos concluir que a análise de conteúdo é uma leitura aprofundada e objetiva que procura estabelecer a descoberta das relações existentes entre o conteúdo e os aspectos externos, ou seja, permite a compreensão, a utilização e a aplicação de um determinado conteúdo (Bardin, 2011).

O Quadro 14 contém as categorias e subcategorias de análise que permitem um melhor entendimento e compreensão dos dados das entrevistas realizadas. Essa categorização é uma forma de agrupamento e subagrupamento que permite uma análise em segmentos distintos.

Quadro 12 - Categorias de análise

Categorias	Subcategorias
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 (GTI e GD)	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 pelo autor (2023).

Nesse sentido, para análise dos dados, inicialmente, definiram-se as categorias de análise construídas com base nos constructos anteriormente definidos e nos quesitos dos roteiros de entrevistas, permitindo uma melhor análise e compreensão das informações ora classificadas e agrupadas. Vale destacar que o agrupamento por categorias visa a buscar uma melhor significação e compreensão dos dados que, segundo Bardin (2011), surgem através de uma "operação de classificação de elementos constitutivos de um conjunto, por diferenciação e, seguidamente, por reagrupamento segundo o gênero (analogia), com os critérios previamente definidos" (Bardin, 2011, p. 117).

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo, são apresentados os resultados provenientes do levantamento de dados na UNI1 e UNI2. Os dados e informações coletados foram arranjados em categorias e subcategorias de análise, conforme Quadro 14. Os resultados serão apresentados e discutidos desde o processo de adequação (com a definição do escopo, histórico), passando pelos processos Comunicacionais, de Governanças, Pessoas, e, não menos importante, a categoria de tratamento de dados pessoais (políticas de segurança, RIPD, incidentes). Por fim, conclui-se a discussão com uma avaliação da adequação da LGPD nas instituições pesquisadas, apresentando-se alguns desafios, dificuldades e perspectivas futuras.

A área de TI na UNI1 denominada "Gerência de Tecnologia da Informação – GTI" está subordinada à Pró-Reitoria Administrativa-Financeira. Ela atende todo o sistema da Arquidiocese de Belo Horizonte: Fundação Mariana Resende - FUMARC, Colégios Santa Maria, Sociedade Mineira de Cultura, Rádio Cultura, Rádio América, TV Horizonte, Pontifícia Universidade Católica de Minas Gerais – PUC Minas e outras. A estrutura é composta por 127 colaboradores, distribuídos em departamentos, para atender ao público interno e externo. Ela está vinculada à alta direção (Pró-Reitoria Administrativa-Financeira) e portanto, relaciona-se com as demais Pró-Reitorias e áreas estratégicas da Arquidiocese. Ela participa da definição das metas estratégicas anuais-plurianuais da instituição quando se trata de TICs. Este último fato permite um alinhamento entre a área de Governança Corporativa e a Gerência de TI da instituição, possibilitando o envolvimento da alta direção no patrocínio e no envolvimento da adequação da LGPD.

A IES2, por sua vez, conta com uma estrutura mais simples, se comparada à UNI1, no que se refere à Tecnologia da Informação. A UNI2 possui a área de TI denominada da mesma forma que na UNI1, "Gerência da Tecnologia da Informação". Ela atende à Universidade Fumec, ou seja, às demais faculdades que compõem a Fundação: a Faculdade de Ciências Administrativas, a Faculdade de Engenharia, a Faculdade de Ciências Humanas. Possui, aproximadamente, 23 colaboradores que estão divididos entre times de Suporte, Banco de Dados, Desenvolvimento e Redes (infraestrutura). Assim como na UNI1, a GTI da UNI2 está vinculada também à alta direção. Ela participa do Comitê da LGPD, eventualmente ou sob demanda do Comitê Estratégico Corporativo.

4.1 Processo de adequação da LGPD nas IES

Na UNI1 e na UNI2, o processo de adequação ocorreu conforme o requerido pela lei e de acordo com os seus requisitos, conforme se segue: a) Tratamento de Dados Pessoais, b) Política de Segurança da Informação, c) Política de Proteção de Dados Pessoais, d) Relatório de Impacto à Proteção de Dados Pessoais, e) Política de Privacidade, f) Controle de Acesso em Sistemas, que foram abordados individualmente, conforme demonstrado ao longo da pesquisa. Exceção para o Sistema de Gestão de Incidentes e o de Utilização de Criptografia, que não foram implementados de forma direta até a finalização das entrevistas.

O processo de adequação da LGPD na UNI1 começou em 2019, quando o Entrevistado 1 assumiu a posição de DPO, informalmente, tendo sido nomeado oficialmente, como DPO da instituição, no ano de 2020.

> [...] 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).

Na UNI1, este processo se iniciou em 12 de março de 2020, quando o Entrevistado, através de portaria, assumiu a posição de DPO formalmente, até junho de 2024. A função exercida por ele, até então, era somente de auditor e, após a publicação da portaria, passou a exercer cumulativamente as funções de DPO e auditor.

Pode-se perceber que, em ambas IES, a LGPD está vigente (incorporada às instituições), e em processo de melhoria contínua. Foram desenvolvidas várias atividades antecedentes à sua adequação. Por exemplo: na UNI1, o Entrevistado destaca que o início do projeto ocorreu pela área de tecnologia, pouco tempo antes do início do projeto. Na UNI2, o Entrevistado 3, em função temporária, assumiu a liderança do Comitê que desenvolveu o projeto de preparação para adequação da LGPD.

Outro ponto relevante na adequação da LGPD na UNI1 deve-se ao fato de a equipe de implementação ter realizado o diagnóstico institucional com relação aos dados selecionados (via formulário) e, depois deste levantamento de informações, os dados foram tratados e classificados em dados pessoais, dados pessoais sensíveis e, ou, confidenciais. Para tal classificação, utilizou-se a metodologia criada especificamente para a realização do diagnóstico/adequação da LGPD.

Destaca-se que, na UNI2, o posicionamento do Entrevistado 1, quando diz que “a implementação da LGPD não é um projeto, é uma jornada que foi inaugurada, e que tem muito

a ser feito.” Com esta afirmação, o Entrevistado 1 aponta que o processo de adequação da LGPD é contínuo na instituição, e, com frequência, deve ser ajustado devido às questões evolutivas da própria lei.

> O processo de adequação da LGPD na UNI2 foi dividido em oito etapas. São elas: plano de comunicação; diagnóstico institucional; capacitação de colaboradores; processos de tratamento de dados; medidas corretivas e preventivas; gestão do consentimento; das bases legais; e relatório de impacto de proteção de dados pessoais (RIPD) (Entrevistado 3).

> [...] a comissão que tratou dessa desse tema, em 2019, nós consolidamos um projeto de adequação. E hoje nós temos, nós implementamos naturalmente o projeto e hoje nós temos um plano de acompanhamento de várias ações porque a nossa ideia é, de fato, consolidar um programa de governança, que é da LGPD; então, nós desenvolvemos, a partir desse projeto de hoje, nós estamos com esse plano de transformar em programa, então nós estamos aqui desenvolvendo várias ações dentro de 8 elementos [...] (Entrevistado 3).

Percebe-se uma estreita relação entre o afirmado por Bioni (2019) “o plano de adequação deve iniciar com o diagnóstico, estruturação do programa, contratos, treinamentos e comunicação e revisão...” e o que aconteceu, na prática, nas duas IES. Tanto na UNI1 quanto na UNI2 o processo de adequação se iniciou com um diagnóstico prévio, com diversos *stakeholders*, e, posteriormente, a estruturação ou o planejamento do programa de adequação da LGPD.

Vale destacar que o levantamento de dados ou *datamaping* ocorreu em todas as unidades das duas instituições pesquisadas, isto é, em pró-Reitorias, Reitorias, setores administrativos, financeiro e acadêmico, graduação e pós-graduação, e, especificamente, na UNI1, também nos colégios sob a sua administração.

> [...] o datamaping, o mapeamento das unidades e das atividades foi realizado; então a gente identificou nas unidades que tratam dados [...] (Entrevistado 1).

É importante salientar que, nas IES pesquisadas, foram criados Comitês para os trabalhos de adequação da LGPD. Eles estão subordinados à presidência das instituições. Esses comitês desempenham funções relevantes e preparatórias para obtenção e êxito na adequação da LGPD. Destaca-se que os Entrevistados já possuíam acesso à alta administração das Instituições. Logo, as ações requeridas pelo projeto foram embasadas pela alta gestão da instituição através da presença do DPO.

Essa nova forma de lidar com as informações, sob a égide da LGPD, dentro das instituições, como afirma Queiroz (2021), é “um novo paradigma na forma de tratamento da privacidade dos dados pessoais pelas organizações brasileiras”.

Os Comitês possuem formação semelhante, ou seja, são compostos por um grupo multidisciplinar que possui representantes das seguintes áreas: Jurídica, Gerência de TI, do DPO e da entidade mantenedora, que possuem competência consultiva, mas não deliberativa. Normalmente, em ambas as IES, o Comitê se reúne uma vez por mês, ou sob demanda, quando são debatidos os assuntos, diretrizes, temas, pontos importantes, bem como atividades relacionadas à privacidade de dados pessoais.

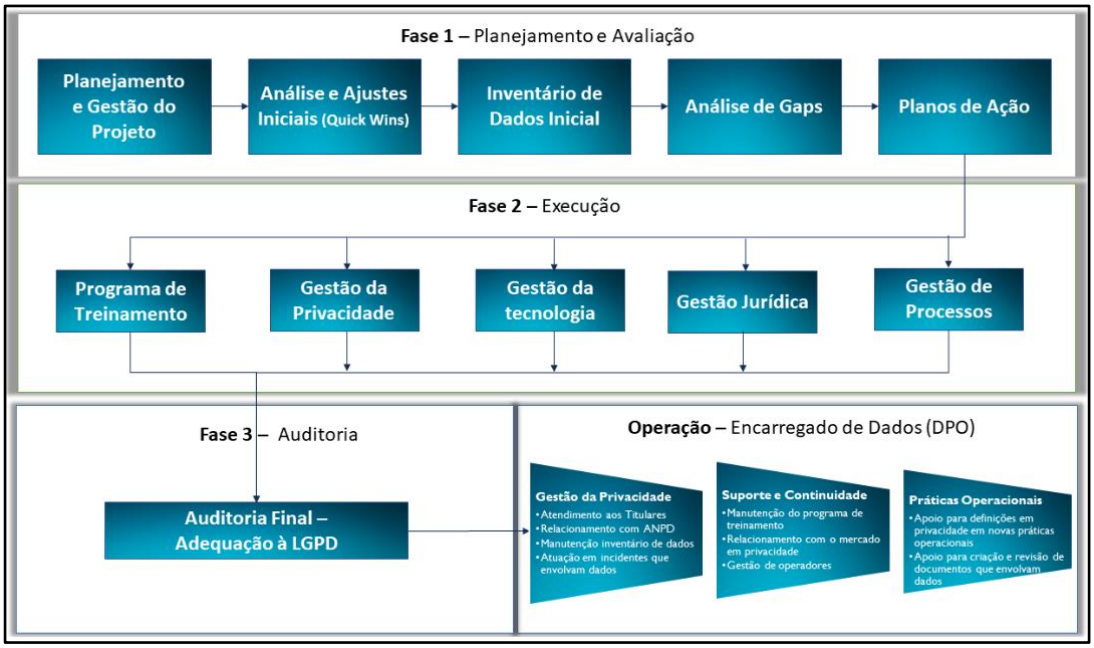
> [...] Nós temos um Comitê de privacidade e proteção de dados, que é basicamente para atender questões pontuais que envolvem um impacto mais amplo. Eu, basicamente, eu tenho autonomia para tomar várias decisões, mas, quando eu entendo que determinada adequação, alguma medida que vai gerar um impacto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

> [...] esse grupo executivo que olha no dia a dia. As definições mais macro a gente leva para a alta administração, quer seja na presidência quer seja no colegiado de diretoria que cuida da parte de tecnologia, porque não há só questão de regramentos de diretrizes institucionais. Há regras de negócio que dependem muito de tecnologia porque os grandes sistemas é que tratam dados pessoais. O processo depende muito de tecnologia, então a gente tem um comitê de tecnologia vinculado à Presidência, que a gente leva lá para essa diretoria [...] (Entrevistado 1).

Em suma, tanto na UNI1 quanto na UNI2 o processo de adequação à LGPD foi realizado com o rigor e critério estabelecido/requerido pela lei, segundo os entrevistados. A ANPD não estabeleceu atos normativos ou regulações em relação à LGPD na sua totalidade, novas edições (atualizações) da Lei podem ocorrer a qualquer a tempo, ou até mesmo novas diretivas provenientes da ANPD, como, por exemplo, edição de atos/instruções normativas e, ou, criação de procedimentos operacionais. Tal processo de adequação institucional à LGPD pode ser estendido ou ser até mesmo contínuo, até que sobrevenha o amadurecimento da legislação e, ou, dos processos complementares/regulatórios da ANPD.

A Figura 13 apresenta os passos em comum que as IES pesquisadas adotaram para a adequação da LGPD em suas instituições. O processo de adequação foi dividido em três etapas/fases: Planejamento e avaliação; Execução; Operação/Auditoria. Cada uma dessas fases possui subatividades, as quais foram utilizadas pelas IES pesquisadas de forma semelhante. A Figura 13 representa o conjunto macro das atividades de adequação da LGPD nas IES pesquisadas, cujo detalhamento não foi aqui discutido em profundidade.

Figura 13 - Trajetória de adequação da LGPD nas IES pesquisadas



Fonte: Rastek (2024).

Percebe-se que o processo de adequação da LGPD nas IES pesquisadas é semelhante ao modelo proposto por Rastek. Nas duas IES, houve a Fase 1 – Planejamento e avaliação do ambiente, posteriormente passou-se à Fase 2 – Execução, onde foi efetivamente realizada a adequação da LGPD junto às instituições. Mapeamento de processos, de dados e informações, definição de dados pessoais e sensíveis, treinamento dentre outras inúmeras ações. E, por fim, já em fase mais adiantada de adequação da instituição à LGPD, executa-se a o processo de auditoria para validação e realização de ajustes que por ventura se fizerem necessários.

4.2 Pessoas

A equipe responsável pela adequação à LGPD, na UNI1, conta com o DPO e mais um assistente (auxiliar de administração). O assistente cuida das questões pertinentes a tecnologia, inclusive na operação de um *software*, o qual está sendo personalizado com algumas parametrizações específicas daquela instituição. Na UNI1, adotou-se um sistema de "embaixadores", isto é, representantes ou responsáveis pelo tratamento de dados pessoais de forma descentralizada. Cada setor possui o seu responsável, que tem, além de sua função precípua contratual, a função adicional de ser o ponto focal naquele setor, quando se trata de assuntos pertinentes ao tratamento de dados pessoais (Entrevistado 1). As demandas que

surgem e que não são resolvidas por tais facilitadores, como revisão de processos e dúvidas, são submetidas ao DPO para apreciação, análise e resolução.

A adequação da LGPD, na UNI1, foi corroborada pelo processo de treinamento, contando com a presença, inclusive, do pró-reitor adjunto Administrativo-Financeiro (envolvimento da alta direção da instituição). A realização desse tipo de conscientização junto aos colaboradores das demais áreas, somada à participação da alta administração, fortalece a importância do processo de implementação. Busca-se maior compromisso dos envolvidos, tanto no processo de adequação quanto no de manutenção e uso da LGPD.

> [...]a conscientização começou *top-down* com as chefias. A entrevista foi feita com o diretor administrativo e, em seguida, a conscientização se estendeu para as demais diretorias. Com o Presidente da mantenedora, diretores, todas as pró-Reitorias da Universidade; aí, depois das chefias específicas, nos cursos [para] as diretorias adjuntas nas unidades. O pró-reitor adjunto (de gestão financeira) participava das entrevistas da conscientização. E na entrevista em que a gente fez esse tratamento de dados, primeiro a gente fazia 30 minutos de conscientização, explicava a norma, impactos, [...] a ideia de fato é conscientizar [...] (Entrevistado 1).

Os meios utilizados para capacitação das equipes e dos demais envolvidos foram diversos, como relatado pelo Entrevistado 1 na UNI1.

> [...] Nós tivemos palestras, seminários, nós aplicamos alguns testes de conhecimento em 3 níveis nos setores, e a gente tem é trabalhado nesse sentido. É de atualização das práticas. É no sentido da aplicação da lei [...] (Entrevistado 2).

No que se refere ao desenvolvimento de competências os treinamentos ocorreram sob demanda. E, assim como na Governança de TI, na Governança de Dados, a capacitação dos colaboradores também ocorre sob demanda, principalmente após a pandemia do COVID-19.

Na UNI2 o time de adequação da LGPD é reduzido, conta apenas com o DPO, contudo há interesse por parte daquele gestor em contratar um colaborador para auxiliar nas atividades pertinentes à LGPD. Atualmente questões pertinentes à gestão dos dados de alunos, por exemplo (com dados pessoais sensíveis ou não) são realizados pela secretaria acadêmica e departamento financeiro. Nestes departamentos existe o ponto focal da LGPD, e quando surge questões pertinentes à tecnologia, o gerente de TI é acionado para auxiliar na resolução de uma demanda ou atividade. Este processo de utilizar os colaboradores dos departamentos nas duas IES são semelhantes, e segundo os entrevistados, possibilita a redução de custo de manutenção da LGPD nas IES.

A adequação da LGPD, na UNI2, foi realizada com treinamentos, alinhamento junto aos setores, palestras, divulgação por e-mail e outras formas. Cabe destacar que neste processo

de adequação houve a participação da alta administração da instituição, o que fortalece a importância e compromisso na adequação da instituição ao novo arcabouço legal.

A Figura 14 demonstra que a UNI2 possui publicado, em seu sítio eletrônico, uma página contendo as informações sobre o Comitê de Privacidade e Proteção de Dados Pessoais da instituição.

Figura 14 - Comitê de Privacidade e Proteção de Dados Pessoais – UNI2

Fonte: Fumec (2024).

A Figura 15 demonstra que a UNI2, em agosto de 2022, realizou um evento para divulgação e conscientização sobre Proteção de Dados Pessoais, em parceria com o Tribunal de Justiça de Minas Gerais. Este evento (virtual) apresenta que a UNI2 está efetivando o processo de comunicação e capacitação, conforme requerido pela LGPD.

Figura 15 - Evento para conscientização sobre Proteção de Dados Pessoais – UNI2

Fonte: Fumec (2024).

