UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO UNIVERSITÁRIA

ALAN RIBEIRO RODRIGUES

DIRETRIZES PARA IMPLEMENTAÇÃO DE UMA POLÍTICA DE GOVERNANÇA PARA PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR - IFES

Florianópolis (SC)

2024

ALAN RIBEIRO RODRIGUES

DIRETRIZES PARA IMPLEMENTAÇÃO DE UMA POLÍTICA DE GOVERNANÇA PARA PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR - IFES

Dissertação submetida ao Programa de Pós-Graduação em Administração Universitária da Universidade Federal de Santa Catarina para a obtenção do Grau de Mestre em Administração Universitária.
Orientador Prof. Maurício Rissi, Dr.
Área de Concentração: Gestão Universitária
Linha de Pesquisa: Políticas Públicas e Sociedade

Florianópolis (SC)

2024

Rodrigues, Alan Ribeiro
DIRETRIZES PARA IMPLEMENTAÇÃO DE UMA POLÍTICA DE GOVERNANÇA PARA PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR - IFES / Alan Ribeiro Rodrigues ; orientador, Mauricio Rissi, 2024.
151 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Administração Universitária, Florianópolis, 2024.

Inclui referências.

1. Administração Universitária. 2. LGPD. 3. Política de Proteção de Dados Pessoais. 4. Governança. 5. IFES. I. Rissi, Mauricio . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Administração Universitária. III. Título.

ALAN RIBEIRO RODRIGUES

DIRETRIZES PARA IMPLEMENTAÇÃO DE UMA POLÍTICA DE GOVERNANÇA PARA PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR - IFES

O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 19 de setembro de 2024, pela banca examinadora composta pelos seguintes membros:

Profa. Luana Renostro Heinen, Dra.
Universidade Federal de Santa Catarina - UFSC

Prof. Raphael Schlickmann Dr.
Universidade Federal de Santa Catarina - UFSC

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Administração Universitária.

Documento assinado digitalmente
Raphael Schlickmann
Data: 26/09/2024 07:26:42-0300
CPF: ***.788.379-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Mauricio Rissi
Data: 26/09/2024 07:21:50-0300
CPF: ***.170.669-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Mauricio Rissi Dr.
Orientador

Florianópolis, 2024.

AGRADECIMENTOS

Em primeiro lugar, agradeço à minha família, que sempre esteve ao meu lado, dando-me forças e coragem para continuar. Em especial, dedico essa conquista à minha mãe, a razão do meu viver, que, com seu amor incondicional e apoio constante, tornou tudo isso possível.

À minha namorada, Karina, que, além de ser minha parceira de vida, sempre me incentivou a ir além nos estudos, acreditando em mim até quando eu duvidava. Obrigado por ser meu porto seguro e, ao mesmo tempo, o vento que impulsiona minhas velas.

Um agradecimento especial ao meu orientador, que, ao aceitar esse desafio no meio do percurso, demonstrou coragem e paciência. Trocar o pneu com o carro em movimento não foi fácil, mas sua orientação foi fundamental para que chegássemos ao nosso destino.

Aos colegas da turma PPGAU/2022, pela jornada de aprendizado repleta de debates acalorados e trocas de saberes, e, principalmente, pela parceria inestimável nos trabalhos acadêmicos – um agradecimento especial aos campeões de colaboração: Taylon, Diogo, Monica, Cor e Rosiani.

Agradeço também aos profissionais do PPGAU, docentes e técnicos administrativos (TAES), que, com seus conhecimentos e dedicação, tornaram essa jornada possível.

Aos colegas de trabalho, que seguraram o rojão no dia a dia, permitindo que eu me dedicasse aos estudos com tranquilidade. Sou grato pelo apoio e compreensão.

Por fim, gostaria de expressar minha sincera gratidão à UFSC pela concessão do afastamento das atividades laborais, o que me proporcionou a oportunidade de me dedicar aos estudos de forma intensa e produtiva. Esse período foi fundamental para o avanço da minha formação acadêmica e para a realização deste trabalho.

A todos vocês, meu muito obrigado!

RESUMO

Essa pesquisa tem como objetivo propor diretrizes para a implementação de uma política de governança para proteção de dados pessoais em Instituições Federais de Ensino Superior (IFES). Para atingir esse objetivo, foram definidos os seguintes objetivos específicos: verificar diretrizes e práticas de proteção de dados pessoais; identificar o processo de elaboração e implementação de políticas de proteção de dados; e elaborar uma minuta de política de proteção de dados para as IFES. No que se refere aos procedimentos metodológicos, foi utilizado o método dedutivo, de natureza aplicada, com abordagem qualitativa descritiva, além de técnicas de coleta bibliográfica, documental e levantamento por meio de entrevista semiestruturada. Os resultados indicam que, embora as IFES estejam progredindo na adequação à LGPD, ainda enfrentam desafios significativos na implementação dessas políticas. Com base na análise das políticas das IFES participantes do estudo e no referencial teórico adotado, foi elaborada uma minuta de política de proteção de dados, que visa servir como modelo prático para auxiliar na conformidade legal e na proteção eficaz dos dados pessoais.

Palavras-chave: Proteção de Dados Pessoais; LGPD; Política de Proteção de Dados Pessoais; Governança; Gestão Universitária.

ABSTRACT

This research aims to propose guidelines for the implementation of a governance policy for the protection of personal data in Federal Institutions of Higher Education (IFES).. To achieve this goal, the following specific objectives were defined: to verify personal data protection guidelines and practices; to identify the process of drafting and implementing data protection policies; and to develop a draft data protection policy for IFES. Regarding the methodological procedures, the deductive method was used, with an applied nature, a descriptive qualitative approach, and techniques for bibliographic and documentary collection, as well as surveys through semi-structured interviews. The results indicate that, although IFES are making progress in adapting to the General Data Protection Law (LGPD), significant challenges remain in the implementation of these policies. Based on the analysis of the policies of the IFES participating in the study and the theoretical framework adopted, a draft data protection policy was developed, aimed at serving as a practical model to assist in legal compliance and the effective protection of personal data.

Keywords: Personal Data Protection; LGPD; Personal Data Protection Policy; Governance; University Management.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
ANPD - Autoridade Nacional de Proteção de Dados
CF - Constituição Federal
CEFETs - Centros Federais de Educação Tecnológica
CPF - Cadastro de Pessoa Física
DP - Dados Pessoais
DPO - *Data Protection Officer*
EC - Emenda Constitucional
FAQ - *Frequently Asked Questions*
FPSI - *Framework* de Privacidade e Segurança da Informação -
GDPR - *General Data Protection Regulation*
GSI - Gabinete de Segurança Institucional
GT - Grupo de Trabalho
IBGC - Instituto Brasileiro de Governança Corporativa
IF - Instituto Federal
IoT - *Internet of Things*
ISO - *International Organization for Standardization*
IES – Instituições de Ensino Superior
IFES - Instituições Federais de Ensino Superior
LGPD -Lei Geral de Proteção de Dados.
LAI - Lei de Acesso à Informação
ME - Ministério da Economia
MGI - Ministério da Gestão e da Inovação em Serviços Públicos
OCDE - Organização para Cooperação e Desenvolvimento Econômico
OGP - *Open Government Partnership*
ONU - Organização das Nações Unidas
PDCA - *Plan, Do, Check, Act*
PDA - Plano de Dados Abertos
PGP - Programa de Governança em Privacidade
PNSI - Política Nacional de Segurança da Informação
PPDP - Política de Proteção de Dados Pessoais
PPGAU - Programa de Pós-Graduação em Administração Universitária
PPSI – Programa de Privacidade e Segurança da Informação
PSI - Política de Segurança da Informação
RBGO - Referencial Básico de Governança Organizacional
RG - Registro Geral
RIPD - Relatório de Impacto de Proteção de Dados Pessoais
SGD - Secretaria de Governo Digital
TCU - Tribunal de Contas da União
UFSC - Universidade Federal de Santa Catarina
UFRJ -Universidade Federal do Rio de Janeiro

SUMÁRIO

1 INTRODUÇÃO

Vivemos numa sociedade caracterizada, principalmente, pelos serviços onde a informação se tornou o elemento fundamental para o desenvolvimento da economia. Neste contexto, os dados pessoais dos indivíduos se tornaram um fator vital (Bioni, 2019). Porém, os dados pessoais constituem fundamental aspecto da personalidade bem como da privacidade dos indivíduos.

Ressalta-se que o direito à privacidade e o direito à proteção de dados estão consagrados na Constituição Federal de 1988. Para garantia desses direitos, foi instituída recentemente uma política pública que regula o tratamento de dados pessoais pelas organizações públicas e privadas, logo as IFES também estão obrigadas a executar tal política (Brasil, 1988, 2018).

A política pública mencionada, trata-se da Lei Geral de Proteção de Dados (LGPD), que além de criar regras específicas, institui a Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A Lei "busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais" (Vainzof, 2019, p. 25). Para isso cria regras, impondo, inclusive, obrigações e sanções (nos casos de descumprimento) às pessoas naturais ou jurídicas de direito público e privado, que realizam o tratamento de dados pessoais. Com vista a garantir o cumprimento das regras (*enforcement)*, este dispositivo institui a ANPD. Ela é incumbida de zelar pelos dados pessoais, pelas lacunas deixadas para interpretações, bem como a regulamentação da própria Lei (Brasil, 2021).

A Lei estabelece que as organizações que lidam com dados pessoais têm a obrigação de "adotar medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilegal" (Brasil, 2018, art. 46). As organizações possuem discricionariedade para criar regras de boas práticas e de governança, que definam as condições de organização, o modo de operação, os procedimentos, incluindo reclamações e solicitações dos titulares, as normas de segurança, os padrões técnicos, as responsabilidades específicas dos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e mitigação de riscos, além de outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018, art. 50).

A adequação à LGPD também impõe às organizações ajustes em seus processos de governança, exigindo a implementação de programas mais robustos para garantir a conformidade. Isso demanda maiores investimentos, atualização de ferramentas e sistemas de segurança, revisão de documentos, aprimoramento dos procedimentos e fluxos de dados, tanto internos quanto externos, além da adoção de mecanismos de controle, auditoria e, sobretudo, uma mudança cultural significativa (Pinheiro, 2018, p. 33).

É importante destacar que, apesar dos vários guias de boas práticas elaborados pela ANPD e de iniciativas de outros órgãos públicos, não foi encontrado nenhum guia, modelo ou diretrizes para a criação de políticas institucionais de proteção de dados voltadas para Instituições de Federais de Ensino Superior (IFES). Considerando a complexidade organizacional dessas instituições e a diversidade e o volume de dados pessoais tratados por elas, surge a seguinte questão: **Quais diretrizes podem ser propostas para a implementação de políticas de governança para proteção de dados pessoais nas IFES?**

1.2 OBJETIVOS GERAL E ESPECÍFICOS

Partindo da definição do problema de pesquisa, formularam-se os objetivos geral e específicos que nortearam o desenvolvimento do trabalho. Neste sentido, o objetivo geral visa propor diretrizes para implementação de política de governança para proteção de dados pessoais em IFES. Com vistas ao alcance desse objetivo, os seguintes objetivos específicos foram definidos:

a) Verificar diretrizes e boas práticas de proteção de dados pessoais;
b) Identificar processos de elaboração e implementação de política de proteção de dados pessoais;
c) Elaborar um modelo de minuta de política de proteção de dados pessoais para IFES.

1.3 JUSTIFICATIVA TEÓRICO-EMPÍRICA

Nos subtópicos a seguir serão apresentadas a justificativa teórica e a justificativa empírica.

1.3.1 Justificativa teórica

Estudar o tema da proteção de dados pessoais é de extrema importância na sociedade atual, uma vez que vivemos em um mundo cada vez mais conectado, em que dados pessoais são coletados, armazenados e utilizados por organizações públicas e privadas de forma constante. Entre as principais razões para se estudar proteção de dados pessoais, pode-se destacar: Garantia de privacidade (a proteção de dados pessoais é fundamental para garantir a privacidade das pessoas, permitindo que elas possam controlar a forma como suas informações são coletadas, utilizadas e compartilhadas); Proteção contra abusos (a proteção de dados pessoais também ajuda a prevenir abusos e discriminações, evitando que informações sensíveis sejam utilizadas de forma inadequada); Regulação da organizações (a proteção de dados pessoais é fundamental para regular a coleta e utilização de dados por organizações, garantindo que elas sigam padrões éticos e legais e evitando práticas abusivas); Segurança da informação (a proteção de dados pessoais também está diretamente relacionada à segurança da informação, evitando que dados sensíveis sejam expostos a riscos de roubo ou vazamento).

Nesse sentido, a justificativa teórica para estudar proteção de dados pessoais é bastante ampla e envolve questões relacionadas à privacidade, segurança da informação, ética, regulação, entre outros aspectos. Por isso, dentre as principais autoridades brasileiras que contribuem para a discussão do tema foram selecionados, entre outros, os renomados autores Bruno Bioni, Danilo Doneda e Rony Vainzof. Esses autores, entre outros, contribuem para a discussão sobre proteção de dados pessoais no Brasil, trazendo diferentes perspectivas e abordagens para o tema. Com isso, busca-se entender a complexidade da proteção de dados pessoais para então propor soluções adequadas para garantir a proteção desses dados.

Por fim, estudar proteção de dados pessoais é fundamental para entender os aspectos jurídicos, técnicos e éticos envolvidos na coleta, uso e compartilhamento de informações pessoais pelas organizações, contribuindo para uma sociedade mais justa, segura e respeitosa com a privacidade das pessoas.

1.3.2 Justificativa empírica

A “proteção da privacidade é elemento indissociável da dignidade da pessoa, razão pela qual qualquer ato capaz de afetar a intimidade do cidadão seria também um ato atentatório à experiência humana de uma vida digna” (Vainzof, 2019, p. 25). “A dignidade da pessoa humana, para além de princípio, configura-se em cláusula geral, apta a abarcar uma infinidade de formas de proteção e promoção do sujeito” (Konder, 2019, p. 261).

As IFES, assim como qualquer órgão público que realize o tratamento de dados pessoais, estão sujeitos à LGPD (política pública regulatória) que já vigora há mais de 5 anos no Brasil (Brasil, 2018). A referida Lei

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

Com base no então regulamento jurídico, ao tratar os dados pessoais de forma indiscriminada, as instituições públicas poderão incorrer em práticas ilegais ou irregulares. Consequentemente poderão violar direitos fundamentais dos indivíduos tais como: o direito à privacidade e o direito proteção de dados pessoais respaldados pela CF (Constituição Federal) de 1988 (Brasil, 1988).

Visando a proteção de dados pessoais, a LGPD cria regras específicas além possiblidades de sanções ao tratamento irregular ou inadequado de dados pessoais à toda organização pública ou privada que, nas suas atividades, oporem de dados pessoais, logo a Lei é transversal. Com o objetivo de garantir essa proteção, a Lei institui também a ANPD (Autoridade Nacional de Proteção de Dados), incumbida de zelar pelos dados pessoais, pelas lacunas deixadas para interpretações, bem como a regulamentação e o *enforcement* da própria Lei (Brasil, 2021). Portanto, é imprescindível que instituições públicas atuem com o objetivo se adequarem (estar em *compliance*) ao referido ordenamento jurídico.

Com vista a adequação, é salutar às organizações implementar um Programa de Governança em Privacidade e Dados Pessoais com o objetivo de criar regras de boas práticas e de governança, que estabeleçam as condições de organização, o regimento de funcionamento, os procedimentos de reclamações e petições, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Vainzonf, 2020). Para isso, as instituições podem elaborar políticas institucionais de proteção de dados com regras e padrões para tratamento de dados pessoais visando a governança em privacidade conforme indicação dos termos do artigo 50 da Lei (Brasil, 2018).

Nesta senda, as IFES precisam priorizar a criação de políticas de governança para proteção de dados pessoais, visto que o Tribunal de Contas da União (TCU) realiza, há três anos consecutivos, auditorias focadas nesse tema. Essa recorrência aponta para a crescente

importância da conformidade com a Lei Geral de Proteção de Dados (LGPD) e da implementação de mecanismos robustos de proteção.

Contudo, tanto no texto da própria Lei, quanto às orientações da ANPD, não há nenhum guia, modelo, esquema ou passo a passo estabelecidos para a elaboração de uma política institucional de proteção de dados pessoais. Portando, torna-se necessário propor diretrizes para implementação de política de proteção de dados pessoais voltada aos IFES.

Neste sentido, por meio desta pesquisa, pretende-se propor diretrizes para implementação de política institucional de proteção de dados pessoais em IFES, bem como elaborar um projeto (minuta) de política institucional de proteção de dados para IFES. Portanto, a pesquisa está alinhada à área de concentração, intitulada "Gestão Universitária" a qual busca estudar e aplicar sistemas, modelos, técnicas e políticas para a profissionalização das instituições de ensino superior.

Tendo vista a importância de execução de políticas públicas de proteção de dados, acredita-se que estudar e propor diretrizes para a implementação de uma política institucional de proteção de dados pessoais, bem como a elaboração de um projeto (minuta) de política institucional de proteção de dados para IFES tem relação direta com a linha de pesquisa "Políticas públicas e Sociedade".

No que diz respeito à sua relevância, a presente pesquisa procura agregar valor à UFSC, uma vez a possiblidade de implementação de uma política institucional de proteção de dados poderá colocá-la no caminho da adequação para estar em *compliance* com LGPD. Assim, lograr êxito na garantida de proteção dos cidadãos. Para o Programa de Pós-Graduação em Administração Universitária (PPGAU), a pesquisa contribuirá gerando conhecimento no âmbito da gestão universitária.

No mais, o pesquisador é servidor da UFSC e foi nomeado para compor o primeiro GT (grupo de trabalho) com o objetivo que elaborar uma política de proteção de dados, porém o GT foi encerrado antes mesmo que um plano de ação fosse implementado. Por isso, essa pesquisa pode ser considerada oportuna no que diz respeito a possibilidade de se propor diretrizes para implementação de uma política proteção de dados pessoais. Além disso, a própria UFSC poderá ser beneficiar com a proposta de elaboração de uma minuta (projeto) de resolução de política institucional de proteção de dados voltada aos IFES.

Quanto à viabilidade da pesquisa, pode-se classificá-la como viável, pois sua realização envolveu o afastamento integral do pesquisador/servidor de suas funções de trabalho, permitindo a dedicação necessária aos estudos. Esse tempo foi investido em cursos, workshops e outras atividades de formação, essenciais para adquirir as novas habilidades

requeridas pela pesquisa. Além disso, os dados e informações necessários à pesquisa são de fácil acesso e disponibilidade, especialmente por se tratarem, em sua maioria, de dados públicos. Assim, não houve necessidade de adquirir bases de dados, assinaturas de revistas científicas ou licenças para acesso a bancos de dados. Nesse contexto, os principais custos foram essencialmente absorvidos pela Universidade.

1.4 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em 5 capítulos: Introdução, Fundamentação Teórica, Procedimentos Metodológicos, Análise e Interpretação dos Dados Coletados e, por fim, Considerações Finais.

No primeiro capítulo, apresenta-se a introdução, que contextualiza o tema e define o problema da pesquisa, os objetivos (geral e específicos) e a justificativa do estudo. O segundo capítulo é dedicado à fundamentação teórica, baseada na revisão da literatura sobre Políticas Públicas, Políticas Institucionais, Proteção de Dados Pessoais, Lei Geral de Proteção de Dados Pessoais, Governança, e Tipos de Políticas Institucionais de Proteção de Dados Pessoais.

O terceiro capítulo detalha a metodologia empregada, especificando os procedimentos metodológicos utilizados para alcançar os objetivos propostos. O quarto capítulo é dedicado à análise e interpretação dos dados coletados, oferecendo uma visão detalhada dos resultados obtidos. Nesse capítulo são apresentadas as diretrizes e boas práticas de proteção de dados pessoais das IFES, os processos de implementação de política de proteção de dados pessoais em Instituições Federais de Ensino Superior (IFES) e, por fim, um modelo de Política de Proteção de Dados Pessoais desenvolvido a partir da análise e dos conceitos teóricos estudados.

Finalmente, o quinto e último capítulo apresenta traz as considerações finais, sintetizando as conclusões do trabalho e apontando possíveis direções para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são apresentadas as principais bases teóricas encontradas na literatura que contribuíram para a construção desta pesquisa. Foram consideradas obras e pesquisas que analisam políticas públicas (tipologias, categorias e processo), privacidade e proteção de dados pessoais à luz do Direito, Lei Geral de Proteção de Dados Pessoais e governança e políticas institucionais para proteção de dados pessoais.

2.1 POLÍTICAS PÚBLICAS

De acordo com Heidemann e Salm (2014), o desenvolvimento político-administrativo da sociedade resulta das decisões formuladas e implementadas pelo governo em consonância com as demais forças sociais. As ofertas de bens e serviços são realizadas por meio de políticas públicas. Política pública pode ser definida como "diretriz elaborada para enfrentar um problema público" (Secchi, 2013, p. 2). Além disso, política pública é uma escolha do governo em agir ou deixar de agir sobre um problema. Também pode ser entendida como "iniciativa sancionada por governos que atuam oficialmente em nome dos cidadãos, [...] sendo toda ação de mudança praticada na sociedade por força de lei ou regulação pública". Numa perspectiva mais ampla, trata-se de um "conjunto de decisões inter-relacionadas [...] tomadas por indivíduos ou órgãos no âmbito do governo com o objetivo de gerar um efeito ou impacto" (Heidemann, 2009, p. 34).

Outros autores definem política pública como:

a) o campo dentro do estudo da política que analisa o governo à luz de grandes questões públicas (Mead, 1995);

b) um conjunto de ações do governo que irão produzir efeitos específicos (Lynn, 1980);

c) a soma das atividades dos governos, que agem diretamente ou através de delegação, e que influenciam a vida dos cidadãos (Peters, 1986);

d) o que o governo escolhe fazer ou não fazer (Dye, 1984).

As políticas públicas são implementadas mediante intencionalidade do Estado (a partir de instrumentos legais), pela governança (capacidade administrativa) e pela gestão (materialidade do ato de governar), ou seja, intenção e ação. De todo modo, “nem toda política pública é realizada de forma exclusiva, plena e satisfatória por governos” (Heidemann; Salm, 2014, p. 33).

Apesar das diferenças dentre os pesquisadores quanto à definição de uma política pública, pode-se extrair e sintetizar seus elementos principais:

> - A política pública permite distinguir entre o que o governo pretende fazer e o que, de fato, faz.
> - A política pública envolve vários atores e níveis de decisão, embora seja materializada através dos governos, e não necessariamente se restringe a participantes formais, já que os informais são também importantes.
> - A política pública é abrangente e não se limita a leis e regras. A política pública é uma ação intencional, com objetivos a serem alcançados. A política pública, embora tenha impactos no curto prazo, é uma política de longo prazo.
> - A política pública envolve processos subsequentes após sua decisão e proposição, ou seja, implica também implementação, execução e avaliação (Souza, 2006, p. 36).

Portanto, mesmo considerando o entendimento e existência de políticas públicas por meio da ação do setor econômico e organizações da sociedade civil, adota-se aqui a visão de políticas públicas por meio da ação do Estado, por sua superioridade hierárquica para corrigir problemas públicos que o mercado e comunidade não conseguem. Além disso, ressalta-se que historicamente o Estado brasileiro é tradicionalmente intervencionista (Melo, 1999). "A abordagem estatista admite que atores não estatais até tenham influência no processo de elaboração e implementação de políticas públicas, mas não confere a eles o privilégio de estabelecer (decidir) e liderar um processo de políticas pública" (Secchi, 2013, p. 3).

Assim, as denominadas políticas governamentais são aquelas desenvolvidas e implementadas por agentes do governo. Entre essas políticas, incluem-se as criadas pelos diferentes órgãos dos poderes Legislativo, Executivo e Judiciário. Atualmente, as políticas governamentais representam o subgrupo mais significativo das políticas públicas (Secchi, 2013).

Desse modo, no que se refere à política pública será utilizado o subgrupo política governamental neste estudo considerando os seguintes elementos: a intenção pública; a resposta a um problema público; o tomador de decisão possui personalidade jurídica estatal e que são diretrizes de nível estratégico, intermediário e operacional (Heidemann, 2010; Secchi, 2013).

2.1.1 Tipologias de políticas públicas

Incialmente, cabe mencionar que a tipologia "é um esquema de interpretação e análise de um fenômeno baseado em varáveis e categorias analíticas. Uma variável é um aspecto discernível de um objeto de estudo que varia em qualidade e quantidade". A política pública como objeto de estudo pode ser analisada por meio desse esquema analítico. Assim, "as

tipologias de políticas públicas são formas de classificar os conteúdos, os atores, os estilos, as instituições dentro de um processo de política pública" (Secchi, 2013, p. 24).

Interpretar o processo de políticas públicas significa compreender como esses fatores interagem e influenciam o fluxo das políticas públicas. Nesse sentido, faz-se necessário analisar as "interações que ocorrem ao longo do tempo entre políticas públicas e atores, eventos, contextos e resultados (Weible; Carter, 2016). Por fim, entre outros, alguns modelos explicativos de políticas públicas foram desenvolvidos para se facilitar o entendimento do porquê o governo faz ou deixa de fazer alguma ação que repercutirá na vida dos cidadãos que serão apresentados mais adiante. (Souza, 2006).

Dado o contexto, a tipologia Lowi (1964, 1972 apud souza, 2006) foi desenvolvida com a premissa de que política pública determina a dinâmica da política. Assim, cada tipo de política pública vai encontrar diferentes formas de apoio e de rejeição onde as disputas em torno de sua decisão passam por arenas diferenciadas. Dependendo do tipo de política pública que está em jogo, "a estruturação dos conflitos, das coalizões e o equilíbrio de poder se modificam" (Secchi, 2013, p. 23).

Na tipologia de Lowi, as políticas públicas são classificadas/categorizadas de acordo com seus atributos funcionais. Assim propõe-se quatro categorias funcionais saber: política distributiva, política constituinte, política reguladora e política redistributiva. A política regulatória tem como objetivo estabelecer os padrões comportamentais da sociedade. Geralmente, essa categoria se desenvolve "dentro de uma dinâmica pluralista, em que a capacidade de aprovação ou não de uma política desse gênero é proporcional à relação de forças dos atores e interesses presentes na sociedade" (Secchi, 2013, p. 25). A política distributiva tem como objetivo direcionar recursos difusos da coletividade para grupos específicos de interesses. A política redistributiva tem como objetivo conceder benefícios a um grupo específico, retirando recursos de outros grupos também específicos de atores. E, por fim, as constitutivas definem as regras que moldam o funcionamento da sociedade, bem como o governo (Secchi, 2013).

Na tipologia de Wilson, o critério adotado é o de distribuição dos custos e benefícios da política pública na sociedade. Essa tipologia se aproxima da tipologia do tipo de Lowi. Nas políticas de tipo clientelista os benefícios são concentrados em certos grupos e os custos são difusos na coletividade, semelhante as políticas distributivas. Nas políticas de grupo de interesse tanto os custos quanto os benefícios estão concentrados em certos grupos, referindo-se às políticas redistributivas. Nas políticas empreendedoras os benefícios são coletivos e os custos são concentrados em certas categorias, não possuindo uma espécie semelhante na

tipologia de Lowi. Por fim, nas políticas majoritárias os custos e benefícios são distribuídos pela coletividade (WILSON, 1983 apud SECCHI, 2013).

Quadro 1. Comparativo dos tipos, categorias, benefícios e custo de políticas públicas

Tipologia de Política	Categoria de Política	Impacto/Benefício	Custo
Lowi	Distributiva	grupos específicos	difusos na coletividade
	Redistributiva	grupos específicos	Grupos
	Regulatória	-	-
	Constitucional	-	-
Wilson	Majoritária	difusos na coletividade	difusos na coletividade
	Clientelista	grupos específicos	grupos específicos
	Empreendedora	difusos na coletividade	grupos específicos
	Grupo de interesse	grupos específicos	grupos específicos

Fonte: Elaborado pelo autor com base em Lowi (1964, 1985); Wilson (1983) apud Secchi (2013).

Ressalta-se que diversas outras maneiras de classificar as políticas estão sujeitas a consideração. Com base nisso,

> o analista de políticas públicas pode realizar sua análise utilizando uma das tipologias já consolidadas na literatura (aplicação dedutiva) ou então pode construir sua própria tipologia (desenvolvimento indutivo). O desenvolvimento indutivo de tipologias se baseia na capacidade do pesquisador em estabelecer um critério diferente para a verificação de uma variável ou estabelecer novas categorias analíticas para a classificação dos fenômenos. A vantagem do desenvolvimento indutivo é a customização de uma tipologia mais adequada ao objetivo da análise (Secchi, 2013, p. 31).

Desse modo, classificação das políticas públicas por tipos e por categorias são meios de simplificar a diversificação encontrada na literatura. Além disso, Weible e Carter, (2016) enfatizam que:

> Além de simplificar a diversidade de políticas públicas por meio da classificação, as políticas públicas podem ser descritas por seus conteúdos. Os blocos de construção do conteúdo da política são geralmente considerados o conteúdo textual, ou a forma escrita dos documentos da política. No entanto, algumas políticas públicas não são escritas, mas compreendidas e aplicadas (muitas vezes de forma implícita) entre um grupo de pessoas envolvidas em um órgão governamental ou situação equivalente. Tais políticas se enquadram nas (chamadas) regras de uso ou regras de trabalho (WEIBLE; CARTER, 2016, p. 4).

Os autores supracitados exemplificam que as regras de trabalho são normalmente adotadas pelos burocratas de nível de rua que, cotidianamente, prestam os serviços públicos.

Ou seja, são os profissionais que executam (praticam) as políticas públicas por meio do atendimento direto aos usurários/ cidadãos (público-alvo das políticas).

Por fim, ainda em termos de simplificação, o analista poderá buscar na literatura modelos de análise de políticas públicas já consolidados que o possibilite formular e implementar a política pública mais apropriada à organização púbica. Nesse sentido, serão apresentados brevemente alguns dos principais modelos de políticas públicas.

2.1.2 Modelos de políticas públicas

A análise de políticas públicas é uma abordagem que considera a política como um processo complexo e dinâmico que envolve múltiplos atores, interesses e recursos. A análise de políticas públicas deve ser entendida como um conjunto de métodos e técnicas que permitem investigar e compreender a elaboração, implementação e avaliação das políticas públicas (Secchi, 2020).

Além disso, a análise de políticas públicas (*policy analysis*) tem como objetivo gerar e organizar informações importantes para o processo de tomada de decisões em políticas públicas. O foco principal dessa atividade é fornecer dados que tornem a política pública mais eficaz na resolução ou mitigação do problema público (Secchi, 2020).

Dado o contexto, os modelos de políticas públicas, surgem com a finalidade de ordenar e simplificar a realidade; identificar o que é relevante; condizer com a realidade; comunicar algo significativo; orientar a pesquisa e a investigação; para simplificar a compressão sobre políticas públicas; identificar aspectos importantes de questões político-sociais; propor as explicações para as políticas públicas, além de prever suas consequências (Dye, 2010).

Ressalta-se ainda que:

> O modelo é uma representação simplificada de algum aspecto do mundo real. Pode ser uma representação física real – um protótipo de aviação, por exemplo, ou as maquetes de edifícios que os planejadores urbanos usam para mostrar como as coisas vão se parecer quando os projetos propostos estiverem efetivamente construídos. Ou pode o modelo ser um diagrama – o mapa de uma estrada, por exemplo, ou o fluxograma que os cientistas políticos usam para mostrar como um projeto de lei se transforma em lei (Dye, 2010, p. 99).

Há dois principais modelos de análise de políticas públicas: positivista (racionalista) e pós-positivista (argumentativa). As duas vertentes convergem quanto a suas origens, objetivos e produto final, mas os valores, métodos, produtos e destinatários da análise podem ser diferentes (Sechi, 2020).

Modelo Racional: nesse modelo, o processo de políticas é baseado no cálculo dos objetivos que devem ser perseguidos. A política racional produz o ganho social máximo, ou seja, "os governos devem optar por políticas cujos ganhos sociais superem os custos pelo maior valor e devem evitar políticas cujos custos não sejam excedidos pelos ganhos" (Dye, 2010, p. 111).

A abordagem racionalista de política pública, na visão de Secchi (2020), é uma abordagem que enfatiza a tomada de decisão baseada em evidências e na análise cuidadosa de opções de políticas. Essa abordagem considera a política pública como um processo racional, no qual os objetivos e as alternativas são claramente definidos e analisados para determinar a melhor opção de ação.

O modelo racionalista é mais adequado em situações que envolvem temas técnicos bem definidos, quando há grande urgência, quando a necessidade de legitimação da análise e da decisão é reduzida e quando a expertise está concentrada em um analista de políticas públicas capaz de dominar as ferramentas racionalistas e, assim, encontrar boas soluções para o problema público em questão (Secchi, 2020).