4.3 Comunicação

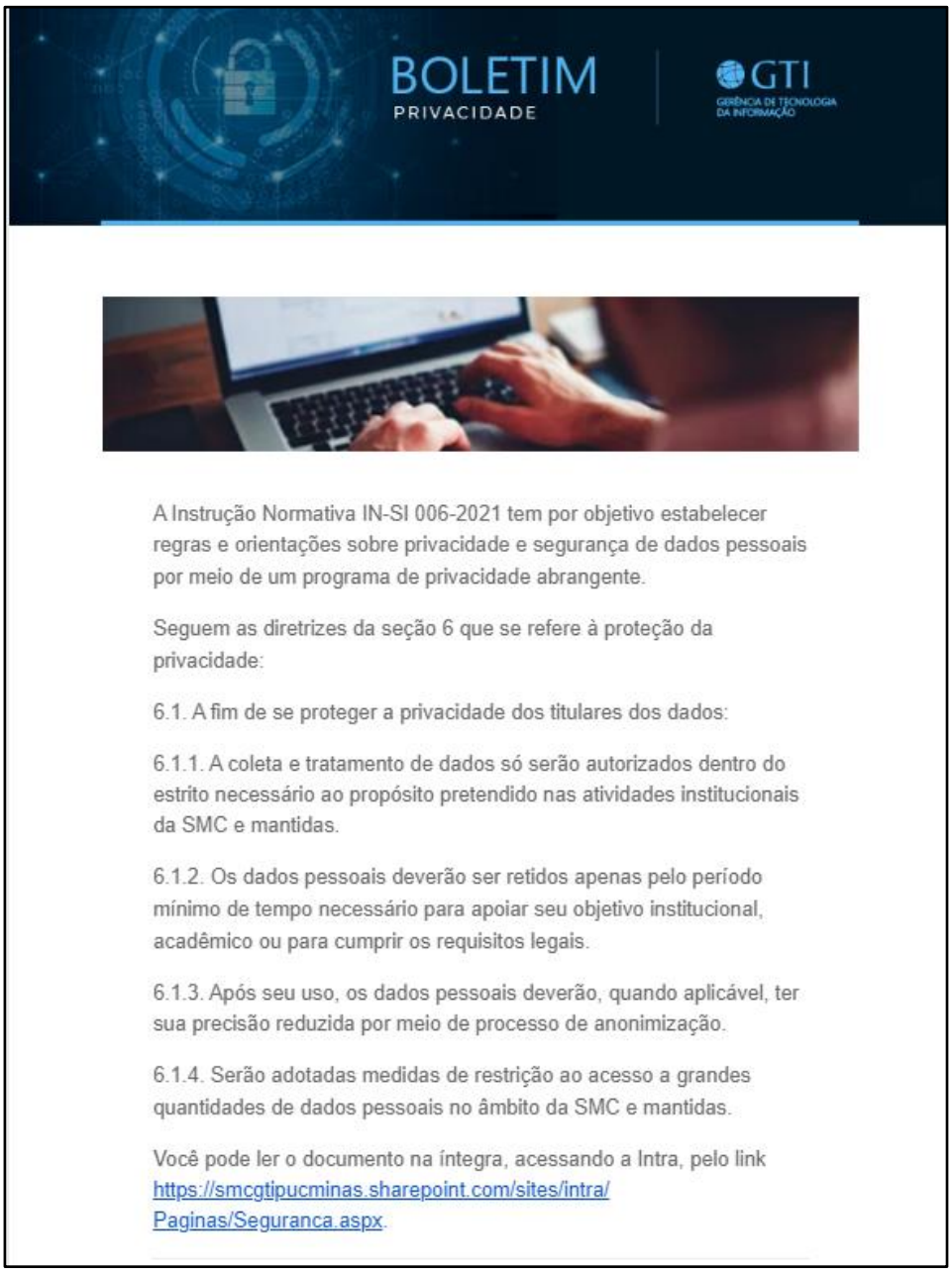
O processo de comunicação é extremamente relevante nas IES e em toda e qualquer organização. Quando se abordam processos corporativos (implementação de sistemas, rotinas, processos, leis e normas), eles devem ser muito bem definidos, orientados, direcionados e amplamente difundidos (ROCHA; LUZ, 2020). Nas IES estudadas, ele se mostrou não menos relevante e é realizado com frequência. Um amplo trabalho de conscientização e disseminação da LGPD foi realizado pelas instituições.

Na UNI1, semanalmente, é enviado um *e-mail* com temas alternados sobre LGPD (Privacidade de dados, da Informação) e sobre Segurança da Informação. Ou seja, a cada semana é enviado um relatório, alternando os temas. No caso da UNI2, as comunicações são

feitas sob demanda, não havendo um processo definido e sistemático. Ou seja, as comunicações ocorrem eventualmente e conforme a necessidade.

A Figura 16 demonstram que a UNI1, por meio da gerência de tecnologia (GTI), conforme processo comunicacional definido, emite boletim de privacidade ou boletim de segurança da informação. O conteúdo é intercalado, isto é, em uma semana publicam-se informações sobre LGPD (no boletim sobre privacidade), e, na semana seguinte, outro boletim sobre segurança da informação, sucessivamente.

Figura 16 - Boletim Privacidade – UNI1



Fonte: PUC Minas (2024).

No caso específico da UNI1, podem ser percebidas ações comunicacionais, conforme afirma o Entrevistado 1.

> [...] 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).

Ainda na UNI1 a comunicação frequente tornou o processo de adequação da LGPD melhor. Todas as semanas são enviados dois boletins para o público interno, sendo um sobre política de segurança e outro sobre boletim de privacidade. Somados a esses boletins, ocorrem *workshops*, com o público interessado (interno ou externo), de forma que permite uma interlocução redobrada e atualizada, ou seja, repassa-se a informação do nível operacional mais básico (conservação e limpeza, segurança) até as diretorias. Tal ação pode auxiliar ainda na descoberta de algum processo novo em determinado departamento.

Outra ação muito consolidada na UNI1 refere-se ao sítio referente à LGPD. Ele se apresenta bem estruturado, com conteúdo esclarecedor, inclusive com vídeo, e cumpre o requerido pela legislação. Possui dados do DPO da instituição, além de canal de comunicação para casos de suspeita de vazamento ou violação de dados.

> [...] Tem o como falar conosco. [?] Página principal / Segurança e Privacidade / Política de Privacidade / item 13 – como fazer contato conosco referente a esta política... tem o formulário que você preenche e aí você tem que anexar no segundo momento, no momento dois, pra gente dar sequência, tem que anexar um documento. Por quê? Para validar que você é você mesmo [...] (Entrevistado 1).

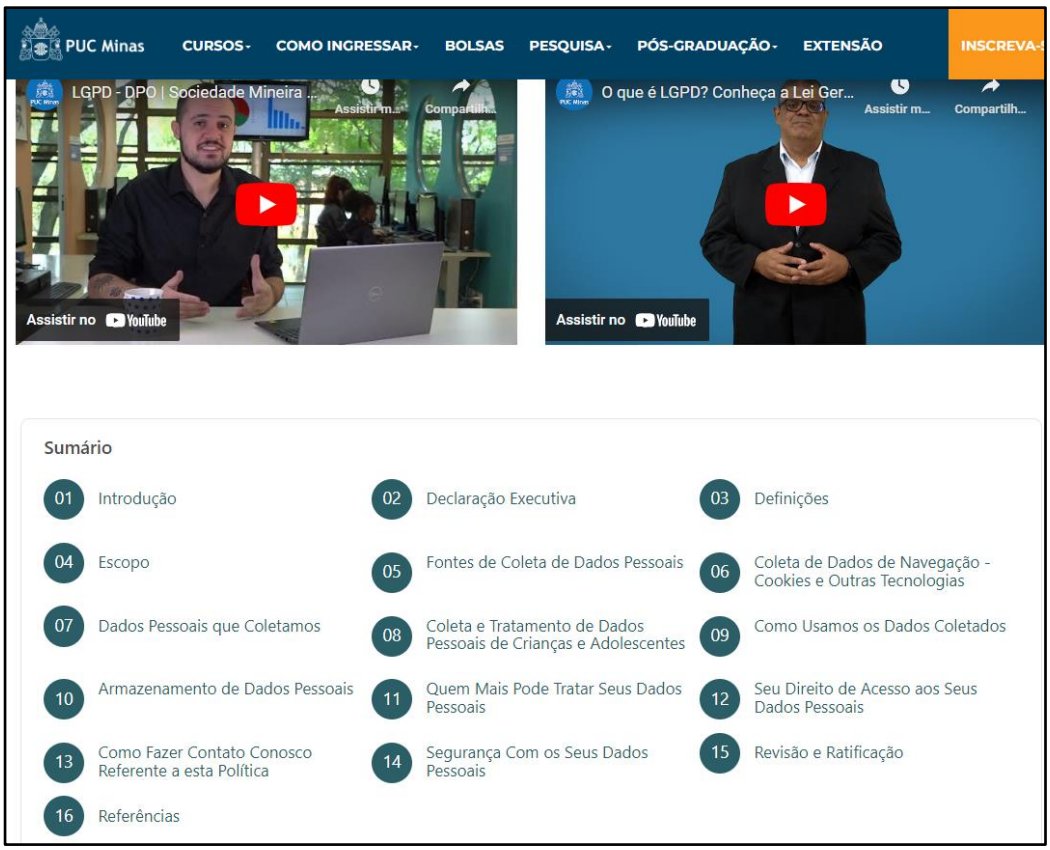
O processo de comunicação da LGPD, e também da Segurança da Informação, na UNI1, estão consolidados, conforme afirma também o gerente de TI:

> [...] a gente tem um boletim de segurança e o boletim de privacidade. Sabe, são bem instituídos, cada semana saindo; então, os boletins são quinzenais ... Então, uma semana sai privacidade, e em outra semana sai segurança e aí a gente pega. Por exemplo, fatos específicos que às vezes estão acontecendo no mercado e divulga, ou a gente pega trechos da política de segurança ou da política de privacidade e divulga. Só para ir reforçando isso e criando a conscientização corporativa, sabe? [...] (Entrevistado 2).

A Figura 17 demonstra que a UNI1 possui seu sítio eletrônico com diversas formas de interação com os usuários. Além de informações textuais, possui também vídeos explicativos

sobre o que é a LGPD, o papel do DPO. Esse tipo de comunicação facilita que o interessado, inclusive usuários com deficiência visual, compreendam o conteúdo também através de áudio.

Figura 17 - Sítio da UNI1 – Menu Privacidade de Dados



Fonte: PUC Minas (2024).

Percebe-se, portanto, que esses meios de comunicação, com a periodicidade estabelecida, contendo regras, comentários e recomendações, além de orientações, qualifica e solidifica todo o processo de adequação e de manutenção da LGPD.

Figura 18 - Sítio da UNI1 – Segurança com Dados Pessoais

Fonte: PUC Minas (2023).

Outro ponto de destaque na comunicação da UNI1 são as formas diversas de comunicação com as partes interessadas (aberto ao público interno e externo da UNI1), conforme relatado pelo gerente de TI:

> [...] *Workshop* de privacidade e segurança foram mais de 300 participantes. A gente gravou e colocou isso na intranet (no portal), a gente trouxe, inclusive uma pessoa do Gartner para poder falar, eu também tive uma fala nesse *workshop*. O Adriano também teve uma fala... falando um pouco sobre o mercado, o que é que está acontecendo, a importância e tudo mais, os riscos, né? E aí a gente entra depois falando um pouco das nossas ações, o que a gente conduziu esse ano, o que que a gente fez, né? Pra melhorar a segurança, as ações de Privacidade e tudo mais [...]. (Entrevistado 2).

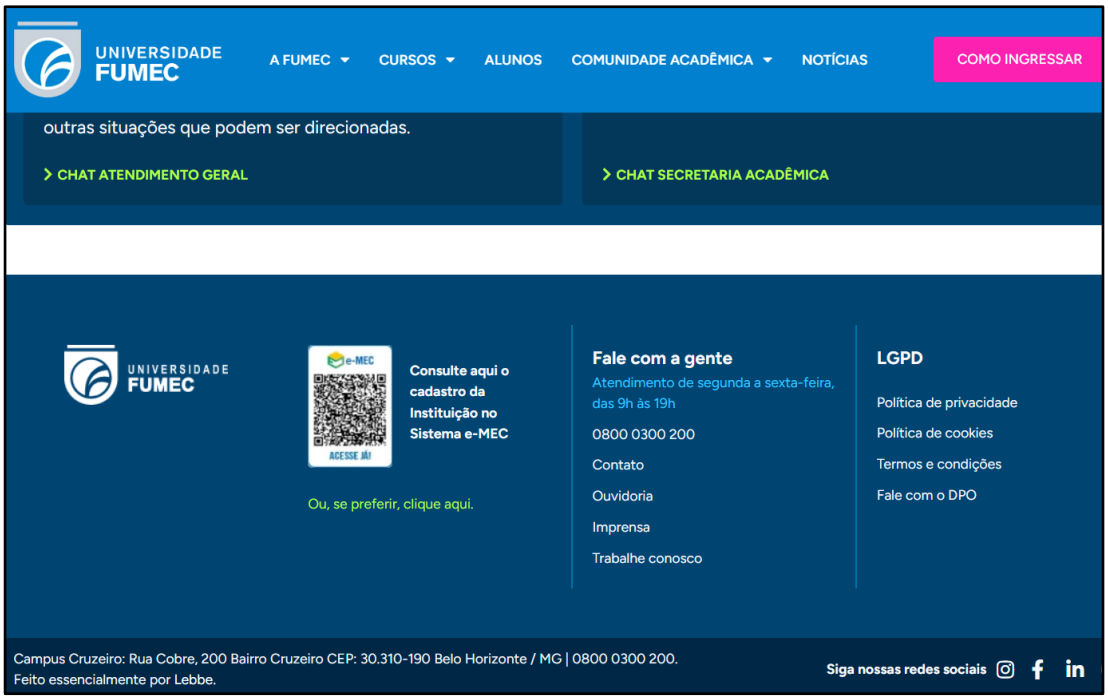
No caso da UNI2, o processo comunicacional abrangeu ambas as instituições de forma interna e externa. foi realizado um trabalho de conscientização e divulgação da adequação da LGPD, tanto para o público interno quanto externo, conforme afirma o Entrevistado 3.

> [...] (quanto ao) plano de comunicação, a gente também tem essa preocupação de trabalhar a comunicação interna e externa com relação à aplicação da lei geral de proteção de dados. [...] (Entrevistado 3).

A Figura 19 apresenta a tela do sítio da UNI2 com informações sobre a LGPD, como a Política de Privacidade, de *Cookies* e o Fale com o DPO (onde se pode contatar diretamente o

DPO da instituição). Esse recurso é requerido pela legislação e está em conformidade com ela. Na UNI1 existe uma tela semelhante, com essas informações.

Figura 19 - Sítio da UNI2 – Canal LGPD



Fonte: Fumec (2024).

O processo de comunicação da TI com os *stakeholders* é realizado oficialmente, na UNI2, por meio de *e-mails* e grupos de WhatsApp. Em caso de necessidade específica, pode ocorrer a comunicação individualizada, ou seja, do técnico ou analista de TI diretamente com o colaborador.

E, ainda dentro do cumprimento das exigências legais, as IES (UNI1 e UNI2) disponibilizam, em seu sítio eletrônico, um formulário específico para recebimento de comunicação externa referente a incidentes de segurança.

> [...] 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 (envolve procedimento) investigativa, 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).

4.4 Governança de TI e de Dados

Na UNI1 utiliza-se o *framework* ITIL parcialmente. Partes relevantes dele, como por exemplo a parte estratégica (que contém o quesito financeiro) está consolidada, segundo o entrevistado, na versão ITIL anterior à vigente, ou seja, utilizam conceitos da ITIL v3, contudo aprimorada com a aplicação de técnicas de agilidade (*framework* ágil).

Possibilitar às organizações a tomada de decisões estratégicas através 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). Assim, conforme identificado na UNI1, que utiliza parcialmente o princípio do *framework* ITIL, fica demonstrado que a GTI está em desenvolvimento dentro da instituição.

Neste sentido, é fortemente recomendável que o *framework* ITIL, ora parcialmente utilizado pela UNI1, seja implementado em sua totalidade, atribuindo a esta IES melhores condições de gerenciamento dos seus serviços de TI, e por via de consequência, melhor aderência à GTI e qualidade de respostas aos stakeholders no que tange à LGPD. Isto é, este *framework* pode trazer benefícios diretos no processo de adequação e uso da LGPD em ambas IES, como por exemplo a gestão de incidentes, a gestão de atendimento aos usuários, o monitoramento do ambiente, dentre outros benefícios.

Na UNI1, o plano de continuidade de negócios está estabelecido e auditorias regulares são realizadas para aferir a aplicação dos requisitos definidos naquele plano, como afirma o gerente de TI:

> [...] Nós temos hoje um plano de continuidade de negócio que a gente reporta anualmente à Price (Pricewaterhouse). A gente é auditado anualmente pela Price, né? A praxe é auditar todos os processos de geração de receita da instituição para poder assinar e respaldar o nosso Balanço... Eles auditam também toda a nossa infraestrutura de TI [...] (Entrevistado 2).

Na UNI1, existem métricas estabelecidas para mensuração de resultados. Os indicadores possuem características diversas, como financeiro, recursos humanos e apropriação de serviços.

> [...] E a gente tem algumas outras métricas. Por exemplo, infraestrutura de telecomunicações, como é que eu distribuo o custo disso pelo número de computadores de cada unidade física que eu atendo; [...] como é que eu faço a distribuição de consumo dos meus serviços, e então tem o RH: [a relação] homem x hora que eu faço apropriação e tem também essa métrica de número de computadores por local [...] A gente apropria isso diariamente, o ano inteiro, mas no final de cada ano a gente faz um rateio entre as instituições [...] (Entrevistado 2).

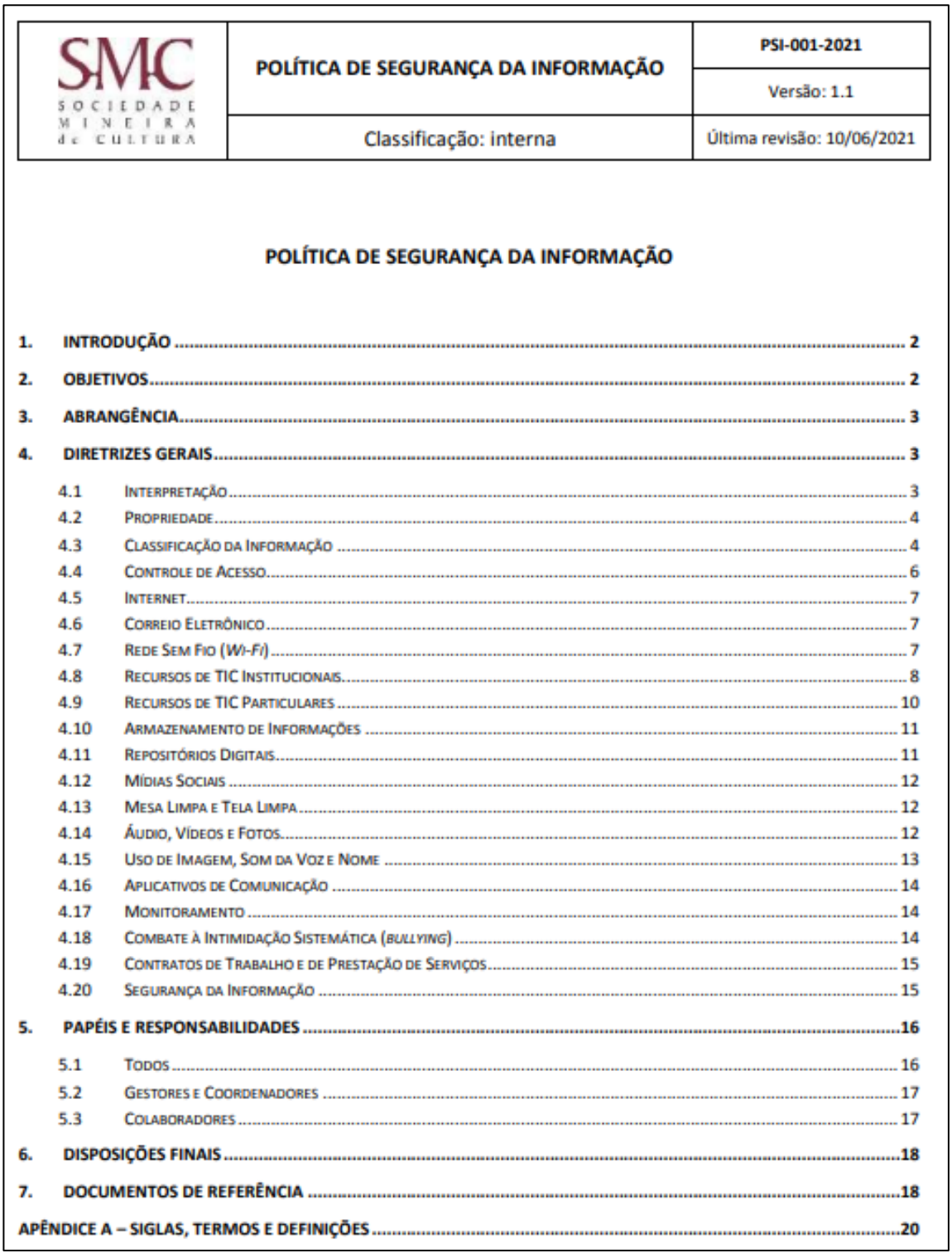
A governança de dados, em relação à LGPD, é relativa na UNI1. Não há política de governança de dados definida ou um setor/departamento específico para esse fim. A

manipulação de dados está restrita aos sistemas de banco de dados, e, quando se trata de assuntos relacionados à LGPD, um analista (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 dentro daquela instituição. Ocorre, de certa forma, um tratamento analítico de dados prévio, sob a ótica de um DBA com expertise em LGPD. Portanto, não há plano de governança de dados estabelecido e nenhum *framework* desta natureza implementado, especificamente ao fim que se destina a GD, apenas uma iniciativa incipiente de gestão de dados organizacionais.

Desta forma, a Governança de Dados, mesmo que incipiente na UNI1, não está sendo utilizada ou explorada em sua plena capacidade ou ainda utilizando-se de todos os recursos a qual oferece. Com a adoção da GD os dados corporativos assumem maior importância na cadeia de valor, inclusive auxiliam na definição de estratégias de negócios (são fatores direcionadores); auxilia na tomada de decisão, possibilita atingir maior eficácia na gestão das informações organizacionais, pois os dados são vistos sob outro prima (maior relevância); os processos organizacionais são reaaranjados diante da relevância dos dados; além de outros aspectos relevantes para a IES. Na Figura 11 apresentou-se as diversas frentes em que o dado pode ser visto e considerado dentro das organizações, de acordo com o guia DAMABOK.

A Figura 20 apresenta o sumário da Política de Segurança da Informação da UNI1. É possível perceber que ela contempla os requisitos elencados, por exemplo, na *ABNT NBR ISO 27.701 – Segurança da Informação*. Merece destaque que ela aborda um amplo conjunto de diretrizes corporativas, bem como apresenta o rol de Papéis e Responsabilidades, demonstrando sinal de maturidade no trato e na gestão da segurança das informações da instituição.

Figura 20 - Índice da Política de Segurança da Informação da UNI1



SMC SOCIEDADE MINEIRA de CULTURA	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2021
		Versão: 1.1
	Classificação: interna	Última revisão: 10/06/2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Fonte: PUC Minas (2024).

Em relação a UNI2, o Entrevistado 4, que atua há onze anos na instituição, exerceu atividades como analista de redes (infraestrutura) e, há dois anos, exerce a atividade de gestor de TI. A TI está subordinada à Reitoria da instituição, cujas atribuições e papéis estão bem

definidos e estruturados, segundo o Entrevistado 3. A TI é vista como uma unidade que gera valor para a instituição, apesar de não haver um Plano Diretor de Tecnologia – PDI (Entrevistado 4).

O alinhamento estratégico com a diretoria ocorre, de certa forma, informalmente, ou seja, o gerente de TI, em caso de necessidade, aciona a diretoria para discutir determinadas ações, projetos ou necessidades. Não há um procedimento formal definido, isto é, o acionamento/alinhamento ocorre sob demanda. Uma das razões para ocorrência de tal fato se dá pela própria facilidade de acesso entre ambos.

No que se refere à inserção da TI nos negócios da IES, o gerente de TI, na UNI2, afirma que praticamente toda a organização reconhece a importância da TI, e, por conseguinte, a comunicação com eles é comum (consciência corporativa). Em caso de demanda de determinado setor, ocorre a interação entre a TI e o solicitante através de reuniões para análise de demanda, desenvolvimento de solução ou correção de problema, e, nessa situação, caso a demanda seja relevante, o gerente de TI aciona o corpo diretivo. Essas demandas são registradas em formulário específico, contido na intranet das instituições. Vale destacar que o mesmo está sendo modificado devido a mudanças estruturais na área de TI (sistemas locais, sistemas em nuvem, infraestrutura e outras).

A Reitoria, junto com a Fundação mantenedora da UNI2, possui um plano de continuidade de negócios, isto é, um plano geral que contém as diretrizes para as instituições componentes da Fundação. Porém, não há um plano específico de governança de TI.

A gerência de TI, na UNI2, está desenvolvendo um plano geral para medição de serviços/atividades de TI, através de KPIs ou indicadores de performance. A UNI2 está implementando um *software* gratuito, denominado GLPI, o qual permite a gestão dos ativos tecnológicos. Logo, após a adequação deste, a intenção é criar os indicadores de forma mais específica e controlada.

Dessa forma, evidencia-se a aplicação de alguns métodos de governança e gerenciamento de TI, isto é, segundo Weill e Ross (2006), as IES necessitam controlar os investimentos em TI (*Hardware* e *Software*) bem como mensurar a contribuição dos seus serviços e sua infraestrutura (inclui-se ativo fixo, custos diretos, indiretos, investimentos) para aquelas instituições com vistas a atingir suas metas corporativas (Weill; Ross, 2006). E a mensuração de resultados, realizada pelo Entrevistado 2, é uma das vantagens do emprego da GTI.

Quanto aos *frameworks* de GTI, a UNI2 não os possui formalmente definidos e publicados na instituição. Ela os utiliza de forma parcial (trechos) ou até mesmo de forma empírica. Estes segmentos ou trechos de procedimentos estão de acordo com as boas práticas dos *frameworks* mais conhecidos, como COBIT e ITIL. Há iniciativas de implementação, porém não efetivamente implementadas. Situação semelhante ocorre com a aplicação/utilização da norma ISO 38500:2015.

A razão assiste a Moreira Neto *et al.* (2019) ao afirmarem que a "TI é essencial para a transformação da administração das organizações [...] mudando seu status para governança", isto é, a adequação da LGPD nas IES foi possível devido à articulação do DPO com as demais áreas de negócio que compõem tais instituições. E, no caso da inserção de comitês para auxiliar na adequação da LGPD, evidencia-se a aderência da GTI naquelas IES.

É importante citar que, na UNI2, o procedimento para gestão de risco está sendo escrito, ou seja, não há um plano implementado, consolidado ou mesmo testado. Na UNI1, os riscos foram mapeados nos quatrocentos processos elencados para a adequação da LGPD. Porém, não foi criado um documento ou procedimento específico para a gestão de risco.

Na UNI1 e na UNI2 não existe uma política de governança de TI formalmente definida, porém existe um comitê executivo, que, em tese, exerce as atividades pertinentes a governança da TI e governança de dados. Ou seja, o comitê de governança de TI naquelas IES não está formalmente instituído para este fim, porém os comitês executivos exercem tal papel de forma adicional.

A gestão de riscos é inerente à GTI e até mesmo à governança corporativa. As organizações, em geral, necessitam de uma estrutura eficaz de gerenciamento de riscos, principalmente após a disponibilização de seus serviços educacionais em plataformas *on-line*. Apesar do entendimento da necessidade de seu uso em escala, ou seja, reconhecimento pelas organizações de sua importância, compreensão da academia científica de sua utilidade, a gestão de risco, em IES, parece ser menos importante (Ariff *et al*., 2014). Identificou-se, na UNI1 e na UNI2, a ausência daqueles procedimentos formais para o tratamento dos riscos advindos da TI, o que permite concluir que há espaço para melhoria do processo de GTI.

> [...] Tem um procedimento. Não existia, nós o estamos escrevendo aos poucos e ele já está amadurecendo [...] (Entrevistado 4).

No caso da UNI2, a Governança de Dados é praticamente inexistente, ou seja, não é utilizado nenhum tipo de *framework* consolidado de mercado ou nem mesmo possui um profissional com função específica para o exercício das atribuições requeridas pela Governança

de Dados. Ambas IES possuem DBA (profissional que gerencia o banco de dado na área de TI), no caso da UNI2, este profissional possui expertise para lidar com as atribuições pertinentes ao cargo além de conhecimento avançado em LGPD. Qualquer atividade que envolva armazenamento, exclusão, alteração ou inclusão de dados que se referem à LGPD no banco de dados da instituição, necessariamente, tem que passar por sua análise.

Não há política de governança de dados definida nem um setor ou departamento, propriamente dito, para este fim. Mesmo que a manipulação de dados seja elevada, com alto fluxo de áudio e vídeo (cursos EAD), e haja grande quantidade de informações de discentes e terceiros, a manipulação de dados, ainda assim, está restrita aos sistemas de banco de dados. A manipulação de dados está restrita aos sistemas de banco de dados. Não foi identificada, nas entrevistas, qualquer tipo de tratamento analítico de dados nas grandes bases de dados existentes dentro da organização. A gestão dos dados fica a cargo dos setores específicos (geradores e usuários destes) e o armazenamento está sob a responsabilidade da TI (administrador de banco de dados ou DBA). Portanto, não há plano de governança de dados estabelecido e nenhum *framework* desta natureza implementado, nem foi identificado, qualquer Comitê de Governança de Dados ou específico para este fim.

Uma condição a ser avaliada, em ambas IES, é a alocação de um profissional com um perfil da dados, como um DBA por exemplo, porém com viés inclinado a análise de dados, como por exemplo, o *data analitycs*, estatística e até mesmo a matemática computacional.

> [...] Não existe um departamento para tratar os dados: todos os dados são tratados na TI. Quem cuida dos dados é a TI, mas na manipulação dos dados existe o setor, por exemplo, é o setor de contabilidade. Que eles ficam responsáveis manipular os dados. Existe o setor de Secretaria, que fica responsável de manipular os dados da Secretaria. Existe o setor de cobrança, eles são responsáveis pela parte dos dados da cobrança [...] (Entrevistado 4).

Esta condição pode remeter a algumas reflexões e cenários, como por exemplo: a) as IES não se atentaram para a real importância da disciplina de Governça de Dados; b) não possuem recursos financeiros para tal investimento; c) não possuem interesse na sua utilização (desconhecimento de benefícios); d) falta de estrutura técnica e humana para atuar com esta disciplina; e) não a consideram relevante; dentre outras inúmeras situações ou conjecturas sobre a própria GD.

Vale destacar que, na UNI1 e na UNI2, não foram criadas políticas específicas, de maneira formal, para a gestão de riscos envolvendo dados; há o procedimento definido pela ANPD, que é o RIPD, para relatar incidentes com dados organizacionais, conforme relata o

Entrevistado 4. O guia DAMABOK2 (2015) ensina que é essencial, para a gestão de dados corporativa, a criação de uma política específica para esse fim. Nessa política se detém o olhar para a coleta, processamento, armazenamento, tratamento e descarte dos dados de uma forma segura e eficaz (DAMABOK2, 2015, p. 27).

> [...] A política ... não foi criada. Ela está sendo um embrião, vamos falar assim, né? É. Quando acontece uma situação dessa (incidente), né? A gente vê quem é a pessoa, por exemplo. Tem uma pessoa do administrativo ali, está consumindo uma coisa muito alta. A gente chega lá e olha quem está na máquina, não é? A gente vê quem está logado, lógico, não é? Chega lá, mas vê visualmente. Quem está logado é o fulano. Não é, senão então, beleza, passa para mim. Eu vou no departamento, pessoal ou vou diretamente no coordenador da pessoa. Informal, só porque tem que amadurecer muita coisa ainda [...] (Entrevistado 4).

A comunicação pertinente a ações que envolvem tratamento de dados, como, por exemplo, uma migração do banco de dados de uma tecnologia para outra, ocorre de maneira formal através de *e-mail* e grupos de WhatsApp. Em determinados casos, o conselho de LGPD (que exerce as funções de Comitê de TI, em certas circunstâncias) analisa a demanda, e, se necessário, envolve a Reitoria da instituição. Caso a situação não requeira uma ação de emergência ou de urgência, o rito é seguido conforme exposto. Porém, em caso de situação grave, o gerente de TI age e comunica posteriormente à alta administração sobre o fato ocorrido e as ações tomadas.

> [...] É, infelizmente, tem urgências e emergências, né, que ocorrem na TI. Está sofrendo um ataque, por exemplo, espera aí que eu vou comunicar. Não vai dar, né? [...] (Entrevistado 4).

4.5 Tratamento de dados pessoais

O processo de tratamento de dados pessoais está estabelecido e é formal nas IES selecionadas (UNI1 e UNI2). Existem canais específicos para o tratamento desse tipo de demanda e dentro do prazo estabelecido. Pode-se ilustrar, em ambas as IES, que existem políticas voltadas para o tratamento de dados pessoais e também para a segurança da informação. Os requisitos mencionados na LGPD são contemplados por essas políticas, ou seja, as IES pesquisadas estão em *compliance* com o requerido legal.

A legislação exige que incidentes relativos à privacidade dos dados devem ser comunicados à ANPD. Em ambas as IES, tanto em seu sítio quanto em suas políticas de privacidade de dados, existem espaços apropriados para tal comunicação e proteção. Isto é, quanto à adequação da lei, as IES estão aderentes e em conformidade com o requerido.

> [...] Recebemos, com uma certa frequência, demandas dos titulares dos dados, e temos atendido dentro do prazo legal e também de acordo com as exposições legais normativas, a parte que envolve tanto as bases legais e a questão da gestão do consentimento; a gente tem trabalhado também nesse sentido, principalmente com as áreas que tratam um volume maior de dados que aqui na instituição; e a questão do relatório de impacto, a proteção de dados pessoais a gente tem trabalhado de forma pontual [...] (Entrevistado 1).

No caso da UNI1, na implementação, inicialmente, foi utilizado o conceito de *Privacy by Default* (privacidade por padrão)[6]. 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* (privacidade pelo desenho ou por concepção)[7], isto é, a implementação da proteção de dados é estabelecida desde a sua concepção, e não mais por um padrão previamente estabelecido. Nesta IES, evidencia-se também que, ao longo da existência da LGPD na instituição, todo o processo relacionado a ele recebe melhorias. A título de exemplo, foi adquirido, no segundo semestre de 2021, um software (DPS (Data Privacy System – da OneTrust), que auxilia na manutenção e controle da legislação aplicada na IES. Em maio de 2022, este *software* se tornou disponível e operacional para a IES (primeira carga do *datamaping*). Logo, entende-se que o sistema é alimentado continuamente, ou seja, está em constante evolução.

> [...] O *datamaping* foi feito em 2020/2021, o sistema foi adquirido no segundo semestre de 2021. Em maio de 2022, ele realmente estava disponível para trabalhar com ele. E agora a gente conseguiu colocar e fazer; agora que a gente conseguiu fazer a primeira versão da carga de mapeamento; isso foi feito primeiramente num formulário e numa planilha do Excel, e agora conseguimos colocar as informações do *datamaping* dentro da informação do sistema [...] (Entrevistado 1).

A Figura 21 apresenta a tela de Política de Privacidade da UNI1. Neste canal, é possível perceber que o conjunto que trata da privacidade de dados pessoais está estruturado por seções (semelhante à estrutura da própria LGPD). Há uma sequência definida e objetiva de

---

[6] *Privacy by Default* (privacidade por padrão): representa a instituição de que todas as ferramentas para preservar a privacidade estejam acionadas como padrão, isto é: a configuração padrão já onfere a maior expectativa de privacidade possível ao titular de dados pessoais. Os agentes de tratamento devem, pois, 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 acidentais ou 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 já estar adequados à LGPD, conforme o art. 46, § 2º.

[7] *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. 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.

informações sobre o tema, inclusive com a opção para o tratamento de dados pessoais (opção 14).