Ainda nessa abordagem, a tomada de decisão é vista como um processo sistemático e analítico, que envolve a avaliação de alternativas de políticas com base em critérios como eficácia, eficiência, equidade e sustentabilidade. As políticas públicas são concebidas como soluções para problemas específicos, e a análise de custo-benefício é frequentemente utilizada para avaliar a viabilidade das opções de políticas.

> A abordagem racionalista é mais adequada para problemas estruturados, a abordagem argumentativa consegue lidar com problemas complexos. [...]. A abordagem argumentativa é a mais indicada, envolvendo *stakeholders* em um processo participativo que pode aumentar a legitimidade da posterior decisão. (Secchi, 2020, p. 83).

Modelo Argumentativo: a abordagem argumentativista de política pública é uma abordagem que valoriza o diálogo e a participação pública na tomada de decisão. Essa abordagem considera que a política pública é um processo dialógico, no qual as partes interessadas apresentam suas perspectivas e argumentos para chegar a uma decisão coletiva. Essa abordagem é baseada em três pressupostos fundamentais: a existência de valores e interesses em conflito, a necessidade de deliberar e negociar entre as partes interessadas e a importância da legitimidade e aceitação social da decisão tomada (Secchi, 2020).

Nessa abordagem, a tomada de decisão é vista como um processo participativo e inclusivo, no qual as partes interessadas são convidadas a contribuir com suas perspectivas e

argumentos. As políticas públicas são concebidas como soluções para problemas complexos que envolvem interesses e valores divergentes, e a argumentação é frequentemente utilizada para chegar a uma decisão coletiva (Sechi, 2020).

De acordo com autor supracitado, é possível adotar ambas as abordagens simultaneamente ou fazer um mix de alguns elementos de cada. Quanto mais se utilizam ferramentas analíticas, maior é a probabilidade de que o trabalho seja realizado de forma mais aprofundada e sofisticada. Entretanto, o ambiente de políticas frequentemente apresenta limitações em termos de recursos humanos, financeiros, organizacionais, tempo e competências para realizar análises com ambas as abordagens. Por isso, é importante avaliar qual abordagem é a mais apropriada para o contexto em que o analista está inserido (Secchi, 2020).

Nesse sentido, pode-se conciliar as correntes analíticas racionalistas e argumentativas de análise de políticas públicas, aproveitando tanto as vantagens "da metodologia simples e didática e as ferramentas analíticas quantitativas da análise racionalista (positivista) quanto a vantagem da análise argumentativa, que é a adoção de métodos participativos e deliberativos que absorvem as perspectivas de uma pluralidade de atores" (Secchi, 2020, p.32).

Por fim, na elaboração do planejamento da análise das soluções, cabe ao analista de políticas públicas a capacidade de observar e decidir qual das duas metodologias de análise (abordagem racionalista ou argumentativa) é mais adequada ao contexto em questão. Para tomar essa decisão, é necessário compreender as características centrais de cada abordagem. Uma vez escolhida a abordagem racionalista, o analista deverá passar por três etapas para concluir seu trabalho: geração de alternativas, estabelecimento de critérios e projeção dos resultados (Secchi, 2020). Cabe também ao analista compreender o processo de construção de política pública, tema que será apresentado no próximo tópico.

2.1.3 Processo de construção de políticas públicas

Interpretar o processo de políticas públicas significa compreender como esses fatores interagem e influenciam todo o fluxo das políticas públicas. Portanto, faz-se necessário analisar as "interações que ocorrem ao longo do tempo entre políticas públicas e atores, eventos, contextos e resultados (Weible; Carter, 2016).

O processo de elaboração de políticas públicas também conhecido como ciclo de políticas públicas "é um esquema de visualização e interpretação que organiza a vida de uma política pública em fases sequenciais e interdependentes" (Secchi, 2013, p. 42).

Não obstante as diversas versões e modelos já elaborados do ciclo de políticas púbicas, Souza (2006, p. 29) “vê a política pública como um ciclo deliberativo, formado por vários estágios e constituindo um processo dinâmico e de aprendizado”. A autora apresenta o ciclo da política pública com os seguintes estágios: i) definição de agenda; ii) identificação de alternativas; iii) avaliação das opções; iv) seleção das opções; v) implementação; e vi) avaliação.

Secchi (2013) apresenta um ciclo com sete fases principiais. Essas fases são: i) identificação do problema; ii) formação da agenda; iii) formulação de alternativas; iv) tomada de decisão; v) implementação; vi) avaliação; e vii) extinção. Esse processo é mais abrangente, suas fases serão apresentadas de forma sucinta a seguir.

A **fase de identificação do problema** diz respeito a percepção do problema por parte dos atores relevantes, a delimitação ou definição do problema e a avaliação da possibilidade de solução. **A formação da agenda** é fazer com que o problema identificado faça parte do “conjunto de problemas ou temas entendidos como relevantes” (Secchi, 2003, p. 46). Na terceira fase serão analisadas as possíveis consequências de cada **alternativa** de solução. **A tomada de decisão** refere-se a fase em que os interesses dos atores e os objetivos e métodos de enfrentamento do problema são explicitados e ponderados. Na **fase de implementação** tem-se a produção dos resultados concretos da política pública. Na **fase de avaliação** ocorre a análise do processo de implementação e o desempenho da política pública. Por fim, a última fase diz respeito a **extinção** da política pública quando o problema for resolvido, ou as alternativas foram ineficazes, ou quando o problema saiu da agenda (Secchi, 2003, grifo nosso).

> As etapas normalmente consideradas em matéria de política pública– formulação, implementação e avaliação – precisam de certo grau de especificação na América Latina. É necessário, por exemplo, distinguir elaboração de formulação. A primeira é a preparação da decisão política; a segunda, a decisão política, ou a decisão tomada por um político ou pelo Congresso, e sua formalização por meio de uma norma jurídica. Implementação também deve ser mais detalhada na América Latina. É necessário separar a implementação propriamente dita, que é a preparação para a execução (ou, em outras palavras, a elaboração de planos, programas e projetos), da execução, que é pôr em prática a decisão política. Essa distinção é necessária, porque cada uma das etapas mencionadas é campo para tipos diferentes de negociação (Saravia; Ferrarezi, 2006, p. 32).

Resumidamente, o autor supracitado aborda uma variação etapas conforme se segue:

1. **Agenda:** Momento em que uma determinada questão, demanda ou necessidade social é reconhecida e inserida na lista de prioridades do governo. Nesta etapa, os problemas sociais se tornam "problemas públicos" e começam a ser debatidos e contestados na

esfera política e midiática, muitas vezes justificando intervenções por parte das autoridades públicas.

2. **Elaboração:** Após a identificação e delimitação de um problema atual ou potencial da comunidade, esta etapa envolve a análise das possíveis soluções ou alternativas disponíveis. São considerados os custos e os efeitos de cada opção, priorizando aquelas que parecem mais adequadas para resolver ou atender ao problema em questão.
3. **Formulação:** Aqui ocorre a seleção e especificação da alternativa considerada mais conveniente para enfrentar o problema identificado. Esta decisão é formalizada por meio de declarações que definem objetivos claros e estabelecem o enquadramento jurídico, administrativo e financeiro da política pública proposta.
4. **Implementação:** Esta etapa envolve o planejamento detalhado e a organização dos recursos necessários para executar a política pública. Isso inclui a alocação de pessoal, financeiro, material e tecnológico, bem como a preparação de planos, programas e projetos que serão necessários para colocar a política em prática.
5. **Execução:** Consiste na realização efetiva das ações planejadas e na implementação dos programas e projetos estabelecidos para atingir os objetivos da política pública. Durante esta fase, são enfrentados os obstáculos práticos e burocráticos que podem surgir, visando alcançar os resultados desejados.
6. **Acompanhamento:** Esta etapa é caracterizada pela supervisão sistemática da execução da política pública. O objetivo é fornecer informações que permitam ajustes e correções ao longo do processo, garantindo que os objetivos estabelecidos sejam alcançados de forma eficiente e eficaz.
7. **Avaliação:** Por fim, realiza-se uma avaliação abrangente dos efeitos produzidos pela política pública na sociedade. Esta análise retrospectiva visa mensurar o impacto das ações realizadas, avaliar o alcance dos objetivos propostos e identificar eventuais consequências não previstas, contribuindo para o aprimoramento contínuo das políticas públicas.

Por fim, após desenhadas e formuladas, “as políticas públicas desdobram-se em planos, programas, projetos, bases de dados ou sistema de informação e pesquisas. Quando postas em ação, são implementadas, ficando daí submetidas a sistemas de acompanhamento e avaliação” (Souza, 2006, p. 26).

Em se tratamento da participação dos atores no processo de implementação de políticas públicas, recomenta-se que elas devem ser baseadas no ideal da democracia. Deve-se afastar a possibilidade de elaboração de forma individual, pois as políticas resultam da interação de

várias atores (indivíduos, grupos ou organizações), eventos e contextos como já mencionado. Nesse sentido, Redford (1969 apud Denhardt, 2012) enfatiza que para lograr êxito na do ideal democrático no âmbito da administração pública, é imprescindível a representação por meio da participação dos interessados no processo de interação entre os tomadores de decisão. "A implementação exige cooperação, coordenação e legitimidade" (Melo, 1999, p. 86). "Uma política ou ação pública é legítima quando os cidadãos têm boas razões para apoiá-la ou obedecê-la" (Fung, 2006).

Complementando, a legitimidade pode assegurar a eficácia no processo de implementação de políticas públicas, além disso a *accountability* desponta como fator crucial.

> Enquanto estivermos comprometidos com o ideal democrático, o estado administrativo só se conseguirá legitimidade se puder demonstrar capacidade de promover o valor individual a igualdade entre todos os cidadãos e a participação universal. É ao longo dessas linhas que devemos examinar a responsividade das organizações públicas (Denhardt, 2012, P. 171).

A participação dos atores pode acontecer em momentos distintos do processo de políticas públicas, podendo, inclusive, se restringir apenas ao momento de prospecção de soluções, ou ainda ser estendida para o momento de decisão formal (Secchi, 2013). Além disso o autor enfatiza que

> A participação de mais atores pode acontecer no momento da implementação da política pública como nos moldes de **governança pública** (por exemplo, parcerias público-privadas, redes de implementação de políticas públicas. O momento de avaliação da política também pode ser abastecido como informações de fornecedores, cidadãos funcionários públicas etc. (Secchi, 2013, p. 142).

Portanto, a participação democrática, no processo de elaboração, afeta substancialmente a legitimidade, o senso de justiça e a eficácia de políticas públicas. Além disso, aumenta a quantidade e qualidade de informações disponíveis para embasar a tomada de decisões mais adequada (Fung, 2006).

2.1.4 Políticas institucionais

O processo decisório no âmbito organizacional deve ser construído com base em políticas institucionais, implementadas após realização de diagnósticos estratégicos (Silva Júnior, 2018). É fundamental que "o diagnóstico estratégico (que envolve a visão, os valores, análise externa, a análise interna e a análise dos concorrentes) seja realista completa e impessoal, evitando possíveis problemas futuros" (Oliveira, 2007, p. 49).

Nesse contexto, um dos aspectos mais relevantes da fase de diagnóstico estratégico é que o resumo das sugestões deve ser elaborado de maneira a despersonalizar as ideias individuais e consolidar as ideias da organização, incluindo possíveis contradições. No entanto, por meio de um debate direcionado, busca-se promover o bom senso e alcançar o consenso (Oliveira, 2007).

Assim, o processo de tomada de decisão e o estabelecimento de estratégias e políticas são interligados, funcionando de forma interativa dentro da organização. Com base nisso, a estratégia pode ser definida como um padrão ou plano que integra as principais metas, políticas e a sequência de ações de uma organização em um todo coerente. Uma estratégia bem formulada ajuda a organizar e alocar os recursos de uma organização em uma posição singular e viável, baseada em suas competências e deficiências internas relativas, nas mudanças antecipadas no ambiente e nas medidas contingenciais tomadas por concorrentes inteligentes (Mintzberg; Quinn, 2006).

Geralmente, as políticas públicas regulatórias (estabelecidas por leis) são principiológicas. Nesse sentido, cabe às instituições do setor público criarem políticas institucionais a fim de se adequarem às leis, cobrir suas lacunas e executar com eficiência e eficácia as políticas públicas objetivando sua efetividade.

Para Buskirk (1971) há cinco funções básicas das políticas institucionais no processo decisório: i) uniformidade do comportamento na organização; ii) continuidade das decisões; iii) sistema de comunicação; iv) facilitador na tomada de decisão; e v) proteção contra pressões imediatas.

As políticas institucionais são regras ou diretrizes que determinam os limites conforme a ação deve ocorrer. Geralmente, essas “regras têm a forma de decisões contingentes para resolver conflitos entre objetivos específicos” (Mintzberg; Quinn, 2006, p. 29). As políticas institucionais tratam de estabelecer regras e declaração de parâmetros para aspectos no âmbito da organização. Há, por exemplo, políticas institucionais de gestão de resíduos; de privacidade e proteção de dados pessoais; de inovação e propriedade intelectual; de segurança da informação; de enfrentamento ao racismo; de combate ao assédio moral e sexual entre outras. Importante ressaltar que a política institucional, provém dos objetivos e desafios da organização determinadas pela alta administração. A política institucional trata-se, portanto, de um instrumento prescritivo do processo de planejamento estratégico das organizações (Oliveira, 2007).

Como já mencionado anteriormente, no processo de construção de política pública, Secchi (2003) apresenta as fases: identificação do problema; formação da agenda; formulação

de alternativas; tomada de decisão; implementação; avaliação; e extinção. Numa implementação de uma política institucional que tem por objetivo seguir o que determina uma política pública estabelecida por lei, a organização pode utilizar o mesmo rito da política como modelo, fazendo as adaptações necessárias ao contexto da organização e/ou ainda fazer uso de outras metodologias e ferramentas de forma combinada.

Uma metodologia simples e muito difundida é o ciclo PDCA, que pode ser combinada com outras metodologias e ferramentas estratégicas como o *benchmarking, brainstorm, nudge* (ambas recomendadas para aplicação no modelo racional de políticas públicas), aplicação de técnicas do modelo argumentativo de política pública e análise ambiental. O ciclo PDCA, geralmente, é aplicado no processo de gerenciamento da qualidade nas organizações. Entretanto o ciclo surge como uma técnica de gestão. [...] "é um método iterativo para a condução de atividades de melhoria, que consiste em quatro grandes fases: planejar (plan), executar (do), avaliar (check) e agir (act)" (Carpinetti; Gerolamo, 2016 p. 12).

A relevância do ciclo reside em aprimorar continuamente a qualidade por meio de um processo iterativo que envolve a avaliação dos resultados, a identificação de erros e suas causas, a reflexão sobre ações corretivas, o planejamento e a implementação dessas ações, seguidos de uma nova avaliação dos resultados, reiniciando o ciclo. O ciclo PDCA destaca princípios essenciais, como a tomada de decisões fundamentadas em dados e fatos e a aprendizagem a partir da análise dos erros (Carpinetti; Gerolamo, 2016).

Em síntese, este método é utilizado para a resolução de problemas e para o cumprimento de metas de forma contínua. Já o *benchmarking* é um "processo contínuo e interativo para com as realidades ambientais para a avaliação do desempenho corrente, estabelecimento de objetivo, bem como para identificação de áreas de aperfeiçoamento e mudanças nas empresas" (Leibfried; McNair, 1994, apud Oliveira, 2007, p.67).

O benchmarking consiste em analisar e sistematizar práticas de referência a fim de gerar ideias de melhoria para as próprias práticas. A essência do benchmarking é examinar casos reais de aplicação de processos, operações, funções, estratégias ou modelos organizacionais que se mostraram bem-sucedidos em outras situações, para que possam inspirar os participantes do processo criativo (APQC, 2015, apud Secchi, 2020).

> O benchmarking aplicado à política pública é uma técnica de pesquisa utilizada para a geração de alternativas com base em experiências de casos de sucesso (benchmarks). O problema identificado raramente é peculiar ao local, ou seja, há grandes possibilidades de que ele acometa outras comunidades políticas. O analista de política pública pode usar o benchmarking para descobrir soluções análogas que outros órgãos públicos, em outras cidades,

> estados ou países, utilizam para enfrentar o mesmo problema (Bogan; English, 1996, apud Secchi, 2020, p. 94)

O benchmarking se mostra como uma fermenta fundamental em se tratando da abordagem racionalista de política pública. Entre outras, sua vantagem está na capacidade de encontrar soluções excepcionais e de sucesso para problemas que ocorrem ou ocorreram em outros lugares. Pode-se também utilizar a técnica *Nudge* para criar alternativas de política pública em diversas áreas. "Para esse tipo de geração de ideias, é preciso 'pensar fora da caixa', ou seja, evitar que o analista de política pública seja uma vítima daqueles cinco vieses comportamentais: ancoragem, disponibilidade heurística, representatividade heurística, resistência às mudanças e senso de manada (Thaler; Sustein, 2008 apud Secchi, 2020, p. 101).

> A técnica *Nudge* consiste em criar estímulos leves para a modificação do comportamento humano. Como uma política pública é uma diretriz que busca influenciar a ação humana, o analista de política pública pode usar técnica '*nudge*' para encontrar soluções simples acessíveis, de baixo custo e eficazes. A técnica Nudge tem base na psicologia social e na economia comportamental e refuta a ideia de que o ser humano seja sempre um maximizador de utilidade. [...] a técnica Nudge parte do princípio de que muitos dos comportamentos públicos e privados das pessoas são automáticos, baseados em cinco vieses comportamentais: Ancoragem: a ação das pessoas é muito condicionada por parcelas de informação (âncoras); Disponibilidade heurística: a opinião das pessoas é muito condicionada pelos exemplos que elas têm à disposição; Representatividade heurística: a opinião das pessoas sobre o que ocorrerá no futuro é muito condicionada por eventos que ocorreram no passado; Resistência às mudanças: a ação das pessoas é muito condicionada pelo que elas já vinham fazendo no passado; Senso de manada: a ação das pessoas é muito condicionada pelo que seus pares fazem (Thaler; Sustein, 2008, apud Secchi, 2020, p. 100).

Já o *brainstorming*, também conhecido como tempestade de ideias, é uma técnica de criatividade em grupo que busca gerar ideias livres e espontâneas para solucionar uma questão ou problema. Essa técnica consiste em reunir um grupo de pessoas em um mesmo ambiente e encorajá-las a pensar coletivamente com o objetivo de gerar ideias criativas (Osborn, 1953, apud Secchi, 2020).

Em se tratando da análise ambiental, essa "corresponde ao estudo dos diversos fatores e forças do ambiente, às relações entre eles ao longo do tempo e seus efeitos ou potenciais efeitos sobre a empresa, sendo baseada nas percepções das áreas em que as decisões estratégicas da empresa deverão ser tomadas" (Oliveira, 2007, p. 72).

Dado o contexto, a política institucional se demonstra como elemento fundamental para que as organizações possam estar em conformidade com políticas regulatórias, inclusive a

de proteção de dados pessoais. Mas o sucesso para a implementação de uma política depende da utilização de um método, sendo que o ciclo PDCA combinado com as ferramentas como *benchmarking, brainstorm, nudge* e análise de ambiental se mostram viáveis dada suas aplicabilidades. Além dessas, as normas ISO surgem como alternativa para implementação de políticas (Oliveira, 2007).

Por fim, compreender a proteção de dados pessoais no contexto brasileiro é primordial para que o analista ou executor de políticas públicas possa implementar uma política no âmbito organizacional. Nesse aspecto, será apresentado um arcabouço teórico sobre o tema no próximo tópico.

2.2 PROTEÇÃO DE DADOS PESSOAIS

A nova configuração de organização social (principalmente pela evolução tecnológica recente), culminou na criação de mecanismos capazes de processar e transmitir informações em uma quantidade jamais imaginável (Bioni, 2019).

> a tecnologia ganhou novo ímpeto e coloração com o incremento na velocidade do seu desenvolvimento em várias áreas, como a eletrônica, as telecomunicações e tantas outras. Essas tecnologias passaram a condicionar diretamente a sociedade, com sua filosofia de trabalho, seus instrumentos de produção, sua distribuição do tempo e de espaço; além de se identificar diretamente com a substância dos instrumentos e mecanismos de controle que podem causar a erosão da privacidade. A dimensão que o fenômeno tecnológico assumiu passou então a se tornar motivo de reflexão para as ciências sociais (Doneda, 2020, p.45).

Do ponto de vista econômico, os dados importam na medida em que podem ser transformados em informações úteis. Os dados precisam ser processados para que possam agregar valor às atividades econômicas. Em face disso, a monetização dos dados modificou a economia vigente. Por outro lado, substancialmente, nas esferas particulares dos indivíduos, além de provocar transformações estruturantes nas relações sociais e políticas, os dados ganharam uma importância transversal, tornando-se balizadores das vidas e das liberdades individuais (Frazão, 2019).

Além disso, Basan (2019) afirma que o desenvolvimento da computação e a ampliação do uso da internet criaram um novo ambiente para as interações humanas, impactando diretamente diversos subsistemas da sociedade (sociais, econômicos, jurídicos, familiares, políticos etc.). Vivemos em uma sociedade centrada na "datificação". Bioni (2019) define datificação como o ato de transformar em dados praticamente toda a vida de um indivíduo. Esse

fenômeno surge como consequência da ubiquidade da internet e dos *smartphones*, ou seja, do ambiente virtual onipresente.

Nesse contexto, os indivíduos estão cada vez mais condicionados em sua participação social devido à crescente digitalização de suas vidas, enfrentando estigmatização e sendo submetidos a uma série de decisões automatizadas e, por vezes, a práticas discriminatórias que impactam o livre desenvolvimento de sua personalidade (Bioni, 2019).

As tecnologias da informação possibilitaram organizar os dados de maneira mais escalável, somando isso à inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e a sua promoção (publicidade), surgiu um novo mercado que se fundamenta na sua extração e "comodificação" dos dados pessoais. Trata-se, portanto, de uma economia que tem como cerne a vigilância com o efeito de colocar o cidadão/consumidor como um simples expectador das suas informações (Bioni, 2019).

Além disso, cresce cada vez a aquisição de fontes preditivas de superávit comportamental como personalidades, nossas vozes e emoções com essa nova dinâmica de mercado. "Os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos provêm da intervenção no jogo de modo a incentivar, persuadir, sintonizar e arrebanhar comportamento em busca de resultados lucrativos" (Zuboff, 2021, p. 23).

> O desenvolvimento da economia baseada em dados (*data driven economy*), a hiperconectividade imanente à Internet das Coisas (*IoT*) e a estruturação do Estado de Vigilância potencializaram a tensão existente entre os valores segurança e privacidade. Ainda que o legislador faça a mediação desses interesses para sobrepor um ao outro em determinadas hipóteses, estima-se que considere, nessa tarefa, a unidade dos valores constitucionais e a importância do princípio da dignidade da pessoa humana para que a solução tenha validade material e formal. Sob essa expectativa, o estado de vigilância não poderá, em defesa da segurança, solapar a privacidade das pessoas sob pena de atacar-lhes frontalmente a dignidade (Menezes; Colaço, 2019, p. 88).

A *data driven economy* é caracterizada pela economia da *Internet of Things* (IoT) - tradução livre em português de Internet das Coisas - onde a conexão inteligente de produtos e serviços é movida pelo tratamento dos dados pessoais dos consumidores. Estabelece-se nesse contexto uma troca entre os serviços e produtos personalizados e os dados oferecidos (Morey; Krajecki, 2016).

Na economia baseada em dados, os capitalistas de vigilância coletam uma infinidade de dados pessoais dos cidadãos para fornecer bens e serviços com o objetivo de obter lucro. No entanto, o tratamento desses dados ocorre de forma indiscriminada, resultando em inúmeras violações da privacidade e personalidade dos indivíduos. Ademais, as "sociedades civilizadas

compreenderam que a proteção da privacidade é indissociável da dignidade humana, de modo que qualquer ação que afete a intimidade do cidadão também constitui um atentado à experiência humana de uma vida digna" (Vainzof, 2019, p. 25).

A dignidade da pessoa humana, além de ser um princípio, constitui uma cláusula geral capaz de englobar diversas formas de proteção e promoção do indivíduo. Por isso, é natural que surjam novas formas de manifestação da dignidade, especialmente quando visam combater novos mecanismos de instrumentalização ou subjugação da pessoa e promover meios para seu livre desenvolvimento (Konder (2019).

Em consonância, Doneda (2019, p. 93) afirma que a privacidade desempenha um papel preponderante na proteção da pessoa humana, sendo um "fio condutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de forma geral. Nesse papel, ela é um pressuposto de uma sociedade democrática moderna."

Nesta senda “a dignidade da pessoa humana [...] se renova, para, por meio de novas manifestações, proteger [...] a liberdade de pessoa humana para ser quem ela é, para livremente construir sua própria personalidade” (Konder, 2019, p. 261). Assim, garantir o direito à privacidade e à proteção de dados pessoais é mais um passo para perseguir a garantia plena da dignidade da pessoa humana como um direito fundamental.

Vainzof (2019) reforça que proteger dados relacionados a uma pessoa, significa resguardar a própria personalidade do indivíduo. Isso se dá porque a personalidade é composta pelas características que distinguem cada pessoa, e o Direito busca proteger todos os atributos, tanto materiais quanto imateriais, que constituem a projeção da pessoa humana contra eventuais violações.

2.2.1 Direito à privacidade e proteção de dados pessoais

No Brasil, o direito à privacidade é considerado um direito fundamental, previsto na Constituição Federal de 1988, que, em seu artigo 5º, incluiu, entre as garantias e direitos fundamentais, a proteção da intimidade e da vida privada (inciso X) e, recentemente, a proteção de dados pessoais (inciso LXXIX). Esse último foi inserido por meio da Emenda Constitucional (EC) 115/2022, com a seguinte redação: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 1988; 2022). Tal inclusão reforça, de maneira ainda mais clara, que esses aspectos estão abrangidos pela proteção da dignidade da pessoa humana (Brasil, 1988).

É relevante destacar que o conceito original de privacidade se referia à ausência de interferência do Estado na vida dos cidadãos. Com o tempo, esse conceito evoluiu para uma visão mais ampla, passando a ser entendido como um direito abrangente que envolve a prerrogativa de não ser alvo de intromissões, independentemente da forma ou de quem seja o agente envolvido (Maldonado, 2019).

Doneda (2019), por sua vez, ensina que o conceito de privacidade está relacionado a diversas necessidades, como a busca por igualdade, liberdade de escolha e o desejo de não ser discriminado, entre outras. Além disso, a privacidade possui uma forte conexão com a personalidade e seu desenvolvimento, sendo um elemento essencial nesse processo, inserido em uma complexa rede de relações que o Direito ainda precisa compreender plenamente.

O conceito de privacidade evoluiu ao longo do tempo, abrangendo atualmente a proteção dos dados pessoais. "Assim, pode-se dizer que a proteção dos dados pessoais é uma das facetas do conceito mais amplo de privacidade, que surgiu e se desenvolveu em decorrência do avanço tecnológico nas últimas décadas" (Maldonado, 2019, p. 243).

Já o termo dados pessoal, trata-se de informações relacionadas a pessoa natural identificada ou identificável tais como: nome, endereço, endereço eletrônico, idade, estado civil de indivíduos e diversas outras possibilidades de informações (Finkelstein; Finkelstein, 2020, p. 296).

A personalidade refere-se ao conjunto de características que diferencia uma pessoa da outra, como o nome, a honra, a integridade física e psíquica, entre outros atributos que compõem essa extensão. Nessa perspectiva, qualquer dado relacionado a uma pessoa pode ser considerado um direito da personalidade. Assim, ele deve ser qualificado como pessoal, sendo uma projeção, extensão ou dimensão de seu titular (Bioni, 2019, p. 98).

O direito à proteção dos dados pessoais, inicialmente concebido como um meio de defesa contra o Estado, expandiu-se para abranger todos os âmbitos, tanto públicos quanto privados. Os dados pessoais representam uma extensão direta da personalidade, de modo que qualquer tratamento desses dados pode impactar a forma como a pessoa é vista pela sociedade. Isso, por sua vez, pode afetar sua personalidade e, consequentemente, violar seus direitos fundamentais (Guedes; Meireles, 2019, p. 118).

De acordo com Cancelier (2017, p. 228), "o direito à privacidade, em qualquer manifestação, valoriza a liberdade, combate a discriminação e protege as escolhas pessoais de cada indivíduo. Respeitar a privacidade é um exercício essencial de cidadania".

No entanto, para a prestação de bens ou serviços, tanto pelo setor público quanto pelo privado, é imprescindível a coleta, processamento e armazenamento de dados pessoais. Embora

o uso de dados pessoais não seja problemático por si só e permita diversas atividades, desde a administração até a pesquisa de mercado e ações humanitárias, é necessário que o tratamento desses dados seja feito de maneira que respeite os parâmetros de proteção dos direitos fundamentais. É fundamental que haja instrumentos regulatórios que garantam aos cidadãos um controle efetivo sobre seus dados pessoais, assegurando o acesso, a veracidade, a segurança, a finalidade de uso e outras garantias essenciais (Doneda, 2019).

A proteção de dados pessoais ocupa um lugar singular, pois além de ser uma legislação preocupada com a dignidade das pessoas é também regulação econômica orientada aos negócios. Em outras palavras, busca o equilíbrio nas disparidades de poder (Bioni; Zanatta (2021).

Frazão (2019) observa que o problema surge na coleta e processamento de dados pessoais, que frequentemente ocorrem sem a autorização ou mesmo o conhecimento dos indivíduos. "Se os cidadãos não conseguem nem mesmo saber quais dados estão sendo coletados, enfrentam ainda maiores dificuldades para entender as diversas finalidades para as quais esses dados podem ser usados e a extensão do impacto em suas vidas" (p. 10).

Além dos problemas relacionados ao (ab)uso no tratamento, há também os furtos e os vazamentos constantes de dados pessoais causados, seja por falha de segurança da informação, seja pelas inadequações no trato dos dados tanto no âmbito do poder público, quanto privado. Daí a necessidade de avançar do direito à privacidade ao direito à proteção de dados pessoais. Importante mencionar que, normalmente, há uma confusão no entendimento do que é privacidade e proteção de dados, admitindo os dois termos como sinônimos. Acontece que estes dois fundamentos caminham juntos e são complementares, ou seja, a proteção de dados é um meio para garantir a privacidade aos titulares de dados pessoais (Micheletti; Borges; Costa, 2022).

Em se tratando da relação entre o direito à privacidade e o direito à proteção dados pessoais, tem-se que,

> o direito à proteção de dados pessoais, em princípio fortemente vinculado ao direito à privacidade, hoje se sofisticou e assumiu características próprias. Na proteção de dados pessoais não é somente a privacidade que se pretende tutelar, porém busca-se a efetiva tutela da pessoa em vista de variadas formas de controle e contra a discriminação, com o fim de garantir a integridade de aspectos fundamentais de sua própria liberdade pessoal. E, ainda, não é mais somente o indivíduo a ser o único afetado[..], porém inteiras classes e grupos sociais (Doneda, 2020, p. 26).

Nesse contexto, ressalta-se a importância dos direitos à privacidade e proteção de dados pessoais estarem elencados no rol de direitos e garantias fundamentais estabelecidas no artigo

5º da CF. Esses direitos e garantias são formas de promover a dignidade humana e de proteger os cidadãos. Assim o direito à privacidade e à proteção de dados pessoais é essencial à vida digna das pessoas, principalmente nesse contexto de total inserção na vida digital (Brasil, 2022).

Apesar da inclusão do direito à privacidade e à proteção de dados na Constituição Federal como direito fundamental, é importante ressaltar que, para garantir a efetividade desse direito, é necessário fortalecer ou criar políticas públicas que abordem essas questões. Além da Constituição, existem leis setoriais e uma legislação específica recentemente aprovada. As leis setoriais são normativas esparsas no ordenamento jurídico brasileiro, abordando, de maneira pontual, aspectos relacionados à privacidade, intimidade, personalidade e, especialmente, à proteção de dados pessoais. Esse conjunto legal é constituído por diversas leis, conforme demonstrado no quadro a seguir.