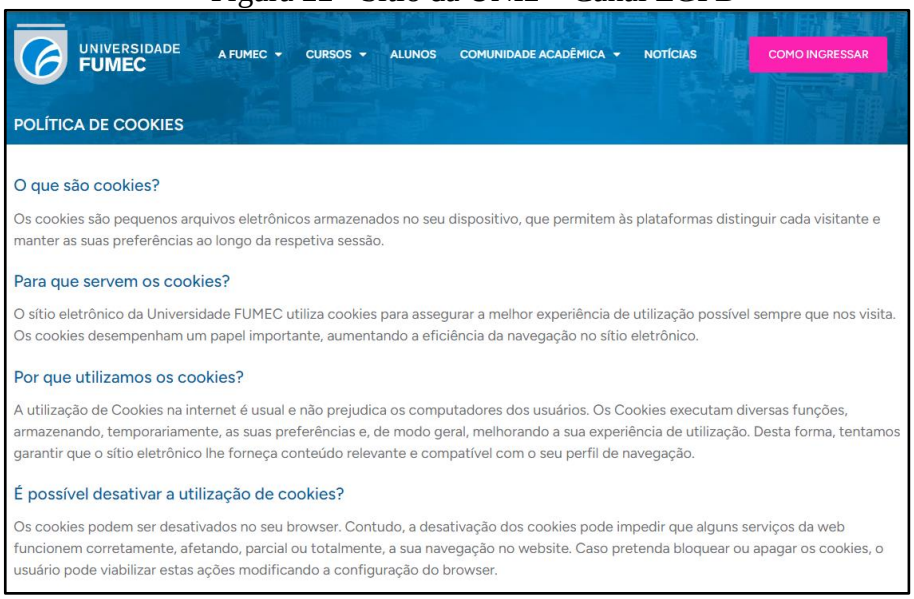
Figura 21 - Sítio da UNI1 – Política de Privacidade

Fonte: PUC Minas (2023).

As IES possuem canal específico para tratamento de dados pessoais. Nota-se que as informações ali expostas se apresentam de maneira clara e objetiva. Demonstra-se com isso que o aparato para tratamento de dados está disponível para consulta pública e atendendo aos preceitos normativos da LGPD.

A Figura 22 apresenta a tela do sítio da UNI2, com informações sobre a LGPD, especificamente, a Política de Tratamento de *Cookies*, ou seja, com informações sobre quais dados serão coletados (ou não) do dispositivo do usuário. Esse recurso é também requerido pela legislação e está em conformidade com ela.

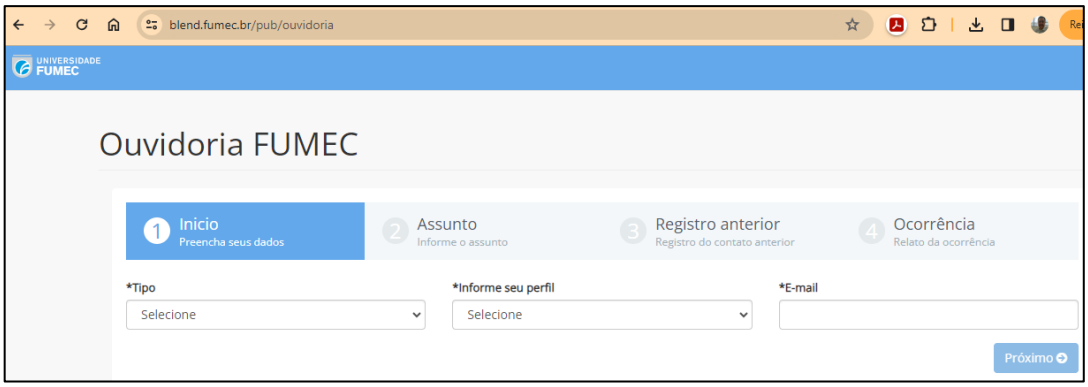
Figura 22 - Sítio da UNI2 – Canal LGPD



Fonte: Fumec (2024).

A Figura 23 apresenta a tela específica do sítio da UNI2, em que se pode acionar a ouvidoria para realizar denúncia. Esta é uma opção ao canal de registro de incidente com dados pessoais, ou seja, é um canal adicional de registro de incidente ou reclamação que a universidade disponibiliza.

Figura 23 - Formulário para contato com a Ouvidoria da Fumec



Fonte: Fumec (2023).

No que se refere a ameaças de sequestro de dados ou invasões nas UNI1 e UNI2, não foram registrados casos desta natureza, e no caso de ocorrência, há plano de ação para tratamento de riscos.

> [...] não tivemos casos de violação. Nós tivemos casos de incidentes de segurança que eu fiz uma análise, vendo p que a lei e os normativos dispõem e, dentro dessas, dessas situações pontuais, eu entendi tecnicamente que não seria necessário acionar ANPD,

> então, por enquanto, não tivemos nenhum caso para fins de acionamento da ANPD [..] (Entrevistado 1).

Houve ocorrência de Incidente na UNI2, mas sem gravidade, sem prejuízo relatado, tendo sido submetido ao DPO e ali tratado. Vale destacar que, conforme diretiva da ANPD, em casos de ocorrência de incidentes de segurança, por força de lei, a instituição deve comunicar o fato imediatamente àquela agência. Para tanto, as IES possuem formulário específico para tal comunicação, baseado no próprio modelo disponibilizado pela ANPD.

As informações abaixo são requeridas no relatório a ser enviado para a ANPD, dentre outras:

Tratamento

a) Descrição do Tratamento

A descrição dos processos de tratamento de dados pessoais, que podem gerar riscos às liberdades civis e aos direitos fundamentais, envolve a especificação da natureza, escopo, contexto e finalidade do tratamento. Conforme a LGPD (art. 5º, X) tratamento de dados é:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos. Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

b) Natureza do tratamento

Como a instituição pretende tratar ou trata o dado pessoal – como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados; medidas de segurança atualmente adotadas; se se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais.

c) Escopo do tratamento

O escopo representa a abrangência do tratamento de dados. Contém as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dados são considerados dados pessoais sensíveis; o volume dos dados pessoais a serem coletados e tratados; a extensão e frequência em que os dados são tratados; o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados; o número de titulares de dados afetados pelo tratamento; e a abrangência da área geográfica do tratamento.

d) Contexto do Tratamento

Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados; destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável. É importante destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados.

e) Finalidade do Tratamento

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

É importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo (Art. 7º e 11º da LGPD), no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;

• atender aos interesses legítimos do controlador ou de terceiro;

• proteção do crédito;

• garantia da prevenção à fraude e à segurança do titular.

Partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o 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 (LGPD, art. 6º, III).

Identificação e avaliação de riscos

O art. 5º, XVII, da LGPD, preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de riscos". Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-se a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Medidas para tratar os riscos

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 (LGPD, art. 46). É importante reforçar que as medidas para tratar os riscos podem ser de segurança, técnicas ou administrativas.

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação. No entanto, se houver um

risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

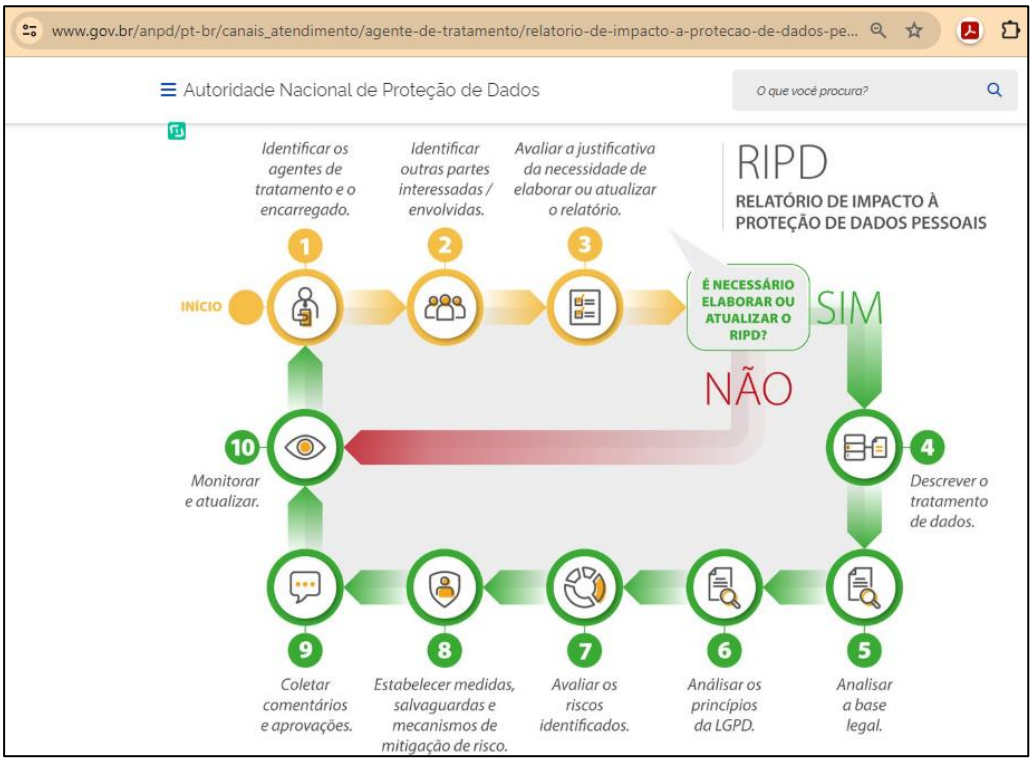
> [...] Nós utilizamos um modelo da própria ANPD; nós temos aqui essa prática. A gente preenche o formulário e debruçamos sobre esse incidente, para ver se realmente é uma questão que se faz necessário comunicar à ANPD ou pode ser trabalhado internamente e não vai gerar nenhum dano a nenhum titular [...] (Entrevistado 3).
> Assim como na UNI2, o RIPD é também é utilizado na UNI1, conforme as definições da própria ANPD (formulário padrão). O propósito deste relatório é realizar a comunicação entre o Controlador/Operador e a ANPD. Esta comunicação torna-se obrigatória quando houver comprometimento de dados organizacionais (invasão, sequestro ou roubo) que possam vir a prejudicar os titulares de dados por exposição destes (Entrevistado 3).

> [...] agora o RIPD 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. Então nós estamos, a partir da leitura da lei 13.709, identificando um detalhamento um pouco maior do público, que é eventualmente impactado se eu tiver alguma situação, algum incidente de dados e que aquelas atividades de que eu trato os dados que têm como base legal para legítimo interesse. Então qual que é o público? Qual que é a extensão do incidente? [...] estamos fazendo esta atividade somente para aquelas que tratam do legítimo interesse. Uma vez que conseguirmos automatizar, faremos para todas. [...] (Entrevistado 2).

Não foram inseridos, nesta pesquisa, exemplos de RIPD das IES pesquisadas, visto que as informações ali contidas são, via de regra, pessoais, uma vez que o titular dos dados utiliza tal relatório para apresentar o incidente ou fato que o considera desabonador de conduta por parte do operador/controlador.

A Figura 24 apresenta o fluxo do processo a ser utilizado, pelas instituições, para elaboração de um relatório de impacto sobre a privacidade de dados (RIPD). É um processo sugerido pela ANPD e não um normativo. A composição do relatório é necessária e obrigatória por força de lei. Contudo, o processo e o formato para elaboração do mesmo não foram estabelecidos compulsoriamente. Cada instituição tem o seu arbítrio para determinar os processos e formas de relato dos incidentes. Contudo, a diretiva apresentada auxilia as organizações neste objetivo. A Universidade de Pelotas disponibiliza um ensaio sobre RIPD, referência https://wikigovernanca.ufpel.edu.br/_media/ens.ripd.ufpel.pdf (UFPel, 2024). Consta no Anexo D um modelo de RIPD, com referência.

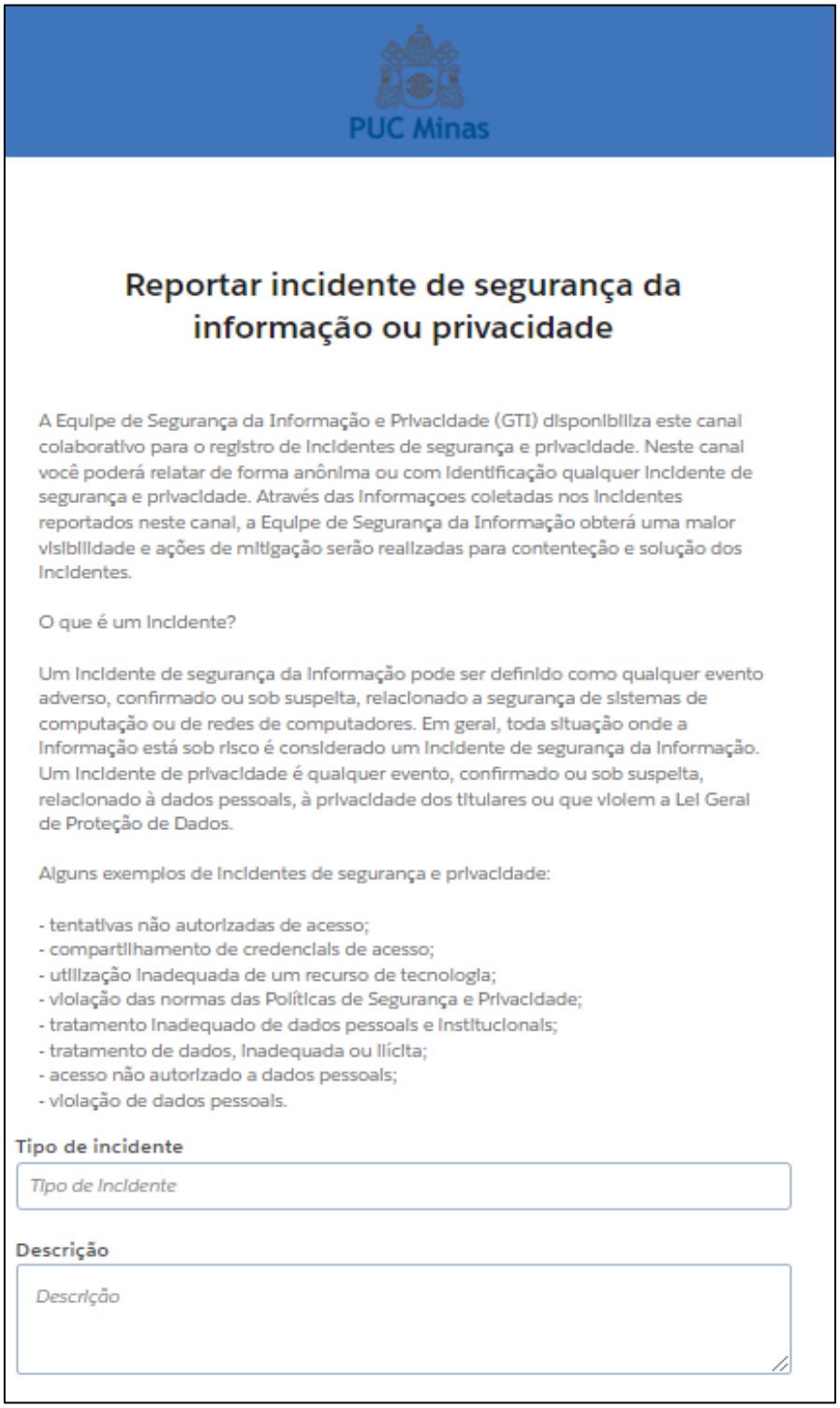
Figura 24 - Fluxo de processo sugerido pela ANPD para aplicação do RIPD



Fonte: ANPD (2023).

A Figura 25 apresenta o formulário para reportar incidente de segurança da informação ou privacidade na UNI1. O formulário está organizado e funcional. No processo de abertura de um incidente, pode-se especificar o seu tipo ou objeto (Intrusão, Farsa, Perda/Roubo, Vazamento de dados pessoais, divulgação de informação não autorizada), descrição do incidente, data de ocorrência e de descoberta e local. Esta possibilidade abre um canal de comunicação diretamente com o DPO da instituição.

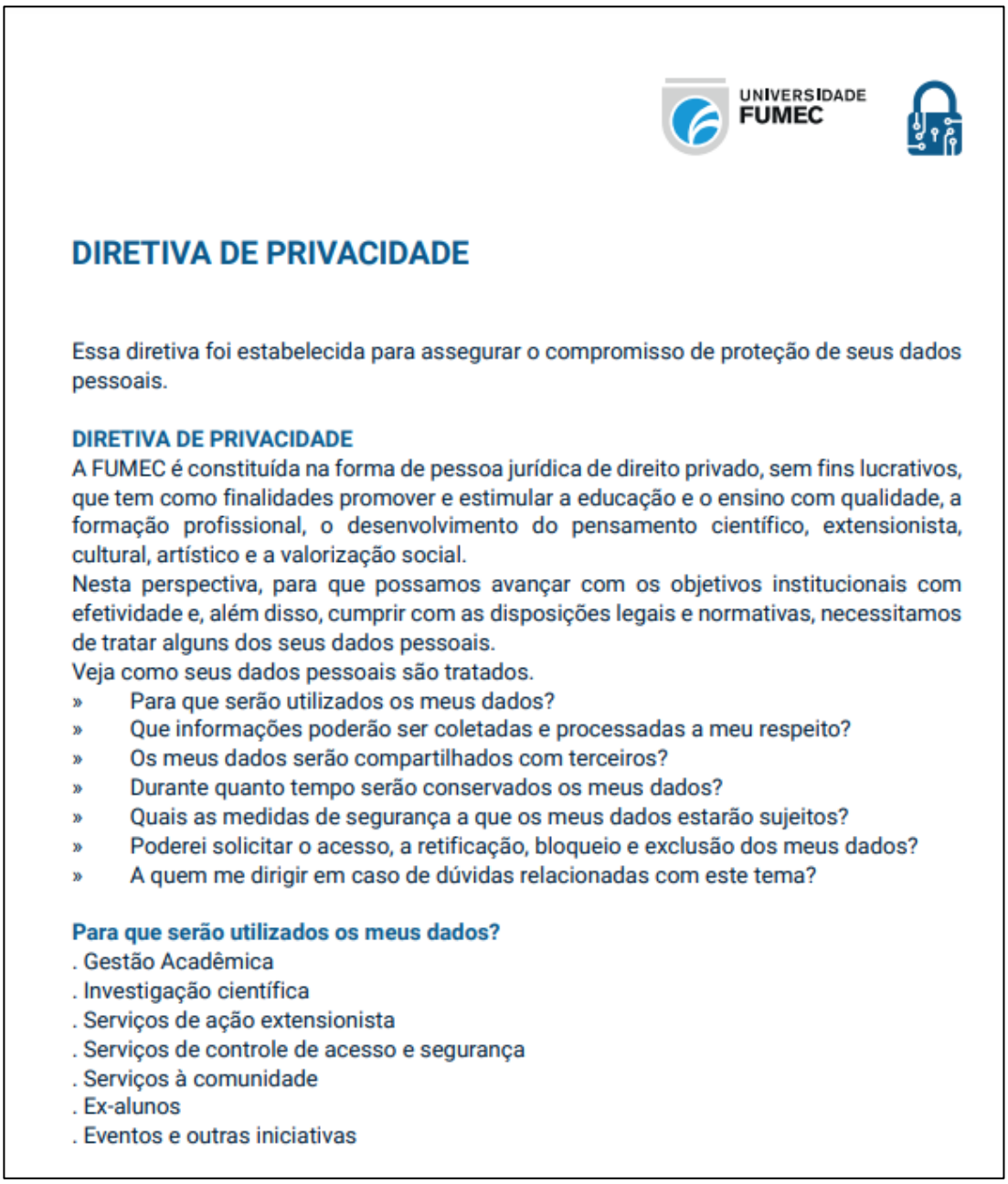
Figura 25 - Formulário para reportar incidente de segurança da informação ou privacidade UNI1



Fonte: PUC Minas (2024).