Quadro 2. Ordenamento jurídico brasileiro de proteção de dados pessoais

Constituição Federal	**Objetivo**	**Quanto à Privacidade e Proteção de dados pessoais**
Art. 5º	Direitos e Garantias Fundamentais	Os incisos X e LXXIX asseguram à privacidade e proteção de dados como direitos e garantias fundamentais (Brasil, 1988).
Legislação infraconstitucional	**Objetivo**	**Quanto à Privacidade e Proteção de dados pessoais**
Código de Defesa do Consumidor - Lei nº 8.078/1990	Dispõe sobre a proteção do consumidor e dá outras providências	Os artigos 43 e 44, estabelecem uma série de direitos e garantias para o consumidor em relação aos dados pessoais presentes em bancos de dados e cadastros (Doneda, 2019).
Habeas Data - Lei nº 9.507/1997	Regula o direito de acesso a informações e disciplina o rito processual do habeas data.	Garante o conhecimento, retificação e esclarecimento sobre dado ou informação do impetrante constante em banco de dados público (Oliveira; Lopes, 2019).
Código Civil - Lei nº 10.406/2002	Institui o Código Civil	A proteção conferida decorre dos artigoss. 12 e 21, isto é, da proteção da vida privada e da pretensão imediata de fazer cessar ameaça ou lesão a este direito (Oliveira; Lopes, 2019).
Lei do Cadastro Positivo - Lei nº 12.414/2011	Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.	A lei estabelece maior rigor quanto a finalidade da coleta e uso dos dados pessoais, principalmente os dados sensíveis, além de reconhecer o direito do cadastrado solicitar uma revisão de decisão baseada exclusivamente em dados automatizados (Oliveira; Lopes, 2019).
Lei de Acesso à Informação - Lei nº 12.527/2011	Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.	O artigo 6º (III) e 31 contêm comandos que impõe proteção da informação no tratamento de dados pessoais, a transparência frente ao seu titular, bem como o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como s liberdade e às garantias individuais (Matos; Ruzyk, 2019).

Lei Carolina Dieckmann - Lei nº 12.737/2012	Dispõe sobre a tipificação criminal de delitos informáticos.	Incluiu o artigo 154-A no Código Penal, definindo o crime de invasão de dispositivo informático que consiste na intrusão desautorizada em dispositivos móveis (smartphones, computadores, notebooks, tablets) do titular (Menezes; Colaço, 2019).
Marco Civil da Internet - Lei nº 12.965/2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.	Os artigos 3º (III) e 11 estabelecem um conjunto de direitos de proteção à privacidade e proteção de dados pessoais ao usuário na internet (Oliveira; Lopes, 2019).
Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018	Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais.	É uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o cumprimento das garantias de privacidade e proteção de dados (Pinheiro, 2018).

Fonte: Elaborado pelo autor com base em Brasil (1988), Pinheiro (2018), Doneda (2019), Oliveira; Lopes (2019), Menezes; Colaço (2018) e Matos; Ruzyk (2019).

Portanto, resumidamente, "a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém, não limitada por esta, faz referência a um gama extensa de garantias fundamentais respaldas no ordenamento jurídico brasileiro" (Doneda, 2019). Por fim, para reforçar esse arcabouço jurídico, recentemente, foi aprovada uma lei específica que desponta como o mais importante regulamento de proteção de dados pessoais. Tara-se da Lei Geral de Proteção de Dados Pessoais (LGPD) que será, brevemente, apresentada na próxima seção.

2.2.2 LGPD - Lei Geral de Proteção de Dados Pessoais

Marcada pela participação democrática, pela transparência no processo de negociações entre os diversos atores envolvidos, inclusive, antagônicos, "a LGPD se caracteriza por um processo multiparticipativo e particularmente bem-sucedido na extração de 'consensos pragmáticos' que impulsionaram sua construção, articulação e aprovação" (Bioni, Rielli, 2021, p.15).

Promulgada em 14 de agosto de 2018, a Lei de n. 13.709/2018, tem sua concepção fundamentada na evolução dos direitos humanos. Porém, o regulamento de proteção de dados europeu (GDPR) é sua principal fonte de inspiração. O objetivo deste diploma legal é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (titular dos dados) por meio de regras no tratamento de dados pessoais realizado por pessoa natural, ou jurídica de direito público ou privado tanto nos meios físicos quantos nos digitais (Brasil, 2022).

Nesse aspecto,

> o titular dos dados pessoais é o núcleo da existência de uma Lei Geral de Proteção de Dados Pessoais, afinal, a preocupação sobre eventuais violações aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade está umbilicalmente vinculada à pessoa natural (Vainzof, 2019, p. 95).

Conforme, o artigo 17 da LGPD "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (Brasil, 2018). O normativo "busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais" (Vainzof, 2019, p. 25). Em outras palavras, além da busca de garantia de direitos fundamentais do cidadão, busca-se também uma segurança jurídica que é fundamental para o desenvolvimento econômico do País.

Portanto, a indigitada Lei se consolida como a principal política pública de proteção de dados pessoais no Brasil. Para isso, os legisladores a arquitetaram dividindo-a em 10 capítulos conforme se observa no quadro a seguir.

Quadro 3. Estrutura da LGPD

Capítulos	**Seções**	**Artigos**
I - Disposições Preliminares	-	1º a 6º
II - Do Tratamento de Dados Pessoais	I - dos requisitos para o tratamento de dados pessoais	7ª a 10
	II - do tratamento de dados pessoais sensíveis	11 a 13
	III - do tratamento de dados pessoais de crianças e de adolescentes	14
	IV - do término do tratamento de dados	15 a 16
III - Dos Direitos do Titular	-	17 a 22
IV - Do Tratamento de Dados Pessoais pelo Poder Público	I - das regras	23 a 30
	II - da responsabilidade	31 a 32
V - Da Transferência Internacional de Dados	-	33 a 36
VI - Dos Agentes de Tratamento de Dados Pessoais	I - do controlador e do operador	37 a 40
	II - do encarregado pelo tratamento de dados pessoais	41
	III - da responsabilidade e do ressarcimento de danos	42 a 45
VII - Da Segurança e das Boas Práticas	I - da segurança e do sigilo de dados	46 a 49
	II - das boas práticas e da governança	50 a 51

VIII - Da Fiscalização	I - das sanções administrativas	52 a 54
IX - Da Autoridade Nacional de proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	I - da Autoridade Nacional de Proteção de Dados (ANPD)	55-A a 55-L
	II - do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	58-A, 58-B e 59
X - Disposições Finais e Transitórias	-	60 a 65

Fonte: Elaborado pelo autor com base em Brasil (2018).

Estão sujeitas à LGPD, a pessoa natural e todas as organizações, seja do poder público, seja do setor privado que realize tratamento de dados pessoais, por meio físico ou digital, em suas atividades (Micheletti; Borges; Costa, 2022).

Conforme os artigos 1º e 3º da Lei.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (Brasil, 2018).

Não importa o objetivo das organizações (com fins lucrativos ou filantrópicos), todas devem cumprir a LGPD quando realizarem tratamento de dados pessoais, a não ser que se enquadre em alguma exceção (Vainzof, 2019). Nesse último aspecto, cabe elencar as situações de tratamento de dados pessoais em que a Lei não aplica.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Além do escopo apresentado no quadro anterior, a Lei se sustenta em cinco eixos principais, sete fundamentos e dez princípios como se pode ver no quadro a seguir.

Quadro 4. Eixos, fundamentos e princípios da LGPD

Eixos	Fundamentos (art. 2º)	Princípios (art. 6º)
I - unidade e generalidade da aplicação da lei; II - legitimação para o tratamento de dados (hipóteses autorizativas); III - princípios e direitos do titular; IV - obrigações dos agentes de tratamento de dados; V - responsabilização dos agentes.	I - o respeito à privacidade; II - a autodeterminação informativa; II - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	I - a finalidade; II - a adequação; III - a necessidade, IV - o livre acesso; V - a qualidade dos dados, quanto a exatidão, clareza, relevância e atualização; VI - a transparência; VII - a segurança; VIII a prevenção; IX - a não discriminação e; X - a responsabilização e a prestação de contas.

Fonte: Elaborado pelo autor com base em Basan (2021) e Brasil (2018).

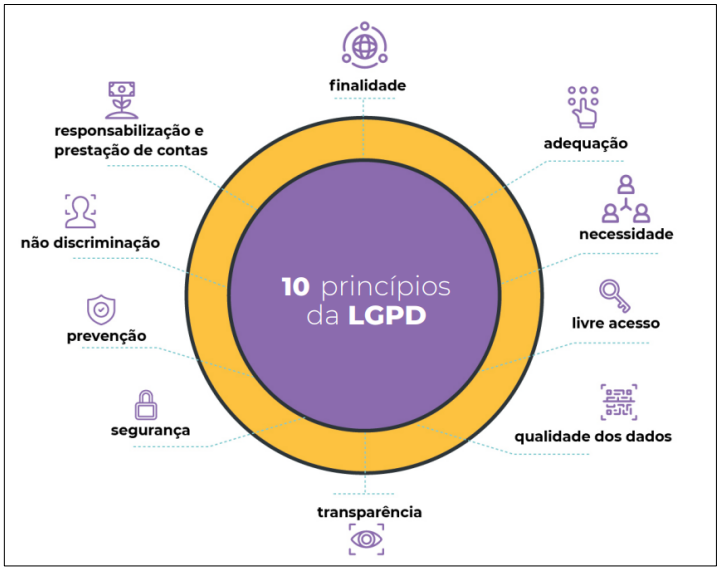
No cerne dessa legislação, os dez princípios fundamentais orientam e estruturam todas as atividades de tratamento de dados pessoais. Esses princípios constituem a espinha dorsal da LGPD, oferecendo diretrizes que devem ser seguidas por todas as organizações que lidam com dados pessoais (Davoli, Oliveira, Silva, 2020).

Esses princípios são essenciais para garantir que o tratamento de dados pessoais seja realizado de forma ética e responsável, assegurando a privacidade e a segurança dos titulares dos dados.

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

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

Figura 1. Princípios da LGPD



Fonte: Davoli, Oliveira, Silva, 2020.

Para a compressão dos limites nas atividades das organizações em relação aos dados pessoais sob sua tutela, faz-se necessária a definição de tratamento de dados. “O termo tratamento, utilizado pela legislação é referente a toda operação realizada com dados pessoais, como as que se referem a coleta, transmissão, arquivamento de informações e entre outras.

Basicamente denota toda operação que pode ser feita ao adquirir, manter ou transmitir dados pessoais" (Finkelstein; Finkelstein, 2020, p. 296).

> a definição de tratamento de dados pessoais, na LGPD, é extremamente abrangente, pois parte da coleta e finda em sua eliminação, englobando todas as possibilidades de manuseio dos dados, independentemente do meio utilizado. Assim, o mero ato de receber, acessar, arquivar ou armazenar dados pessoais está contido dentro do conceito de tratamento (Maldonado, 2019, p. 108).

O tratamento de dados pessoais engloba qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018; Maldonado, 2019; Lima, 2019).

Nesse sentido, quando houver ocorrência de tratamento de dados pessoais, é obrigatório o enquadramento, bem como a indicação expressa de uma hipótese de tratamento (base legal), somente assim o tratamento dos dados pessoais será legitimo. Ressalta-se que a LGPD estabeleceu um rol com dez hipóteses de tratamento – bases legais - (expressamente descritas no artigo 7º). Portanto, não existe nenhuma outra hipótese, além dessas. Ainda, é importante destacar que "basta o atendimento de uma das dez bases para o tratamento ser considerado legítimo (sendo possível cumular bases legais), cabendo realçar que todas as demais bases legais mencionadas nos incisos II a X são independentes do consentimento" (Lima, 2019, p. 201).

Ao apresentar um rol de bases legais – condições que autorizam o tratamento de dados pessoais – que não se limitam ao consentimento do titular, reconhece-se que tanto entidades públicas quanto privadas precisam processar informações pessoais. Esse fluxo de dados nem sempre deve depender da vontade do titular. Uma das bases legais estabelece que entidades públicas e privadas devem tratar dados pessoais para cumprir uma obrigação legal ou regulatória, conforme previsto no art. 7º, II, da LGPD (Bioni; Silva; Martins, 2022).

Assim, seguem descritas as hipóteses de tratamento (bases legais) para fins da LGPD:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018).

Tratar os dados pessoais dentre umas das hipóteses é uma forma de mitigar os riscos e dar efetividade aos fundamentos e princípios da LGPD. Assim, o "tratamento de dados pessoais será irregular quando deixar de observar qualquer hipótese nela prevista, ou quando não fornecer a segurança que o titular dele pode esperar" (Vainzof, 2019, p 36).

É importante ressaltar que a Lei define dados pessoais como informações que se referem a uma pessoa natural identificada ou identificável (Brasil, 2018). Por outro lado, dados pessoais sensíveis são aqueles que, em geral, podem causar algum tipo de discriminação quando processados, como informações sobre origem racial, convicções religiosas, opiniões políticas, dados de saúde, entre outros exemplos. Além disso, dados genéticos e biométricos, devido à sua natureza crítica, também se enquadram como dados pessoais sensíveis. Esses dados podem representar riscos e vulnerabilidades mais significativas para os direitos e liberdades fundamentais dos titulares (Vainzof, 2019, p. 85).

É relevante destacar também que, de acordo com a Lei, dados anonimizados não são classificados como dados pessoais, a menos que seja possível identificar o titular desses dados. A legislação trata de dados referentes a indivíduos cuja identidade não pode ser determinada, considerando os meios técnicos razoáveis e disponíveis no momento do processamento. Portanto, dados cuja autoria seja não apenas indeterminada, mas também impossível de ser determinada, não são protegidos por essa legislação (Vainzof, 2019).

Conforme o expresso no artigo 5ª, inciso III, o dado anonimizado é "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Portanto, a anonimização de dados pessoais é uma técnica utilizada para impossibilitar a identificação do indivíduo em relação aos seus dados.

Outro aspecto importante que merece ser destacado, diz respeito as figuras/atores, presentes na legislação. Assim, embora o titular de dados seja o protagonista, há outros atores

a saber: controlador, operador, encarregado e ANPD. O controlador e operador são considerados agentes de tratamento. As definições desses dois agentes de tratamento encontram-se amparadas no capítulo I, artigo 5º da Lei. Assim, define-se o controlador como "pessoa natural ou jurídica de direito público ou privado a quem competem as decisões referentes ao tratamento de dados pessoais". já o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Brasil, 2018).

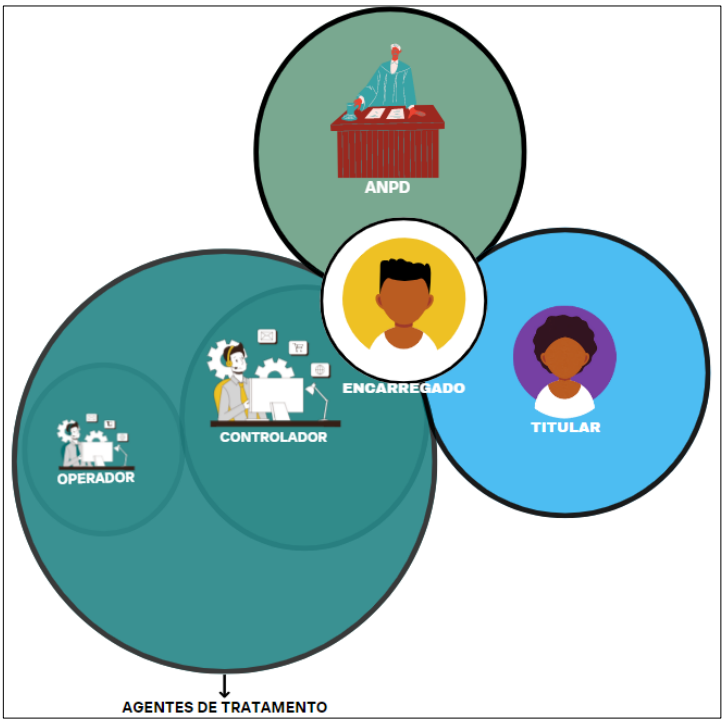
Contudo, ressalta-se que

> os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento. No contexto de uma pessoa jurídica, a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos. Mas, além disso, o agente de tratamento é definido para cada operação de tratamento de dados pessoais, portanto, a mesma organização poderá ser controladora e operadora, de acordo com sua atuação em diferentes operações de tratamento (Brasil, 2022, p.7)

O encarregado de dados é definido como pessoa física ou empresa indicada pelo controlador e operador para ser o canal entre o titular de dados e os agentes de tratamento, bem como entre esses agentes e a Autoridade Nacional de Proteção de Dados (ANPD). O encarregado poderá ser funcionário ou servidor do próprio quadro funcional da organização, bem como uma empresa contratada para exercer a função. A Regra geral é que toda organização (exceto empresas de pequeno porte) deve indicar uma pessoa para esse papel. Portanto, o encarregado não é considerado um agente de tratamento.

Já a ANPD é um órgão que tem atuação similar à de uma agência reguladora. Trata-se de uma autarquia com autonomia técnica e decisória, sendo responsável por zelar pela proteção dos dados pessoais, e por orientar, regulamentar e fiscalizar o cumprimento da legislação. É, portanto, responsável pela interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação (Brasil, 2018; 2022). Veja na figura os atores a seguir.

Figura 2. Atores da LGPD



Fonte: Elaborado pelo autor com base em Brasil (2018).

Os direitos do titular de dados pessoais estão preceituados no capítulo III, artigos 17 e 18. Em razão disso, os titulares poderão realizar uma série de requisições ao controlador em relação aos seus dados tratados por ele. As atividades dos agentes de tratamento e do encarregado estão descritas na seção I e II do capítulo VI respectivamente. Já as principais atividades da ANPD estão descritas na seção I do capítulo IX (Brasil, 2018).

Retornando ao assunto do encarregado, o artigo 41 da LGPD estabelece que a sua indicação é uma obrigação do controlador. “O controlador deverá indicar encarregado pelo tratamento de dados pessoais” (Brasil, 2018). No entanto, a Lei não especifica critérios objetivos sobre o conhecimento e o perfil do encarregado. Recomenda-se, portanto, que não haja conflito de interesses e que o controlador preste atenção ao nível de conhecimento desse colaborador (Micheletti; Borges; Costa, 2022).

Ainda, o colaborador indicado como encarregado deve ter amplos conhecimentos técnicos e jurídicos acerca dos temas de privacidade e segurança da informação para auxiliar o controlador, incluindo também entre as suas funções:

> a) atendimento às demandas dos titulares;
> b) o assessoramento na emissão do relatório de impacto à proteção de dados pessoais (RIPD);
> c) a elaboração de opiniões e pareceres técnicos acerca da proteção de dados pessoais pela entidade;

> d) o monitoramento da conformidade das atividades de tratamento de acordo com as legislações e regulamentações aplicáveis; e
> e) a recomendação de elaboração de relatórios de impacto à proteção de dados pessoais (RIPD) sempre que necessário (Micheletti; Borges; Costa, 2022, p. 79).

Importante frisar que o tratamento inadequado de dados pessoais, seja por condutas dolosas, negligentes, imprudentes ou incompetentes, pode expor a intimidade dos titulares e afetar diretamente sua honra e imagem. Isso ocorre, por exemplo, na exposição de dados financeiros, informações sobre doenças, orientação sexual, ou no acesso indevido a mensagens. Dados biométricos, logins e senhas, quando sob a responsabilidade dos agentes de tratamento, se vazados, podem permitir que terceiros não autorizados acessem diversas informações íntimas e privadas dos titulares, como fotos, vídeos, textos, áudios e prontuários médicos, entre outros exemplos (Vainzof, 2019).

Ocorrendo tais situações, resta claro que o agente de tratamento incorre em incidentes de segurança. À luz da LGPD (art. 46), o termo incidente de segurança pode ser definido como:

> violação das medidas adotadas pelos agentes de tratamento para salvaguardar a integridade e o sigilo dos dados pessoais sob sua administração, resultando em acessos não autorizados e em situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Souza, 2019, p. 251)

Sem dúvida, a violação de dados pessoais é uma situação bastante crítica, uma vez que, de forma permanente, põe em risco os direitos dos titulares. Além disso, é muito provável que essa situação venha a manchar a reputação do controlador e do operador, que de alguma forma, falharam na sua obrigação de proteção dos dados que lhes foram confiados. “Nessas ocasiões, os agentes também ficam expostos, com maior evidência, às possíveis sanções administrativas e responsabilizações civis. Ou seja, os efeitos são contundentes e prejudiciais a todos, titulares e agentes do tratamento” (Vainzof, 2019, p. 142).

Nessa toada, “a proteção adequada dos dados pessoais não é uma faculdade dos agentes de tratamento. Trata-se, na verdade, de uma imposição legal cujo descumprimento enseja a aplicação de sanções administrativas e eventual responsabilização civil” (Souza, 2019, p. 241).

Nesse diapasão, Vainzof (2019, p. 155) enfatiza que o controlador ou o operador que deixar de adotar as medidas de segurança previstas e adequadas devem respondem pelos danos decorrentes da violação da segurança dos dados. “Ambos, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”

De acordo com o autor supracitado, além de sanção pecuniária, poderá ser aplicado sanções como advertência, com indicação de prazo para adoção de medidas corretivas; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e eliminação dos dados pessoais a que se refere a infração.

No contexto da Administração Pública, esses desafios são ampliados pelo grande volume de dados pessoais geridos em diversas e dispersas atividades. Além disso, o interesse público, que é um objetivo essencial de toda atuação administrativa, influencia as discussões sobre o tratamento de dados pessoais, estando associado a outros princípios, como o da transparência (Brasil, 2021).

Ressalta-se, por fim, que antes de divulgar dados pessoais, o poder público precisa ponderar dois direitos fundamentais: o direito à privacidade e à proteção de dados pessoais, e o direito do público em geral de estar informado sobre as atividades do poder público. Nesse contexto, o próximo tópico irá apresentar os principais aspectos relacionados a LGPD, LAI e Política de Dados Abertos no tratamento de dados pessoais pelo Poder Público.

2.2.3 A relação entre LGPD, LAI e a Política de Dados Abertos no tratamento de dados pessoais pelo Poder Público

As leis LGPD, LAI e a Política de Dados Abertos (instituída pelo Decreto nª 8.777 de maio de 2016) são conflitantes ou convergentes? É sabido que existem algumas falhas na compreensão de alguns órgãos do poder público em divulgar determinadas informações. O problema ocorre, principalmente, quando os agentes públicos restringem os acessos às informações, classificando-as de forma equivocada como sigilosas ou em conflito com a LGPD. Com vistas a esclarecer essa incompreensão, faz-se necessário contextualizar a relação entre a LGPD, LAI e da Política de Dados Abertos.

Em se tratando de LGPD e LAI, muitas vezes, os agentes públicos não promovem a divulgação de informações baseando-se na LGPD de forma equivocada. A LGPD não fala de sigilo. Porém, essa confusão não se limita aos agentes públicos, pois “paira sobre os cidadãos, gestores públicos, jornalistas e pesquisadores” (Piza; Assis, 2022).

Entretanto, em teoria, não há incompatibilidade entre essas leis: uma assegura a publicidade de informações públicas, e a outra protege os direitos fundamentais do cidadão relacionados aos seus dados pessoais. Tanto a liberdade de informação quanto o exercício da cidadania são fundamentos da LGPD. Entretanto, a LGPD tem se transformado em um escudo

argumentativo para impedir o acesso a informações de natureza pública (Arcoverde; Ramos; Zanatta, 2021).

Na verdade, a LAI é quem trata sobre os requisitos de sigilo, enquanto a LGPD apenas complementa a LAI com parâmetros e princípios que devem observados para a divulgação (observância dos direitos, a segurança e a proteção da privacidade). Essas legislações devem ser observadas em conjunto. Então não há de se falar que a LGPD trouxe grau de sigilo para as informações pessoais, pelo contrário, ela trouxe uma proteção (caráter protetivo). E isso é importante na análise (LGPD, 2022).

Figura 3. LGPD x LAI

Fonte: Data Privacy Brasil, 2023.

Portanto, a aplicação incorreta da Lei Geral de Proteção de Dados Pessoais não pode ser usada como justificativa para enfraquecer a Lei de Acesso à Informação e comprometer a transparência pública. As duas leis integram o ordenamento jurídico brasileiro e devem ser aplicadas de forma conjunta e coerente pelos agentes públicos. A interpretação da LGPD deve estar alinhada com seus princípios fundamentais, em vez de ser baseada em artigos isolados que servem para ocultar informações de interesse público. Isso exigirá um esforço cívico e a vigilância contínua da comunidade jurídica e política no Brasil (Arcoverde; Ramos; Zanatta, 2021).

Cabe mencionar ainda que a Administração Pública percorre quatro deveres a respeito das informações públicas: “o dever de abertura, o dever de transparência, o dever proteção e o dever de regulação, os quais podem ser, na teoria, objeto de estudos diferentes, mas, operacionalmente, devem ser analisados como um ciclo único e interligado” (Cristóvam; Hahn, 2020, p. 3). A LAI e a Política de Dados Abertos se encarregam, fundamentalmente, da

transparência e da abertura dos dados respectivamente, enquanto a LGPD; da proteção e regulação no tratamento de dados pessoais.

Além diso, o livre acesso à informação pública é essencial para o efetivo funcionamento das democracias, pois possibilita aos cidadãos o acompanhamento de políticas públicas e um efetivo controle social, ou seja, o objetivo do direito de acesso à informação pública está imbricado à fiscalização do poder público e a materialização do princípio da publicidade e transparência. Assim, o direito de acesso à informação deve seguir as seguintes premissas: máxima divulgação, acesso facilitado e sem custos para os cidadãos e limitação das exceções ao acesso à informação (Bioni; Silva; Martins, 2022).

A obrigatoriedade imposta ao poder público em dar transparência às informações, está prevista no artigo 5º da Constituição Federal, que dispõe sobre os direitos e garantias fundamentais individuais e coletivos.

> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (Brasil, 1988)

As informações devem ser divulgadas mesmo que não haja solicitação. Assim, qualquer pessoa pode solicitar e receber dos órgãos públicos informações produzidas por eles ou sob sua tutela, com base no princípio da publicidade da Administração Pública (Bioni; Silva; Martins, 2022). Tal princípio está previsto no artigo 37, também da CF:

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência (Brasil, 1988).

Importante mencionar a diferença entre os termos **publicidade** e **transparência** para melhor entendimento. A transparência se preocupa não somente em deixar a informação pública, mas também acessível e inteligível para os cidadãos (Brasil, 2022). Numa análise mais aprofundada,

> os arts. 5º, XXXIII, e 37, § 3º, II, da CF, concretizam o princípio da publicidade administrativa, previsto no art. 37, caput, da CF. A partir do qual a LAI visa assegurar a transparência. Deste modo, o poder público tem de conferir ampla publicidade aos seus atos. A publicidade é a regra e o sigilo a exceção. Neste contexto, a transparência que não vem explícita na CF podendo ser extraída do princípio da publicidade (art. 37, caput, CF), do princípio democrático insculpido já no art. 1º da CF e do direito à informação (art. 5º, XXXIII, CF). Daí pode-se concluir que a publicidade é o gênero

> (previsão do princípio em sede constitucional) do qual a transparência é espécie (prevista em leis infraconstitucionais) (Limberger, 2022, p. 121).

Na prática, os princípios da transparência e publicidade se manifestam de diversas maneiras na Administração pública. As principais formas de transparência são: transparência ativa; transparência passiva; transparência orçamentária-financeira; transparência dirigida ou direcionada *(targeted transparency*); perguntas frequentes (FAQ - *Frequently Asked Questions*); transparência de processos; dados abertos (Brasil, 2022).

O direito de acesso à informação previsto Constituição Federal de 1998, passou a ser regulado apenas em 2011, com a edição da LAI, que teve inspiração da *Open Government Partnership* (OGP), em português, Parceria para Governo Aberto. a LAI tornou-se o regulamento pioneiro em acesso à informação no mundo ao incorporar à dimensão da transparência e o paradigma dos dados abertos (Possamai; Souza, 2020).

A Parceria para Governo Aberto é baseada na ideia de que um governo aberto é mais acessível, mais responsivo, mais transparente e responsável para seus cidadãos, e que melhorar a relação entre pessoas e seus governos traz benefícios de longo prazo para todos (Brasil, 2022).

A LAI, LGPD e Política de Dados Abertos são, portanto, normativos que regulamentam direitos fundamentais estabelecidos pela Constituição Federal. A primeira visa garantir a transparência e publicidade, a segunda; a privacidade e a proteção dos dados pessoais. Já a terceira é basicamente uma forma de transparência ativa em que o Estado fornece dados em formato digital aberto e livre, que podem ser acessados por softwares não proprietários e usados sem restrições jurídicas (Brasil, 2022).

A Administração Pública deve ser aberta e transparente em relação aos seus dados, informações e conhecimentos, a fim de garantir o controle de sua eficiência e legalidade. No entanto, é importante que essa transparência não vá além dos limites da privacidade do cidadão, expondo seus dados pessoais, que são acessados em razão da prestação de serviços públicos e análise de deveres civis. Encontrar um equilíbrio sensível, dinâmico e complexo entre esses dois aspectos é crucial (Cristóvam; Hahn, 2020).

Os autores supracitados defendem o ideal de Governo Aberto, que promova a transparência e a publicidade das informações públicas (preceitos da LAI e da Política de Dados Abertos) ao mesmo que defende a privacidade e proteção dos dados pessoais (preceitos da LGPD). Ambos, direitos fundamentais.

A Organização para Cooperação e Desenvolvimento Econômico (OCDE) caracteriza Governo Aberto como uma abordagem de governança que incentiva os princípios de transparência, integridade, responsabilidade e participação das partes interessadas, visando

apoiar a democracia e promover um crescimento inclusivo (OCDE, 2017). Implementar a cultura de Governo Aberto poder potencializar a melhoraria de políticas e serviços públicos, ampliar a confiança da população no governo, gerar soluções inovadoras e aumentar a capacidade de implementar ações (Brasil, 2022).

A combinação das normas, aqui tratadas, alinhada as análises de diversos autores possibilita a distinção dos conceitos de informação, dados abertos e informação/dado pessoal. Informação é "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato" (Brasil, 2011, art. 3º, I).

Dados Abertos são:

> dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte (Brasil, 2016, art. 2ª, III).

Para a Open Knowledge Foundation (2019) apud Cristóvam e Hahn (2020, p. 3) os "dados são abertos quando qualquer pessoa pode livremente usá-los, reutilizá-los e redistribuí-los, estando sujeito a, no máximo, a exigência de creditar a sua autoria e compartilhar pelas mesmas regras". Importe mencionar que a LAI compreende os dados abertos pela expressão informações públicas. Os dados tratados e disponibilizados pelo poder público são considerados dados abertos governamentais.

Os dados abertos governamentais são bases de dados públicos que são proativamente disponibilizados para serem reutilizados pela sociedade, sem ônus financeiro (necessidade de comprar software para usar os dados), com compatibilidade de leitura de máquinas (robôs, inteligências artificiais, aplicativos e outras soluções acessem diretamente o dado) e barreiras legais (licenças de uso) (Brasil, 2022).

Já a informação pessoal é "aquela relacionada à pessoa natural identificada ou identificável" - redação da LAI - (Brasil, 2011, art. 4º, IV). Dado pessoal é "informação relacionada a pessoa natural identificada ou identificável" - redação da LGPD - (Brasil, 2018, art. 5º, I). Nota-se que não há diferença no conceito, apenas nos termos "informação' e 'dado'. Ou seja, informação pessoal e dado pessoal tem o mesmo sentido.

Tanto a LAI quanto a LGPD compartilham uma concepção similar do que é considerado um dado pessoal. Além disso, ambas as leis estabelecem medidas para proteger as informações pessoais dos titulares desses dados, preservando sua intimidade, vida privada, honra e imagem,

restritas apenas aos próprios titulares e aos agentes de tratamento de dados pessoais (Teixeira, 2020).

Nota-se que a administração Pública tem uma série de normativos que orientam a implementação das políticas de dados abertos governamentais. O principal nesse aspecto, é o já mencionado Decreto nº 8.777/2016 que institui a Política de Dados Abertos do Poder Executivo Federal. "No âmbito dessa política cada órgão deve elaborar, a cada dois anos, seu Plano de Dados Abertos (PDA). O PDA planeja as ações que visam à abertura e sustentação de dados nas organizações públicas, indicando o conteúdo e o formato das bases que serão abertas, o cronograma de abertura, assim como se estão sujeitas ou não ao sigilo" (Avelino; Pompeu; Fonseca, 2021, p.22).

A Política de Dados Abertos visa promover a transparência governamental e a acessibilidade de informações públicas, permitindo que elas sejam disponibilizadas em formato aberto e reutilizáveis pela sociedade em geral. Busca incentivar a participação cidadã, estimular a inovação e fomentar o desenvolvimento econômico e social por meio da disponibilização de informações que antes eram restritas ou de difícil acesso. Dessa forma, a política de dados abertos busca melhorar a prestação de serviços públicos, aumentar a eficiência e a efetividade do governo, bem como ampliar a capacidade dos cidadãos de compreender e monitorar a atuação do Estado (Brasil, 2016).

A principal relação entre Política de Dados Abertos, a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados Pessoais é a gestão transparente e responsável da informação pública e dos dados pessoais, embora cada uma tenha objetivos diferentes (Cravo, 2022). A LAI foi constituída tendo como regra a publicidade e o sigilo como exceção. Seu objetivo é garantir o direito fundamental de acesso às informações públicas ao cidadão previsto na CF, tornando obrigatório aos órgãos públicos disponibilizar informações de interesse coletivo ou geral, bem como de interesse particular de por meio da transparência ativa ou passiva (Bioni; Silva; Martins, 2022).