A Figura 26 apresenta a Diretiva de Privacidade da UNI2. Ela possui o propósito de assegurar o compromisso da instituição com a proteção de dados pessoais. Ela é estruturada, informando por que os dados pessoais serão utilizados, por qual setor, entre outras informações.

Figura 26 - Diretiva de Privacidade (proteção de dados) da UNI2



UNIVERSIDADE FUMEC

DIRETIVA DE PRIVACIDADE

Essa diretiva foi estabelecida para assegurar o compromisso de proteção de seus dados pessoais.

DIRETIVA DE PRIVACIDADE

A FUMEC é constituída na forma de pessoa jurídica de direito privado, sem fins lucrativos, que tem como finalidades promover e estimular a educação e o ensino com qualidade, a formação profissional, o desenvolvimento do pensamento científico, extensionista, cultural, artístico e a valorização social.

Nesta perspectiva, para que possamos avançar com os objetivos institucionais com efetividade e, além disso, cumprir com as disposições legais e normativas, necessitamos de tratar alguns dos seus dados pessoais.

Veja como seus dados pessoais são tratados.

» Para que serão utilizados os meus dados?
» Que informações poderão ser coletadas e processadas a meu respeito?
» Os meus dados serão compartilhados com terceiros?
» Durante quanto tempo serão conservados os meus dados?
» Quais as medidas de segurança a que os meus dados estarão sujeitos?
» Poderei solicitar o acesso, a retificação, bloqueio e exclusão dos meus dados?
» A quem me dirigir em caso de dúvidas relacionadas com este tema?

Para que serão utilizados os meus dados?

. Gestão Acadêmica
. Investigação científica
. Serviços de ação extensionista
. Serviços de controle de acesso e segurança
. Serviços à comunidade
. Ex-alunos
. Eventos e outras iniciativas

Fonte: Fumec (2024).

A Figura 27 apresenta a Diretiva de Privacidade da UNI2. Ela possui o propósito de assegurar o compromisso da instituição com a proteção de dados pessoais. Ela é bem estruturada, informando por que os dados pessoais serão utilizados, por qual setor e de que forma.

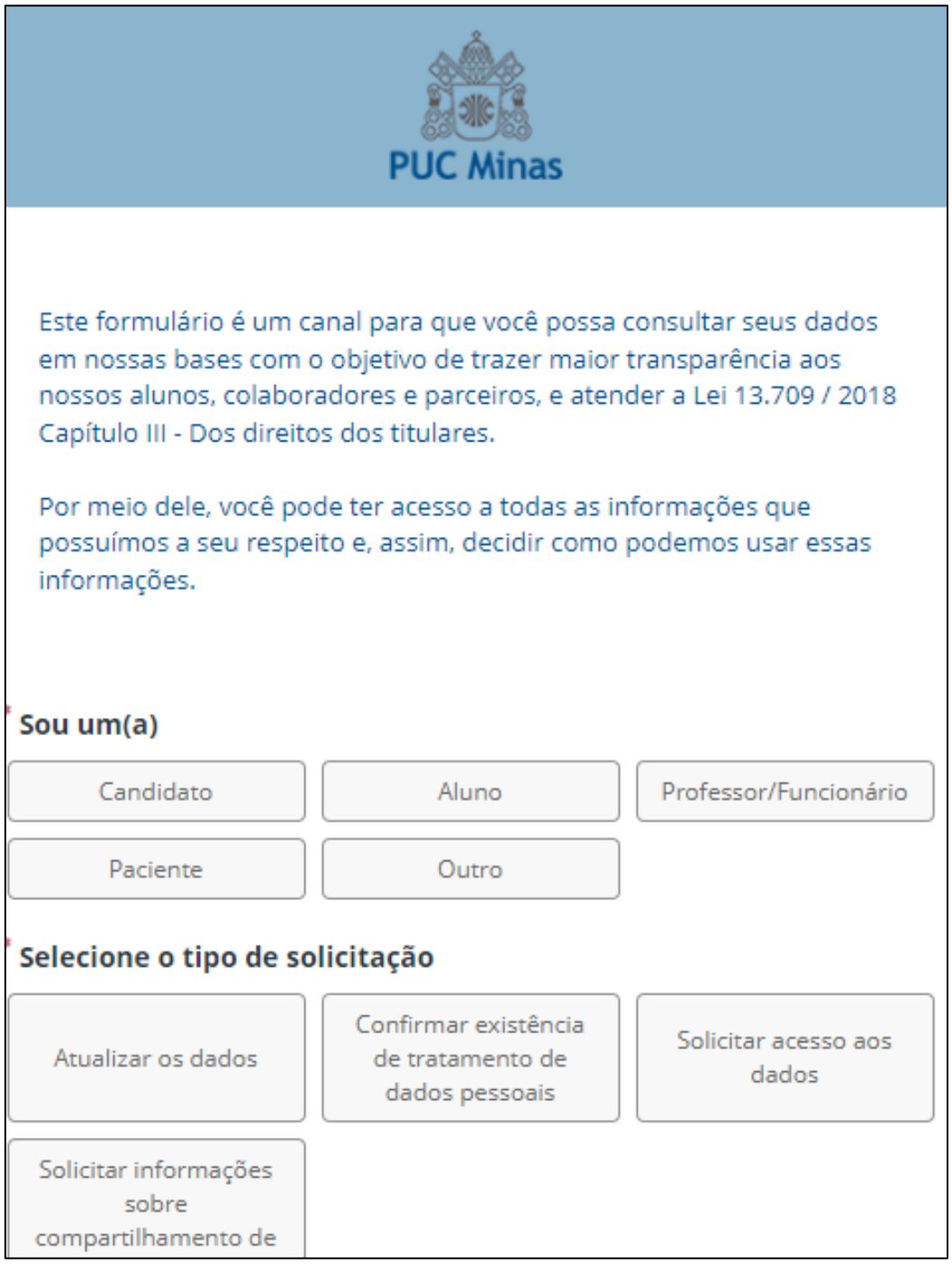
Figura 27 - Categoria de informações para coleta de dados da UNI2

Categorias	Exemplos
Dados de identificação	nome; registro acadêmico; fotografia; filiação; nacionalidade; naturalidade; data de nascimento; gênero; estado civil; CPF; número do documento de identificação.
Dados de contato	endereço; e-mail; contato(s) telefônico(s).
Dados acadêmicos	forma de ingresso; estabelecimento de origem; nota processo seletivo; curso; frequência; nota; disciplina e situação de vínculo acadêmico.
Dados de pagamento	histórico situação financeira; número de identificação bancária; boletos; recibos de pagamentos e negociações.
Dados de saúde	atestados médicos; exame médico periódico.
Dados de imagem	Fotos e vídeos
Dados biométricos	matriz de impressão digital.
Dados técnicos	endereço de IP; data e hora de consulta; cookies.

Fonte: Fumec (2024).

A Figura 28 apresenta um formulário para consulta de dados por alunos na base de dados legal da UNI1. Este processo possui o propósito de promover a transparência das informações, conforme requerido pelo LGPD. Por meio dele, pode-se ter acesso a todas as informações que a UNI1 possui a respeito de um aluno e decidir como ela poderá usar essas informações, conforme seu consentimento.

Figura 28 - Formulário para acesso a informações pessoais - UNI1



Fonte: PUC Minas (2024).

4.6 Avaliação do processo de adequalçao da LGPD

Foi solicitado aos Entrevistados que relatassem algum ponto considerado importante e, ou, alguma dificuldade encontrada no processo de adoção e adequação da LGPD em sua IES.

Na UNI1 o sistema está bem estruturado e aderente às unidades da instituição, de acordo com o relato dos entrevistados. Um aspecto merecedor de destaque é o processo comunicacional periódico. A frequência de divulgação de boletins e informativos sobre segurança da informação e proteção de dados pessoais é interessante, o que permite o comprometimento e conscientização de todos os atores envolvidos com a instituição, direta ou indiretamente.

> [...] Nesse momento, eu comento a necessidade de conscientização. Porque essa conscientização parte, primeiro, parte do indivíduo, sabe, porque não é somente dados da instituição, são dados da vida privada dele. [...] se isso é importante para mim eu acho que a instituição tem que preservar também. E aí, a partir disso, vai criar um mecanismo para monitorar se é de fato as pessoas responsáveis os atores... de forma adequada [...] (Entrevistado 2).

Percebe-se que os processos de implementação, manutenção e uso da LGPD nas instituições pesquisadas, segundo os entrevistados, foi bem conduzido, acompanhado e implementado. Pontos de melhoria existem, sendo que os DPO's estão atentos, principalmente às novas diretivas da ANPD. Portanto, percebe-se credibilidade e maturidade no sistema regulatório de proteção de dados pessoais implementado nessas IES.

Na UNI2, observou-se que o sistema está em consolidação, e também em expansão. Foi realizada a adequação com envolvimento de vários colaboradores de diversas áreas, além da conscientização dos mesmos e do público externo. Ressaltou-se que, à medida que as orientações forem provenientes da ANPD, a instituição estará preparada para realizar tais adaptações.

> [...] Eu quero, eu quero só reforçar aqui que, na (UNI2), de um modo geral, ela zela pela segurança da informação de todo o nosso corpo administrativo e público externo também. E além dos nossos alunos, é claro. E 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. Então, a gente tem atuado nesse sentido, e, além disso, a gente tem também trabalhado para sempre desenvolver medidas preventivas, justamente para evitar a corretiva. Então, a gente tem que trabalhar nesse sentido, fazendo, inclusive, análise SWOT de alguns processos, de algumas atividades.
> Então, assim, a instituição tem atuado pra que a gente tenha um padrão de atendimento e também que gere segurança para os nossos colaboradores, nosso público externo e também para os nossos alunos. É um processo que a gente está, como eu disse, no início, William, nós estamos trabalhando no sentido de avançar, o que é possível efetivamente, modelo ideal ainda nós não chegamos, mas nós estamos aí, vislumbrando: em breve, a gente tem um programa efetivo. E a questão da tecnologia é a nosso favor também. [...] sempre está conosco aqui na gestão da LGPD, aqui na (UNI2) [...] (Entrevistado 3).

4.7 Síntese dos casos analisados

O processo de adequação da LGPD nas IES pesquisadas ocorreu no período de 2019/2020, logo após a entrada em vigor da lei (2018). Em ambas, o processo de adequação ocorreu em conformidade aos requerimentos da legislação, contudo ainda está em andamento devido, dentre outros fatores, à própria evilução da lei. A designação de um DPO para o exercício da função, requerimento obrigatório da lei, e nas IES pesquiadas revelou-se que são profissionais experientes, com forte conhecimento em gestão corporativa, gestão da LGPD e vasto *know-how* no negócio das instituições (prestação de serviços educacionais). Destaca-se que o DPO da UNI2 possui a certificação DPO pela EXIN (entidade certificadora).

Os entrevistados exercem a função nomeados formalmente pela alta gestão das instituições. Porém, ainda acumulam os cargos aos quais estavam formalmente designados antes de assumiram a responsabilidade pela adequação da LGPD nas IES, isto é, acumulam a função original com a função de DPO. Eles também ocupam posição nos Comitês Gestores da LGPD, em suas respectivas instituições.

A presença do Comitê gestor da LGPD nestas instituições é um importante fator, que demonstra o amadurecimento do processo de adequação da LGPD. Nos dois casos, houve a participação da alta gestão das instituições, que envolveu reitores, pró-reitores, diretores, gerentes, fato que demonstra a importância da existência da adequação da nova legislação junto às IES pesquisadas. Há semelhança de funções comuns na composição desses comitês, formados por membros da área jurídica, da TI e o próprio DPO, podendo conter profissionais adicionais, como reitores/pró-reitores e diretores, dentre outros cargos da alta gestão. E, com a implementação da nova lei, em ambas as instituições, os encontros destes comitês são regulares (mensais). Outra característica comum dos Comitês refere-se à competência consultiva e não deliberativa.

Considerando o porte destas IES, merece destaque que os trabalhos foram realizados em todas as unidades das instituições, envolvendo grupos multidisciplinares e estruturas diversas, como unidades descentralizadas, departamentos, seções e setores (dos Serviços Gerais à Presidência).

A adequação iniciou-se com a criação de uma estrutura básica (designação da função de DPO – mesmo que nomeado precariamente, com envolvimento da TI e da Alta Administração). Aprofundou-se o estudo e entendimento da Lei, por este grupo de trabalho, e, posteriormente, realizou-se diagnóstico institucional com relação aos dados tratados (levantamento de

informações e dados pessoais: se um determinado dado pessoal era sensível e, ou, confidencial). Enfim, realizada a classificação das informações, dentro de uma metodologia (criada especificamente para a realização do diagnóstico e adequação da LGPD), pode-se aplicar as devidas orientações oriundas da LGPD no que tange ao tratamento e proteção de dados pessoais.

Os processos de tratamento de dados pessoais, nestas instituições, estão estabelecidos de modo formal. Percebe-se que, inicialmente, foi utilizado o conceito de *Privacy by Default* (privacidade por padrão), durante a fase de implementação, e, à medida que a adequação evoluiu ou um processo já estabelecido foi revisitado, avaliou-se o processo de tratamento do dado dentro do conceito *Privacy By Design* (privacidade pelo desenho ou por concepção), isto é, a implementação da proteção do dado é estabelecida desde a sua concepção (na origem do dado), e não mais por um padrão previamente estabelecido e utilizado.

Entende-se que o processo de adequação à LGPD dividiu-se em etapas em ambas as IES. Compreende-se que as atividades seguintes foram comuns e eficazes: estabelecimento do Comitê direcionador dos trabalhos; análise ampla dos dados (diagnóstico institucional); classificação e tratamento dos dados pessoais (inclusive sensíveis); criação de plano de comunicação; capacitação de colaboradores; estabelecimento de medidas corretivas e preventivas; gestão do consentimento, das bases legais e relatório de impacto de proteção pessoais (RIPD).

Um aspecto relevante para a adequação do projeto de LGPD, nas IES, refere-se à realização de capacitação dos colaboradores por meio da conscientização sistemática e contínua (palestras, *workshops*, *folders*), treinamentos constantes no processo de implementação, inclusive de colaboradores das áreas envolvidas indiretas, fortalecendo o processo de adequação e evidenciando a importância da LGPD, com perspectivas para se alcançar maior compromisso dos envolvidos e êxito na manutenção e operação institucional da LGPD.

Percebeu-se que a equipe designada diretamente para a LGPD é reduzida, contando com a presença do DPO e com um auxiliar administrativo na UNI1. O conceito utilizado pelas IES é interessante, visto que se buscou, nas duas IES pesquisadas, a identificação de responsáveis em cada setor, cada departamento ou unidade. Estabeleceu-se, portanto, a figura de um "embaixador", como foi nomeado em ambas as universidades, ou seja, um ponto chave de contato, que responde pela LGPD onde atua. Com isso, a redução de custo é evidente, pois manteve-se a nova seção "DPO" contando com um quadro reduzido de colaboradores, talvez quase inexistente, contando apenas com a figura do gestor (o DPO). Dessa forma, além de

manter o custo reduzido, buscou-se o envolvimento e responsabilização dos pontos chave, ou seja, o compromisso de atuar não apenas como um interlocutor, mas como um colaborador compromissado e parceiro da LGPD na instituição. Por outro lado, tal colaborador assume uma nova função/tarefa que até então não estava contemplada no seu *job description* (afazeres do cargo) que, por sua vez, pode gerar passivo trabalhista, caso a condição não seja atualizada e ajustada pela instituição.

Outro aspecto relevante, que cabe destacar, é o processo de comunicação corporativa destas instituições quando o assunto é a LGPD. Ele abrangeu as IES de forma interna e externa. Foi realizado um amplo trabalho de conscientização e divulgação da adequação da LGPD. O processo estabelecido de comunicação (o qual envolveu a área de comunicação corporativa em ambas IES) permitiu o sucesso na adequação da LGPD. Como exemplo, na UNI2, semanalmente, são enviados dois boletins para público interno, sendo um sobre política de segurança e outro sobre boletim de privacidade. Vale dizer que esse processo permite um contato maior com os colaboradores, maior proximidade, o que pode agregar a descoberta de algum processo novo ou alguma informação que necessita de readequação ou nova classificação em função de mudanças ocorridas entre um e outro processo comunicacional.

Outra ação consolidada nas IES refere-se ao sítio da LGPD. Ele se apresenta bem estruturado e funcional, de fácil acesso e entendimento. Possui conteúdo esclarecedor (inclusive com vídeo na IES1), e cumpre o requerido pela legislação. Possui dados do DPO da instituição, facilmente identificados, além de canal de comunicação para casos de suspeita de vazamento ou violação de dados.

Um ponto a ser destacado refere-se à violação de dados. Nas duas IES pesquisadas, não foram relatados registros de incidentes relevantes dessa natureza. E, em caso de ocorrência, elaborou-se um processo para tal situação, o qual está (em tese) adequado ao propósito a que se destina. As IES possuem plano de contingência para tratamento de riscos, porém este não foi colocado em prática, o que impede de verificar se ele é eficiente. Um ponto negativo, neste caso, refere-se à não realização de testes de incidente, como, por exemplo, intrusão, sequestro, *ransomware*. Tais testes podem apontar se o procedimento estabelecido é eficaz ou não. Cabe frisar que, em caso de qualquer incidente de segurança ou violação de dados pessoais, por força de lei, a instituição deve, obrigatoriamente, comunicar o fato à ANPD.