> Uma das consequências que se pode extrair da LAI é no sentido de possibilitar o controle dos atos da administração pública, sendo no aspecto de controle social (realizado pelo cidadão ou sociedade) ou os controles administrativos ou judiciais, entendidos como a possibilidade de fiscalização recíproca entre os poderes, instituições e cidadania, atualizando o Princípio da Separação dos Poderes. Estes mecanismos se sofisticaram com a lei que estatui os dados abertos, possibilitando um cruzamento e intensificando a fiscalização deles, pois é permitida a cada cidadão a criação de sua própria plataforma (Limberger, 2022, p. 124).

É possível estabelecer uma relação harmoniosa entre o direito à proteção dos dados pessoais e o acesso à informação pública. O tratamento desses dados deve sempre priorizar o interesse das pessoas, especialmente quando se trata do poder público, que tem a obrigação de servir à coletividade. Embora o direito à proteção de dados não seja absoluto, ele deve ser ponderado em conjunto com outros direitos fundamentais e com os princípios que regem o ordenamento jurídico de acordo com as circunstâncias do caso (Limberger, 2022).

Tanto a LGPD quanto a LAI compartilham o objetivo de aumentar a transparência, tanto ativa quanto passiva, das informações e dados produzidos ou armazenados por órgãos e entidades públicas. Esse fortalecimento da transparência possibilita a redução de assimetria informacional entre o cidadão e o Estado, garantindo um maior controle e participação do cidadão (Bioni, Silva; Martins, 2022).

> Outro ponto de harmonização é que a administração pública, ao concretizar o princípio da transparência, deve buscar formas alternativas de dar publicidade aos dados, sem divulgar aqueles que são pessoais e sejam desnecessários. Além disso, é possível buscar soluções inovadoras que possibilitem o controle democrático, mas que, ao mesmo tempo, também observem as normas de proteção de dados, seja por meio da anonimização, seja por meio da aplicação do princípio da minimização (Cravo, 2021, p. 37).

E ainda, a LAI e a LGPD comungam das diretrizes voltadas ao tratamento de dados pessoais pautados no tripé confidencialidade, integridade e disponibilidade, preocupação estas alinhadas aos princípios da prevenção e da segurança (Teixeira, 2020). A novidade trazida pela LGPD é no tocante as regras de utilização dos dados dos indivíduos (Piza; Assis, 2022). As disposições da LAI reforçam os direitos os titulares previstos na LGPD, a respeito do acesso e da transparência. Desse modo, os titulares poderão acessar os dados referentes à sua pessoa, bem como todas as informações relacionadas ao tratamento dos seus dados (Cravo, 2021).

Ao solicitar informações à administração pública, tanto o cidadão quanto o agente público devem atentar sobre qual o teor do acesso, se é dado pessoal ou coletivo/geral, pois a depender da requisição poderá aplicar ora a LAI, ora a LGPD (Teixeira, 2020). A LGPD apenas "complementa as disposições previstas na LAI". Ou seja, não criou regras ou hipóteses de sigilo a respeito da LAI, e sim no contexto da proteção de dados/informações pessoais (Cravo, 2021, p. 35).

A LGPD reforça a proteção de dados pessoais ao estabelecer regras para a coleta, tratamento, armazenamento e compartilhamento de dados pessoais, incluindo a exigência de consentimento explícito dos titulares dos dados, o estabelecimento de medidas de segurança

para proteção dos dados e a criação de mecanismos para a correção e exclusão dos dados, quando necessário (Brasil, 2018).

Corroborando:

> A LAI dá acesso a informações públicas, enquanto a LGPD protege dados pessoais, o que já demonstra claramente feixes de atuação completamente dissociados entre as leis. Ao contrário do senso comum, o objetivo da LGPD, principalmente no âmbito público, não é restringir a circulação da informação e dificultar a transparência, mas tão somente estimular o fluxo de dados, ou seja, aquele capaz de resguardar a proteção de dados pessoais (Piza; Assis, s.p, 2022).

Neste aspecto, haver um aparente tensionamento entre a transparência e a privacidade impostas pela LAI e LGPD, mas há na verdade uma complementariedade entre elas. "A primeira impressão pode ser no sentido de contradição, mas esta é apenas aparente. O ordenamento jurídico deve ser interpretado de forma sistemática, buscando-se um diálogo harmonioso" (Limberger, 2022, p. 121). Assim, embora tenham objetivos distintos, os dois regulamentos são complementares e harmônicos entre si.

Percebe-se, portanto, que não há superioridade de uma lei em relação à outra, mas sim particularidades em ambas. Enquanto uma busca garantir o acesso à informação, em geral, a outra visa assegurar a privacidade dos dados pessoais. Ambas buscam proteger as informações pessoais de terceiros não autorizados, porém, somente a LGPD exige a documentação da análise de impacto de privacidade, políticas de privacidade e proteção, bem como políticas de resposta a incidentes. Portanto, é evidente que as leis, apesar de suas diferenças, contribuem mais para a proteção dos dados pessoais comuns e especiais do que se opõem (Teixeira, 2020)

Não há conflito aparente entre a LAI e a LGPD, pois "a lógica da proteção de dados e a moldura normativa da LGPD não é de restringir a circulação da informação, mas, muito pelo contrário, de estimulá-la. Seu objetivo último é garantir um fluxo informacional adequado" (Bioni; Silva; Martins, 2022, p. 10).

As leis são tão complementares que a Lei de Acesso à Informação, que existe há mais tempo do que a LGPD, já estabeleceu equilíbrio e regras de proporcionalidade para o fluxo de informações regulado por ela. O artigo 31 da lei, por exemplo, demonstra que informações relacionadas à privacidade, intimidade, honra e imagem podem ser restringidas ou condicionadas ao consentimento do titular (Bioni; Silva; Martins, 2022).

Observa-se que,

> não é toda e qualquer informação pessoal que goza de um regime específico de proteção. Apenas aquela com potencial de vulnerar os direitos de

> personalidade, tais como definidos no art. 5º, X da Constituição Federal, estaria sob uma proteção especial. No núcleo desse conjunto de dados, estaria o que se denominou, com amparo na doutrina existente, a informação pessoal sensível. Ou seja, aquela informação que viola o direito de autodeterminação da imagem ou que possa levar a que terceiros adotem ações discriminatórias contra o titular daquele dado. A existência de gradações desta natureza mostrou-se bastante importante ao longo dos últimos anos, pois passou a indicar limites à mitigação da expectativa de privacidade no caso em que os titulares dos dados eram os próprios agentes públicos (Brasil, 2022, p. 20).

Assim, ambas as legislações resguardam a informação pessoal, o que as diferem é quanto ao processo de tratamento no ciclo de vida dos dados ante as políticas de privacidade e proteção, assim como suas bases legais e princípios autorizadores. Assim, resta claro que apesar da relação preponderante de convergência entre os referidos regulamentos, mas haverá situações em que ocorrerá um tensionamento entre o que é de interesse público e o que deve ser resguardado por dizer respeito à vida íntima de uma pessoa (Bioni; Silva; Martins, 2022).

Portanto, LGPD, LAI e a Política de Dados Abertos não conflitam e não divergem, uma vez que ambas estão totalmente alinhavadas nos quesitos transparência, publicidade, segurança, integridade, confidencialidade e acessibilidade das informações públicas, porém a LGPD se destaca entre elas pelo seu papel fundamental de proteger a privacidade dos cidadãos e garantir o tratamento adequado dos dados pessoais. Por isso, a LGPD dedicou um capítulo inteiro para disciplinar exclusivamente o tratamento de dados pessoais pelo poder público. Tema que será abordado no tópico seguinte.

2.2.4 O Tratamento de dados pessoais pelo poder público

Dado o volume de dados sob tutela do Poder Público e sua relação de desigualdade entre os titulares de dados, é dever dos órgãos e entidades do da Administração Pública promover a transparência e a segurança no tratamento de dados pessoais. A transparência visa a inspirar no titular de dados a credibilidade no ente público controlador dos dados e a necessária responsabilidade a que está submetido, numa clara relação com um princípio peculiar da lei protetiva nacional, o da responsabilização e prestação de contas (Brasil, 2021).

Como já mencionado, as regras estabelecidas para o adequado tratamento de dados pessoais pelas pessoas jurídicas de direito público no âmbito da LGPD estão intrinsicamente relacionadas aos preceitos já estabelecidos pela Lei de Acesso à Informação. Nesse contexto a LGPD reservou um capítulo específico para o tratamento de dados pessoais pelo Poder Público.

O regramento se inicia pelo artigo 23, ao delimitar os entes que compõem poder público com base na LAI.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e
> II - seja indicado um Encarregado quando realizarem operações de tratamento de dados pessoais (Brasil, 2018).

O artigo 23 da LGPD traz como pressupostos, o atendimento de uma finalidade pública, a persecução de um interesse público e a execução, pelo ente público, de suas competências legais ou cumprimento de suas atribuições. Trata-se, na verdade, de preceito legal que complementa a base legal de tratamento de dados pelo Poder Público, expresso no artigo 7°, inciso III, onde prevê a autorização de tratamento de dados para a execução de políticas públicas (Vainzof, 2019).

> O tratamento de dados deve estar associado sempre a uma finalidade, a qual, no setor público, pode se referir à execução de políticas públicas previstas em leis, normas ou instrumentos similares ou a obrigações legais ou regulatórias. Quanto a esse aspecto, o órgão deve observar a eventual necessidade de explicitamente obter o consentimento do titular dos dados e, quando dispensável, de comunicar as operações executadas, como, por exemplo, ao compartilhar dados com órgãos públicos ou ao transferi-los a terceiros, questões essenciais para se alcançar a conformidade com a indigitada lei (IBGP, 2022, p.88).

Ainda, com base no referido artigo, o poder público pode coletar e tratar dados pessoais apenas quando necessário para o desempenho de suas atribuições legais ou para o exercício de suas funções públicas. Além disso, a coleta e o tratamento de dados pessoais pelo poder público devem ser realizados de forma transparente, respeitando a privacidade dos titulares dos dados. Fica estabelecida, também, a obrigatoriedade do controlador de nomear um encarregado pela proteção de dados pessoais, que será responsável por receber as reclamações e comunicações dos titulares dos dados, além de orientar os funcionários e colaboradores do poder público sobre as práticas de tratamento de dados pessoais (conforme já mencionado anteriormente).

Além das regras previstas nos artigos 23. A Lei prevê em seu artigo 7°, dez hipóteses (como visto anteriormente) que autorizam o tratamento de dados, bem como estabelece os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais (Brasil, 2020). As bases legais são fundamentais para que se possa analisar o porquê se trata e o que ampara o poder público no tratamento de dados pessoais.

As bases legais comumente aplicáveis no âmbito do poder público são: consentimento, legitimo interesse, cumprimento de obrigação legal ou regulatória pelo controlador e execução de políticas públicas. Não obstante, entres as demais, o consentimento não figura como mais adequada para tratamento de dados pelo poder público, quando isso é necessário para a sua atividade pública, ou fim específico/regulatório). Quando o titular é obrigado a fornecer informações para acessar um serviço público, há um desequilíbrio de poder que torna o consentimento não livre. Nesse sentido, é importante analisar cuidadosamente a solicitação dessas informações pelo órgão responsável pela atividade pública, pois o consentimento pode não ser a base mais apropriada para legitimar tal ação (LGPD, 2022).

A base legal do legítimo interesse permite o tratamento de dados pessoais pelo controlador, mas não se aplica a dados sensíveis. Essa base só pode ser utilizada para atender aos interesses legítimos do órgão público no desempenho de atividades ou fornecimento de serviços. Apesar disso, é importante destacar que essa base legal é bastante flexível. Recomenda-se que quando for fazer um enquadramento do tratamento baseado no legítimo interesse, deve-se sempre fazer um balanceamento que possa verificar o legítimo interesse do controlador e a legítima expectativa e os direitos dos titulares dos dados. Isso é fundamental. Muitas vezes, essa não se mostra ser é a base mais adequada para o serviço público, considerando a execução de uma atividade pública, ou um serviço público (obrigação legal) (LGPD, 2022).

Nesse aspecto, a melhor base seria o cumprimento de obrigação legal e regulatória pelo controlador (normas de conduta e normas de organização) (Art. 7º, II). As normas de conduta são aquelas normas que estabelecem alguma atividade ou alguma imposição que o órgão deve cumprir devido aos regulamentos, as agências reguladoras e outros). Normas de organização são as que organizam as instituições e definem suas obrigações legais. Nesse caso, o fornecimento do serviço ou de uma atividade nada mais é que uma obrigação legal do órgão (Brasil, 2018; LGPD, 2022).

Fora do caso em tela, geralmente a base legal execução de políticas públicas (Art. 7º, III) é a mais utilizada e adequada para o enquadramento pelo Poder Público.

> No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Tais políticas públicas, vale destacar, devem estar inseridas nas atribuições legais do órgão ou da entidade da administração pública que efetuar o referido tratamento. Outra finalidade corriqueira para o tratamento de dados no serviço público é o cumprimento de obrigação legal ou regulatória pelo controlador. Nessas duas situações, o consentimento do titular de dados é dispensado (Brasil, 2018, p. 12).

Portanto, para o tratamento de dados pessoais pelo Poder Público, é necessário se valer de uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. É importante interpretar esses dispositivos de forma sistemática e conjunta com os critérios adicionais elencados no art. 23, que complementam e auxiliam na interpretação e na aplicação prática das bases legais no âmbito do Poder Público (Brasil, 2022).

Além das bases legais, há de se observar os princípios de proteção de dados pessoais pelo poder público impostos pela LGPD que devem, fundamentalmente, ser equacionados com os princípios da administração pública. Na administração os princípios são: legalidade, impessoalidade, moralidade, publicidade, eficiência e supremacia do interesse público. Os princípios da LGPD são: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas (*accountability*) (LGPD, 2022).

Veja a seguir, algumas medidas que devem ser consideradas quando do tratamento de dados pessoais pelo poder público: Limitação da coleta dos dados pessoais ao mínimo necessário para o alcance das finalidades do tratamento; Adoção de cautela quando envolvidos dados pessoas sensíveis, conforme a definição do art. º, II da LGPD; Respeito aos diretos dos titulares e observância ao princípio da transparência, fornecendo-se aso titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; e Implementação de medidas de prevenção e segurança eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, priorizando-se, sempre que possível a pseudonimização ou a anonimização dos dados (LGPD, 2022)

Em se tratando de compartilhamento de dados entre entidades do poder público:

> O compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública. De forma mais específica, a LGPD utiliza o termo ‘uso compartilhado de dados’, que é definido como a “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos

> e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Brasil, 2022, p. 16).

O compartilhamento dentro da administração pública no âmbito da execução de políticas públicas é permitido pela lei, dispensando o consentimento específico. No entanto, o órgão responsável pela coleta de dados deve comunicar de forma clara que dado será compartilhado e com quem será compartilhado. Por outro lado, quando um órgão solicita acesso a informações coletadas por outro órgão, é necessário justificar esse acesso com base na execução de uma política pública específica e claramente definida. Isso inclui descrever o motivo da solicitação de acesso e como os dados serão utilizados. É importante observar que informações protegidas por sigilo ainda devem seguir normas e regras específicas para sua proteção (Brasil, 2022).

Vainzof (2019) concorda que a LGPD estabelece, no art. 26, que o compartilhamento de dados pessoais pelo próprio Poder Público deve servir a finalidades específicas relacionadas à execução de políticas públicas e às atribuições legais dos órgãos e entidades públicas, respeitando os princípios de proteção de dados pessoais descritos no art. 6° da Lei. A transferência desses dados para entidades privadas é proibida, exceto em algumas circunstâncias

Deve-se, portanto, sopesar valores quando realizar o compartilhamento de dados pessoais pelo Poder Público. Nesse caso, o controlador precisa, necessariamente, responder às seguintes questões: “Em quais situações o interesse público de prevalecer sobre o direito individual à privacidade? Como proteger dados pessoais tornados públicas em razão de políticas de transparência?” Com isso, deve-se ater à necessidade de publicação ou compartilhamento desse dado, fazer o balanceamento da proporcionalidade e adotar medidas técnicas de segurança para proteção” (LGPD, 2022, n.p). Com base no guia orientativo Tratamento de Dados Pessoais Pelo Poder Público é possível observar no quadro a seguir os principais requisitos e recomendações para o compartilhamento de dados (LGPD, 2022; Brasil, 2022).

Quadro 5. Requisitos e recomendações para compartilhamento de dados pessoais pelo poder público

Requisitos	Recomendações
Formalização e registro	1. Instauração de processo administrativo; 2. Análise técnica jurídica; 3. Decisão administrativa ou celebração de contrato, convênio ou instrumento congênere; 4. Edição de ato normativo interno.
Objeto e finalidade	1. Descrição dos dados pessoais de forma objetiva e detalhada;

	2. Indicação da finalidade específica; 3. Avaliação da compatibilidade entre a finalidade original e a finalidade do compartilhamento.
Base legal	1. Indicação da base legal utilizada
Duração do tratamento	1. Definição do período (duração) do uso compartilhado dos dados, de forma fundamentada, e esclarecimento sobre a possibilidade de conservação ou necessidade de eliminação após o término do tratamento.
Transparência e Direitos dos titulares	1. Divulgação das informações pertinentes na página eletrônica dos órgãos e das entidades responsáveis; 2. Divulgação de maneira que as informações sobre dados pessoais tratados pela entidade sejam de fácil compreensão; 3. Definição de responsabilidades e de procedimentos relativos ao atendimento de solicitações de titulares.
Prevenção e segurança	1. Descrições das medidas técnicas e administrativas adotadas para proteger os dados pessoais de incidentes de segurança.
Outros requisitos	1. Autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais; 2. Ônus financeiro (sem ônus por parte do titular); 3. Requisitos específicos para compartilhamento de dados pessoais com entidades privadas (art. 26, § 1º e art. 27, LGPD); 4. Elaboração do relatório de impacto à proteção de dados pessoais, caso necessário; 5. Identificar as funções e responsabilidades dos agentes de tratamento.

Fonte: Brasil (2022); LGPD (2022).

Portanto, a Administração Pública poderá fazer o uso compartilhado de dados, desde que tal se dê com o estrito objetivo de executar políticas públicas expressamente previstas na legislação (Lima, 2019). Cabe ressaltar, no entanto, que mesmo nas situações em que a LGPD não se aplica ao poder público, é necessário que o tratamento de dados pessoais seja realizado com respeito aos direitos fundamentais e às garantias constitucionais, como a privacidade, a intimidade e a proteção de dados pessoais.

Finalmente, tendo em vista o grande volume de dados pessoais tratados pelo poder público, faz-se necessário jogar luz sobre como se dá o tratamento de dados pelas IFES dada suas complexidades e peculiaridades.

2.2.4 O Tratamento de Dados Dessoais Pelas IFES

As IFES são instituições de educação superior mantidas pela União, com autonomia didático-científica, administrativa e de gestão financeira e patrimonial. São formadas pelas seguintes entidades: Universidades Federais e Institutos Federais de Educação, Ciência e Tecnologia (IFs), Universidade Tecnológica Federal, Centros Federais de Educação

Tecnológica (Cefets) e Colégio Pedro II. Todas mantidas pelo governo federal (Brasil, 1988; 1996; 2008).

As IFES são peculiares, tendo em vista que "sua natureza organizacional incorpora preceitos da administração pública brasileira e de sistemas colegiados" (Silva; Melo, 2021, p. 16). Nesse sentido, qualquer ferramenta estratégica, serviços, produtos, políticas e processos não podem ser incorporados a elas sem que haja uma customização.

Cabe mencionar a complexidade e peculiaridade das instituições educacionais. No caso das IFES, embora sejam mantidas pelo governo federal, não se trata de uma entidade governamental, nem tampouco empresarial. A universidade é uma organização *sui generis* cuja complexidade, objetivos e especificidades influenciam sua administração. A literatura na área destaca que a universidade tem sido caracterizada como burocracia, colegialidade, anarquia organizada, arena política, sistema frouxamente articulado e sistema cibernético (Meyer Jr, 2021). O autor destaca ainda que é:

> Impossível ignorar a complexidade das organizações educacionais na compressão da sua realidade, comportamento e desempenho. Administrar uma organização acadêmica, cuja missão é educar seres humanos requer visão, intuição, sensibilidade e o uso de ferramentas administrativas adequadas às especificidades desse tipo de organização (Meyer Jr, 2021, p. 47).

Dada as peculiaridades e o cumprimento dos seus objetivos, as IFES realizam tratamentos de dados pessoais no âmbito do ensino, da pesquisa e da extensão (atividades-fim), além das atividades administrativas (atividades-meio).

As universidades frequentemente coletam dados durante o processo de matrícula, quando os alunos fornecem informações e entregam seus documentos pessoais. Ao longo de sua permanência na instituição, várias outras informações passam por setores como secretarias acadêmicas, bibliotecas e outras áreas de apoio estudantil, incluindo contratos de financiamento com programas de bolsas públicos ou privados, informações sobre desempenho acadêmico e até dados bancários. Todas as informações sobre o desempenho acadêmico são registradas no histórico escolar, um documento pessoal que o estudante pode solicitar a qualquer momento para fins de consulta, comprovação ou transferência entre instituições de ensino superior (IES).

Além disso, também são coletados dados dos servidores, técnicos-administrativos e professores para fins de concursos, contratações, parcerias com outras instituições, projetos de pesquisa e desenvolvimento profissional, entre outros. A coleta de dados dos servidores também é regida pela LGPD (UFRJ, 2023).

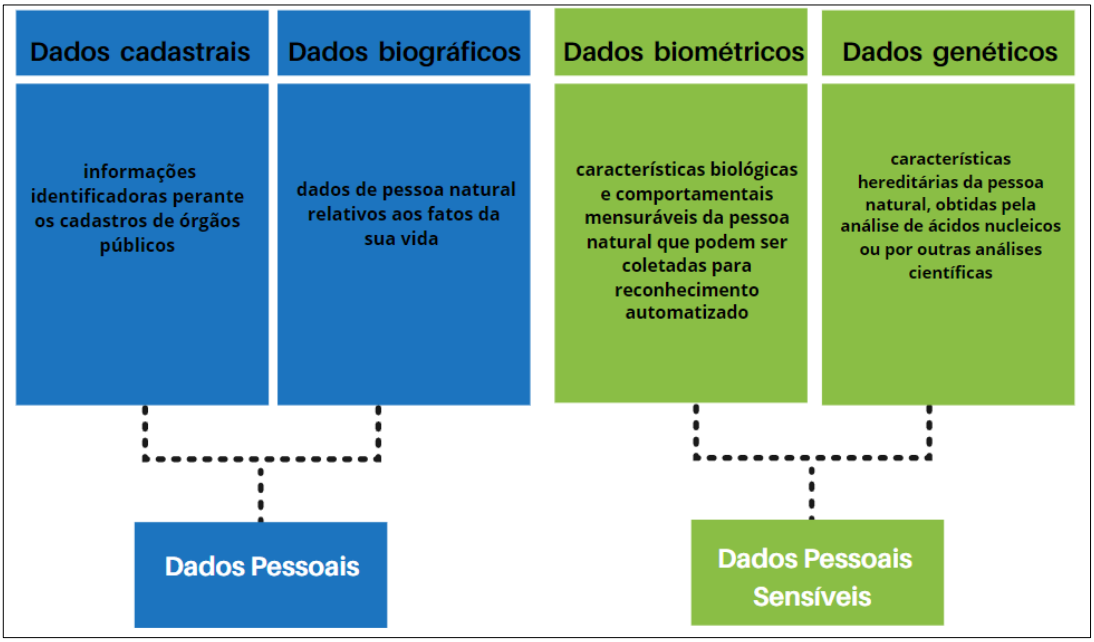
Para garantir a conformidade das IFES à LGPD, é necessário cumprir integralmente a lei sempre que houver tratamento de dados pessoais para fins que não sejam relacionados para fins exclusivamente acadêmicos. Por exemplo, ao coletar dados pessoais para fins administrativos, mesmo que esses dados tenham alguma relação indireta com as atividades acadêmicas. Isso inclui a coleta de dados de alunos para matrículas, estágios, processos seletivos, registros de presença e notas de avaliação, bem como o tratamento de dados pessoais de servidores pelo setor de gestão de pessoas (Brasil, 2022).

Nesse aspecto, conforme as diversas atividades executadas pelas IFES, depreende-se que há tratamento de dados pessoais de várias categorias (cadastrais, biográficos, biométricos e genéticos) e tipos (dado pessoal e dado pessoal sensível) com base na LGPD e no Decreto nº 10.046/2019, que dispões som o compartilhamento de dados no âmbito da administração pública federal (Brasil, 2019).

Os dados cadastrais são informações que identificam uma pessoa em uma base de dados, como número de identificação pessoal (CPF, RG, título de eleitor), número de telefone, endereço de e-mail, endereço residencial, entre outros. Esses dados são usados para fins de cadastro e identificação em serviços e sistemas diversos, como por exemplo, cadastros governamentais. Dados biográficos são informações sobre a história pessoal de uma pessoa, como nome completo, data de nascimento, endereço, profissão, estado civil, entre outros. Esses dados podem ser utilizados para fins de identificação, pesquisa de antecedentes e avaliação de riscos. Dados biométricos são medidas físicas ou características do corpo humano, como impressões digitais, íris, retina, rosto, voz, entre outros (Brasil, 2019).

Esses dados são usados para identificação e autenticação de indivíduos. Dados genéticos são informações sobre o DNA de um indivíduo, incluindo variações genéticas que podem estar associadas a características físicas, doenças e susceptibilidade a certas condições. Esses dados podem ser utilizados em pesquisas científicas, diagnóstico de doenças genéticas, prevenção e tratamento de doenças (Brasil, 2018; 2019; 2020).

Figura 4. Matriz de categoria de dados



Fonte: Elaborado pelo autor com base em Brasil (2018; 2019; 2020)

É importante ressaltar que todas as categorias de atributos constituem informações pessoais, pois dizem respeito a uma pessoa física identificada ou identificável. Atributos genéticos e biométricos, conforme a definição legal, são considerados dados pessoais sensíveis. Já atributos biográficos, junto com informações como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor, são classificados como dados cadastrais, que, de acordo com a LGPD, são também dados pessoais. Isso ocorre porque qualquer dado, incluindo os cadastrais, que esteja relacionado a uma pessoa natural identificada ou identificável será considerado dado pessoal. Dependendo de seu conteúdo, os atributos biográficos podem ou não ser considerados sensíveis. Segundo a Lei, são considerados sensíveis aqueles atributos biográficos que se referem a crença religiosa, opinião política, filiação a sindicato ou a organizações de natureza religiosa, filosófica ou política (Brasil, 2020).

Entre as diversas situações tratamento de dados pessoais pelas IFES, algumas poderão estar elencadas nas exceções da aplicação da LGPD, tais como o tratamento para fins exclusivamente: jornalístico e artístico; para fins acadêmicos e para a realização de estudos por órgão de pesquisa previstos no artigo 4, conforme já apresentado no tópico LGPD – Lei Geral de Proteção de Dados Pessoais (Brasil, 2018).

Importante mencionar que, além da LGPD, o tratamento de dados pessoais realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos, seguem os preceitos instituídos pela Constituição Federal, Lei de imprensa, Lei de Direitos Autorais e a Lei de Diretrizes e

Bases da Educação Nacional. Com base nessa coleção jurídica, é dever respeitar a liberdade de expressão, de informação e realizar o tratamento de forma compatível com as finalidades específicas da atividade (Brasil,1953; 1988; 1996;1998).

> É justamente no contexto do perigo de que uma legislação de tamanha envergadura possa interferir e impactar em atividades de importância louvável é que a LGPD criou a exceção também quando o tratamento de dados seja realizado exclusivamente para fins jornalísticos e artísticos. A isenção visa a proteção do jornalismo, mas não concede uma isenção automática e geral da LGPD para mídias e entidades que processem dados pessoais. Qualquer informação relacionada a pessoa natural identificada ou identificável é considerada dado pessoal, mesmo que o acesso seja público, devendo o tratamento desses dados levar em consideração a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização, sendo dispensado a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios na Lei (Vainzof, 2019, p.65).

As IFES podem tratar dados pessoais ao executam atividades de jornalismo por meio de suas TVs e departamentos de comunicação. Nas vezes que a instituição exerce atividade de jornalismo, torna-se fundamental fazer algumas ponderações que podem ser aplicadas à interpretação da LGPD. Essas ponderações incluem: (i) analisar e justificar a razão pela qual os dados estão sendo tratados para fins jornalísticos; (ii) agir com transparência e honestidade, sempre informando os titulares dos dados coletados quando possível, mas entendendo que em muitos casos pode não ser viável informá-los previamente ao tratamento de seus dados; (iii) em situações em que informar os titulares possa prejudicar a atividade jornalística, não é necessário fazê-lo (Vainzof, 2019).

Por fim, instituições que desejam utilizar a exceção jornalística ao tratar dados, devem ser extremamente cuidadosas ao separar diferentes conjuntos de dados de acordo com suas respectivas finalidades. Elas precisam ser capazes de demonstrar que certos dados são usados exclusivamente para fins jornalísticos, justificando os motivos pelos quais chegaram a essa conclusão, para que possam se beneficiar da exceção prevista na legislação (Vainzof, 2019).

A pesquisa, para fins acadêmicos, deve seguir as mesmas recomendações da exceção da Lei em relação ao tratamento de dados pessoais para fins exclusivamente jornalísticos, principalmente ter cuidado ao divulgar o trabalho científico, equilibrando o interesse público e os direitos do titular dos dados. Além disso, a interpretação da lei deve ser restrita (Vainzof, 2019).

De acordo com a natureza das IFES, elas podem também ser enquadradas como órgãos de pesquisa, definidas:

> Art. 5º [...]
> XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Brasil, 2018).

A LGPD prevê a hipótese de tratamento de dados pessoais por órgãos de pesquisa com o objetivo de realizar estudos, incluindo a possibilidade do tratamento de dados pessoais sensíveis, sem a necessidade de consentimento do titular dos dados (Brasil, 2020).

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - [...]
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) - [...];
> b) - [...];
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (Brasil, 2018).

Nas investigações cientificas, seja em nome de universidades ou outras entidades, os pesquisadores poderão coletar, classificar, processar, armazenar, avaliar ou controlar dados pessoais da forma que lhe convier, desde que consigam demonstrar a finalidade exclusivamente acadêmica, sendo recomendável, também, observarem os princípios da LGPD, principalmente os da finalidade, adequação, necessidade e segurança.

Nesse aspecto, o tratamento de dados, deve considerar os seguintes aspectos (i) a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização; (ii) realização de estudos por órgão de pesquisa, inclusive com dados sensíveis, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) realização de estudos em saúde pública, por órgãos de pesquisa (Vainzof, 2019). Veja a seguir o que dispõe o artigo 13 da LGPD:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

> § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
> § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
> § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
> § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (Brasil, 2018)

Assim, embora o consentimento possa ser dispensado sob a perspectiva da legislação de proteção de dados pessoais, deve-se ser considerado necessário do ponto de vista ético. Além disso, pode-se adotar medidas as medidas as referidas medidas técnicas anonimização e pseudonimização sempre que possível. Reforçando que quando os dados pessoais são anonimizados perdem o alcance da LGPD. Assim "os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". (BRASIL, Art. 12). Ainda, conforme o regulamento, o dado anonimizado é um "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Brasil, 2018, Art. 5º, III).

A anonimização é utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Brasil, 2018, Art. 5º, XI). Já a pseudonimização "é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Brasil, 2018, Art. 13, § 4º).

Cabe mencionar que a anonimização ou a pseudonimização de dados pessoais não foram criadas pela LGPD como medidas de segurança impositivas, ou seja, que devem realizadas em todos os casos de estudos e pesquisas. Do mesmo modo, a LGPD não determinou que a anonimização ou pseudonimização sejam requisitos técnicos para a divulgação pública ou compartilhamento de dados pessoais para fins de pesquisa e estudos, mas é importante reconhecer que, em certos casos, a identificação dos titulares pode ser fundamental para alcançar os objetivos da pesquisa (Vainzof, 2019).

Outra situação em que a LGPD não se aplica no contexto da IFES, é quando o tratamento de dados pessoais é realizado para fins exclusivos de atividades de investigação (Procedimentos Administrativos Disciplinares), previsto no artigo 4º (Brasil, 2018). Nesse caso, o tratamento de dados pessoais, geralmente realizado pelas unidades correcionais de cada instituição, deve observar as legislações específicas que estabeleçam as condições, garantias e direitos dos titulares dos dados.

Portanto, como entidades do Poder Público, as IFES devem adotar boas práticas assim como qualquer outra organização, adotando por exemplo medidas segurança da informação, salvaguardas e mecanismos de mitigação de risco, bem como avaliação da necessidade e da proporcionalidade da coleta e processamento dos dados pessoais para atingir a finalidade pretendida (Vainzof, 2019). Em decorrência da LGPD, as IFES precisam implementar um programa de aderência à legislação, incluindo a implementação de políticas internas, revisão de documentos e treinamentos visando garantir seu *compliance* (Pinheiro, 2020).

Por fim, as IFES devem seguir os mesmos preceitos da LGPD aplicados ao Poder Público, mas, devendo readequar seus processos de coleta, tráfego e armazenamento de dados conforme suas peculiaridades. Para isso poderá implementar programas de governança de dados pessoais e políticas institucionais (que serão abordadas no tópico seguinte) por meio de iniciativa própria para dar cumprimento às diretrizes/desdobramentos de políticas públicas regulatórias com o objetivo de proteger o direito à privacidade e à proteção de dados pessoais.

2.3 GOVERNANÇA

A origem da palavra governança vem do vocábulo grego, que significa direção. Ultimamente, o termo governança tem sido discutido bastante no discurso acadêmico, no âmbito do setor público, e outras instituições, se administram e de que forma administram suas relações com a sociedade (Peters, 2013).

Para a Organização das Nações Unidas (ONU), a governança não se refere necessariamente a uma entidade física nem ao ato de governar cidadãos. Em uma perspectiva mais prática, é vista como um processo em que instituições, organizações e cidadãos se orientam mutuamente. A governança também envolve a interação entre o setor público e a sociedade, bem como a forma como esta se organiza para a tomada de decisões coletivas, assegurando que existam mecanismos transparentes para que essas decisões sejam implementadas (ONU, 2002).

Já o Instituto Brasileiro de Governança Corporativa (IBGC) afirma que a governança corporativa é o sistema que orienta, monitora e incentiva a gestão de empresas e outras organizações, abrangendo as relações entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle, além de outras partes interessadas (IBGC, 2015). Assim, a governança corporativa não se restringe a empresas privadas, pois pode ser adaptada a qualquer tipo de organização. O próprio Instituto ainda assevera que os princípios e práticas de boa Governança Corporativa são aplicáveis a qualquer tipo de organização, independentemente de seu porte, natureza jurídica ou tipo de controle podendo ser adaptados a outras formas de organizações, como, por exemplo, órgãos governamentais (IBGC, 2019).

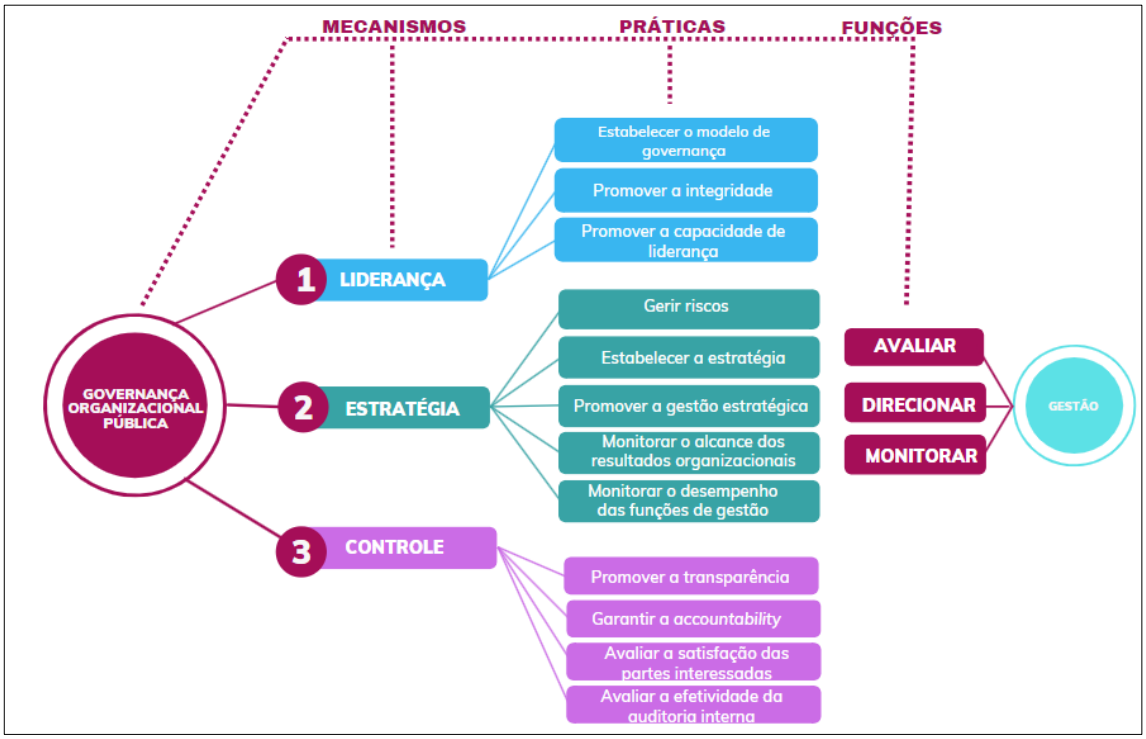
Neste sentido, a governança pode ser aplicada em diversos tipos organizações, inclusive às públicas, tendo vista que seus princípios e ações objetivam otimizar os resultados pretendidos pelos gestores e usuários do serviço público. No âmbito da Administração Pública, "[...] a sociedade (principal) faz o papel dos acionistas e os gestores públicos (agente) se equiparam ao corpo gerencial das empresas, na medida em que recebem da sociedade o poder para gerenciar os recursos arrecadados e devolvê-los na forma de serviços aos cidadãos" (Nardes, 2013, p. 17).

Para o GesPública, governança pública é o sistema que visa assegurar às partes interessadas, o governo estratégico das organizações públicas e o efetivo monitoramento da alta administração (Brasil, 2009). Nardes (2013) enfatiza ainda que a governança pública possibilita que a Administração Pública (agente) proporcione um ambiente seguro e favorável para a formulação e implementação de políticas públicas em benefício da sociedade (principal).

Com base no art. 2º do Decreto nº 9.203/17, que dispõe sobre a política de Governança da administração pública federal direta, autárquica e fundacional considera-se a governança pública: "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade" (Brasil, 2017).

A governança publica organizacional tem como objetivo a entrega de resultados aos usuários dos serviços públicos, cidadãos e sociedade em geral. Em suma, a governança pública organizacional é o emprego de práticas de liderança, estratégia e controle. Tais práticas possibilitam aos mandatários de uma organização pública e as partes interessadas avaliar seu status e demandas, direcionar a sua atuação e monitorar o seu funcionamento, de modo a ampliar as oportunidades de entregar bons resultados aos cidadãos, em relação a prestação de serviços (Brasil, 2020). Assim do conjunto de mecanismos: liderança, estratégia e controle, desdobram-se as práticas. Como resultado, as práticas possibilitam avaliar, monitorar e avaliar a gestão.

Figura 5. Práticas relacionadas aos mecanismos de governança



Fonte: Elaborado pelo autor, adaptado de Brasil (2020).

Depreende-se, portanto, que os referidos mecanismos e as práticas são fundamentais para que as atividades/funções (avaliar, direcionar e monitorar) alcance a efetividade em governança pública. A governança é regida por políticas, e por meio delas que se determina o padrão integrado e são essas políticas que vão determinar o padrão integrado, ou seja, de conhecimento e de valores, a ser perseguido por pessoas e sistemas, numa organização. Assim, não existe se não for por meio de políticas (Cots, 2020).

> a boa governança depende, entre outras variáveis, da construção de organizações eficazes [...]. Além de ter servidores públicos motivados e bem treinados, esses indivíduos devem ser organizados em estruturas que promovam a melhoria do desempenho e minimizem as disfunções geralmente associadas à burocracia pública. Além disso, essas organizações devem ser conduzidas de forma eficaz por indivíduos que possuam as habilidades necessárias para que elas funcionem sem problemas (Brasil, 2018, p. 31).

De acordo com o Referencial Básico de Governança Organizacional (RBGO) do TCU, a governança não pode ser confundida com gestão. Nesse aspecto,

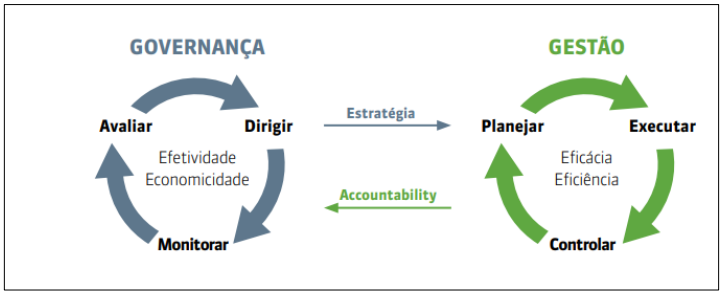
> **a governança** se preocupa com a qualidade do processo decisório e sua efetividade: como obter o maior valor possível para [...] as partes interessadas? Os problemas priorizados foram resolvidos? Como, por quem e por que as decisões foram tomadas? Os resultados esperados foram alcançados?

> **A gestão**, por sua vez, recebe o direcionamento superior e se preocupa com a qualidade da implementação desta direção, com eficácia e eficiência: está claro o que deve ser feito? Tem-se os recursos necessários? Quais os riscos mais relevantes para o cumprimento da missão? Quanto é razoável gastar? (Brasil, 2021, p. 17, grifo nosso).

A governança é a função direcionadora, enquanto a gestão é a função realizadora. A governança é, portanto, "o direcionamento do esforço de gestão das organizações para resultados de interesse da sociedade, não se confundindo com a própria gestão" (Brasil, 2020, p. 37).

> a governança envolve as atividades de avaliar o ambiente, os cenários, as alternativas, e os resultados atuais e os almejados, a fim de direcionar a preparação e a coordenação de políticas e de planos, alinhando as funções organizacionais às necessidades das partes interessadas; e monitorar os resultados, o desempenho e o cumprimento de políticas e planos, confrontando-os com as metas estabelecidas. Já as atividades básicas de gestão são: planejar as operações, com base nas prioridades e os objetivos estabelecidos; executar os planos, com vistas a gerar resultados de políticas e serviços; e controlar o desempenho, lidando adequadamente com os riscos (BRASIL, 2021, p. 12).

Figura 6. Relação entre governança e gestão



Fonte: Brasil, 2020.

2.3.1 Programa de governança em privacidade e proteção dados pessoais

A necessidade de proteger a privacidade e os dados pessoais tornou-se evidente devido à exposição dos titulares de dados e informações, especialmente com o aumento do volume de dados e informações pessoais produzidos. Assim, destaca-se a importância de controlar esses dados e informações e de estabelecer modelos de governança para seu tratamento adequado, com o objetivo de proteger os direitos fundamentais (Shintaku et al, 2021).

Como visto, a LGPD visa promover mudanças efetivas nas práticas dos agentes de tratamento, com o objetivo de garantir que os direitos fundamentais sejam materializados nos processos informacionais. Portanto, alguns importantes elementos dessas mudanças podem ser

observados na adoção de boas práticas por agentes de tratamento por meio de diversos instrumentos (Martins; Cruz, 2022).

Na administração pública, a governança da privacidade deve englobar as estratégias, competências, pessoas, processos e ferramentas necessárias para que os órgãos e entidades possam ganhar a confiança dos servidores e cidadãos, ao mesmo tempo em que atendem às exigências estabelecidas pelos normativos de privacidade. Um Programa de Governança em Privacidade (PGP) reúne e consolida os requisitos de privacidade com o objetivo de orientar e influenciar a maneira como os dados pessoais são tratados ao longo de todo o seu ciclo de vida (Brasil, 2020).

Em síntese, na seção 2 sobre boas práticas e governança, o artigo 50 da LGPD estabelece que controladores e operadores podem definir regras de boas práticas e governança para guiar o tratamento de dados pessoais. Essas regras devem incluir organização, procedimentos, normas de segurança, padrões técnicos, responsabilidades dos envolvidos, ações educativas, mecanismos de supervisão e mitigação de riscos, entre outros aspectos, ressaltando a importância da implementação de um Programa de Governança em Privacidade (PGP) (Brasil, 2018).

O controlador deve implementar um PGP que demonstre o comprometimento em adotar processos e políticas internas abrangentes para cumprir normas e boas práticas de proteção de dados pessoais. Esse programa deve ser aplicável a todos os dados sob seu controle, independentemente de como foram coletados, e adaptado à estrutura, escala, volume de operações e sensibilidade dos dados tratados. Políticas e salvaguardas adequadas devem ser estabelecidas com base em avaliações sistemáticas de impactos e riscos à privacidade (Vainzof, 2019).

Ainda, o programa deve promover uma relação de confiança com os titulares, por meio de transparência e participação, e estar integrado à estrutura geral de governança, com mecanismos de supervisão internos e externos. Planos de resposta a incidentes e remediação devem estar incluídos, e o programa deve ser constantemente atualizado com base em monitoramento contínuo e avaliações periódicas. Essas regras de boas práticas e governança devem ser publicadas e atualizadas periodicamente, podendo ser reconhecidas e divulgadas pela ANPD, que incentivará a adoção de padrões técnicos para facilitar o controle dos dados pelos titulares. privacidade (Brasil, 2018, Vainzof, 2019).

Com base no exposto e no artigo 50 da LGPD, a figura a seguir ilustra os requisitos mínimos para implementação de um PGP.

Figura 7. Requisitos mínimos para implementação de Programa de Governança em Privacidade

Fonte: Data Privacy Brasil, 2023.

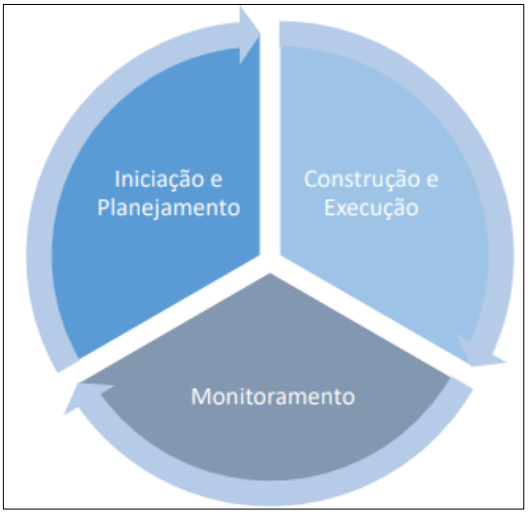
A implementação e a consolidação de um Programa de Governança em Privacidade (PGP) devem ser compatíveis com as necessidades da organização. Um programa desse tipo pode estabelecer as melhores práticas para o tratamento de dados pessoais, considerando o volume de operações, a escala e a estrutura da organização, bem como o risco de potenciais danos aos titulares. O objetivo de estruturar um programa de governança em privacidade e proteção de dados é definir padrões para as atividades que envolvem o uso de dados pessoais, documentá-los e possibilitar a verificação periódica da aderência das práticas organizacionais a esses padrões.

Um Programa de Privacidade é, pela própria definição de programa, um conjunto de medidas ou atividades relacionadas com um objetivo específico de longo prazo. A estrutura de um PGP orienta os profissionais de privacidade e proteção de dados atuarem com mais segurança no direcionamento da organização a adequação/conformidade com a legislação, e para além disso, contribuir para o bem comum. Essa estrutura deve levar em consideração todo normativo de proteção de dados vigente que incida sobre a operação da organização, e devendo incorporar a privacidade desde a concepção e por padrão (*Privacy by Design* e *Privacy by Default)* (Cabella, 2020).

O PGP deve ser visto como um processo dinâmico e permanente, que acompanhe as constantes mudanças dentro da organização, como o desenvolvimento de novos serviços e produtos, a modificação de processos internos, a contratação de novos colaboradores e a implementação de novas práticas. Somente através de um programa bem-estruturado e atualizado continuamente, a organização poderá assegurar a conformidade com a LGPD e proteger efetivamente os dados pessoais que trata (Davoli, Oliveira, Silva, 2020).

Nesse sentido, a Secretaria de Governo Digital (SGD), elaborou um framework que auxilia os órgãos e entidades do poder público na elaboração de um PGP. Trata-se de um modelo genérico de estrutura de PGP inspirada no Ciclo PDCA (Plan, Do, Check e Act). Além disso tem como base normas regulamentadoras como ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27005:2011, Código de Prática para Controles de Segurança da Informação e Gestão de riscos de segurança da informação (BRASIL, 2024).

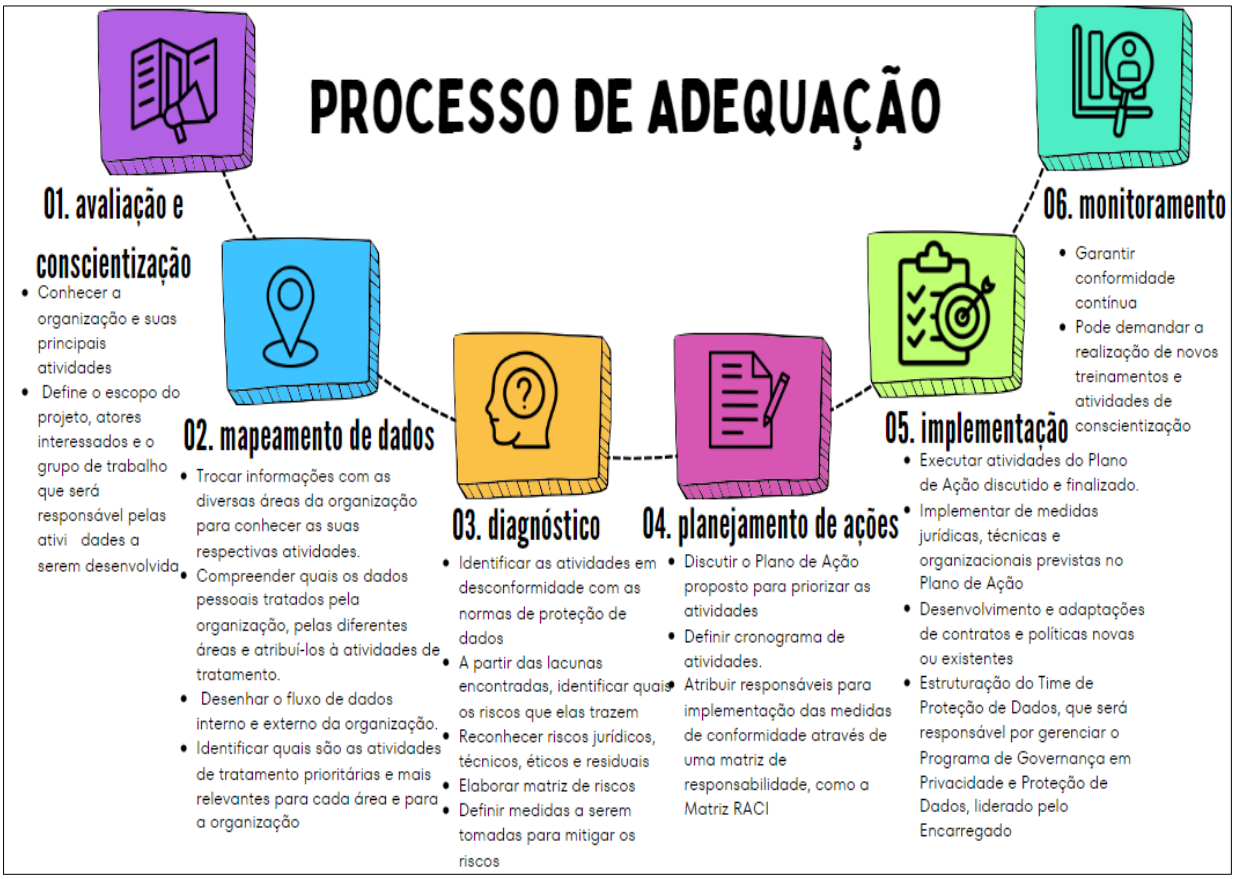
Figura 8. Modelo genérico de estrutura de PGP



Fonte: Brasil, 2024.

Para o desenvolvimento do PGP, é imprescindível a elaboração e implementação de um projeto de adequação. Entre as diferentes estruturas existentes, há o framework de plano de adequação à LGPD baseado na metodologia tradicional utilizado e difundido pelo Data Privacy Brasil. O modelo é composto por 6 (seis) fases no processo de adequação. São elas: (i) avaliação e conscientização; (ii) mapeamento de dados (data mapping); (iii) diagnóstico (gap analysis); (iv) planejamento de ações; (v) implementação do projeto e (vi) monitoramento. Cada fase está interligada à próxima, de modo que o desenvolvimento mais adequado, embora não exclusivo, das atividades de uma fase depende diretamente da conclusão ou maturidade das atividades das fases anteriores (Davoli, Oliveira, Silva, 2020; Halfeld, Guedes, 2022). A imagem a seguir sintetiza o modelo de plano de adequação como um processo.

Figura 9. As 6 fases do processo de adequação à LGPD



Fonte: Elaborado pelo autor, adaptado de Halfeld e Guedes, 2022.

Ressalta-se que independente da implementação de um PGP, todas as partes interessadas (titular, ANPD, organização, dirigente, servidor/funcionário e sociedade em geral) têm a responsabilidade por garantir a privacidade e proteção dos dados pessoais. Portanto, a implementação de boas práticas e de governança é fundamental para que todos, ou pelo menos a maioria, dos requisitos necessários à proteção dos dados pessoas sejam efetivados. Nesse aspecto, para alcançar uma boa governança, basicamente, depende da definição e da implantação de um modelo de governança adequado ao tamanho, complexidade, negócio e perfil de risco da organização.

Por fim, considerando as boas práticas e a governança, surge a necessidade de implementação de metodologias e ferramentas para consolidação de um PGP. Por isso, no próximo tópico será apresentado o *Framework* de Privacidade e Segurança da Informação.

2.3.2 *Framework* de Privacidade e Segurança da Informação - FPSI

Não há privacidade sem segurança da informação!

Brasil, 2024.

Diante dos muitos desafios para implementar a proteção de dados nos processos internos, levando em conta as especificidades de cada organização, é crucial adotar uma abordagem integrada que considere tanto as regulamentações recentes de proteção de dados quanto os instrumentos já existentes de segurança da informação. Isso inclui legislações internacionais, setoriais, normativas e padrões. Uma interpretação que harmonize e complemente essas regulamentações e instrumentos (como os princípios da Lei Geral de Proteção de Dados junto aos padrões e normas de segurança da informação) pode ajudar a estabelecer medidas práticas e eficazes para proteger informações e garantir a conformidade legal (França; Martins, 2024).

A instituições estão aprendendo que a gestão e o uso apropriado de dados são fundamentais para a proteção de dados. Os dados devem ser geridos de maneira adequada em todo o seu ciclo de vida incorporando as melhores práticas de proteção de dados (Brasil, 2024). Para isso, é fundamental que as instituições cumpram os regulamentos vigentes e adotem as melhores práticas de gestão de dados, privacidade e segurança da informação ao lidar com qualquer tipo de dado, seja pessoal ou não. Isso envolve a implementação de controles adequados de privacidade e segurança da informação, além da adoção de políticas de gestão de dados que garantam a coleta, armazenamento, uso e eliminação dos dados de forma ética e segura, sempre em conformidade com a legislação vigente (Brasil, 2024).

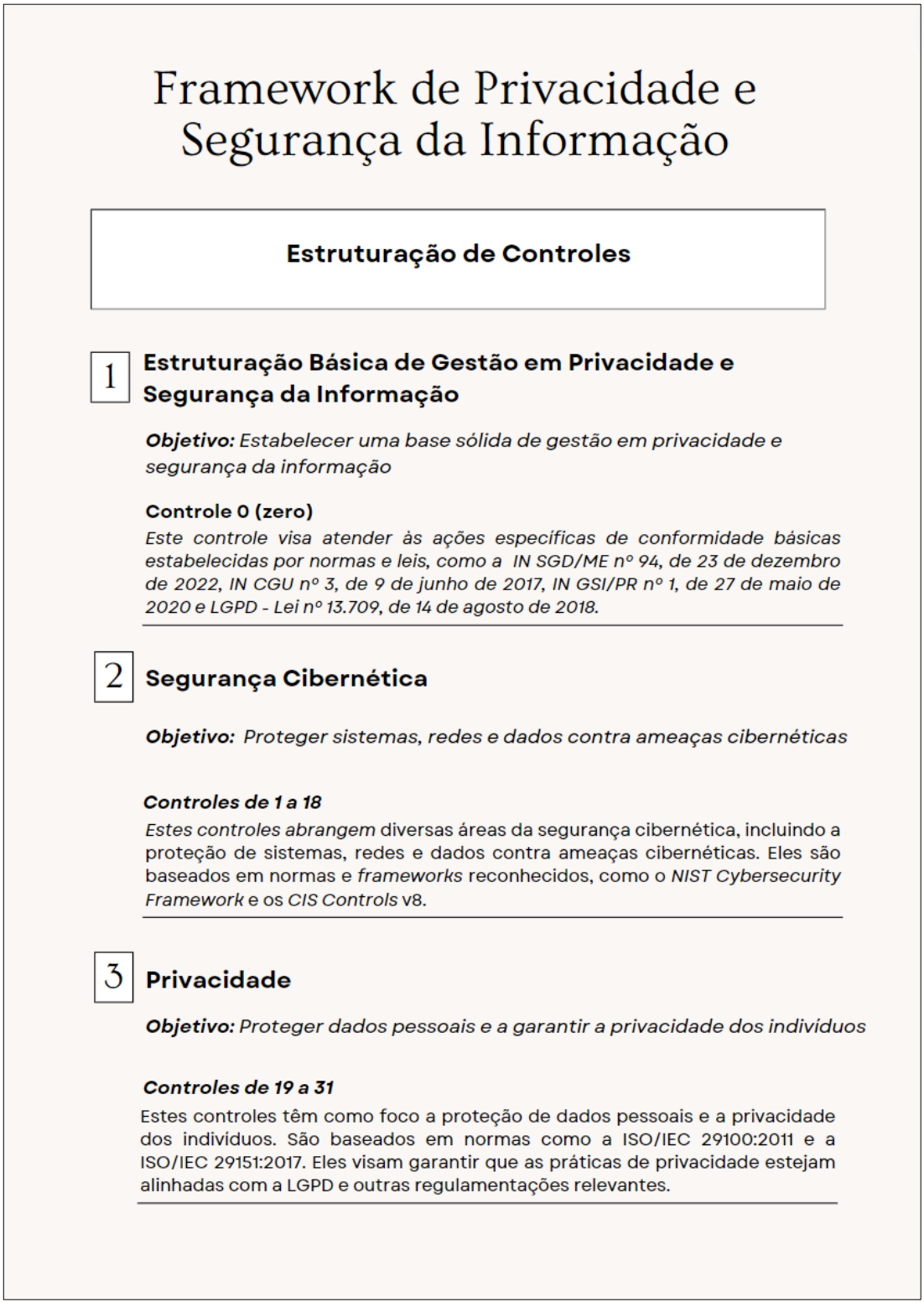
Para concretizar a governança e gestão da privacidade de dados e segurança da informação, as instituições podem lançar mão do uso de *frameworks* importantes que fornecem diretrizes e boas práticas que visam proteger informações sensíveis e garantir a conformidade com regulamentos. Nesse sentido, vale apresentar alguns *frameworks* de boas práticas já consolidados, como Normas ABNT NBR (16167); ISO/IEC 27000 *family standards* (27001, 27002, 27701, etc.); CIS *Critical Security Controls* v8; NIST *Cybersecurity Framework* (CSF); ISO/IEC 29000 *family standards* (29100, 29134, 29151, 29184, etc.); CIS *Controls Privacy Guide*; e NIST *Privacy Framework*. Essas ferramentas são essenciais para auxiliar a estruturação de um programa de governança e gestão de dados robusto e eficaz. Assim, além da proteção dos dados pessoais, a adoção destes documentos proporciona o cumprimento com regulamentações legais (Brasil, 2024).

Assim como outras intuições públicas, as IFES são destinatárias de projetos de proteção de dados pessoais e segurança da informação desenvolvidos pela Secretaria de Governo Digital (SGD). Assim, como desdobramento do Programa de Privacidade e Segurança da Informação

(PPSI) elaborado pela SGD, surge o *Framework* de Privacidade e Segurança da Informação (FPSI). A implementação pelas instituições da Administração Pública Federal (APF) é de caráter obrigatório, como estabelece a Portaria SGD/MGI nº 852, de 28 de março de 2023.

O objetivo do PPSI é aumentar a maturidade e resiliência das organizações públicas, promovendo as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos. Já o FPSI é consolida diversas obrigações, diretrizes e recomendações contidas em normas e boas práticas, com o objetivo de fomentar a privacidade e a segurança da informação nas instituições públicas (Brasil, 2024).

Figura 10. Estrutura básica do FPSI



Fonte: Elaborado pelo autor com base em Brasil, 2024.

Lançado em novembro de 2022, o referido *Framework* é inspirado, principalmente, na abordagem de controles e implementação do CIS, na estrutura central do *Privacy Framework* NIST e nas normas ISO/IEC e ABNT NBR. Segue regulamentos e documentos de referência

como LGPD, normativos do Gabinete de Segurança Institucional (GSI) e a Política Nacional de Segurança da Informação (PNSI). Ou seja, está alinhado às melhores práticas internacionais e aderente às orientações, normas e regulamentações em âmbito nacional. Neste documento, 32 controles foram estruturados. A imagem a seguir ilustra sua estrutura básica (Brasil, 2024).

A governança, gestão de privacidade e segurança da informação na Administração Pública Federal são fundamentadas em princípios e diretrizes essenciais para garantir a conformidade legal e a proteção de dados pessoais. Nesse sentido, o controle 0 (zero) 'Estruturação Básica de Gestão em Privacidade e Segurança da Informação' está alicerçada na política de governança da Administração Pública Federal (direta, autárquica e fundacional), conforme estipulado pelo Decreto nº 9.203/2017, que define governança pública como o conjunto de mecanismos de liderança, estratégia e controle utilizados para avaliar, direcionar e monitorar a gestão (Brasil, 2024).

Essa norma oferece diretrizes para a alta administração das organizações da APF, que deverão criar, manter, monitorar e melhorar sistemas de gestão de riscos e controles internos. Esses sistemas têm o objetivo de identificar, avaliar, tratar, monitorar e realizar análises críticas dos riscos que possam afetar a implementação da estratégia e o alcance dos objetivos da organização no cumprimento de sua missão institucional, seguindo os princípios estabelecidos no Decreto (Brasil, 2024).

Assim, a Estrutura Básica de Gestão em Privacidade e Segurança da Informação (controle 0 'zero' define os papéis fundamentais para a condução e implementação deste FPSI (Brasil, 2024). Em suma, essa estrutura consiste na definição de papéis relevantes para garantir o mínimo necessário à implantação de uma estrutura adequada de privacidade e segurança da informação, onde o PPSI possa ser implementado, ou seja, onde o referido documento possa ser aplicado. Na figura adiante, é possível verificar como se dá a governação no contexto do programa.

Figura 11. Papeis, responsabilidades e medidas do controle 0 (zero)

Fonte: Elaborado pelo autor com base em Brasil, 2024.

Como visto, além da Estrutura Básica de Gestão em Privacidade e Segurança da Informação, o FPSI é concebido para abranger todos os aspectos essenciais da segurança cibernética e da privacidade, garantindo que as organizações públicas possam implementar e manter práticas robustas e conformes com as regulamentações vigentes. Na figura seguinte é possível verificar as demais abordagens de controles e implantações de cibersegurança e privacidade.

Dado o contexto, os controles de cibersegurança utilizados do FPSI se baseiam no documento CIS, que reúne um conjunto de ações prioritárias que atuam conjuntamente na defesa de sistemas e infraestrutura de rede, utilizando controles que aplicam as melhores práticas para mitigar os tipos mais comuns de ataques cibernéticos. Ainda no contexto da cibersegurança, levando em conta os impactos na privacidade e proteção de dados pessoais tratados pela instituição, o guia complementar de privacidade se apresenta com objetivos de desenvolver as melhores práticas e orientações para a implementação dos CIS.

Figura 12. Abordagens e controles e implementações em cibersegurança e privacidade

Fonte: Elaborado pelo autor com base em Brasil, 2024.

Referente aos controles e implementações de privacidade, como de percebe, são essenciais para garantir a proteção dos dados pessoais e a privacidade dos indivíduos dentro das

organizações. Esses controles consistem, também, em um conjunto diretrizes, boas práticas, políticas e procedimentos que visam assegurar que o tratamento de dados pessoais seja realizado de maneira segura e em conformidade com os regulamentos aplicáveis.

Ainda, na figura a seguir é possível verificar os controles de cibersegurança de privacidade.

Figura 13. Controles de cibersegurança e privacidade do FPSI

Fonte: Elaborado pelo autor com base em brasil, 2024.