De acordo com os DPO’s entrevistados, o processo de adequação está em consolidação e em expansão. A adequação contou com envolvimento de vários colaboradores de diversas áreas, além da conscientização dos mesmos e também do público externo. É possível inferir

que a adequação da LGPD nas IES é uma realidade. Mesmo com poucos recursos humanos e com as demais dificuldades decorrentes da COVID-19, esta legislação é utilizada dentro daquelas instituições.

Em ambas as IES, a adequação dos requisitos da LGPD está em processo de implementação, operacional e em uso cotidiano, tendo-se estabelecido a cultura de proteção de dados pessoais, segundo os entrevistados. Há formas e processos solidificados e a comunicação das partes interessadas (interna e/ou externa) com as IES é de fácil acesso, bem como com o canal de denúncias. Logo, diante destes recursos comunicacionais, o tratamento de questões pertinentes à LGPD pode ser direcionadas e tratadas pelos responsáveis pelos dados e até mesmo diretamente pelo DPO.

O Quadro 15 apresenta uma síntese, de forma resumida, das categorias e subcategorias de análise por instituição. Percebe-se que há certa similaridade nos resultados comparativos entre as instituições UNI1 e UNI2, visto que o processo ou programa de adequação da LGPD foi, de certa forma, conduzido de forma semelhante pelos DPO's.

Ainda de acordo com o Quadro 15 pode-se concluir que alguns pontos relevantes merecem atenção especial atenção ou o seu desenvolvimento / implementação, por parte das IES, como por exemplo:

I) No que se refere a categoria "Pessoas"

- O número de colaboradores alocados para o exercício da LGPD é reduzido, sugere-se a ampliação do quadro.
- No caso da IES2 a subcategoria "Capacitação (Seminário, Palestras, Treinamentos)" pode ser melhor definida, com o estabelecimento de periodicidade e calendário oficial fixo.

II) No que se refere a categoria "Comunicação"

- Subcategoria Periodicidade: No caso da UNI2, sugere-se que o processo seja semanal, assim como na UNI1.

III) No que se refere a categoria Governança (GTI e GD)

- Subcategoria "Papel (Plano Diretor de Informática)": Estabelecimento do Plano em ambas IES.
- Subcategoria "Papel *Frameworks* e Normas*":*

  - Sugere-se a adoção do framework ITIL v4 na sua totalidade em ambas as IES.

  - Sugere-se a adoção do framework COBIT, no mínimo, de forma parcial em ambas as IES.

- Sugere-se a adoção do framework DAMABOK, parcial ou integralmente em ambas as IES.

- Sugere-se a adoção da norma NBR/ISO 38.500 – integralmente em ambas as IES.

IV) No que se refere a Categoria "Tratamento de Dados Pessoais"

- Subcategorias "Riscos e Incidentes": Melhorar e consolidar o Plano em ambas IES.

- Por fim, quando avalia-se a GTI e GD, de maneira geral, na IES1 percebe-se um avanço em relação a IES2. Uma das razões pode-se ser o quantitativo de colaboradores, enquanto na IES1 há cerca de 127 pessoas na IES2 há cerca de 25.

V) No que se refere a categoria "Avaliação"

- No que se refere as subcategorias "Resultados / Dificuldades / Desafios"

- Os resultados na adequação da LGPD nas IES foi cinsiderado bom pelos entrevistados. Se considerar o período de pandemia COVID019, e demais dificuldades impostas decorrentes deste malfadado vírus, o projeto de adequação foi satisfatório. As instituições pesquisadas buscaram se adequar e conseguiram tal feito. As dificuldades que podem ainda permanecer refere-se aos recursos humanos e principalmente financeiros, os quais merecem avaliações e investimentos para manutenção e uso da LGPD naquelas IES. Não menos importante, é o desafio de expandir o alcance da legislação dentro das IES pesquisadas. Por natureza a própria lei evolui com o tempo e adequações são compulsoriamente necessárias.

- Subcategoria "Perspectivas Futuras (Pontos relevantes/diferenciais)"

  - Quanto a GTI: Faz-se necessário a implementação em ambas a IES (fortemente sugerido). Como ponto de partida a implementação da NBR/ISO 38.500 e o *framework* ITIL.

  - Quanto a GD:

  No caso específico da UNI1, cabe evoluir a ação inicial de alocação de DBA com viés em LGPD, ou seja, estender o conceito da cultura de dados para a TI e demais setores da IES.

  No caso da UNI2, sugere-se a implementação da cultura de dados para a TI e demais setores da IES.

  Em suma, faz-se necessário a implementação da GD em ambas a IES (fortemente sugerido).

Quadro 13 - Síntese categorias de análise por IES

Categorias	Subcategorias	UNI1	UNI2
Processo de adequação	Escopo	Definido	Definido
	Relação com o negócio	Existente	Existente
	Alta Direção	Participa	Participa
	Instituição de Comitê e política de privacidade	Sim	Sim
Pessoas	Equipe	DPO/Assistente/DBA	DPO/Assistente
	Capacitação (Seminário, Palestras, Treinamentos)	Sim, frquente	Sim, sob demanda
Comunicação	Público-alvo	Interno/Externo	Interno/Externo
	Periodicidade	Semanal	Eventual
	Meios	*e-mail*, *Website*, *folders* e outros	e-mail, *WhatsApp*, *website* e outros
Governança (GTI e GD)	Papel (Plano Diretor de Informática)	Não	Não
	Normas [8]	Uso conceitos - parcial	Uso conceitos - parcial
	Frameworks[9]	ITIL parcial	ITIL incipiente
	Interface com outros órgãos/parceiros	Sim	Sim
Tratamento de Dados Pessoais	Políticas de segurança	Definida	Definida
	RIPD [10]	Sim	Sim
	Riscos[11]	Trata – via procedimento operacional. Sem política formal definida para tratamento de riscos.	Trata – via procedimento operacional. Sem política formal definida para tratamento de riscos.
	Incidentes (Ameaças, Denúncias, vazamentos)[12]	Sim	Sim
Avaliação da adequação da LGPD	Resultados	Positivo	Positivo
	Dificuldades	Recursos (financeiros, humanos e outros)	Recursos (financeiros, humanos e outros)
	Desafios	Manutenção programa Capital humano	Manutenção programa Capital humano
	Perspectivas Futuras (Pontos relevantes/diferenciais)	Implementar Governança de TI Evoluir e consolidar cultura/dados Implementar GD	Ampliação programa LGPD Implementar GD (desenvolvimento de cultura/dados) Melhorar controles de TI Implementar Governança de TI Melhorar periodicidade da comunicação Desenvolvimento de políticas GTI

Fonte: Elaborado pelo autor (2024).

[8] Utilizam como referência a linha ISO 27.000 (27.001 e 27.002) – Segurança da Informação, porém não implementada na íntegra.

[9] Utilizam ITIL como referência.

rém não há procedimento específico definido para atuação.

[11] Há o tratamento conforme política de segurança da informação, contudo não há mapeamento prévio de riscos definidos em política específica.

[12] Possuem recursos técnicos para tratamento e procedimentos padrões, conforme política de segurança da informação, porém cabe melhoria nos processos existentes bem como integração com softwares de governança.

A adequação realizada por ambas as instituições atende aos requisitos da legislação em vigor, e, adicionalmente, atendem também à normas e boas práticas de governança de TI. Há utilização de normas como referência para se estabelecerem políticas de segurança e privacidade de dados e também de segurança da informação.

Adaptações e melhorias são necessárias, inclusive no decorrer da implementação. Identifica-se durante a fase de mapeamento, ou *Site Survey*, em que é necessário aplicar certas correções ou ajustes em processos, procedimentos e regras, antes mesmo da adequação da LGPD e seu o complexo arcabouço legal.

A adequação é contínua, visto que a ANPD realiza ajustes e melhoria no processo pertinente à LGPD, inclusive modifica relatórios, cria regras novas, ajusta mecanismos de controle, ou seja, a própria agência de controle governamental realiza, com certa frequência, atualizações nas formas de controle e fiscalização de seus instrumentos, o que afeta diretamente as IES pesquisadas e demais organizações.

Percebeu-se que as IES possuem mais de uma base legal[13] atendida, a saber: Consentimento; Cumprimento de obrigação legal ou regulatória, execução ou criação de contrato, dentre outros. Logo, a aderência do programa (e não projeto) de adequação da LGPD, nas IES pesquisadas, tem sido meritosa e adequada ao propósito estabelecido.

[13] No Art. 7º, a LGPD determina 10 hipóteses ou bases legais que devem justificar o tratamento de dados pessoais. Estas bases são fundamentais para garantir que a empresa esteja em conformidade com a lei.

5 CONSIDERAÇÕES FINAIS

A proteção de dados, no Brasil, é um tema tratado pelas legislações brasileiras e, inclusive, na Carta Magna, de 1988. Contudo, as abordagens e as devidas considerações para resguardar os direitos do sujeito (pessoa física) não se integravam em uma legislação específica, destinada a esse fim. Evoluções, após a CF de 1988 ocorreram, mas não ao nível desejado de manter-se resguardada a privacidade do cidadão. Criou-se o Marco Civil da Internet, a Lei de Acesso à Informação, o aprimoramento da legislação ordinária (Código Civil, Estatuto da Criança e Adolescente, dentre outras). Ainda assim, persistiu uma lacuna, no direito brasileiro, faltando um ordenamento que abordasse de forma objetiva a proteção de dados pessoais do indivíduo.

Em 2018, surge a Lei Geral de Proteção de Dados (pessoais), com base na GDPR europeia. Vale destacar que a GDPR foi idealizada em 2012 e lançada em 2016 na União Europeia. Após tal fato, diversos países do mundo se movimentaram no sentido de criar legislação específica para o fim de proteção de dados pessoais, como é o caso do Brasil.

A partir de 2018, a questão tem sido bastante debatida, nas esferas pública e privada. Na esfera civil, empresas e organizações passam a discutir o seu conteúdo, formas de adoção (que passou a ser compulsória), operacionalização, e todas as regras que deviam ser adotadas conforme o rigor da lei. Os questionamentos encaminhados à recém-criada ANPD fizeram com que a legislação não entrasse em vigor após a sua criação. O Governo postergou sua vigência para setembro de 2020.

Destarte, as organizações precisaram implementar a LGPD a partir de então. E, nas IES, a necessidade não foi diferente. Para se manter no competitivo e desafiador mercado educacional, eles necessitaram (e ainda necessitam) se adequar às novas regras.

A implementação, uso e manutenção da LGPD requer, para ser minimamente operacional e responder às necessidades da legislação, um aparato de suporte e sustentação tecnológicos. Não se cogita o seu uso de forma manual. A TI, neste caso, é um instrumento essencial para o seu funcionamento. Logo, a GTI, com seus *frameworks*, normas (ABNT/ISO), regras e procedimentos, permite a adequação e sucesso no uso cotidiano, como foi demonstrado nas entrevistas com profissionais das universidades, objeto de pesquisa neste trabalho.

Portanto, pode-se aferir que, para implementar e utilizar a LGPD, é necessário o suporte da GTI associada aos recursos tecnológicos (rede de computadores, sistemas, banco de dados, infraestrutura computacional, internet) oferecidos pela TI das IES.

Esta pesquisa teve como objetivo identificar as ações e iniciativas utilizadas por duas IES privadas, sem fins lucrativos, Fundação Mineira de Educação e Cultura - Universidade FUMEC e a Pontifícia Universidade Católica de Minas Gerais - PUC Minas, para adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD).

Embasada na revisão da literatura, esta pesquisa apresenta contribuições de natureza teórica e, principalmente, prática, amparada nas informações obtidas junto aos entrevistados e às bases de dados pesquisadas.

É importante destacar que os objetivos foram atingidos.

Em consonância com o primeiro objetivo específico, identificou-se como a privacidade dos dados pessoais é tratada pelas IES. A LGPD está implementada e em evolução nas instituições. Foi implementada utilizando-se de conceitos modernos de gestão e guiada por líderes (DPO´s) bem atuantes os quais envolveram diversos setores por meio de eficientes meios de comunicação;

O segundo objetivo específico buscava identificar quais normas e, ou, *frameworks* de Governança de Tecnologia da Informação foram utilizados pelas IES no suporte à adequação e uso da LGPD. O *framework* ITIL foi eleito por ambas, que o utilizaram como referência, mas não na sua totalidade;

O terceiro objetivo específico visava identificar quais normas e, ou, *frameworks* de Governança de Dados foram utilizados pelas IES no suporte à adequação e uso da LGPD. Em ambas as IES 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 GD;

Finalmente o quarto objetivo específico buscou-se verificar quais os principais desafios encontrados na adequação e no uso da LGPD.

Após a realização das entrevistas foi possível identificar as dificuldades encontradas pelas IES que, às vezes, tiveram dificuldades de 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 e, efetivamente, de disseminar o conteúdo e importância da proteção de dados pessoais nas instituições.

Portanto, entende-se que a LGPD, nas IES pesquisadas, está bem implantada e gerida, segundo relato dos entrevistados, contudo sujeita a melhorias em áreas subjacentes de apoio, como a GTI e GD, principalmente. Com relação à adequação, mesmo tendo ocorrido, em grande parte, durante a pandemia COVID-19, obteve-se o êxito esperado. Apesar de a GTI e seus

modelos/*frameworks* serem utilizados parcialmente, pode-se afirmar o sucesso na implementação. O processo de governança apoiou a adequação da LGPD nestas instituições e o êxito deve-se à atuação dos DPO's destas instituições, devido à condução, empenho e conhecimento sobre práticas de governança, gestão e LGPD. Esses profissionais conseguiram, como afirma Wu (2015), realizar o alinhamento entre o negócio e a tecnologia por meio da associação positiva do desempenho da governança de TI.

A opção metodológica, baseada em estudos de caso, em duas IES, apresentou duas principais limitações. A primeira limitação referiu-se ao conjunto de duas universidades, o que pode prejudicar a representatividade e a generalização dos resultados. A segunda limitação referiu-se ao grupo limitado de entrevistados, representantes de duas áreas, DPO e TI. Por outro lado, os entrevistados estão posicionados em cargos hierárquicos relevantes e, portanto, possuem uma visão estratégica de suas instituições, e, no caso específico da TI, apresentam também vastos conhecimentos técnicos e operacionais

Como toda e qualquer pesquisa científica que possui suas limitações, barreiras e dificuldades, nesta deparou-se com as seguintes: a) Disponibilidade de agenda dos *stakeholders* para realização das entrevistas; b) Obtenção de informações (disponibilidade/coleta); c) Escassez de tempo hábil para coletar e analisar dados uma maior gama de entrevistados de outras áreas de negócio das IES; d) Tempo hábil para a realização dos procedimentos e finalização do trabalho pós entrevista; e) Impossibilidade de generalização dos achados e conclusões obtidos, pois a amostragem foi de duas IES.

São contribuições desta pesquisa: Colaborar para 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; Colaborar para adequação das IES escolhidas no que se refere ao uso e importância dos conceitos de Governança de TI e de Governança de Dados; Facilitar o caminho de adequação da LGPD nas IES; e por fim, elevar o nível de maturidade de TI nas IES, promovendo e incentivando o uso da GTI e GD.

Outras contribuições de caráter técnico-teórico e técnico-prático foram identificadas nesta pesquisa, por exemplo: matriz para comparação entre tipos de governanças e matriz de fatores viabilizadores e inibidores, dentre outros.

Para pesquisas futuras, sugere-se o desenvolvimento dos temas Governança de Dados e Governança de Informação e sua interseção com a LGPD e a GTI, aplicados ao segmento educacional, pois este aspecto ainda é pouco explorado no Brasil.

Por fim, considerada a escassa literatura sobre a LGPD em IES no Brasil, bem como o caráter inédito desta obra, aconselha-se a exploração do tema e seus impactos em um número maior de IES, inclusive nas pertencentes à esfera pública.

REFERÊNCIAS

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

ANTONIALLI, Fabio; *ANTONIALLI, Luiz Marcelo; ANTONIALLI*, Renan. Uses and Abuses of the Likert Scale: Bibliometric Study in the Proceedings. *Revista Reuna*, Belo Horizonte, v. 22, n. 4, p. 1-19, 2017.

ARIFF, M. S. B. M.; ZAKUAN, N.; TAJUDIN, M. N. M.; AHMAD, A., ISHAK, N.; ISMAIL, K. A framework for risk management practices and organizational performance in higher education. *Review of Integrative Business and Economics Research*, [*s. l.*], v. *3, n.* 2, 422-432, 2014.

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.

ASSIS, Celia Barbosa. *Governança da informação: viabilizadores e inibidores para adoção organizacional*. 2018. Tese [Doutorado em Engenharia de Produção] – Escola Politécnica, Universidade de São Paulo, São Paulo, 2018. doi:10.11606/T.3.2018.tde-27042018-102121. Acesso em: 07 fev. 2024.

ASSOCIAÇÃO BRASILEIRA DE MANTENEDORAS DE ENSINO SUPERIOR - ABMES. 2023. Disponível em: https://abmes.org.br/. Acesso em: 09 fev. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 38500*: Governança corporativa de tecnologia da informação. Rio de Janeiro: ABNT, 2018.

ASTA, D. D. Estratégias viabilizadas por uma instituição de ensino superior privada na implantação do ensino à distância: um estudo de caso. *Perspectivas em Gestão & Conhecimento*, João Pessoa, v. 5, n. 2, p. 226-239, jul./dez. 2015.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 09 fev. 2024.

AXELOS. *ITIL Foundation*. 4th. ed. Londres: TSO, 2019. v. 1, p. 19-310. ISBN 9780113316076.

BANCO MUNDIAL. 1992. Disponível em: https://www.worldbank.org/en/home. Acesso em: 09 fev. 2024.

BARATA, André Montoia. *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. Acesso em: 04 fev. 2024.

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

BARBOSA, T. S.; SILVA, M. S.; TELES, E. O.; PIAU, D. D. N. D.; LOPES, J. M. *et al*. A Lei Geral de Proteção de Dados (LGPD) nas instituições públicas de ensino: possíveis impactos e desafios. In: ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL - ENPI, 7., 2021, Aracaju. [*Anais...*]. Aracaju: ENPI, 2021. p. 2114-2123.

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

BIONI, B. R.; SILVA, P. G. F. da; MARTINS, P. B. L. Intersecções e relações entre a lei geral de proteção de dados (LGPD) e a lei de acesso à informação (LAI): análise contextual pela lente do direito de acesso. *Cadernos Técnicos da CGU*: v. 1 (2022): Coletânea de artigos da pós-graduação em ouvidoria pública, [*S. l.*], v. 1, 2022.

BRASIL. Câmara dos Deputados. *Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais - LGPD 2018*. Disponível em: http://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html. Acesso em: 15 fev. 2023.