O PPSI reuniu as melhores práticas em segurança da informação e privacidade por meio do Framework de Privacidade e Segurança da Informação. Esse framework serve como uma

base estruturada para a implementação de controles de segurança da informação e de privacidade dentro das organizações.

Ele abrange diversas diretrizes e recomendações, como o uso de medidas técnicas para proteção de dados, a adoção de políticas claras de controle de acesso, a realização de auditorias periódicas, e o treinamento contínuo dos colaboradores sobre práticas de segurança e privacidade que podem verificadas nos anexos I, II, III, IV e V do FPSI (Brasil, 2024).

Importante ressaltar que, os controles e as medidas priorizadas pelo FPSI são avaliados pelo TCU. Portanto, ao estabelecer o PPSI e implementar este *framework*, as entidades públicas se beneficiam de uma estrutura robusta e sistematizada para identificar, acompanhar e preencher lacunas de privacidade e segurança da informação, por meio de controles, assegurando a conformidade legal e a proteção eficaz dos dados pessoais sob sua gestão.

Por fim, como visto na Figura 17, o FPSI estabelece o Controle 22: Políticas, Processos e Procedimentos, que tem como objetivo definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, tanto internos quanto externos, direcionados às ações de proteção de dados pessoais e privacidade. Esse controle é fundamental para garantir que a organização atenda aos requisitos legais estabelecidos pela LGPD, promovendo a conformidade contínua e mitigando riscos (Brasil, 2024).

A implementação dessas diretrizes proporciona um ambiente de governança estruturado, em que as obrigações legais são respeitadas e os direitos dos titulares de dados são resguardados. Além disso, a adoção de políticas bem definidas e atualizadas reflete o compromisso da instituição com a segurança da informação e a proteção dos dados, fortalecendo a confiança de todos os interessados e usuários nos processos organizacionais

No próximo tópico, serão discutidas em maior profundidade as políticas de proteção de dados como parte essencial desse processo de conformidade e governança, detalhando suas estruturas e aplicabilidade nas instituições públicas.

2.3.3 Tipos de políticas de governança para proteção de dados pessoais

Para Micheletti, Borges, Costa, (2022), as políticas são verdadeiros guias para provocar uma mudança de conduta necessária dentro da organização, possibilitando assim o surgimento de uma verdadeira cultura de proteção de dados pessoais, sobretudo se considerado também do ponto de vista da segurança da informação. Ou seja, as políticas são muito além de meros documentos de orientação.

Ressalta-se, contudo, que não há uma delimitação normativa de quais políticas são necessárias e suficientes para adequação à LGPD. Afinal, esse tipo de medida administrativa pode variar muito conforme o porte e a atividade da organização. Mesmo assim, a prática recomendada que existam ao menos uma política de privacidade e uma política de política de segurança da informação em todas as organizações (Teixeira; Stinghen, 2022).

Visando estar em *compliance* com a Lei, as organizações podem se atentar para algumas políticas importantes como:

> 1) a política de privacidade e proteção de dados;
> 2) a política de segurança da informação;
> 3) a política de backup;
> 4) a política de criptografia;
> 5) a política de senhas;
> 6) a política de registro de logs;
> 7) a política de cookies;
> 8) a política de acesso às instalações físicas da empresa; e
> 9) e a política e plano de resposta a incidentes de segurança.
> (Micheletti; Borges; Costa, 2022, p. 121).

Os autores supracitados afirmam ainda que as referidas políticas além facilitarem no processo de conformidade da organização à Lei, possibilitam uma pronta resposta na ocorrência de possíveis problemas no que tange a segurança da informação e a privacidade dos dados pessoais (Micheletti; Borges; Costa, 2022).

A política de proteção de dados é fundamental para deixar claro, tanto o mundo externo (política no site da empresa) quanto o mundo interno (política para funcionários e terceiros), quais são as diretrizes que a empresa utiliza para o tratamento de dados pessoais (IDESP, 2021).

Cots (2022) apregoa que é comum as organizações instituírem alguns tipos de políticas em prol da privacidade e proteção de dados pessoais tais como: política geral, política de privacidade, política de proteção de dados pessoais e política de segurança da informação. A política geral tem como objetivo declarar como a organização pretende atender aos requisitos da LGPD. A política de privacidade é direcionada ao público externo: titulares, a política de segurança da informação tem como objetivo estabelecer regras e controles e mecanismos de segurança em relação ao tratamento de dados pessoais. Já a política de proteção de dados pessoais é direcionada ao público interno: colaboradores, servidores e operadores.

Conforme orientação do Guia de Elaboração de Termos de Uso e Política de Privacidade para Serviços Públicos, o termo política de privacidade indicado na ABNT/NBR/ISO 29100:2011 se refere, frequentemente, às políticas de privacidade interna e externa à organização. “Numa política de privacidade interna são declarados os objetivos, regras,

obrigações, restrições e/ou controles que uma organização adota para satisfazer os requisitos de privacidade relacionados ao processamento de dados pessoais realizado" (Brasil, 2022, p. 34). Já uma política de privacidade externa exprime aos usuários externas à organização um aviso/comunicado sobre as práticas de privacidade adotadas, além de informações relevantes como: "a identidade e o contato do encarregado, como a informação coleta os dados, quais as operações de tratamento realizadas, por quanto tempo retém esses dados" (Brasil, 2022, p. 34).

> No contexto do Framework da ABNT/NBR/ISO 29100:2011, o termo 'política de privacidade' é usado para se referir à política de privacidade interna de uma organização, enquanto as políticas de privacidade externas são chamadas de avisos de privacidade. É importante notar que ambos os termos não estão presentes na LGPD e frequentemente são utilizados de forma intercambiável. No contexto deste documento, utiliza-se o termo política de privacidade para se referir à política externa, voltada ao titular dos dados pessoais. Porém, caso julgue mais adequado, o órgão ou entidade pode utilizar o termo aviso de privacidade (ABNT/NBR/ISO 29184:2021) para a política externa, principalmente quando já possui uma política de privacidade interna ou a esteja elaborando (Brasil, 2022, p. 34).

Em suma, no Guia de Elaboração de Termos de Uso e Política de Privacidade para Serviços Públicos o termo política de privacidade diz respeito à política de privacidade externa. Já a norma ABNT/NBR/ISO 29100:2011 utiliza o termo política de privacidade para se referir a política de privacidade interna. Uma vez que não há uma definição e diferenciação na LGPD, bem como orientação da ANPD acerca dos referidos termos, fica então a critério das organizações estabelecerem suas políticas e nomeando-as como melhor entenderem. Não obstante, é evidente que as nomenclaturas das políticas sugeridas por Cots (2022), pela ABNT/NBR/ISO 29100:2011 e pelo Guia de Elaboração de Termos de Uso e Política de Privacidade para Serviços Públicos podem auxiliar nessa diferenciação a fim de não gerar ainda mais confusão.

Dessa forma seguiremos as seguintes definições para fins desta pesquisa: A Política de privacidade será compreendida como política institucional direcionada ao público interna da organização (colaboradores, funcionários, servidores e outras partes interessadas), que poderá ser compreendida também como Política de proteção de dados. Já o aviso privacidade será compreendida como política institucional direcionada ao público externo da organização (usuários em geral e titulares de dados).

2.3.4 Política de segurança da informação

O aspecto mais importante da segurança da informação é a política de segurança. Em analogia, o autor Peltier (2005, p. 17) aduz que “Se a segurança da informação fosse uma pessoa, a política de segurança seria o sistema nervoso”. Para ele, a PSI é a base da segurança da informação, pois “providencia a estrutura e define os objetivos dos demais aspectos da segurança da informação”

De acordo com Fontes (2012, p.15),

> A política é o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. A política é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades. O principal documento da política indicará qual é a filosofia da organização para o uso da informação pelos seus funcionários, prestadores de serviço, estagiários, diretores, acionistas e até pelo executivo-presidente. As regras definidas valem para todos. E se o tratamento for diferente para tipos de usuários diferentes, esta definição deve estar formalizada na política e nos demais regulamentos de segurança da informação.

Em se tratando atendimento aos requisitos de boas práticas e governança estabelecidos pela LGPD, é fundamental que o controlador tenha uma PSI para que o processo de proteção da informação possa ser elaborado, implantado e mantido. “Esta política (ou conjunto de políticas) definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação” (Fontes, 2012, p. 7).

A necessidade de implementação da PSI é descrita na NBR ISO/IEC 27002:2005, onde:

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ABNT, 2005, p. 10).

Contudo, essa necessidade varia entre organizações com descreve a NBR ISO/IEC 27002:2013:

> Políticas internas são especialmente úteis em organizações maiores e mais complexas onde aqueles que definem e aprovam os níveis esperados de controle são segregados daqueles que implementam os controles, ou em situações onde uma política se aplica a muitas pessoas ou funções diferentes na organização. Políticas de segurança da informação podem ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados (ABNT, 2005, p.9).

De forma abrangente, a segurança da informação pode ser definida como “o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação” (Brasil, 2021, p. 5). Esse conjunto de ações impacta todo o ambiente institucional das empresas, com objetivo de prevenir, detectar e combater as ameaças digitais.

> A política de segurança da informação - PSI, consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização. [...] O propósito fundamental da PSI é ser uma ferramenta que apoie a implementação de um processo estruturado de segurança da informação adequado a cada organização,
> considerando seu negócio e seu porte (Brasil, 2021, p. 8).

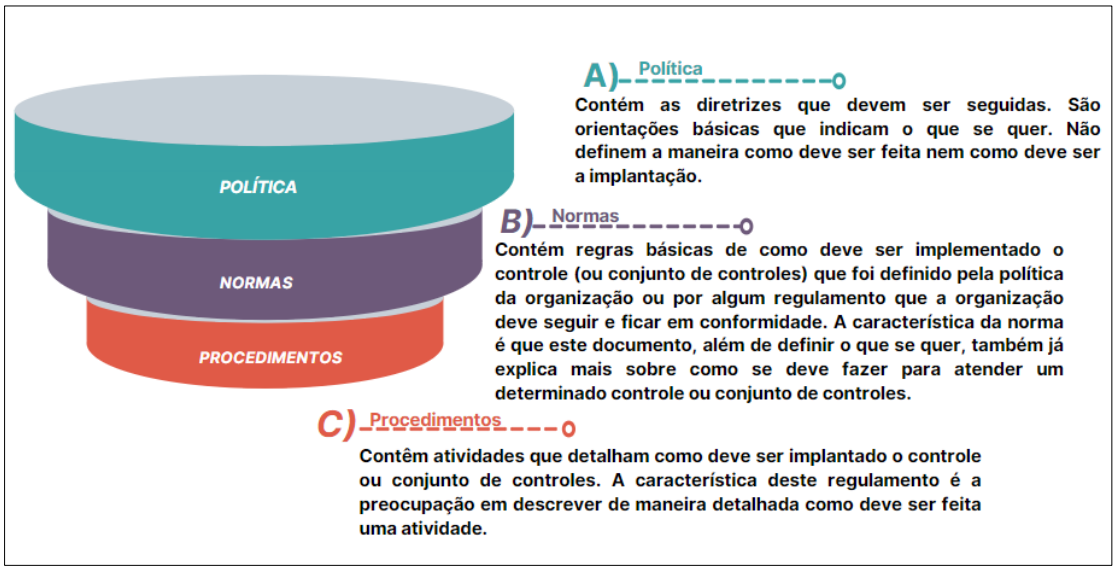
Mesmo não sendo obrigatória, a implementação de uma PSI pela LGPD, ela é incentivada pela ANPD, pois evidencia boa-fé e diligência na segurança dos dados pessoais sob sua custódia e fornecem as diretrizes para a gestão da segurança da informação. Autoridade sugere que na medida do possível, seja estabelecida uma política de segurança da informação pela organização, podendo ser, inclusive, simplificada, mas que seja prevista uma revisão periódica (Brasil, 2021, p. 8).

Sem o estabelecimento de uma política de segurança da informação, as organizações estarão ainda mais sujeitas aos riscos inerentes ao tratamento de dados pessoais. Nesse aspecto, Fontes adverte que

> a não implantação da política impede o desenvolvimento adequado da segurança da informação na organização, uma vez que faltarão referenciais para implantação dos controles. Sem a política não haverá a definição do escopo que delimita o campo de ação dos controles, e esta falta de limites fará com que o processo de segurança da informação seja infinito e nunca possa ser avaliado adequadamente.
> O risco de não existência da política deve ser minimizado e até eliminado. Para que isto aconteça é necessário implantar o conjunto de regulamentos, iniciando pela política principal (diretriz) que definirá o escopo e os limites da própria gestão de risco (2012, p.21).

Ainda, de acordo com Fontes (2012, p.77), o conjunto da PSI e dos demais regulamentos deve ter uma arquitetura que facilite a estruturação desses regulamentos. “Não existe uma estrutura rígida de separação dos tipos de orientações. Recomendo o seguinte nível de granularidade das regras transmitidas pelos regulamentos: a) Política, b) Norma e c) Procedimentos”. Nesse sentido, a figura a seguir apresenta uma síntese sobre cada regulamento.

Figura 14. Níveis de regulamentos

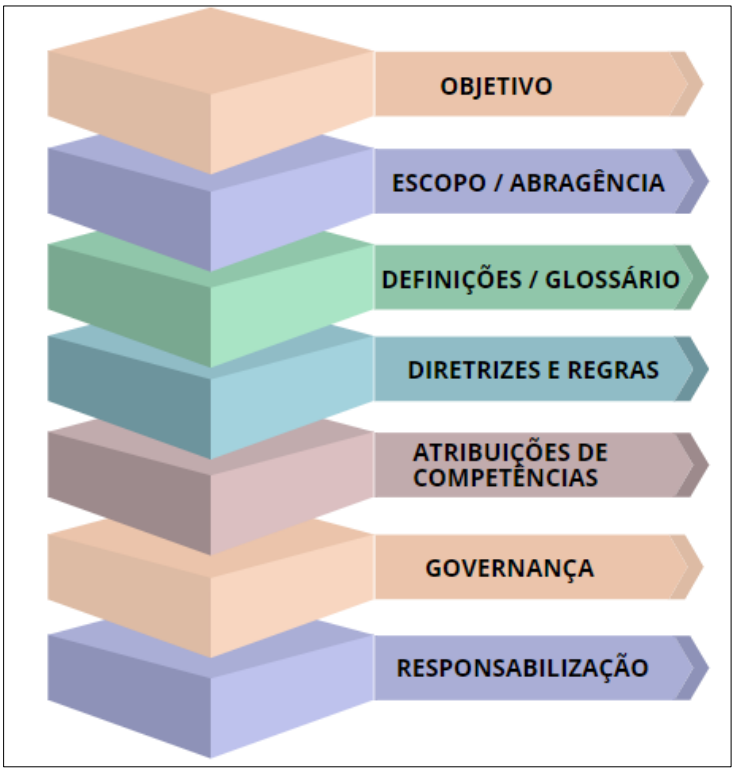


Fonte: Elaborado pelo autor com base em Fontes, 2012.

Além da implementação de uma PSI, das Normas e procedimentos, recomenda-se a elaboração de manual de boas práticas. Ressalta-se, que a diferença entre política e manual é que a primeira tem como aspectos: abrangente, caráter técnico e normativo. Já o segundo; é mais detalhado e linguagem mais acessível aos colaboradores, funcionários e servidores (Teixeira; Stinghen, 2022).

Sobre uma estrutura de PSI, Teixeira e Stinghen (2022) recomendam dividir o documento nos seguintes tópicos: objetivo; escopo (abrangência); definições básicas (glossário); diretrizes de segurança da informação, atribuições e competências. Além desses foram incluídos os tópicos governança e responsabilização com base em Fontes (2012) e no Decreto nº 9.203/17 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Nesse aspecto, tem-se um modelo básico de PSI com um conjunto elementos conforme se vê na figura a seguir.

Figura 15. Modelo básico de PSI



Fonte: Elaborado pelo autor com base em Fontes (2012), Teixeira; Stinghen (2022).

Importante mencionar que a estrutura não necessita seguir a mesma sequência disposta na imagem e que a empresa pode, de acordo com sua necessidade, incluir ou excluir elementos, mas, o autor Fontes enfatiza que uma organização que tenha uma PSI fraca, "pelas mais diversas razões, (cultura, ambiente interno, integridade dos executivos, momento, exigência de legislação) não quer proteger adequadamente a sua informação" (2012, p. 82). Assim, sem exceção, todas as organizações podem proteger adequadamente as informações das informações, sobretudo, os dados pessoais dos titulares.

2.3.5 Aviso de privacidade/Política de Privacidade

O aviso de privacidade é o documento informativo pelo qual a organização informa aos usuários e demais partes interessadas como efetua o tratamento de dados, qual a legitimidade desse tratamento e como os direitos dos titulares estão sendo respeitados (Teixeira; Stinghen, 2022). É comum em serviços online, nelas as organizações demonstram as regras sobre o uso dos dados pessoais coletados, estabelecendo um compromisso com o interagente. Para o

interagente do outro lado do computador, a política de privacidade se torna uma ferramenta que o auxilia a avaliar e decidir a forma com que seus dados são tratados (Siebra; Xavier, 2020).

Por meio de observação empírica em organizações que estão em conformidade com a LGPD, Teixeira e Stinghen (2022) mencionam que uma política de privacidade deve conter no mínimo:

a) conceitos e orientações básicas sobre direitos dos titulares;

b) a relação de dados tratado;

c) o tipo de tratamento realizado e a finalidade;

d) a legitimação do tratamento (bases legais);

e) a relação de agentes de tratamento com os quais os dados são compartilhados.

A LGPD determina que a organização a informe sobre realização de tratamento de dados pessoais. Para isso é importante que a organização disponibilize em seu site informações relacionadas à privacidade e proteção de dados pessoais, apresentando com detalhes quais dados são coletados, para qual finalidade, por quanto tempo será utilizado. Além disso, deve ser apresentando meios para que o titular possa se comunicar com o encarregado (DPO). O acesso ao aviso de privacidade, aos termos de uso, às políticas de cookies, com possibilidade de ajustes deve ser de facilitado. A linguagem deve ser simples e de fácil entendimento (Lima; Almeida; Maroso, 2020).

Corroborando, Siebra e Xavier (2020) afirmam que as políticas de privacidade devem estar disponibilizadas de forma a serem facilmente identificadas/localizadas ao usuário, possibilitando-o realizar a modificação de suas opções sempre que desejar. Devem estabelecer uma comunicação com o usuário de forma inteligível, para que ele compreenda as decisões que precisa tomar. A política deve conter, no mínimo, informações referentes ao tratamento de dados pessoais como: tipos de dados coletados, a forma de coleta, justificativa de atividade de coleta, a finalidade e o compartilhamento de dados com terceiros.

Sugere-se criar no site organização uma área específica para a LGPD, contendo informações sobre privacidade e proteção de dados. Pode ser, inclusive, uma aba, onde tudo poderá ser facilmente encontrado; onde deve constar todas as respostas que o titular possivelmente pode estar procurando (Lima; Almeida; Maroso, 2020).

2.3.6 Política de proteção de dados pessoais

Retomando ao que dispõe artigo 50, parágrafo 2º, inciso I, alínea (a) da LGPD, o controlador poderá implementar um PGP que no mínimo: “demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais” (Brasil, 2018). “Convém que a alta direção da organização envolvida no tratamento de dados pessoais estabeleça uma política de privacidade interna” (ABNT, 2020, p. 15). A formulação de políticas internas é então um dos meios para que aas organizações estejam em *compliance* com a Lei.

A Política de Proteção de Dados pessoais é um documento, com foco mais interno, que apresenta as medidas técnicas que os colaboradores e outras partes interessadas devem cumprir para que a organização garanta a proteção dos dados pessoais e a privacidade dos titulares (Lima; Alves, 2021). “Uma política de privacidade interna documenta os objetivos, regras, obrigações, restrições e/ou controles adotados por uma organização para atender aos requisitos de proteção de privacidade pertinentes para o tratamento de DP (ABNT, 2020, p. 15).

Ainda, é um regulamento institucional que define regras e diretrizes para o tratamento e a governança de dados pessoais dentro de uma organização. Estabelecer papéis e responsabilidades de forma clara e objetiva, definir diretrizes de tratamento e implementar meios para monitorar o cumprimento da política são processos essenciais para assegurar a privacidade e a proteção dos dados pessoais sob a guarda da organização (Brasil, 2023).

Esse tipo de política não pode ser confundido com o Código de conduta e ética, nem com o aviso de privacidade que deve estar no site da empresa e é voltada para o público externo. Aquela trará em seu escopo informações sobre como a organização tratará questões relacionadas à privacidade e à proteção de dados pessoais. Deve conter, inclusive, indicações de sanções para casos de infringência às regras (Lima; Almeida; Maroso, 2020).

As organizações poderão, por iniciativa própria, formular regras de boas práticas e de governança que estabeleçam as condições de organização, os padrões técnicos, as normas de segurança, canais de comunicações para reclamações e petições de titulares, os procedimentos para atendimento das obrigações específicas em relação ao tratamento de dados, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos levando em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento (Brasil, 2018; Vainzof, 2019). Tudo isso pode ser

orientado por meio de uma política interna de proteção de dados pessoais integrada a outras políticas como a de segurança da informação e de privacidade.

No processo de implementação de uma política de privacidade interna é importante que ela seja documentada por escrito; comunicada dentro da organização; apropriada ao objetivo da organização; esteja disponível para as partes interessadas, conforme apropriado; inclua um compromisso com a melhoria contínua; forneça a estrutura para a determinação de objetivos; inclua um compromisso em satisfazer os requisitos aplicáveis de salvaguarda da privacidade; que seja complementada por regras e obrigações; e contenha controles (por exemplo, controle de acesso, disposições de aviso, auditorias etc) (ABNT, 2020).

Conforme orienta Associação Brasileira de Normas Técnicas, convém à organização identificar e implementar controles de privacidade para atender aos requisitos de proteção de privacidade identificados pelo processo de avaliação e tratamento de risco de privacidade. Além disso,

> convém que os controles de privacidade identificados e implementados sejam documentados como parte da avaliação de risco de privacidade da organização. Certos tipos de tratamento de DP podem exigir controles específicos para os quais a necessidade só se torna aparente uma vez que um tratamento previsto tenha sido cuidadosamente analisado. Uma avaliação de risco de privacidade pode ajudar as organizações a identificar os riscos específicos de violação de privacidade envolvidos em uma operação planejada.[...] Convém que esforços sejam feitos pelas organizações para desenvolver os seus controles de privacidade como parte de uma abordagem geral de "*privacy by design*", isto é, convém que a *compliance* com privacidade seja levada em conta na fase de projeto dos sistemas de tratamento de DP, em vez de ser implementada em um estágio subsequente (ABNT, 2020, p. 15).

De acordo com a redação dada pelo art. 46, § 2o, da LGPD: "As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução." Isso é *privacy by design*, ou seja, a noção de que produtos e serviços precisam tomar a segurança e o sigilo de dados como um elemento a ser levado em conta em todas as suas fases de concepção, desenvolvimento, aplicação e avaliação.

Importante mencionar que antes de qualquer implementação de uma política institucional de proteção de dados, é fundamental realizar mapeamento de dados pessoais sob custódia da instituição. Para obter um mapeamento dos dados pessoais utilizados pelo órgão, recomenda-se a realização de um inventário de dados, especialmente dos dados pessoais. Conforme o Guia de Elaboração de Inventário de Dados Pessoais, o Inventário de Dados Pessoais (IDP) é um documento fundamental para registrar o tratamento de dados pessoais realizado pela instituição, conforme o disposto no art. 37 da LGPD. O inventário é uma

ferramenta eficaz para avaliar como o órgão ou entidade lida com os dados pessoais, identificando quais dados são tratados, onde estão localizados e quais operações são realizadas com eles (Brasil, 2020).

Geralmente, esse registro mantido pelo Inventário envolve a descrição das informações em relação ao tratamento de dados pessoais realizado pela instituição como atores envolvidos (agentes de tratamento e o encarregado); finalidade (como a instituição utiliza os dados pessoais); hipótese (conforme os artigos 7º e 11 da LGPD); base legal; dados pessoais tratados pela instituição; categorias dos titulares dos dados pessoais; período de retenção dos dados pessoais; instituições com as quais os dados pessoais são compartilhados; transferência internacional de dados (art. 33 da LGPD); e medidas de segurança atualmente em vigor (Brasil, 2021).

O IDP é essencial para a governança de dados pessoais e serve como base para avaliar o impacto na proteção desses dados, a fim de verificar se a instituição está em conformidade com os requisitos estabelecidos pela LGPD. O mapeamento de dados deve ser um trabalho multidisciplinar. Ou seja, realizado em conjunto com vários atores e departamentos da instituição, com ajuda técnica e jurídica para análise das possíveis vulnerabilidades e riscos que sejam encontradas (Brasil, 2021).

O Ministério da Gestão e da Inovação em Serviços Públicos (MGI), através da Secretaria de Governo Digital (SGD), desenvolveu e disponibilizou um modelo de PPDP com o objetivo de fornecer diretrizes que auxiliem os órgãos e entidades na criação de suas Políticas de Proteção de Dados Pessoais no contexto institucional. O MGI, órgão da administração direta, é responsável por implementar reformas na máquina pública e promover a eficiência governamental (Brasil, 2023).

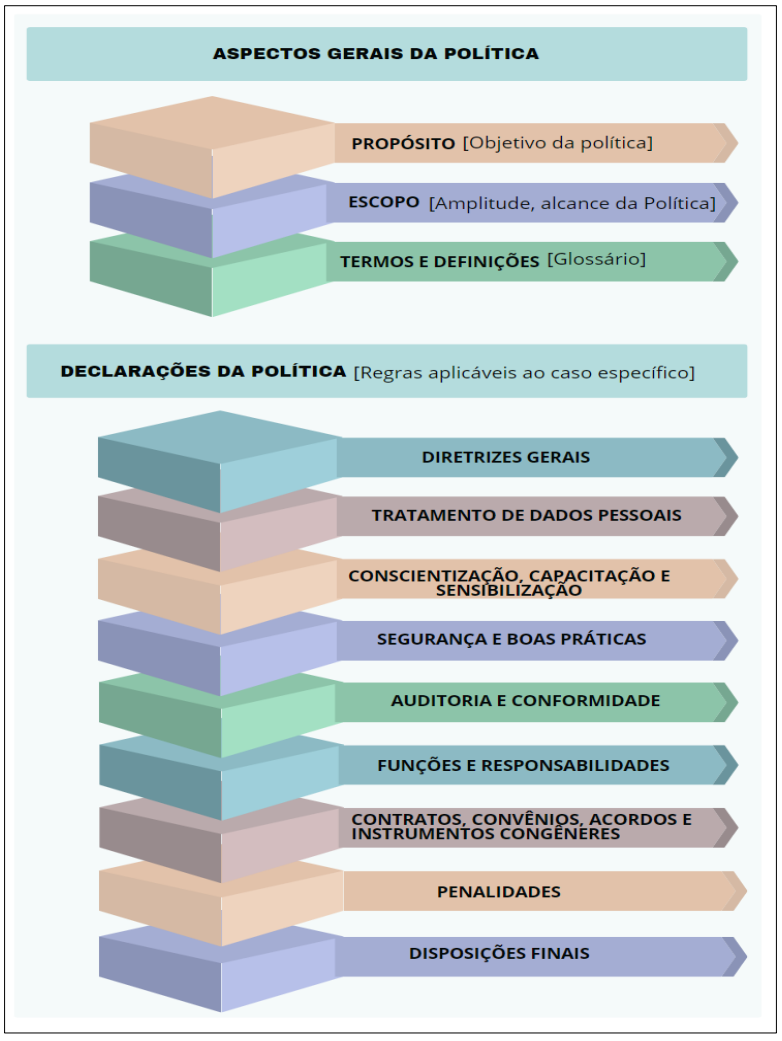
Esse Modelo, especialmente recomendado para os órgãos e entidades da Administração Pública Federal (APF), tem como finalidade apoiar a elaboração da Política de Proteção de Dados Pessoais, conforme estabelecido no art. 50 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD exige que a Administração Pública, ao prestar diversos serviços que envolvem o tratamento de dados pessoais, formule regras de boas práticas e de governança, estabelecendo as condições de organização, funcionamento, procedimentos para reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas para os envolvidos no tratamento, ações educativas, mecanismos internos de supervisão, mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Além de atender à LGPD, a elaboração da Política de Proteção de Dados Pessoais busca cumprir outros regulamentos vigentes sobre

privacidade e proteção de dados. Este documento baseia-se no Guia do Framework de Privacidade e Segurança da Informação, que faz referência a diversas publicações e documentos técnicos amplamente utilizados por profissionais da área de privacidade e segurança da informação, como as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST) (Brasil, 2023).

Dado o contexto, genericamente o modelo dispõe da estrutura como se vê na figura a seguir.

Figura 16. Estrutura genérica do modelo de PPDP do SGD/MGI



Fonte. Elaborado pelo autor com base em Brasil, 2023.

Importa mencionar o modelo ora apresentado é genérico. Então as instituições devem considerar as particularidades técnicas especificas do seu contexto organizacional a fim de implementar uma política que seja adequada a sua realidade.

3 PROCEDIMENTOS METODOLÓGICOS

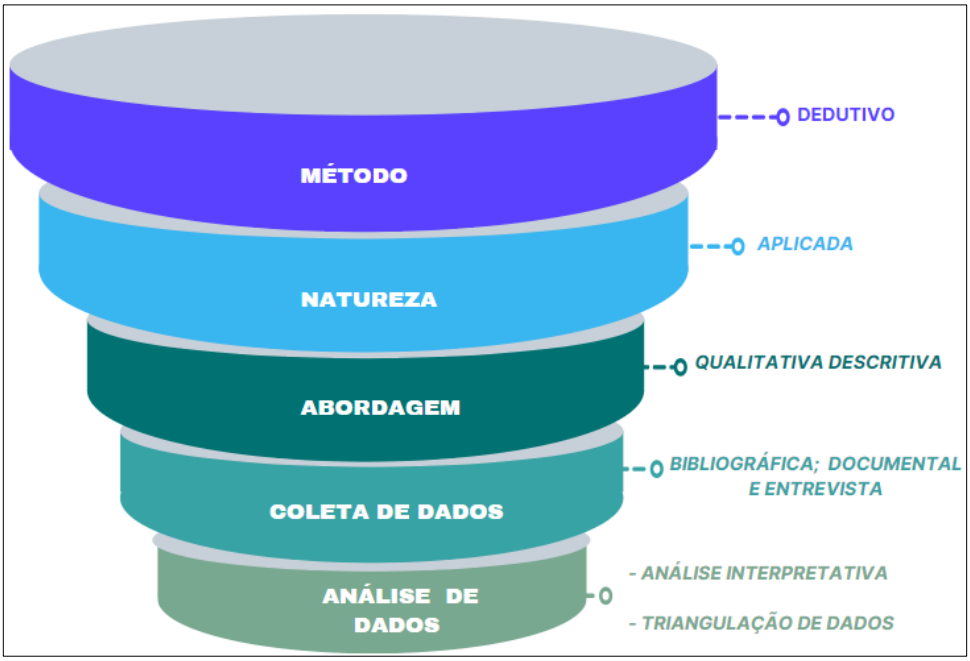
Neste capítulo, aborda-se os aspectos metodológicos que serão utilizados no estudo para atender ao problema de pesquisa bem como ao objetivo proposto. Será abordado a caracterização da pesquisa, permeando o método, objetivo, abordagem, coleta de dados e análise de dados.

3.1 CARACTERIZAÇÃO DA PESQUISA

Toda pesquisa resulta de levantamento de dados de fontes diversas, indiferente do método ou técnicas aplicadas. Esse material-fonte geral é necessário para de obter conhecimentos que servem de *back-ground* ao campo de interesse, bem como para "evitar possíveis duplicações e/ou esforços desnecessários; pode, ainda, sugerir problemas e hipóteses e orientar para outras fontes de coleta" (Marconi; Lakatos, 2003, p. 174).

Com o objetivo esclarecer os procedimentos a serem adotados, foi realizado um delineamento da pesquisa que parte do aspecto mais amplo ao mais específico. Para isso, foi elaborado uma representação gráfica inspirada no modelo *research onion* criado por Saunders, Lewis e Thornhill (2016) como se vê na figura a seguir.

Figura 17. Delineamento da pesquisa



Fonte: Elaborado pelo autor adaptado de Saunders; Lewis; Thornhill (2016).

O **método** se caracteriza por uma abordagem mais ampla, em nível de abstração mais elevado, dos fenômenos da natureza e da sociedade é, portanto, denominado método de abordagem, que engloba o indutivo, o dedutivo, o hipotético-dedutivo e o dialético" (Marconi; Lakatos, 2003, p. 221). No raciocínio dedutivo, o pesquisador parte do mais geral para o mais específico. Neste sentido, a abordagem dedutiva é considerada uma abordagem de cima para baixo, pois a conclusão deve surgir logicamente da premissa (Saunders; Lewis; Thornhill, 2016).