BRASIL. *Constituição da República Federativa do Brasil*. 1988. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 05/10/1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 01 ago. 2023.

BRASIL. Governo Federal. *Compartilhamento de dados. Kit para dados abertos – implementando uma Política de Dados Abertos*. 2018. Disponível em: http://kit.dados.gov.br/Elabora%C3%A7%C3%A3o-do-PDA/. Acesso em: 15 mar. 2023.

BRASIL. Tribunal de Contas da União (Plenário). *Lei de acesso à informação – LAI. Lei nº 12.527*, 18/11/2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 20 jan. 2024.

BRASIL. Tribunal de Contas da União (Plenário). *Marco Civil da Internet. Lei nº 12.965, 23/04/2014*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jan. 2024.

BURKART, D. V. V. *Proteção de dados e o estudo da LGPD*. 2021. Dissertação [Mestrado em Mídia e Tecnologia) – Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, 2021.

CAVALCANTI FILHO, Hermano. *Investigação da influência da governança de TI nas instituições federais de ensino superior: estudo de caso*. 2011. Dissertação [Mestrado] – Universidade Federal de Pernambuco, Recife, 2011.

CHAPPLE, M. Speaking the same language: Building a Data Governance Program For Institutional Impact. *Educause Review*, [*s. l.*], v. 48, n. 6, p.14-27, nov./dez. 2013.

CARR, N. *IT doesn't matter*. *Harvard Business Review*, [*s. l.*], May 2003.

COMITÊ Gestor de Internet no Brasil. CGI.br. 2009. Acesso em: 09 fev. 2024.

DAMA-BRASIL. *Dama Framework.* 2012. Disponível em: https://www.damabrasil.net/. Acesso em: 21 jun. 2023.

DATA MANAGEMENT ASSOCIATION. *Dama Framework*. DAMA, 2014. Disponível em: https://www.dama.org/sites/default/files/download/DAMA-DMBOK2-Framework-V2-20140317-FINAL.pdf. Acesso em: 20 nov. 2022.

DMBOK2. *DAMA-DMBOK2 Data Management Body of Knowledge*. 2nd ed. Basking Ridge: Tecnics Publications, 2015.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. *Implantando a governança de TI, da estratégia à gestão de processos e serviços*. 3. ed. São Paulo: Brasport Livros e Multimídia Ltda., 2012.

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. l.*], v. 13, n. 1, p. 402-420, abr. 2023.

GONÇALVES, A. P. *et al*. Governança de Tecnologia da Informação: uma análise do nível de maturidade em empresas atuantes no Brasil. *Revista de Gestão e Projetos*, [*s. l.*], v. 7, n. 1, p. 56-69, 2016.

GONÇALVES, A. P.; GASPAR, M. A.; CARDOSO, V. C.*et al*. Governança de Tecnologia da Informação: uma análise do nível de maturidade em empresas atuantes no Brasil. *Revista de Gestão e Projetos*, [*s. l.*], v. 7, n. 1, p. 56-69, 2016.

GONÇALVES, C. A.; MEIRELLES, A. M. *Projetos e relatórios de pesquisa em Administração*. São Paulo: Atlas, 2004.

IBM. *How to know if a big data solution is right for your organization*. 2022. Disponível em: https://developer.ibm.com/articles/bd-archpatterns2/?mhsrc=ibmsearch_ a&mhq=big%20data. Acesso em: 21 jan. 2023.

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION - ISACA. *COBIT 5: Modelo corporativo para governança e gestão de TI da organização*. ISACA: [*S. l.*], 2019.

INFORMATION TECNOLOGY SENIOR MANAGEMENT FORUM. 2023. Disponível em: https://ITSMFleaders.org/. Acesso em: 09 fev. 2023.

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

INSTITUTO DE PESQUISAS ECONÔMICAS APLICADAS - IPEA. *Carta de Conjuntura*. Nota Técnica, nº 47. Brasília: IPEA, 2020.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA - INEP. 2021. Disponível em: **www.gov.br/inep/pt-br**. Acesso em: 09 fev. 2024.

IT GOVERNANCE INSTITUTE - ITGI. *COBIT 4.1: Modelo, Objetivos de Controle, Diretrizes de Gerenciamento e Modelos de Maturidade*. Rolling Meadows: IT Governance Institute, 2007.

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

LUNA, Francisco Djalma Silva. *Instituições de ensino superior brasileiras e sua jornada para a transformação digital*. 2020. Dissertação [Mestrado em Empreendedorismo] - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2020. doi:10.11606/D.12.2020.tde-15102020-154313. Acesso em: 04 fev. 2024.

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.

MEIRELLES, F. *Pesquisa anual do uso de TI nas empresas*. 34. ed. São Paulo: FGV: Centro de TI Aplicada, 2023.

MERLUGO, William Z.; CARRARO, Wendy B. W. H.; PINHEIRO, Alan B. Transformação digital na contabilidade: os contadores estão preparados? *Revista Pensamento Contemporâneo em Administração*, [*s. l.*], v. 15, n. 1, p. 180-196, 2021.

MINAYO, M. C. S. Introdução. In: MINAYO, M. C. S.; ASSIS, S. G.; SOUZA, E. R. (Org.). *Avaliação por triangulação de métodos*: abordagem de programas sociais. Rio de Janeiro: Fiocruz, 2010. p. 19-51.

MINISTÉRIO DA EDUCAÇÃO E CULTURA - MEC. 2023. Disponível em: https://www.gov.br/inep/pt-br/assuntos/noticias/censo-da-educacao-superior/ead-registra-3-milhoes-de-ingressantes-em-2022. Acesso em: 09 fev. 2024.

OLIVEIRA, M.M. Como Fazer Pesquisa Qualitativa. Petrópolis – RJ: Vozes, 2007.

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. ISSN 2358-8322.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS - PUC Minas. 2023. Disponível em: https://www.pucminas.br/. Acesso em: 08 fev. 2024.

QUEIROZ, R. C. Z. *A proteção de dados pessoais*: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Dissertação (Mestrado em Administração) – Universidade de São Paulo, São Paulo, 2021.

SCHIAVON, M.; LIMA, H. G. F.; PIRES, S. R. Construindo estruturas organizacionais de TI para a otimização da prática da governança de TI. *In*: CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO - CONTECSI, 7., 2010, São Paulo. [*Anais*…]. São Paulo: FEA-USP, 2010.

SERPRO. SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. 2024. Disponível em: www.serpro.gov.br. Acesso em: 09 fev. 2024.

SILVA, Rogério G. P. *Proteção de dados no ensino superior: uma proposta de framework para conformidade à Lei Geral de Proteção de Dados em uma instituição de ensino superior.* 2020. Dissertação [Mestrado em Ciências Contábeis] – Centro Universitário Álvares Penteado, Fundação Escola de Comércio Álvares Penteado - FECAP, São Paulo, 2020.

SILVA, S. de A. A. da. *Privacidade de dados e regime de informação: uma análise da plataforma Facebook Business.* 2021. Tese [Doutorado em Sistemas de Informação e Gestão do Conhecimento] – Faculdade de Ciências Empresariais, Universidade Fumec, Belo Horizonte, 2021.

SIRQUEIRA, Aieda Batistela de. *Governança corporativa e otimização de portfolios: a relação entre risco e retorno e boas práticas de governança*. 2007. Dissertação [Mestrado em Engenharia de Produção] – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2007. doi:10.11606/D.18.2007.tde-07042008-101452. Acesso em: 09 fev. 2024.

SONZA, I. B.; KLOECKNER, G. de O. A Governança Corporativa Influencia a Eficiência das Empresas Brasileiras? *Revista Contabilidade & Finanças*, [*s. l.*], v. 25, n. 65, p. 145-160, 2014.

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: 10.21723/riaee. v17i3.16789. Disponível em: https://periodicos.fclar.unesp.br/ iberoamericana/article/view/16789. Acesso em: 8 fev. 2024.

STELZER, J.; GONÇALVES, E. DAS N.; BAPTISTA, R. R. F.; VAZ, R. M. P.; WIEIRA, K.; FIDELIS, M. DE M. A Lei Geral de Proteção de Dados Pessoais e os desafios das instituições de ensino superior para a adequação. *In*: COLÓQUIO INTERNACIONAL DE GESTÃO UNIVERSITÁRIA, 19., 2019, Florianópolis. [*Anais*...]. Florianópolis: [s. n.], 2019. Disponível em: https://repositorio .ufsc .br/handle/123456789/201939. Acesso em: 14 abr. 2023.

THE DATA GOVERNANCE INSTITUTE. *Definitions of Data Governance.* Disponível em: https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/. Acesso em: 03 set. 2022.

TRIBUNAL DE CONTAS DA UNIÃO - TCU. (Plenário). TC *Auditoria: 039.606/2020-1*. 2020. Disponível em: https://portal.tcu.gov.br/data/files/B4/25/78/27/ D9C818102DFE0FF7F18818A8/038.172-2019-4-AN%20-%20auditoria_Lei%20Geral%20de %20 Protecao%20de%20Dados.pdf. Acesso em: 03 mar. 2023.

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

VALENTIM, MLP. Inteligência competitiva em organizações: dado, informação e conhecimento. *DataGramaZero,* Rio de Janeiro, v. 3, n. 4, p. 1-13, 2002.

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. l.*], v. 39, n. 2, p. 497-518, 2015.

YIN, R. K. *Estudo de Caso*: planejamento e métodos. 4. ed. Porto Alegre: Bookman, 2004.

APÊNDICE A – ROTEIRO DE ENTREVISTA - PERFIL DPO – *DATA PROTECTION OFFICER*

Entrevista – EA

Identificação pessoal		
#	Questão	Resposta
1	Qual seu nome completo?	
2	Qual o seu melhor e-mail?	
3	Cargo que ocupa?	
4	Qual função desempenha?	
5	Qual setor/departamento que exerce a sua função?	
6	Quanto tempo em exercício nesta função?	
7	Qual o nome do setor da LGPD em sua IES?	
8	No organograma corporativo, a LGPD está vinculada a qual área?	

Avaliação dos aspectos da Governança da LGPD

Avalie cada aspecto da LGPD em sua instituição de acordo com a sua percepção. Solicitamos que você, baseadoem sua vivência e experiência, responda as questões abaixo.		
#	Questão	Resposta
1	A LGPD está implementada e em funcionamento na sua IES? Se sim, todas as seções ou capítulos/artigos foram atendidos? Há um plano de adequação da organização à LGPD em curso?	
2	Há profissional dedicado para a LGPD (DPO)? Se não, há a intenção de contratar ou terceirizar? Ele possui fácil acesso a alta administração?	
3	Como é a composição do comitê de governança LGPD? É formalmente instituído? É composto por representantes de quais áreas da IES?	
4	A identidade e as informações de contato do encarregado foram divulgadas publicamente, de forma clara e objetiva, no *website* do controlador?	
5	Os princípios da LGPD são aplicados a todo tratamento de dados pessoais realizados pela IES, tanto para funcionários e, ou, colaboradores e, ou, terceiros?	
6	Ao mapear e tratar os dados pessoais, a IES os relacionou à competência legal/finalidade? Classificou-os entre dados pessoais e dados pessoais sensíveis? foi coletado com nível de consentimento?	
~~7~~	Como é o processo de comunicação das possíveis violações de dados pessoais aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD)?	
8	Como a IES gera evidências para comprovar que tomou medidas de segurança para proteger os dados pessoais contra ameaças externas e internas?	
9	De que forma e quando ocorre a elaboração do Relatório de Impacto à Privacidade de Dados Pessoais – RIPD?	
10	Como a IES trata os riscos identificados no Relatório de Impacto à Proteção dos Dados Pessoais?	
11	Como é realizada a gestão de incidentes (plano de resposta) para tratar possíveis violações dos dados?	
12	De que forma a IES possibilita ao titular do dado cumprir o direito de retificação de suas informações – como por exemplo: a correção de dados incompletos, inexatos ou desatualizados?	
13	A(s) área(s) envolvidas com tratamento de dados participam(aram) de algum treinamento de proteção de dados pessoais?	
14	Qual meio a IES utiliza para recebimento de denúncias e de alertas de ocorrências de irregularidades, como por exemplo: - denúncias de possíveis vazamento de dados e falhas de segurança?	

APÊNDICE B – ROTEIRO DE ENTREVISTA - PERFIL GTI - GOVERNANÇA DE TI

Entrevista - EB

Identificação pessoal		
#	Questão	Resposta
1	Qual seu nome completo?	
2	Qual o seu melhor e-mail?	
3	Cargo que ocupa?	
4	Qual função desempenha?	
5	Qual setor / departamento que exerce a sua função?	
6	Quanto tempo em exercício nesta função?	
7	Qual o nome do setor da GTI em sua IES?	
8	No organograma corporativo, a GTI está vinculada a qual área?	

Avaliação dos aspectos pertinentes a Governança de TI (GTI)

Avalie cada aspecto da GTI em sua instituição de acordo com a sua percepção. Solicitamos que você, baseadoem sua vivência e experiência, responda as questões abaixo.		
	Perguntas	Resposta
	O papel da TI na instituição é bem definido? É vista como área estratégica? Ela auxilia na geração de valor para a IES?	
	A IES possui um Plano Diretor de TI vigente e publicado internamente? É alinhado com o planejamento estratégico organizacional?	
	Como ocorre o alinhamento da TI ao negócio? As estratégias e objetivos são alinhados aos da organização?	
	De que modo ocorre o alinhamento na IES com a legislação emitida pelos órgãos de controle externos (p. ex. MEC/CAPES/ANPD e outros)?	
	A IES possui uma Política de GTIC? Se sim, Como é composto o comitê de governança de TI? É formalmente instituído? Os papéis e responsabilidades do time de GTI são comunicados para a organização?	
	De que modo a continuidade do negócio é tratada nas práticas de governança de TI? Existe um plano específico?	
	A TI utiliza métricas ou KPIs para mensuração de resultados para os seus serviços de TI?	
	Qual o *framework* de práticas ou governança de TI é adotado pela IES? Ele foi adaptado?	
	Como a gestão de risco é tratada na TI? É contemplada nas práticas de governança?	
0	A IES possui plano de capacitação para suprir as necessidades de competências de TI quanto a GTI? (gestores e técnicos)	
1	Como ocorre o processo de comunicação com os stakeholders?	

APÊNDICE C – ROTEIRO DE ENTREVISTA - PERFIL GD - GOVERNANÇA DE DADOS

Entrevista – EC

Identificação pessoal

#	Questão	Resposta
1	Qual seu nome completo?	
2	Qual o seu melhor e-mail?	
3	Cargo que ocupa?	
4	Qual função desempenha?	
5	Qual setor / departamento que exerce a sua função?	
6	Quanto tempo em exercício nesta função?	
7	Qual o nome do setor da GD em sua IES?	
8	No organograma corporativo, a GD está vinculada a qual área?	

Avaliação dos aspectos pertinentes a Governança de Dados (GD)

Avalie cada aspecto da GD em sua instituição de acordo com a sua percepção.
Solicitamos que você, baseadoem sua vivência e experiência, responda as questões abaixo.

	Perguntas	Resposta
	O papel da GD na instituição é bem definido? É vista como área estratégica? Ela auxilia na geração de valor para a IES?	
	A IES possui um Plano de GD? É alinhado com o planejamento estratégico organizacional ou com a GTI?	
	Como ocorre o alinhamento da GD ao negócio? As estratégias e objetivos são alinhados aos da organização?	
	A IES possui uma Política de GD? Se sim, Como é composto o comitê de governança de GD? É formalmente instituído? Os papéis e responsabilidades deste comitê são comunicados para a IES?	
	Qual o *framework* de GD é adotado pela IES? Ele foi adaptado?	
	Como a gestão de risco é tratada junto a GD? Possui política ou processo para este fim?	
	A IES possui plano de capacitação para suprir as necessidades de competências de TI quanto a GD?	
	Como ocorre o processo de comunicaçãoda GD com os stakeholders?	

APÊNDICE D – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - TCLE

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Convidamos o (a) Sr. (a) para participar da Pesquisa "Uma investigação sobre a implantação e uso da Lei Geral De Proteção de Dados Pessoais em Instituições de Ensino Superior: Um estudo multicasos", sob a responsabilidade do pesquisador William Machado Botelho Arabi, a qual pretende identificar quais são as iniciativas das Instituições de Ensino Superior, no Estado de Minas Gerais, para a garantir a implementação e uso da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018.

A presente pesquisa justifica-se, pois, permitirá compreender o cenário atual das IES, no que se refere a implementação e uso da LGPD, e como a Governança de Tecnologia da Informação auxiliou/auxilia o processo de implementação e uso da LGPD.

Se o/a Sr.(a) aceitar participar, as respostas obtidas por esta pesquisa poderão contribuir com relevantes informações para as Instituições de Ensino Superior que não implementaram a LGPD ou estão em fase de implementação (não concluída) e, ou, apresentem impedimentos/dificuldades para concluir a sua implementação, conforme requerido pela lei.

Sua participação é voluntária e se dará por meio de preenchimento de questionário eletrônico e entrevista semiestruturada com questões abertas e, ou, fechadas, individual (presencial ou remota), sendo que as questões que compõem a pesquisa serão pertinentes, exclusivamente, à LGPD, Governança de Dados e Governança da Tecnologia da Informação.

Para a realização da pesquisa será aplicado um questionário sobre tais assuntos, contendo questões, abertas e, ou, fechadas. O preenchimento do questionário eletrônico demora cerca de 30 minutos. O tempo estimado para realização da entrevista é de aproximadamente 1 (uma) hora.

Se o/a Sr.(a) aceitar participar, as respostas obtidas por esta pesquisa poderão contribuir para que instituições de ensino superior possam compreender o processo de implementação da LGPD, e como a Governança de Tecnologia da Informação auxilia(ou) neste processo (justificativa).

Caso depois de consentir a sua participação o/a Sr. (a) desistir de continuar participando, tem o direito e a liberdade de retirar seu consentimento em qualquer fase da pesquisa, seja antes ou depois da coleta dos dados, independente do motivo e sem nenhum prejuízo a sua pessoa.

O/a Sr. (a) não terá nenhuma despesa e não receberá nenhuma remuneração referente a esta pesquisa.

O risco mapeado refere-se ao constrangimento pessoal no momento da entrevista. Neste caso, você poderá não responder a alguma pergunta ou se retirar da entrevista, sem nenhum prejuízo. Para minimizar a possível ocorrência do risco mapeado, as perguntas elencadas na entrevista podem ser enviadas ao participante, com antecedência, caso seja de seu interesse.