Neste aspecto, quanto ao método, esta pesquisa classifica-se como dedutiva, visto que, por meio de instrumentos de coleta de dados, o pesquisador irá identificar as possibilidades e limitações de propor diretrizes para implementação de uma política institucional de proteção de dados pessoais em publicas instituições de educação superior.

Quanto à **natureza** da pesquisa, classifica-se como aplicada, pois objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos (Gil, 2008). Neste aspecto, o pesquisador pretende propor diretrizes para implementação de política institucional de proteção de dados pessoais em instituições de educação superior, bem como elaborar um projeto (minuta) de política institucional para IFES (Instituições Federais de Educação Superior). Corroborando, a pesquisa aplicada tem finalidade prática orientada para a resolução de problemas concretos (Vergara, 2013).

Quanto a **abordagem**, esta pesquisa classifica-se como qualitativa, pois busca aprofundar o conhecimento acerca de políticas de proteção de dados pessoais sob o viés subjetivo. A pesquisa qualitativa fundamenta-se em dados coligidos nas interações interpessoais, na coparticipação das situações dos informantes, analisadas a partir da significação que estes dão aos seus atos (Chizzotti, 2010). Ainda, a pesquisa qualitativa visa avaliar e aprimorar um plano ou programa a partir de sua efetividade, leva em consideração o ambiente e o contexto, exercendo influência sobre as pessoas que realizam ações em função do seu ponto de vista sobre o ambiente (Roesch, 2010). Nesse sentido, o pesquisador participa, compreende e interpreta.

A pesquisa fundamentada na fenomenologia é essencialmente descritiva. Como as descrições dos fenômenos estão repletas dos significados que o ambiente lhes atribui e são produto de uma visão subjetiva, ela rejeita qualquer forma de expressão quantitativa. Assim, a interpretação dos resultados emerge da totalidade de uma reflexão baseada na percepção de um fenômeno dentro de um contexto. Por essa razão, essa interpretação não é vazia, mas sim coerente, lógica e consistente (Triviños, 1987).

Dado esse contexto em relação a abordagem qualitativa, a classificação descritiva torna-se fundamental na exposição de características de determinado fenômeno estabelecendo relações entre variáveis por meio da utilização de técnicas padronizadas de coleta de informações (Vergara, 2016; Gil, 2008).

3.2 SUJEITOS DA PESQUISA

Conforme o objetivo deste estudo (propor diretrizes para implantação de uma política proteção de dados pessoais IFES). Foram selecionadas as instituições federais de ensino superior que já implementaram uma política institucional de proteção de dados pessoais.

Todos os participantes desta pesquisa são servidores públicos, ocupante de cargos efetivos em Instituições Federais de Ensino Superior que exercem, por meio de designação, a função de Encarregados de tratamento de dados conforme estabelece o artigo 5º e 41 da LGPD em suas respectivas instituições. Tais encarregados foram também incumbidos de elaborar e implementar a política de proteção de dados pessoais nas instituições selecionadas.

Os critérios utilizados para a seleção das instituições foram os seguintes:

1º filtro – Selecionar dentre as universidades públicas federais, as que possuem governança em privacidade e proteção de dados. Para isso, foi extraída do site do Ministério da Educação a relação de todas as universidades públicas federais. Obteve-se uma lista com o total de 69 universidades. Porém, 2 universidades não foram encontradas na Plataforma Fala.BR, restando apenas 67 universidades que foram contactadas. Dessas; 63 responderam.

Buscou-se verificar e selecionar, dentre essas 63 instituições, as que já possuíam os três tipos de políticas: Política de Proteção de Dados Pessoais (PPDP), Aviso de Privacidade (AP) ou Política de Privacidade (PP) e Política de Segurança da Informação (PSI). Assim verificou-se que apenas que somente 13 (treze) possuem as referidas políticas.

2º filtro - Das 13 (treze) universidades, foram excluídas aquelas que elaboraram suas Políticas de Proteção de Dados Pessoais (PPDPs) e Políticas de Privacidade ou Aviso de privacidade (PPs/APs) no mesmo documento, ou seja, uma política única. Resultou que somente 7 (sete) universidades atendem a esses critérios.

3 º filtro – Dessas 7 (sete) universidades, 1 (uma) foi excluída por ter elaborado a Política de Proteção de Dados Pessoais (PPDP) e a Política de Segurança da Informação (PSI) no mesmo documento. Assim, chegou-se ao número de 6 universidades federais.

4 º filtro – Com o objetivo de contemplar as especificidades dos Institutos Federais (IFs), foram selecionados, aleatoriamente, 2 institutos contemplados com os três tipos de políticas (PPDP, PP ou AP e PSI).

Por fim, das 6 (seis) universidades, não houve resposta de 3 (três), bem como houve negativa de participação de 2 (dois) gestores por conta de problemas relacionados aos seus fluxos internos de trabalho. Assim, restou apenas 1 (uma) universidade. Neste sentido, as instituições participantes selecionadas são 1 universidade e 2 institutos federais.

3.3 TÉCNICA DE COLETA DE DADOS

Tendo em vista classificação da abordagem desta pesquisa, a coleta e a análise de dados foram realizadas concomitantemente:

> o processo de pesquisa qualitativa não admite visões isoladas, parceladas, estanques. Ela se desenvolve em interação dinâmica retroalimentando-se, reformulando-se constantemente, de maneira que, por exemplo, a Coleta de Dados num instante deixa de ser tal e é Análise de dados, e esta em seguida, é veículo para nova busca de informações (Triviños, 1987, p. 137).

Em relação aos procedimentos técnicos, a presente pesquisa classifica-se como bibliográfica, documental e de levantamento possibilitando a investigação de elementos que possibilitem a compreensão do fenômeno pesquisado (Gil, 2008). A pesquisa bibliográfica e documental foi constituída, principalmente, de livros, trabalhos acadêmicos e artigos de periódicos, bem como de documentos institucionais, verificando-se as contribuições de diversos autores.

> A pesquisa bibliográfica, ou de fontes secundarias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros pesquisas monografias, teses[...]até meios orais: rádio, gravações em fita magnética e audiovisuais: filmes e televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritas por alguma forma, querem publicadas, quer gravadas (Marconi; Lakatos, 2003, p. 183).

Ressalta-se ainda que “a pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras” (Marconi; Lakatos, 2003, p. 183). Portanto, em se tratando da pesquisa bibliográfica, as principais fontes a serem utilizadas serão livros,

trabalhos acadêmicos (monografias, dissertações e teses), artigos de periódicos, jornais e revistas verificando-se as contribuições de diversos autores.

A característica da pesquisa documental é que a fonte de coleta de dados está restrita a documentos, constituindo-se como fontes primárias. As fontes de documentos podem ser arquivos públicos, arquivos particulares e fontes estatísticas. Por fim os documentos podem ser escritos ou não (Marconi; Lakatos, 2003). Nesse aspecto, a pesquisa documental neste estudo foi constituída por arquivos públicos disponíveis em sites governamentais como notícias, reportagens, seminários, fóruns, projetos de leis, leis, decretos, regimentos, estatutos, ofícios, portarias, instruções normativas, programas, planos e relatórios, políticas institucionais de Proteção de dados e guias de boas práticas em proteção de dados pessoais de órgãos governamentais.

A pesquisa de levantamento foi realizada por meio de uma entrevista semiestruturada junto aos encarregados de dados de IFES que já implementaram uma política institucional de proteção de dados identificadas como boas práticas para esse estudo. Essa técnica parte de "questionamentos básicos, apoiados em teorias e hipóteses, que interessam à pesquisa, e que, em seguida oferecem amplo campo de interrogativas, fruto de novas hipóteses que vão surgindo à medida que se recebem as respostas do informante" (Triviños, 1987, P. 146). Ainda conforme o autor, a entrevista semiestruturada pode ser entendida como um conjunto básico de perguntas que aponta fundamentalmente para a medula que preocupa o investigador, é, portanto, uma das ferramentas que se utiliza na pesquisa qualitativa para alcançar seus objetivos (Triviños, 2001). No quadro a seguir é possível verificar a relação entre os objetivos propostos neste estudo e a coleta e análise dos dados.

Quadro 6. Objetivos específicos X Técnica de coleta

Objetivos específicos	**Coleta de dados**
a) Verificar diretrizes e práticas de proteção de dados pessoais;	bibliográfica e documental
b) Identificar processos de elaboração e implementação de política de proteção de dados;	bibliográfica, documental e entrevista semiestruturada
c) Elaborar minuta de política de proteção de dados para IFES.	Triangulação de dados

Fonte: Elaborado pelo autor

As entrevistas foram realizadas no formato remoto por meio da plataforma de videoconferência TEAMS da Microsoft. O instrumento de coleta de informações: Roteiro de Entrevista – Encarregados, encontra-se no Apêndice A. A coleta foi realizada no período de agosto a setembro de 2023 posteriormente a aprovação pelo Comitê de Ética em Pesquisa com Seres Humanos (CEPSH-UFSC), por meio do parecer nº 6.306.892. Antes da aplicação do instrumento de coleta de dados, foram solicitadas a anuência dos sujeitos participantes por meio do Termo de Consentimento Livre e Esclarecido, conforme Apêndice B – Entrevista.

Os participantes da pesquisa, tiveram suas identidades preservadas e suas falas foram mencionadas a partir dos pseudônimos: Skynet, Fornet e Cybernet. As instituições participantes também tiveram seus nomes pseudonimizados visando garantir a preservação dos entrevistados. Assim receberam os seguintes pseudônimos: **Inst.1, Inst.2** e **Inst.3**. Coube, nesse aspecto, apenas relacionar os entrevistados às suas respectivas instituições: Skynet/**Inst.1;** Fortnet/ **Inst.2** e Cybernet/**Inst.3**.

Por fim, visando cumprir o objetivo específico "c" (Elaborar minuta de política de proteção de dados para IFES), o pesquisador aplicou a triangulação de dados como técnica. A "triangulação de dados consiste em usar diferentes fontes de dados, sem usar métodos distintos. Neste caso, os dados são coletados em momentos, locais ou com pessoas diferentes" (Zappellini; Feuerschütte, 2005, p. 247). O próximo tópico apresenta a análise e interpretação dos dados coletados.

3.4 TÉCNICA DE ANÁLISE E INTERPRETAÇÃO DOS DADOS COLETADOS

Após a coleta e a manipulação dos dados e obtenção dos resultados, os próximos passos são analisá-los e interpretá-los com base no núcleo central da pesquisa. Assim, mesmo a análise e a interpretação se mostrando como atividades distintas, elas são estreitamente relacionadas. A "análise (ou explicação) é a tentativa de evidenciar as relações existentes entre o fenômeno estudado e outros fatores". A interpretação é a "atividade intelectual que procura dar um significado mais amplo às respostas, vinculando-as a outros conhecimentos. Em geral a interpretação significa a exposição do verdadeiro significado do material apresentado, em relação aos objetivos propostos e ao tema" (Marconi; Lakatos, 2003, p.167).

Nesse aspecto, para a realização da análise e interpretação de dados, foi utilizada nessa pesquisa a técnica de triangulação de dados. A triangulação "tem por objetivo básico abranger

a máxima amplitude na descrição, explicação e compreensão do foco em estudo" (Triviños, 1987, p.138).

> Por ser a Coleta de Dados e a Análise de Dados uma etapa no processo de pesquisa qualitativa, ou duas fases que retroalimentam constantemente, só didaticamente podemos falar, em forma separada, deste tríplice enfoque no estudo de um fenômeno social. Isto quer dizer que qualquer ideia do sujeito, documento etc. é imediatamente descrita, explicada e compreendida, à medida que isso seja possível, na perspectiva da técnica de triangulação" (Triviños, 1987, p.139).

A análise interpretativa, baseia-se "em três aspectos fundamentais: a) nos resultados alcançados no estudo (respostas aos instrumentos, ideias dos documentos etc.); b) na fundamentação teórica (manejo dos conceitos-chaves das teorias e de outros pontos de vista); c) na experiência pessoal do investigador" (Triviños,1987, p. 173).

4 ANÁLISE E INTERPRETAÇÃO DOS DADOS COLETADOS

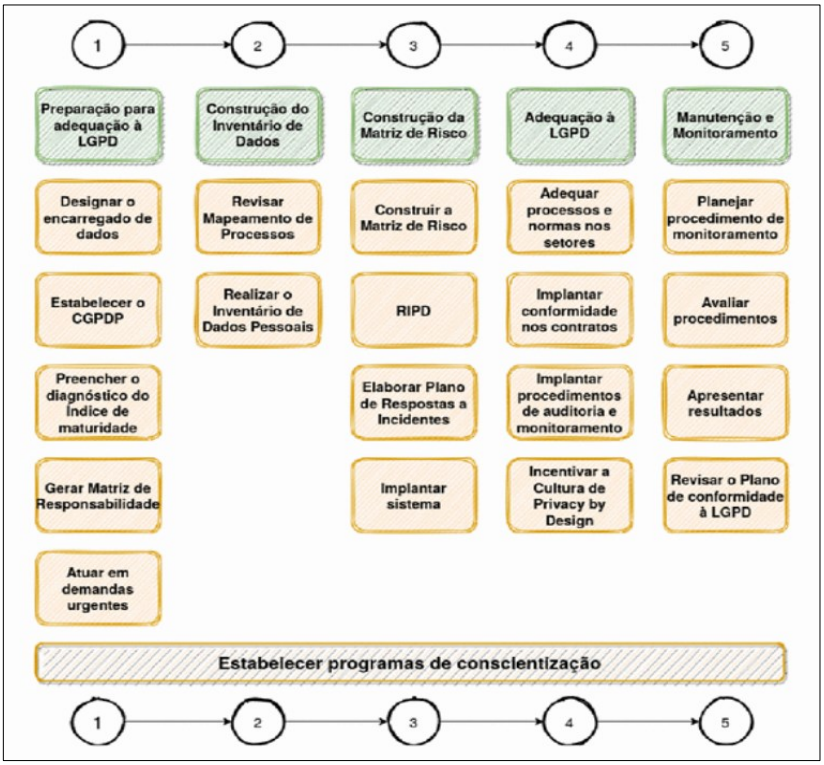
Este capítulo apresenta uma análise detalhada dos dados coletados durante a pesquisa, organizada em três partes principais: a verificação das diretrizes e práticas de proteção de dados pessoais empregadas nas instituições analisadas; a identificação dos processos de elaboração e implementação da política de proteção de dados; e a elaboração de um modelo de minuta de política de proteção de dados para as IFES.

4.1 DIRETRIZES E PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS DAS IFES

Para a concretização do objetivo deste tópico, as diretrizes e práticas de proteção de dados adotadas pelas IFES participantes serão apresentadas e comparadas às melhores práticas identificadas no referencial teórico.

Primeiramente, a **Inst.1** apresentou um Plano de Conformidade à LGPD estruturado em cinco etapas, abrangendo desde a preparação inicial até a fase de monitoramento contínuo. Uma das características marcantes é a presença de programas de conscientização em todas as etapas, evidenciando o foco na mudança cultural e no envolvimento dos colaboradores. Além disso, a instituição criou um Comitê Gestor de Proteção de Dados Pessoais e designou tanto um encarregado quanto um gestor de Segurança da Informação, responsáveis pela execução das diretrizes. A instituição também implementou uma Política de Proteção de Dados Pessoais e uma Política de Segurança da Informação, além de outras ferramentas práticas, como boletins e dicas de segurança. A inclusão de canais de atendimento para titulares de dados demonstra a preocupação com a transparência. Contudo, algumas etapas, como a implantação do *Privacy by Design* e o plano de respostas a incidentes, ainda estão em fase de implementação, sugerindo a necessidade de melhorias.

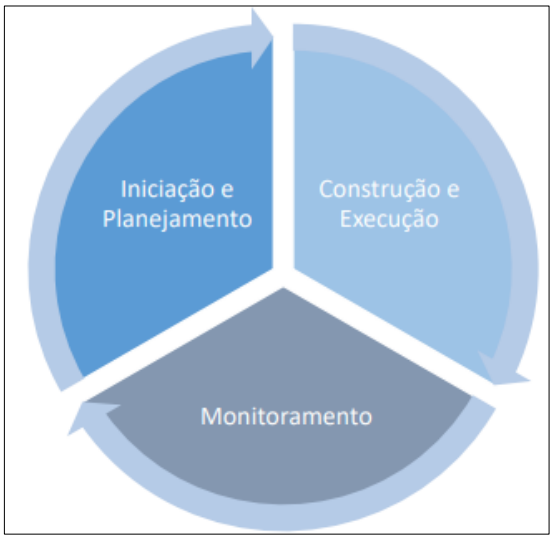
Figura 18. Etapas e medidas do Plano de Conformidade à LGP da Instituição 1



Fonte: Inst.1, 2024.

A **Inst.2** desenvolveu um Programa de Governança em Privacidade (PGP), baseado no Guia de Elaboração de Programa de Governança em Privacidade do Ministério da Economia, com adaptações à sua realidade institucional. O programa está dividido em três etapas: iniciação e planejamento, construção e execução, e monitoramento. Assim como na primeira instituição, houve a criação de um Comitê Gestor de Proteção de Dados Pessoais e a designação de um encarregado e de um gestor de Segurança da Informação. A instituição também implementou uma Política de Proteção de Dados Pessoais e uma Política de Segurança da Informação, além de medidas robustas como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). O programa se destaca por seu foco na capacitação contínua dos colaboradores e na implementação de indicadores de desempenho e gestão de incidentes, o que contribui para a governança eficiente de dados.

Figura 19. Etapas do PGP da Instituição 2



Fonte: Brasil, 2024.

A **Inst.3** adotou um Plano de Conformidade dividido em várias etapas, desde a criação de grupos de trabalho temáticos até o monitoramento e conformidade contínua. Assim como nas outras instituições, foi criado um Comitê Gestor de Proteção de Dados Pessoais, e foram designados tanto um Encarregado quanto um gestor de Segurança da Informação. A instituição também implementou uma Política de Proteção de Dados Pessoais e uma Política de Segurança da Informação, além de outras políticas, como a Política de Classificação e a Política de Cookies. A estratégia de mobilização e conscientização contínua, com workshops e até gamificação para testar o conhecimento sobre a LGPD, reflete um compromisso educacional significativo.

Figura 20. Etapas do Plano de Conformidade da Instituição 3

Fonte: **Inst.3**, 2024.

A partir da análise das práticas adotadas pelas instituições públicas para se adequarem à Lei Geral de Proteção de Dados (LGPD), é possível identificar um esforço considerável no cumprimento das exigências legais. Observa-se que o processo de conformidade foi iniciado no final de 2020 e no início de 2021, logo após a promulgação da lei. Nesse contexto, as instituições contaram com poucos recursos estruturados à disposição além da própria legislação, apoiando-se, sobretudo, em práticas de benchmarking e no Programa de Governança em Privacidade (PGP), lançado pelo Ministério da Economia por meio da Secretaria de Governos Digital (SGD).

Entretanto, em 2023, com a reorganização da governança voltada para a transformação digital, a SGD foi estrategicamente realocada para o Ministério da Gestão e da Inovação em Serviços Públicos (MGI). Esse órgão foi estabelecido com o objetivo de fortalecer a política de transformação digital do governo federal e aumentar a interação sobre o assunto com todos os entes federativos (Brasil, 2024).

Com isso, houve um avanço significativo na padronização e no suporte oferecido às instituições públicas. Como já visto, a SGD desenvolveu o Programa de Privacidade e Segurança da Informação (PPSI), seguido pelo Framework de Privacidade e Segurança da Informação (FPSI), que detalha e orienta o cumprimento dos requisitos de privacidade e segurança de dados. Esses novos instrumentos trouxeram uma abordagem mais robusta e alinhada com as melhores práticas globais, oferecendo diretrizes claras para que as instituições públicas alcancem a plena conformidade com a LGPD.

Embora o progresso até o momento tenha sido significativo, com a implementação de comitês gestores de proteção de dados, políticas de proteção e segurança da informação, além da designação de encarregados e gestores de segurança, ainda há um caminho a ser percorrido. As políticas existentes nas instituições analisadas indicam um avanço na cultura de proteção de dados, mas a adoção integral do PPSI e do FPSI ainda não é uma realidade para nenhuma delas.

Recomenda-se, portanto, que as instituições públicas sigam a estrutura do PPSI e implementem as medidas de controle e monitoramento previstas no FPSI. Esse alinhamento proporcionará uma abordagem mais coordenada e eficiente para a gestão de riscos relacionados à privacidade e segurança de dados pessoais, reforçando a conformidade com a LGPD e garantindo maior proteção aos direitos dos titulares de dados. Além disso, ao adotar essas diretrizes, as instituições estarão mais preparadas para enfrentar os desafios decorrentes do tratamento de dados em um cenário de crescente digitalização e exposição a riscos cibernéticos.

4.2 PROCESSOS DE ELABORAÇÃO E IMPLENTAÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS PESSSOAIS NAS IFES

Com o intuito de sistematizar o processo analítico na identificação dos processos de elaboração e implementação da política de proteção de dados, essa etapa foi estrategicamente dividida em duas fases distintas: o processo de elaboração e o processo de implementação propriamente dito. Para a fundamentação da análise da primeira etapa, foram considerados os seguintes fatores: a estrutura básica para a elaboração da política; as metodologias e ferramentas empregadas; os desafios enfrentados durante o processo de elaboração; e os elementos constituintes e o conteúdo da política. Quanto à segunda etapa, os fatores de análise considerados foram: a estrutura básica para a implementação; as metodologias e ferramentas utilizadas; e os desafios encontrados no processo de implementação.

Essa abordagem bifásica permite uma compreensão mais aprofundada e sistemática dos processos envolvidos na criação e execução da PPDP, fornecendo uma base sólida para as discussões e proposições de melhorias.

4.2.1 Etapa 1 - Processo de elaboração

Primeiramente, ressalta-se que a criação de estrutura mínima para a elaboração e implementação de uma política institucional de proteção de dados pessoais é crucial por vários motivos como: conformidade legal (*compliance*), definição de papéis e responsabilidades, coerência e uniformidade na implementação, gestão de riscos e fomento à cultura de privacidade. Essa estrutura serve como uma base organizacional e operacional para garantir que todos os aspectos relacionados à proteção de dados sejam abordados de maneira eficaz e conforme a legislação vigente.

Para Vainzof (2019), as organizações têm a autonomia para elaborar regras de boas práticas e governança, definindo condições de organização, padrões técnicos, normas de segurança, canais de comunicação para reclamações e petições de titulares, além de procedimentos para cumprimento de obrigações específicas no tratamento de dados e ações educativas. Entretanto, a construção de estruturas bem definidas e indivíduos com habilidades adequadas são importantes para garantir a eficiência, eficácia e efetividade num projeto ou programa. É crucial que essas estruturas sejam capazes de promover melhorias no desempenho e minimizar disfunções típicas da burocracia no setor público (Brasil, 2018).

Em se tratando das instituições analisadas, é possível verificar que cada uma delas criou uma estrutura mínima em formato de grupo de trabalho (GT) para iniciar o processo de adequação da instituição à LGPD e criar uma política de proteção de dados pessoais. No caso em tela, vale ressaltar que os GTs têm um prazo determinado para alcançar seus objetivos, não sendo, portanto, uma estrutura permanente.

No quadro a seguir é possível verificar como cada uma instituição criou a estrutura e a composição para elaboração da PPDP.

Quadro 7. Estrutura básica para elaboração da PPDP

ORGANIZAÇÃO		
Instituições	**Estrutura**	**Composição do GT**
Inst.1	Grupo de Trabalho	1 (um) Encarregado - presidente do GT -; 1 (um) representante do Gabinete da Reitoria; 1 (um) representante da Ouvidoria; 1 (um) representante da Diretoria de Gestão de Pessoas; 1 (um) representante da Coordenação Geral de Comunicação e Marketing;1 (um) representante da Comissão Permanente de Avaliação de Documentos Sigilosos;1 (um) representante do Setor de Contratos;1 (um) representante da Diretoria de Tecnologia da Informação;1 (um) representante de cada Pró-reitoria de Administração;1 (um) representante de cada Pró-reitoria de Desenvolvimento Institucional;1 (um) representante de cada Pró-reitoria de Extensão;1 (um) representante de cada Pró-reitoria de Pesquisa, Pós-Graduação e Inovação;
Inst.2	Grupo de Trabalho	1 (um) representante da Engenharia de Sistemas e Tecnologia da Informação (presidente do GT); 2 (dois) representantes da Ouvidoria- 2 (dois) representantes da Tecnologia da Informação; 2 (dois) representantes da Diretoria de Gestão de Pessoas; 1 (um) representante da Biblioteca; 1 (um) representante do Setor de Compras e Contratos; 1 (um) representante da Pró-reitoria de Administração; 1 (um) representante da Pró-reitoria de Pesquisa, Pós-graduação; 1 (um) representante da Pró-reitoria de Graduação; 1 (um) representante da Pró-reitoria de Extensão; 1 (um) um representante de campus fora de sede.
Inst.3	Grupo de Trabalho	1 (um) Encarregado - presidente do GT -; 1 (um) representante do Gabinete da Reitoria;1 (um) representante da Ouvidoria;3 (três) representantes de EAD; 4 (quatro) representantes da Diretoria Executiva; 2 (dois) representantes da Tecnologia da Informação; 2 (dois) representantes da Pró-Reitoria de Planejamento e Desenvolvimento Institucional;1 (um) representante da Biblioteca; 1 (um) representante do Setor de Compras e Contratos; 2 (dois) representantes da Pró-reitoria de Ensino; 1 (um)

		representante da Pró-reitoria de Pesquisa, Pós-graduação e Inovação; 2 (dois) representantes de campus fora de sede.

Fonte: Elaborado pelo autor com base nas Inst.1, Inst.2 e Inst.3, 2024.

Na fase de elaboração da política, recomenda-se que o trabalho seja multidisciplinar. Ou seja, realizado em conjunto com vários atores e departamentos da instituição, com ajuda técnica e jurídica para análise das possíveis vulnerabilidades e riscos que sejam encontradas (Brasil, 2021). Conforme análise. todas as instituições seguiram essa estratégia.

Na **Inst.1,** a composição do GT incluiu representantes de áreas críticas como a Reitoria, Ouvidoria, Tecnologia da Informação, Gestão de Pessoas, e vários outros departamentos relacionados à administração e à pesquisa. Essa diversidade permite uma abordagem integrada que cobre tanto os aspectos técnicos quanto os operacionais e administrativos do tratamento de dados pessoais. Já na **Inst.2**, verifica-se uma forte presença de representantes de Tecnologia da Informação, o que reflete uma ênfase na segurança cibernética e na infraestrutura tecnológica. A inclusão de representantes da Ouvidoria, Biblioteca, e outros setores administrativos também destaca a intenção de incluir vozes que lidam diretamente com o público e com a gestão de informação. Por último, na **Inst.3**, observa-se uma abordagem inclusiva, pelo grande número de representantes da Educação a Distância (EAD), o que pode indicar uma ênfase em garantir que as políticas de proteção de dados sejam também aplicáveis em contextos digitais na área fim.

A formação dos GTs com membros de áreas como a Reitoria, Comunicação, Gestão de Pessoas, e Segurança da Informação é indicativa de um enfoque multidisciplinar necessário para a elaboração de uma política de proteção de dados eficaz. Essa composição diversificada assegura que todas as dimensões da proteção de dados pessoais, desde o cumprimento legal até as questões de segurança técnica e a comunicação com os titulares dos dados, sejam adequadamente consideradas. Ainda, essa diversidade é fundamental, pois assegura que múltiplas perspectivas e conhecimentos especializados sejam incorporados no processo de elaboração, permitindo que a política resultante atenda de forma eficaz às necessidades específicas de cada setor e às particularidades envolvidas no tratamento de dados dentro da instituição.

Sobre a liderança, em todas as instituições, esse papel é assumido por cargos de alta responsabilidade, como o Encarregado pelo Tratamento de Dados Pessoais ou representantes de alto nível de Tecnologia da Informação. Isso é crucial porque demonstra o comprometimento da alta administração com a proteção de dados, o que é um fator determinante para o sucesso na implementação de políticas de privacidade.

Nas instituições analisadas diversas etapas foram identificadas, além de metodologias e fermentações específicas conforme se apresenta no quadro a seguir.

Quadro 8. Etapas, metodologias e ferramentas utilizadas na elaboração da PPDP

ORGANIZAÇÃO		
Instituições	**Etapas de elaboração**	**Metodologia e ferramentas**
Inst.1	1 - Diagnóstico institucional (análise do ambiente interno); 2 - Elaboração da minuta de PPDP; 3 - Análise do Conselho de Governança Digital; 4 - Aprovação do Conselho Superior (órgão máximo); e 5 – Publicação da política	Diagnóstico institucional; *benchmarking*; PDCA e 5W2H
Inst.2	1 - Elaboração da minuta de PPDP; 2 - Análise do Comitê de Compatibilização dos Regimentos e Normas; 3 - Análise da Procuradoria; e 4 - Aprovação do Conselho Superior (órgão máximo); e 5 – Publicação da política.	*Benchmarking*.
Inst.3	1 - Diagnóstico institucional (análise do ambiente interno e externo); 2 - Elaboração da minuta de PPDP; 3 - Análise Comitê de Governança Digital; 4 - Aprovação do Conselho Superior (órgão máximo); e 5 - Publicação da política.	Diagnóstico institucional; SWOT (FOFA); *benchmarking*; PDCA; 5W2H, Metodologia Ágil e Power BI (Excel).

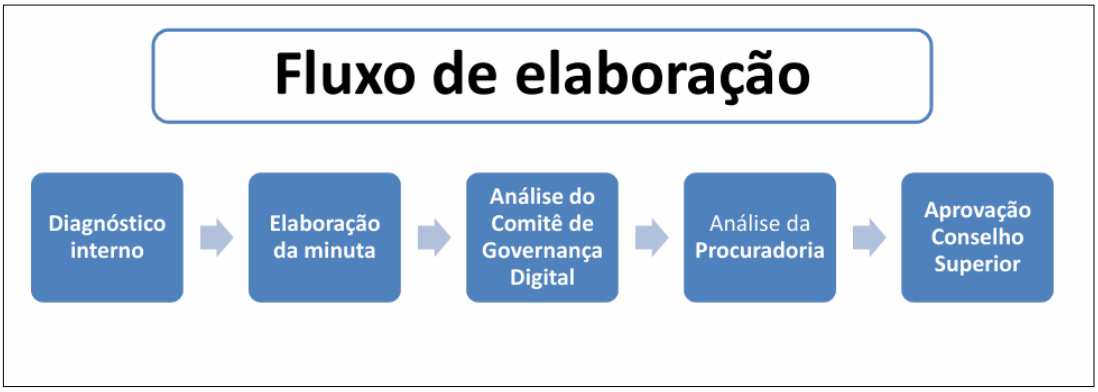
Fonte: Elaborado pelo autor com base em Inst.1, Inst.2 e Inst.3, 2024.

Uma análise comparativa evidencia que as etapas de elaboração da PPDP nas três instituições apresentam semelhanças, especialmente nas fases de elaboração da minuta, análise e aprovação do conselho superior. No entanto, as instituições diferem em suas abordagens iniciais e nas metodologias utilizadas. A **Inst.1** e a **Inst.3** realizaram diagnósticos institucionais, enquanto a **Inst.2** focou na análise de compatibilidade normativa.

Visando otimizar o processo, integrando boas práticas observadas nas três instituições e ampliando a abrangência para atender às realidades de IFES com estruturas menores. A inclusão do diagnóstico institucional logo no início é essencial para compreender o ambiente e

as vulnerabilidades existentes, como nas Inst. 1 e Inst. 3, garantindo que a política seja moldada à realidade interna. A análise pela Procuradoria, ausente nos fluxos de duas instituições, fortalece a conformidade jurídica do processo. Esse elemento traz maior robustez ao processo, garantindo que a política seja compatível com o arcabouço legal. Uma nova proposta otimizada no fluxo de elaboração figura seguinte.

Figura 21. Proposta de fluxo do processo de elaboração de PPDP



Fonte: Elaborado pelo autor

Essa proposta se solidifica ao integrar os diagnósticos, a governança e a análise jurídica, equilibrando a eficiência e a necessidade de adaptação. O diferencial aqui é a flexibilidade para instituições com menos recursos, garantindo que a estrutura enxuta não comprometa a qualidade do processo de implementação. A criação de um fluxo padronizado, com flexibilidade para ajustes locais, pode ajudar na harmonização das práticas entre as IFES.

Sobre as metodologias, a **Inst.1** e a **Inst3**. utilizaram fermentações como PDCA e 5W2H, enquanto a **Inst.2** se concentrou apenas no benchmarking.