Os resultados da pesquisa serão analisados e publicados, mas a sua identidade não será divulgada, uma vez que será guardada em sigilo.

Para qualquer outra informação, o (a) Sr. (a) poderá entrar em contato com o/a pesquisador/a no seguinte endereço: Rua COBRE, 200. BAIRRO CRUZEIRO. BELO HORIZONTE, MINAS GERAIS. CEP: 30.310-190, pelo telefone (31) 99902-8484 (telefone pessoal) ou poderá entrar em contato com o Comitê de Ética em Pesquisa da Universidade Fumec Rua COBRE, 200. BAIRRO CRUZEIRO. BELO HORIZONTE, MINAS GERAIS. CEP: 30.310-190, PRÉDIO D – SALA D 408 OU PELOS telefones – (31) 3269-5235/5259 OU 0800.0300.200. O e-mail é: cep@fumec.br.

CONSENTIMENTO PÓS–INFORMAÇÃO

Eu, _____, fui informado sobre o que o pesquisador quer fazer e porque precisa da minha colaboração, e entendi a explicação. Por isso, eu concordo em participar da pesquisa, sabendo que não vou ganhar nada e que posso sair quando quiser. Este documento é emitido em duas vias originais, as quais serão assinadas por mim e pelo pesquisador, ficando uma via com cada um de nós.

Diante do exposto:
( ) autorizo gravação em áudio e vídeo
( ) não autorizo gravação em áudio e vídeo

_____

Assinatura do(a) participante da pesquisa

Data: _____ / _____ / _____

_____

Assinatura do Pesquisador responsável

ANEXOS

ANEXO A – SUMÁRIO LEI GERAL DE PROTEÇÃO DE DADOS

Capítulo	Título	Artigos
I	Disposições Preliminares	1º ao 6º
II	Do Tratamento de Dados Pessoais	7º a 16
III	Dos Direitos do Titular	17 a 22
IV	Do Tratamento de Dados Pessoais pelo Poder Público	23 a 32
V	Da Transferência Internacional de Dados Pessoais	33 a 36
VI	Dos Agentes de Tratamento de Dados Pessoais	37 a 45
VII	Da Segurança e das Boas Práticas	46 a 51
VIII	Da Fiscalização	52 a 54
IX	Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	55 a 59
X	Disposições Finais e Transitórias	60 a 65

Fonte: Brasil, 2021. Elaborado pelo autor.

ANEXO B – PROCESSOS DO COBIT 5

Processos do *framework* COBIT 5 e seus 37 processos e respectivos 5 (cinco) domínios de governança.

Avaliar, Dirigir e Monitorar		
EDM01	Assegurar o Estabelecimento e Manutenção do *Framework* de Governança	Analisa e articula os requisitos para a governança corporativa de TI, coloca em prática e mantém estruturas, princípios, processos e práticas, com clareza de responsabilidades e autoridade para alcançar a missão, as metas e os objetivos da organização.
EDM02	Assegurar a Entrega de Benefícios	Otimiza a contribuição de valor para o negócio a partir dos processos de negócios, serviços e ativos de TI resultantes de investimentos realizados pela TI a custos aceitáveis.
EDM03	Assegurar a Otimização de Riscos	Assegura que o apetite e tolerância a riscos da organização são compreendidos, articulados e comunicados e que o risco ao valor da organização relacionado ao uso de TI é identificado e controlado.
EDM04	Assegurar a Otimização de Recursos	Assegura que as capacidades adequadas e suficientes relacionadas à TI (pessoas, processos e tecnologia) estão disponíveis para apoiar os objetivos da organização de forma eficaz a um custo ótimo.
EDM05	Assegurar a Transparência para as partes interessadas	Assegura que a medição e relatórios de desempenho e conformidade da TI corporativa sejam transparentes para os *stakeholders* aprovarem as metas, métricas e as ações corretivas necessárias.

Alinhar, Planejar e Organizar		
APO01	Gerenciar o *Framework* de Gestão de TI	Esclarece e mantém a missão e visão da governança de TI da organização. Implementa e mantém mecanismos e autoridades para gerenciar a informação e o uso da TI na organização.
APO02	Gerenciar a Estratégia	Fornece uma visão holística do negócio e ambiente de TI atual, a direção futura, e as iniciativas necessárias para migrar para o ambiente futuro desejado.
APO03	Gerenciar a Arquitetura Corporativa	Estabelece uma arquitetura comum que consiste em processos de negócios, informações, dados, aplicação e tecnologia para realizar de forma eficaz e eficiente as estratégias de negócio e de TI por meio da criação de modelos e práticas-chave que descrevem arquitetura de linha de base.
APO04	Gerenciar a Inovação	Mantém uma consciência de TI e tendências de serviços relacionados, identifica oportunidades de inovação e planeja como se beneficiar da inovação em relação às necessidades do negócio. Influencia o planejamento estratégico e as decisões de arquitetura corporativa.
APO05	Gerenciar o Portfólio	Executa o conjunto de orientações estratégicas para os investimentos alinhados com a visão de arquitetura corporativa e as características desejadas do investimento e considerar as restrições de recursos e de orçamento. Avalia, prioriza programas e serviços, gerencia demanda dentro das restrições de recursos e de orçamento, com base no seu alinhamento com os objetivos estratégicos e risco. Move programas selecionados para o portfólio de serviços para execução. Monitora o desempenho de todo o portfólio de serviços e programas, propondo os ajustes necessários em resposta ao programa e desempenho do serviço ou mudança de prioridades da organização.
APO06	Gerenciar Orçamento e Custos	Administrar as atividades financeiras relacionadas a TI tantos nas funções de negócios e de TI, abrangendo orçamento, gerenciamento de custos e benefícios e priorização dos gastos com o uso de práticas formais de orçamento e de um sistema justo e equitativo de alocação de custos para a organização.

APO07	Gerenciar Recursos Humanos	Fornece uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as habilidades dos recursos humanos. Isso inclui a comunicação de papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas.
APO08	Gerenciar as Relações	Gerencia o relacionamento entre o negócio e TI de uma maneira formal e transparente, que garanta foco na realização de um objetivo comum.
APO09	Gerenciar os Acordos de Serviço	Alinha serviços de TI e níveis de serviço com as necessidades e expectativas da organização, incluindo identificação, especificação, projeto, publicação, acordo, e acompanhamento de serviços de TI, níveis de serviço e indicadores de desempenho.
APO0 10	Gerenciar os Fornecedores	Gerencia serviços relacionados a TI prestados por todos os tipos de fornecedores para atender às necessidades organizacionais, incluindo a seleção de fornecedores, gestão de relacionamentos, gestão de contratos e revisão e monitoramento de desempenho de fornecedores para a efetividade e conformidade.
APO0 11	Gerenciar a Qualidade	Define e comunica os requisitos de qualidade em todos os processos, os procedimentos e os resultados das organizações, incluindo controles, monitoramento contínuo, e o uso de práticas comprovadas e padrões na melhoria contínua e esforços de eficiência.
APO0 12	Gerenciar os Riscos	Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.
APO0 13	Gerenciar a Segurança	Define, opera e monitora um sistema para a gestão de segurança da informação.

Contruir, Adquirir e Implementar		
BAI01	Gerenciar Programas e Projetos	Gerenciar todos os programas e projetos do portfólio de investimentos em alinhamento com a estratégia da organização e de forma coordenada. Inicia, planeja, controla e executa programas e projetos, e finaliza com uma revisão pós-implementação.
BAI02	Gerenciar a Definição de Requisitos	Identifica soluções e analisa os requisitos antes da aquisição ou criação para assegurar que eles estão em conformidade com os requisitos estratégicos corporativos que cobrem os processos de negócio, aplicações, informações/ dados, infraestrutura e serviços. Coordena com as partes interessadas afetadas a revisão de opções viáveis, incluindo custos e benefícios, análise de risco e aprovação de requisitos e soluções propostas.
BAI03	Gerenciar a Identificação e Construção deSoluções	Estabelece e mantém soluções identificadas em conformidade com os requisitos da organização abrangendo design, desenvolvimento, aquisição/terceirização e parcerias com fornecedores/vendedores. Gerencia configuração, teste de preparação, testes, requisitos de gestão e manutenção dos processos de negócio, aplicações, informações/dados, infraestrutura e serviços.
BAI04	Gerenciar a Disponibilidade e Capacidade	Equilibra as necessidades atuais e futuras de disponibilidade, desempenho e capacidade de prestação de serviços de baixo custo. Inclui a avaliação de capacidades atuais, a previsão das necessidades futuras com base em requisitos de negócios, análise de impactos nos negócios e avaliação de risco para planejar e implementar ações para atender as necessidades identificadas.

BAI05	Gerenciar a Implementação de Mudança Organizacional	Maximiza a probabilidade de implementar com sucesso a mudança organizacional sustentável em toda a organização de forma rápida e com risco reduzido, cobrindo o ciclo de vida completo da mudança e todas as partes interessadas afetadas no negócio e TI.
BAI06	Gerenciar Mudanças	Gerencia todas as mudanças de uma maneira controlada, incluindo mudanças de padrão e de manutenção de emergência relacionadas com os processos de negócio, aplicações e infraestrutura. Isto inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, acompanhamento, elaboração de relatórios, encerramento e documentação.
BAI07	Gerenciar Aceite e Transição de Mudança	Aceita e produz formalmente novas soluções operacionais, incluindo planejamento de implementação do sistema, e conversão de dados, testes de aceitação, comunicação, preparação de liberação, promoção para produção de processos de negócios e serviços de TI novos ou alterados, suporte de produção e uma revisão pós-implementação.
BAI08	Gerenciar o Conhecimento	Mantém a disponibilidade de conhecimento relevante, atual, validado e confiável para suportar todas as atividades do processo e facilitar a tomada de decisão. Plano para a identificação, coleta, organização, manutenção, utilização e retirada de conhecimento.
BAI09	Gerenciar os Ativos	Gerencia os ativos de TI através de seu ciclo de vida para assegurar que seu uso agrega valor a um custo ideal. Os ativos permanecem operacionais e fisicamente protegidos e aqueles que são fundamentais para apoiar a capacidade de serviço são confiáveis e disponíveis.
BAI010	Gerenciar a Configuração	Define e mantém as descrições e as relações entre os principais recursos e as capacidades necessárias para prestar serviços de TI, incluindo a coleta de informações de configuração, o estabelecimento de linhas de base, verificação e auditoria de informações de configuração e atualizar o repositório de configuração.

Entregar, Servir e Suportar		
DSS01	Gerenciar as operações	Coordena e executa as atividades e procedimentos operacionais necessários para entregar serviços de TI internos e terceirizados, incluindo a execução de procedimentos operacionais, padrões pré- definidos e as atividades exigidas.
DSS02	Gerenciar Requisições de Serviço e Incidentes	Fornecer uma resposta rápida e eficaz às solicitações dos usuários e resolução de todos os tipos de incidentes. Restaurar o serviço normal; recorde e atender às solicitações dos usuários e registro, investigar, diagnosticar, escalar e solucionar incidentes.
DSS03	Gerenciar Problemas	Identifica e classifica os problemas e suas causas-raízes e fornece resolução para prevenir incidentes recorrentes. Fornece recomendações de melhorias.
DSS04	Gerenciar a Continuidade	Estabelece e mantém um plano para permitir o negócio e TI responder a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócios e serviços de TI necessários e mantém a disponibilidade de informações em um nível aceitável para a organização.
DSS05	Gerenciar Serviços de Segurança	Protege informações da organização para manter o nível de risco aceitável para a segurança da informação da organização, de acordo com a política de segurança. Estabelece e mantém as

		funções de segurança da informação e privilégios de acesso e realiza o monitoramento de segurança.
DSS06	Gerenciar os Controles de Processos de Negócio	Define e mantém controles de processo de negócio apropriados para assegurar que as informações relacionadas e processadas satisfazem todos os requisitos de controle de informações relevantes.

Monitorar, Avaliar e Medir		
MEA01	Monitorar, Avaliar e Medir o Desempenho e Conformidade	Coleta, valida e avalia os objetivos e métricas do processo de negócios e de TI. Monitora se os processos estão realizando conforme metas e métricas de desempenho e conformidade acordadas e fornece informação que é sistemática e oportuna.
MEA02	Monitorar, Avaliar e Medir o Sistema de Controle Interno	Monitora e avalia continuamente o ambiente de controle, incluindo auto-avaliações e análises de avaliações independentes. Permite o gerenciamento de identificar deficiências de controle e ineficiências e iniciar ações de melhoria.
MEA03	Monitorar, Avaliar e Medir a Conformidade com Requisitos Externos	Avalia se processos de TI e processos de negócios suportados pela TI estão em conformidade com as leis, regulamentos e exigências contratuais. Obtém a garantia de que os requisitos foram identificados e respeitados, e integrá-los à conformidade com o cumprimento global da organização.

ANEXO C – SANÇÕES ADMINISTRATIVAS LGPD

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00(cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Leinº 13.853, de 2019)
§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de2019) Vigência
§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junhode 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)
§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor fora presentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)
§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº13.853, de 2019)
I - Somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)
II - Em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)
§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.
§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.
§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

ANEXO D – *TEMPLATE* RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

RELATÓRIO DE IMPACTO
À PROTEÇÃO DE DADOS PESSOAIS

Local>, <dia> de <mês> de <ano>

Histórico de Revisões

Data	Versão	Descrição	Autor
XX/XX/20XX	1.0	Conclusão da primeira versão do relatório	XXXXXXXXXXX
XX/XX/20XX	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	XXXXXXXXXXX

ATENÇÃO!

<Os trechos marcados em azul neste template são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.
<Template Versão 1.0 – Atualizado em 07/12/2020>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO	
Controlador	
<Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI)>.	
Operador	
<Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII)>.	
Encarregado	
<Nome da 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 (LGPD, art. 5º, VIII).>	
E-mail Encarregado	Telefone Encarregado
<xxxx.xxxx.gov.br>	<(99)9999-9999>

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

<Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:
• para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
• quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
• a qualquer momento sob determinação da ANPD (art. 38).>
<Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.>
< A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.>
<Além dos casos específicos previstos pela LGPD no início desta seção 2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:
• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
• rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);
• tratamento de 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" (LGPD, art. 5º, II);
• processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);

• tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
• tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
• tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.
< Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.>

3 – DESCRIÇÃO DO TRATAMENTO

<A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.>
<A LGPD (art. 5º, X) considera 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".>
<O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.>
<Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.>

3.1 – NATUREZA DO TRATAMENTO

<A natureza representa como a instituição pretende tratar ou trata o dado pessoal.>
<Importante descrever, por exemplo:
• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
• fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
• com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;
• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;
• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
• medidas de segurança atualmente adotadas.>
<Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.>

3.2 – ESCOPO DO TRATAMENTO

<O escopo representa a abrangência do tratamento de dados.>
< Nesse sentido, considerar destacar:
• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
• o volume dos dados pessoais a serem coletados e tratados;
• a extensão e frequência em que os dados são tratados;
• o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
• o número de titulares de dados afetados pelo tratamento; e
• a abrangência da área geográfica do tratamento.>
< O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.>

3.3 – CONTEXTO DO TRATAMENTO

<Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.>

<O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:
• natureza do relacionamento da organização com os indivíduos;
• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
• destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.>

3.4 – FINALIDADE DO TRATAMENTO
<A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.>
<Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7 º e 11 da LGPD), no que for aplicável:
• cumprimento de obrigação legal ou regulatória pelo controlador;
• execução de políticas públicas;
• alguma espécie de estudo realizado por órgão de pesquisa;
• execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
• exercício regular de direitos em processo judicial, administrativo ou arbitral;
• proteção da vida ou da incolumidade física do titular ou de terceiro;
• tutela da saúde;
• atender aos interesses legítimos do controlador ou de terceiro;
• proteção do crédito; e
• garantia da prevenção à fraude e à segurança do titular.>
<Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.
Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:
• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.>
< Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.
Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os
dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento
de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
<Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.>

4 – PARTES INTERESSADAS CONSULTADAS

<Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.>
<Nessa seção, é importante identificar:
• quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º,

VIII), gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e
• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).>
< Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.>

5 – NECESSIDADE E PROPORCIONALIDADE

<Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o 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 (LGPD, art. 6º, III). >
< Nesse sentido, destacar:
• A fundamentação legal para o tratamento dos dados pessoais.
• Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.
• Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
• Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
• Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
• Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
• Quais são as salvaguardas para as transferências internacionais de dados.>
< O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

<O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".>
<Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.>

<Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.>

<Como exemplo, parâmetros escalares podem ser utilizados 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. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:>

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

<A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.>

<O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.
Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.>

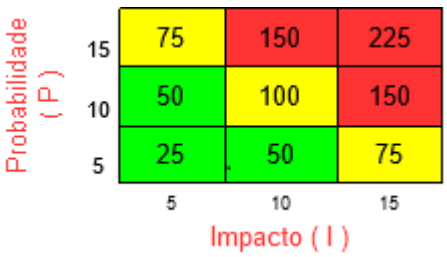


Figura 1: Matriz Probabilidade x Impacto

<As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016>.

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

<A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.>

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	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao	5	15	75

	titular.			
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

7 – MEDIDAS PARA TRATAR OS RISCOS

<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 (LGPD, art. 46.).>
<Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.
<A coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.>
<A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto-, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.>

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
<Risco 1>	<Medida 1; Medida 2; Medida N>					
<Risco 2>	<Medida 1; Medida 2; Medida N>					
<Risco N>	<Medida 1; Medida 2; Medida N>					

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.
[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.
[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

<A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior>.

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	1. CONTROLE DE ACESSO LÓGICO 2. DESENVOLVIMENTO SEGURO 3. SEGURANÇA EM REDES	Reduzir	5	10	50	Sim
R04 Roubo.	1. CONTROLE DE ACESSO LÓGICO 2.CONTROLES CRIPTOGRÁFICOS 3. PROTEÇÃO FÍSICA E DO AMBIENTE	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

8 – APROVAÇÃO

<Esta seção visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa>.

<O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição. Detalhes sobre a necessidade de revisão do RIPD podem ser observados no item 2.5.2.9 do Guia de Boas Práticas LGDP, disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<Nome do responsável> Matrícula/SIAPE: xxxxx <Local>, <dia> de <mês> de <ano>	<Nome do encarregado> Matrícula/SIAPE: xxxxx <Local>, <dia> de <mês> de <ano>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
<Nome do representante> Matrícula/SIAPE: xxxxx <Local>, <dia> de <mês> de <ano>	<Nome do representante> Matrícula/SIAPE: xxxxx <Local>, <dia> de <mês> de <ano>