> Uma das primeiras etapas, antes de qualquer coisa, antes de plano de ação, antes de tudo, foi a gente fazer um diagnóstico como que estava a implementação da lei dentro da nossa instituição, qual que era a maturidade tanto dos servidores como do sistema, então a gente fez esse diagnóstico para poder elaborar a política (Skynet/**Inst.1** , 00:00:58).
> Nós usamos análise SWOT, no início, para analisar as ameaças, as oportunidades e o 5W2H no planejamento, junto com o PDCA (Cybernet/**Inst.3**, 00:16:15).

Nessa seara, as metodologias e ferramentas mais utilizadas durante o processo de elaboração são o PDCA, 5W2H e Análise SWOT com destaque para o *benchmarking* que foi adotada com unanimidade na constituição dos elementos e conteúdo da PPDP. No quadro a seguir demonstra os elementos das PPDP.

Quadro 9. Elementos das Políticas de Proteção de Dados da IFES

Instituição	Elementos da PPDP
Inst.1	objetivos, abrangência, princípios, conceitos e definições, bases legais para tratamento da dados pessoais, tratamento de dados pessoais, compartilhamento de dados pessoais, destinatários e figuras legais (controlador, encarregado, comitê gestor de proteção de dados pessoais), direito do titular, plano de conformidade às leis de proteção de dados, segurança e violação de dados, fiscalização e descumprimento e disposições finais.
Inst.2	objetivos, público-alvo, princípios, definições, funções e reponsabilidades, tratamento de dados pessoais, direitos do titular de dados, avaliação de impacto à proteção de dados pessoais, comitê gestor, disposições finais.
Inst.3	Objetivos, abrangência, princípios, conceitos e definições, hipóteses autorizativas de tratamento de dados pessoais, tratamento de dados pessoais, compartilhamento dos dados pessoais, transferência internacional de dados pessoais, destinatários e figuras legais (controlador, operador, encarregado e comitê gestor de proteção de dados), direito do titular, segurança e violação de dados, fiscalização e descumprimento e disposições finais.

Fonte: Elaborado pelo autor com base nas Inst.1, Inst.2 e Inst.3, 2024.

Outro aspecto analisado foi a identificação dos possíveis desafios enfrentados durante a elaboração da PPDP. Embora a maioria dos entrevistados não tenha fornecido detalhes específicos sobre erros ou falhas cometidos nesse processo, alguns pontos importantes puderam ser destacados: a dificuldade de participação ativa de alguns membros da equipe, que se mostraram menos engajados e colaborativos; a necessidade de entender profundamente a realidade da instituição e seus processos internos para garantir a eficácia da política; e a falta de dedicação exclusiva dos membros da equipe ao tema de proteção de dados, o que compromete o desenvolvimento das ações.

> Na elaboração, acho que a maior dificuldade talvez tenha sido a participação de alguns membros mesmo. A gente sabe que tem um ou outro que é mais ativo que colabora um pouco mais, mas quando a gente trata de comissão e comitê que envolve muitas pessoas, muitos (não colaboram) (Fortnet/**Inst.2**, 00:20:12).

Cybernet/**Inst.3** menciona que durante o processo de implementação da política de proteção de dados, é natural que ocorram erros e que seja necessário ajustar a estrutura conforme a implementação avança. A dedicação integral de uma equipe para lidar com a proteção de dados surge como uma grande dificuldade. Além disso, um erro identificado durante o processo de elaboração da política de proteção de dados foi o gasto excessivo de tempo na escolha de uma ferramenta para coletar informações das unidades, sem chegar a uma solução adequada que se encaixasse na estrutura da instituição. Cita ainda que mesmo uma

equipe sem experiência prévia na área e à ausência de uma estrutura consolidada, foram tanto desafiadoras quanto dificultosas, porém todas as tentativas eram consideradas válidas (tentativa erro e acerto).

Conforme relataram os entrevistados, foi possível inferir, também, que os principais desafios enfrentados incluíram a falta de conhecimento de LGPD (pela recenticidade da lei) e outras legislações relacionadas a proteção de dados pessoais, e a compreensão da realidade institucional.

Com o objetivo otimizar os recursos no processo de elaboração seguem algumas considerações e sugestões: instituir um comitê gestor desde o início do processo ao invés de um grupo de trabalho temporário. Um comitê permanente garante a continuidade e retenção do conhecimento acumulado durante todo o processo de elaboração da Política PPDP, evitando a perda de informações críticas e experiências adquiridas.

É fundamental reconhecer a importância do benchmarking como uma metodologia crucial, especialmente para instituições que estão começando esse processo. O benchmarking permite avaliar práticas e padrões adotados por outras organizações e adaptar essas melhores práticas às necessidades específicas da instituição.

No entanto, é importante não descartar outras ferramentas metodológicas valiosas que podem complementar e enriquecer o processo. O PDCA oferece uma abordagem estruturada para o planejamento, execução e melhoria contínua das ações relacionadas à PPDP. A Análise SWOT é útil para identificar pontos fortes, fracos, oportunidades e ameaças, ajudando a desenvolver estratégias eficazes e a mitigar riscos. Já o 5W2H auxilia no planejamento detalhado e na definição de responsabilidades, garantindo clareza e organização.

Portanto, embora o benchmarking seja essencial para identificar e adaptar práticas de sucesso, a integração de metodologias como PDCA, SWOT e 5W2H proporcionará uma abordagem mais robusta e completa na elaboração e implementação da PPDP. Essa combinação garantirá um planejamento bem-informado, uma execução eficaz e uma gestão contínua da política, adaptada às especificidades da instituição e às melhores práticas do mercado.

4.2.2 Etapa 2 - Processo de implementação

Inicialmente, é importante destacar que as políticas são postas em prática pela governança e pela gestão, refletindo tanto a intenção quanto a ação (Heidemann; Salm, 2014).

A política compreende não apenas sua formulação, mas também etapas posteriores, como a implementação, execução e avaliação (Souza, 2006)

A governança de proteção de dados pessoais, por meio do Comitê de Privacidade e Proteção de Dados Pessoais, é fundamental para garantir que uma organização gerencie os dados pessoais em conformidade com as regulamentações. O comitê deve composto por membros de diversas áreas, como segurança da informação, jurídica, compliance, tecnologia da informação e outras áreas estratégicas, garantindo uma abordagem multidisciplinar na gestão da privacidade e proteção de dados (Brasil, 2024).

A instituição do comitê é uma medida adotada para garantir uma estrutura mínima de governança dos dados dentro da instituição e para assegurar a efetiva implementação da política de proteção de dados. Entre outras atribuições do comitê, auxiliar o encarregado nas atividades relacionadas à privacidade e proteção de dados se destaca (Brasil, 2024)

Assim como no processo de criação/elaboração, no processo de implementação da PPDP, todas as instituições instituíram um Comitê Gestor de Proteção de Dados.

> O GT foi extinguido. Ele entregou os trabalhos com a minuta. Então, fez um relatório, entregou a minuta, que era a atribuição do GT. Com a instituição da resolução, foi criado o comitê. E esse comitê tem essa tarefa de implementação (Cybernet/**Inst.3**, 00:28:24).
>
> A gente considerou isso também, a criação de um comitê gestor permanente ligado ali à proteção de dados pessoais, então a gente prevê nessa política que tem que ter um comitê permanente para auxiliar o encarregado na implementação da lei, prever também na política um plano de conformidade

A estruturação do Time de Proteção de Dados (Comitê) é responsável por gerenciar a implementação e deve ser liderado pelo Encarregado. Ressaltando que, geralmente, esse time é diferente do Time de Projeto (Equipe de elaboração ou Grupo de Trabalho) (Halfeld, Guedes, 2022).

A composição, atribuições e competências dos comitês das **Inst.1** e **Inst.3** foram estabelecidas por meio das suas políticas de proteção de dados. Na **Inst.2**, a criação do comitê foi apenas prevista na política de proteção de dados, sendo que sua composição, atribuições e competências são estabelecidas pelo Regimento da Administração Central.

Ainda sobre a composição e as competências dos comitês, as três instituições mostram uma abordagem robusta e alinhada às melhores práticas de governança de dados, com ênfase na conformidade legal e na criação de uma cultura institucional de proteção de dados. Todas as instituições têm estruturas que permitem tanto a revisão contínua quanto a atualização das políticas de proteção de dados pessoais, adaptando-se às mudanças na legislação e às necessidades específicas de cada instituição. A **Inst.2** se destaca por incluir atribuições que

promovem a cooperação interinstitucional e a resposta a incidentes, o que pode ser considerado uma prática avançada para a gestão de privacidade e segurança da informação.

A estrutura e as competências dos Comitês de Proteção de Dados Pessoais nas três instituições demonstram princípios sólidos de governança e gestão. A governança, neste contexto, refere-se ao conjunto de mecanismos, processos, e relações pelas quais as instituições são dirigidas e controladas, assegurando que as políticas de proteção de dados sejam implementadas em conformidade com a legislação vigente. Ressalta-se que:

> A estruturação básica de gestão em privacidade e segurança da informação tem bases na política de governança da APF direta, autárquica e fundacional estabelecida no Decreto nº 9.203, de 22 de novembro de 2017, que define governança pública como o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade, bem como apresenta o conceito de gestão de riscos como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (Brasil, 2024, p.19)

Cada instituição teve sua forma de estruturar o comitê de proteção de dados, refletindo suas próprias prioridades organizacionais e o contexto em que operam. Portanto, todas elas demonstram um compromisso significativo com a proteção de dados e a privacidade, integrando múltiplas perspectivas e áreas funcionais para alcançar uma abordagem abrangente e aderente.

Para a seleção dos membros dos comitês, todas as instituições aproveitaram algumas pessoas que haviam participado do grupo de trabalho (GT). Vale destacar que, em alguns casos, os membros dos comitês foram indicados pelos gestores das unidades envolvidas, como as pró-reitorias, por exemplo. Isso evidencia a importância de envolver diferentes áreas e assegurar a representatividade de todos os setores relevantes na implementação da política de proteção de dados. No quadro a seguir, é possível observar a composição do comitê e a representação dos setores chave por meio de seus integrantes.

Quadro 10. Estrutura básica para implementação da PPDP

Instituições	Estrutura	Composição dos comitês
Inst.1	Comitê Gestor de Proteção de dados	1 (um) Encarregado pelo Tratamento dos Dados Pessoais (presidente); 1 (um) representante da Diretoria de Gestão de Pessoas; 1 (um) representante da Coordenação-geral de Comunicação Social e *Marketing;* 1 (um) representante da Comissão Permanente de Avaliação de Documentos Sigilosos; 1 (um) representante do Gabinete da Reitoria; 1 (um) representante da Pró-Reitoria de Ensino; 1 (um) representante do Arquivo Central; 1 (um) Gestor da Segurança da Informação; 1 (um) Gestor do Serviço de Informação ao Cidadão (SIC).
Inst.2	Comitê gestor de Proteção de Dados	Encarregado (presidente); 1 (um) representante da Reitoria; 1 (um) representante da ouvidoria; 3 (três) representantes da Diretoria de Tecnologia da Informação; 1 (um) representante da Pró-Reitoria de Administração; 3 (três) representantes da Pró-Reitoria de Gestão de Pessoas; 2 (dois) representantes da Pró-Reitoria de Graduação; 1 (um) representante da Pró-Reitoria de Pesquisa e Pós-Graduação; 1 (um) Representante da Pró-Reitoria de Extensão; 1 (um) representantes da Diretoria do Campus fora de sede 1; 2 (dois) representantes das Unidades Acadêmicas (campus fora de sede 1); 1 (um) representante das Unidades Acadêmicas (campus fora de sede 2).
Inst.3	Comitê gestor de Proteção de Dados	1 (um) Encarregado e Gestor do Serviço de Informação ao Cidadão (SIC); 1 (um) representante da Governança e Gestão de Riscos; 1 (um) representante do Gabinete; 1 (um) representante da Pró-Reitoria de Planejamento e Desenvolvimento Institucional e Diretoria de Tecnologia da Informação e Comunicação; 1 (um) representante da Pró-reitoria de Pesquisa, Pós-graduação e Inovação; 1 (um) representante da Pró-Reitoria de Gestão de Pessoas; 1 (um) representante da Diretoria de Comunicação; 1 (um) representante da Pró-Reitoria de Administração; 1 (um) representante Pró-Reitoria de Ensino; 1 (um) representante da Comissão Permanente de Avaliação de Documentos; 1 (um) representante do Arquivo Central; 1 (um) Gestor da Segurança da Informação.

Fonte: Elaborado pelo autor com base nas Inst.1, Inst.2 e Inst.3, 2024.

A composição dos comitês das três instituições revela uma diversidade significativa nas representações setoriais, refletindo diferentes abordagens e prioridades na implementação da política de proteção de dados. A composição da **Inst.1** indica uma tentativa de integrar diversos setores estratégicos para assegurar que a PPDP seja abrangente e considere múltiplos aspectos institucionais, desde a gestão de pessoas até a segurança da informação. A inclusão de representantes de comunicação e marketing também destaca a preocupação com a transparência e a comunicação sobre práticas de proteção de dados.

> Os principais envolvidos na execução das etapas de implementação [...] devem dispor de meios aptos a manter uma comunicação eficiente durante os seus trabalhos. A interação multidisciplinar nesses contatos é um elemento essencial ao correto tratamento de questões que envolvam a revisão de

> procedimentos internos, relações com parceiros e funcionalidades de sistemas, por exemplo (Davoli; Oliveira; Silva, 2020, p. 30).

A abordagem da **Inst.2** sugere um foco na representação ampla e inclusiva, buscando garantir que todas as áreas da instituição, incluindo aquelas geograficamente descentralizadas, tenham voz na implementação da PPDP. Enquanto a **Inst.3** define um arranjo que destaca a preocupação em integrar tanto a gestão estratégica quanto a operacional, refletindo uma abordagem holística na proteção de dados pessoais. A inclusão de representantes de Governança e Gestão de Riscos é particularmente notável, apontando para uma atenção cuidadosa aos riscos institucionais associados ao tratamento de dados pessoais.

Em suma, a composição dos comitês de proteção de dados nas três instituições analisadas reflete diferentes estratégias e ênfases, mas todas convergem para a importância de uma abordagem multidisciplinar. A representação de diversas áreas garante que a política de proteção de dados seja formulada com base em uma visão ampla e inclusiva, contemplando os variados aspectos da vida institucional que são impactados pelo tratamento de dados pessoais. Essas diferenças de composição demonstram como cada instituição adapta suas práticas à sua própria estrutura e necessidades, buscando assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais e a eficácia na proteção dos dados pessoais sob sua custódia.

Em se tratando das etapas para implementação PPDP nas instituições examinadas, revela-se que diferentes abordagens, metodologias e uso de ferramentas refletem as necessidades e características particulares de cada organização. “Ambas as metodologias podem ser implementadas com a ajuda de um time multidisciplinar, envolvendo, por exemplo, jurídico, área técnica, de produtos, engenharia de dados, segurança da informação, UX, entre outras” (Davoli; Oliveira; Silva, 2020, p.14).

No quadro a seguir é possível verificar uma síntese das etapas, metodologias e ferramentas utilizadas no processo de implementação.

Quadro 11. Etapas, metodologias e ferramentas utilizadas na implementação da PPDP

Instituições	Etapas de implementação	Metodologia e ferramentas
Inst.1	As etapas foram estabelecidas por meio de um plano de conformidade: *Etapa 1* - Preparar a Instituição para à adequação à LGPD; *Etapa 2* - Construção do Inventário de Dados; *Etapa 3* - Construção da Matriz de Risco; *Etapa 4* - Adequação da Instituição à LGPD; e *Etapa 5* - Monitoramento e manutenção	Plano de Conformidade; PDCA; 5W2H; Inventário de Dados; Matriz de Riscos; RIPD; ISO/IEC 31000:2018; e FalaBR.
Inst.2	As etapas foram estabelecidas por meio de um programa de governança em privacidade: *Etapa 1* - Iniciação e Planejamento; *Etapa 2* - Construção e Execução; e *Etapa 3* - Monitoramento.	Programa de Governança em Privacidade; PDCA; 5W2H; ISO/IEC 27001:2013; ISO/IEC 27001:2019; ISO/IEC 27005:201; RIPD; e FalaBR.
Inst.3	As etapas foram estabelecidas por meio de um plano de adequação: *Etapa 1* - Preparação; *Etapa 2* - Mobilização/conscientização e Formação Continuada; *Etapa 3* - Maturidade/assessment (avaliação); *Etapa 4* - Inventário/mapeamento de dados; Etapa 5 - Política de Governança de Dados Pessoais; e Etapa 6 - Monitoramento e conformidade contínua.	Plano de Adequação; PDCA; 5W2H; Inventário de Dados; RIPD; Power BI; Matriz de Riscos; COSO; Sistema de Gestão de Riscos (Sistema Ágatha); e FalaBR.

Fonte: Elaborado pelo autor com base nas Inst.1, Inst.2 e Inst.3, 2024.

Em detida análise, observa-se que a **Inst.1** elaborou um plano de conformidade com cinco etapas definidas: preparação, construção do inventário de dados, construção da matriz de risco, adequação, e monitoramento e manutenção. A abordagem estruturada reflete uma estratégia focada na preparação inicial e na análise de riscos, seguidas por uma fase de implementação e um ciclo contínuo de monitoramento. A utilização do Plano de Conformidade como metodologia principal, apoiado por ferramentas como PDCA e 5W2H, proporciona um *framework* de melhoria contínua e análise estruturada de problemas e soluções. Ferramentas específicas como Inventário de Dados para mapeamento de informações, Matriz de Riscos para avaliação de riscos, RIPD e a norma ISO/IEC 31000:2018 para gestão de riscos, são fundamentais para garantir que a instituição não só atenda aos requisitos legais, mas também crie um ambiente seguro para o tratamento de dados pessoais.

Por sua vez, a **Inst.2** estruturou seu processo através de um Programa de governança em Privacidade (PGP), dividido em três macro etapas: iniciação e planejamento, construção e execução, e monitoramento. A metodologia utilizada, centrada no Programa de Governança em

Privacidade, sugere uma abordagem mais holística e integrada, focando não apenas na conformidade inicial, mas também na governança contínua de privacidade e proteção de dados. A aplicação de normas específicas como ISO/IEC 27001:2013, ISO/IEC 27001:2019, e ISO/IEC 27005:201 indica um compromisso robusto com a segurança da informação e a gestão de riscos associados à privacidade ao adotar o RIPD. Além disso, o PDCA e 5W2H são empregados para a melhoria contínua e análise de implementação da PPDP.

Já a **Inst.3** optou também por um plano de adequação detalhado em seis etapas: preparação, mobilização/conscientização e formação continuada, maturidade/assessment, inventário/mapeamento de dados, política de governança de dados pessoais, e monitoramento e conformidade contínua. Este plano reflete uma abordagem extensa e abrangente, começando com a preparação, conscientização dos envolvidos (o próprio comitê e todos os servidores que tratam dados pessoais na instituição) e culminando com um ciclo de monitoramento contínuo. A utilização de metodologias como PDCA e 5W2H proporciona uma base sólida para o planejamento, execução, verificação e atuação sobre os resultados. A inclusão de ferramentas como Power BI para análise de dados e visualização, e o uso de metodologias de gestão de riscos como COSO e o Sistema de Gestão de Riscos Ágatha, demonstram um esforço para integrar análises de risco com práticas de gestão de dados. O uso de ferramentas como Inventário de Dados e RIPD assegura que a instituição esteja continuamente mapeando e avaliando o impacto de suas práticas de tratamento de dados pessoais.

A utilização do ciclo PDCA na implementação da PPDP nas IFES proporciona uma abordagem sistemática e contínua para assegurar a conformidade com a LGPD. As instituições estudadas seguem estratégias que abrangem desde o planejamento inicial e a execução das políticas até o monitoramento e a adoção de medidas corretivas. Esse ciclo possibilita ajustes frequentes, promovendo uma cultura organizacional sólida e eficaz em proteção de dados

Já o **Fala.BR** é uma plataforma utilizada por todas as instituições como uma ferramenta de transparência passiva. É atualmente o principal canal da Administração Pública Federal, que tem como o objetivo de atender às solicitações, petições, reclamações e denúncias dos titulares de dados, permitindo que indivíduos exerçam seus direitos em relação ao tratamento de suas informações pessoais. Através dessa interface, as instituições podem responder de maneira organizada às demandas dos titulares, promovendo uma maior transparência e garantindo o cumprimento dos princípios da LGPD.

Importante destacar, os fatores que contribuíram para o sucesso e os desafios encontrados durante o processo de implementação é o derradeiro fator de análise desse estudo.

Como se vê no quadro a seguir, analisou-se as experiências vividas pelas três instituições com base nessas perspectivas.

Quadro 12. Fatores críticos de sucesso e desafios na implementação da PPDP

Instituição	Fatores críticos de sucesso	Desafios
Inst.1	Apoio da alta gestão e da equipe do comitê	Colaboração da comunidade universitária, sensibilização, conscientização, fomento e fortalecimento da cultura de proteção de dados, dedicação exclusiva de servidores (principalmente o encarregado) e resistência de alguns servidores (não acreditam na legislação).
Inst.2	Apoio da alta gestão e da equipe do comitê	Sensibilização, conscientização, fomento e fortalecimento da cultura de proteção de dados, realização do inventário de dados, resistência de alguns servidores (não acreditam na legislação).
Inst.3	Apoio da alta gestão e da equipe do comitê	Sensibilização, conscientização, capacitação, fomento e fortalecimento da cultura de proteção de dados e dedicação exclusiva de servidores (principalmente o encarregado).

Fonte: Elaborado pelo autor com base nas Inst.1, Inst.2 e Inst.3, 2024.

Em se tratando dos fatores críticos de sucesso, observa-se que um ponto comum entre as três instituições foi o apoio da alta gestão e o apoio da equipe do comitê gestor. O comprometimento da alta gestão é um fator determinante para o sucesso da implementação das políticas de proteção de dados. O apoio dos líderes institucionais não apenas legitima a importância da política dentro da instituição, mas também garante que os recursos necessários sejam alocados adequadamente.

A liderança proativa da alta gestão contribui para a criação de um ambiente favorável à mudança e ao cumprimento das normas de proteção de dados, promovendo uma cultura de respeito à privacidade, à proteção de dados pessoais e à segurança da informação. Ressaltando novamente que é de responsabilidade da alta gestão garantir a estrutura básica para que se efetivem a governança e gestão de dados na instituição (Brasil, 2024).

O envolvimento ativo da equipe do comitê é outro fator crítico de sucesso. Um comitê desempenha um papel vital na coordenação das atividades relacionadas à proteção de dados, desde a elaboração de políticas até a supervisão da conformidade contínua. A expertise e o comprometimento dos membros do comitê facilitam a implementação da política, principalmente na sensibilização necessária em toda a instituição. Portanto, esses elementos são fundamentais para a implementação eficaz de qualquer política institucional, especialmente aquelas que demandam mudanças culturais e operacionais.

Apesar dos fatores de sucesso, as três instituições enfrentaram desafios semelhantes, embora com algumas variações específicas em cada caso. Esses desafios estão relacionados principalmente à sensibilização, conscientização, capacitação e fortalecimento da cultura de proteção de dados, além de questões específicas como a realização do inventário de dados e a resistência à mudança.

Em relação aos desafios, a respeito da sensibilização e conscientização, eles se apresentam como significativos, pois como visto, a disseminação de conhecimento sobre a Lei a LGPD e sua aplicação prática dentro da instituição é essencial para garantir o cumprimento das normas. A falta de entendimento ou o entendimento inadequado dos princípios da LGPD entre os membros da comunidade universitária pode resultar em práticas que comprometem a segurança e a proteção dos dados pessoais. Além disso, pode ferir princípios da administração pública como transparência e publicidade.

As políticas são muito além de meros documentos de orientação, são verdadeiros guias para provocar uma mudança de conduta necessária dentro da organização, possibilitando assim o surgimento de uma verdadeira cultura de proteção de dados pessoais e de segurança da informação. Nesse aspecto a sensibilização e conscientização são fundamentais (Micheletti; Borges; Costa, 2022).

Outra dificuldade enfrentada foi o fomento e fortalecimento de uma cultura de proteção de dados. Estabelecer uma cultura que valorize a privacidade e a proteção de dados requer mudanças comportamentais e atitudinais, o que é muitas vezes um processo lento e desafiador. Em ambientes acadêmicos, onde a liberdade de informação é valorizada, pode haver resistência à implementação de práticas mais restritivas de manejo de dados. Pinheiro (2018) enfatiza que para a garantir a privacidade e a proteção de dados, alguns ajustes dos processos de governança organizacional são necessários, mas acima de tudo a mudança de cultura.

A dedicação exclusiva de membros do comitê, especialmente do Encarregado de proteção de dados, foi um desafio destacado pelas **Inst.1** e **Inst.3**. A dificuldade se dá pela necessidade de os servidores dividirem suas atenções entre múltiplas funções.

A resistência de alguns servidores à nova legislação foi um obstáculo relevante, tanto na **Inst.1** quanto na Inst. 2. Do ponto de vista dos entrevistados, essa resistência pode ser resultado de uma percepção de que a proteção de dados é uma prioridade secundária ou de uma crença de que as exigências da LGPD são desnecessárias (“essa Lei não vai vingar”).

A realização do inventário de dados foi destacada como um desafio específico na **Inst.2** O inventário de dados é um processo crítico que exige um mapeamento detalhado de todos os

dados pessoais coletados e tratados pela instituição. Esse processo é muitas vezes complexo e consome bastante tempo, especialmente em grandes instituições com múltiplas fontes de dados.

Apenas a **Inst.3**, aponta o desafio da capacitação como um ponto crítico. O entrevistado enfatiza que a capacitação contínua dos membros da equipe, bem como de toda a comunidade acadêmica, é essencial para garantir que todos compreendam suas responsabilidades em relação à proteção de dados e sejam capazes de identificar e mitigar riscos potenciais.

Skynet/**Inst.1** reforça a ideia de que, durante o processo de implementação da política de proteção de dados, é natural que ocorram erros e que seja necessário ajustar a estrutura conforme a implementação avança. Ela destaca a importância de realizar revisões periódicas para identificar o que precisa ser corrigido e melhorado.

Em suma, a análise dos fatores críticos de sucesso e desafios enfrentados pelas três instituições na implementação de suas políticas de proteção de dados revela que, embora existam elementos comuns que promovem o sucesso, como o apoio da alta gestão e dos comitês gestores, há desafios significativos que precisam ser superados para garantir a conformidade com a LGPD. Esses desafios, que vão desde a sensibilização até a resistência de alguns servidores, demonstram a complexidade do processo de implementação e a necessidade de abordagens estratégicas contínuas para promover uma cultura de proteção de dados pessoais.

Por fim, a forma como esses comitês são estruturados e operam reflete uma forte governança e gestão em relação à proteção de dados pessoais. Isso é evidenciado nas suas atribuições e competências, pela inclusão de múltiplos atores, pelo compromisso com a melhoria contínua e pela capacidade de resposta a riscos. Essas práticas são indicativas de instituições que buscam não apenas cumprir a legislação, mas também adotar as melhores práticas para assegurar a privacidade e a segurança da informação de forma sustentável e eficaz.

Tendo em vista o exposto seguem algumas considerações e sugestões que poderão contribuir para na otimização do processo de implementação da PPDP. Sugere-se que o comitê tenha na sua composição um servidor da área jurídica. O seu conhecimento é crucial para assegurar a conformidade legal contínua e para fornecer consultoria sobre aspectos jurídicos da proteção de dados. Como visto na estrutura mínima de governança do FPSI, outras figuras importantes que também poderiam compor o Comitê são: representante do Comitê de Governança, Riscos e Controles; Gestor de Auditoria Interna e Gestor de Segurança da Informação (SI).

Indo mais além, para otimizar os recursos e aprimorar a governança institucional seria a criação de um comitê único que integre as áreas de privacidade, proteção de dados pessoais e segurança da informação, ao invés de manter comitês separados para cada um desses temas.

Essa abordagem unificadora não só promove uma gestão mais coesa e eficiente, como também evita a fragmentação do conhecimento e a duplicação de esforços, favorecendo uma melhor alocação de recursos.

Dentro dessa estrutura centralizada, seria possível criar subcomitês ou grupos de trabalho temáticos que focassem em questões específicas, como privacidade, compliance com a Lei Geral de Proteção de Dados (LGPD), gestão de riscos, auditoria e segurança da informação. Esses subcomitês garantiriam que cada área de especialidade tivesse atenção adequada, mantendo a flexibilidade necessária para atender às demandas específicas, sem perder de vista a visão estratégica unificada da instituição.

Essa proposta também pode contribuir para uma melhor coordenação das atividades e uma comunicação mais eficaz entre os diferentes setores, fortalecendo a integração entre os princípios da proteção de dados pessoais e as normas de segurança da informação. Além disso, ao reunir especialistas de diferentes áreas dentro de um único comitê, a instituição assegura uma maior retenção do conhecimento adquirido durante o processo de elaboração e implementação da Política de Proteção de Dados Pessoais (PPDP), bem como uma visão mais ampla e estratégica sobre a privacidade e a segurança da informação como um todo.

Considerando o contexto das IFES, sugere-se uma nova proposta (modelo) para integrar as melhores práticas para a implementação de uma PPDP no ciclo PDCA, como se pode ver figura a seguir. No primeiro estágio, **Planejar (Plan)**, a alta administração deve garantir o comprometimento e o apoio necessários para o trabalho do comitê, que se encarregará do processo de implementação como um todo da PPDP. Assim, Comitê Gestor, liderado pelo Encarregado de Proteção de Dados (DPO), realizará o diagnóstico inicial, o mapeamento de dados pessoais e atividades de tratamento (*Data Mapping*); e a avaliação de riscos associados ao tratamento de dados.

Na fase **Executar (Do)**, o Comitê Gestor implementa a PPDP por meio de programas de treinamento e conscientização, promovendo uma cultura organizacional voltada para a proteção de dados. Além disso, medidas técnicas, como criptografia e controle de acesso, são adotadas para assegurar a segurança dos dados. A documentação e os registros das atividades de tratamento devem ser mantidos de forma acessível, facilitando a consulta e a auditoria.

Figura 22. Proposta de implementação da PPDP

Fonte: Elaborado pelo autor

A etapa **Verificar (Check)** envolve a realização de auditorias e fiscalizações regulares pelo Comitê Gestor e/ou pelo setor de auditoria interna, que assegura a conformidade com a PPDP e promove revisões conforme necessário. É fundamental manter canais abertos de comunicação com os titulares de dados, permitindo a coleta de feedback e a transparência nas práticas de tratamento.

Por fim, na fase **Agir (Act)**, o Comitê Gestor deve consultar a Autoridade Nacional de Proteção de Dados (ANPD) quando apropriado, além de colaborar com outras instituições para compartilhar melhores práticas. A revisão contínua das ações, com base em auditorias e feedback, é essencial para promover melhorias no tratamento de dados pessoais.

Finalmente, essas propostas poderão contribuir para uma melhor governança, ao facilitar a tomada de decisões estratégicas, garantir conformidade com a legislação vigente e promover uma cultura organizacional mais consciente e integrada em relação à proteção de dados e à segurança da informação.

4.3 POLÍTICA DE PROTEÇÃO DE DADOS PARA IFES

Neste tópico serão analisados os conteúdos das PPDPs das IFES participantes e do modelo de política elaborado pelo MGI, a partir dos quais será proposto um modelo genérico de PPDP para as IFES.

Incialmente, conforme teorizado neste estudo, as políticas de proteção de dados são instrumentos fundamentais para assegurar a conformidade com a LGPD no Brasil. A análise dos elementos constitutivos dessas políticas em diferentes instituições permite compreender como cada organização estrutura suas diretrizes para atender às exigências legais e mitigar os riscos associados ao tratamento de dados pessoais. Nesta seção, será realizada uma análise comparativa dos elementos presentes nas políticas de proteção de dados das **Inst.1, Inst.2**, e **Inst.3**, considerando suas particularidades e a abrangência dos seus conteúdos. Além disso, foi incluído o modelo de PPDP elaborado pelo MGI. Com base nessa análise comparativa, será elaborada uma minuta de PPDP para as Instituições Federais de Ensino Superior (IFES), incorporando os melhores aspectos dos modelos comparados. Também será realizada uma análise para verificar a aderência dessas políticas à LGPD, conforme os critérios mencionados por Basan (2021), quais sejam: I - unidade e generalidade da aplicação da lei; II - legitimação para o tratamento de dados (hipóteses autorizativas); III - princípios e direitos do titular; IV - obrigações dos agentes de tratamento de dados; e V - responsabilização dos agentes.

A análise das políticas de proteção de dados das instituições selecionadas revela uma diversidade de abordagens e elementos constitutivos, refletindo diferentes estratégias para conformidade com a LGPD. Cada instituição estruturou suas diretrizes de acordo com suas necessidades específicas, mas com foco comum em garantir a proteção dos dados pessoais e o respeito aos direitos dos titulares.

Nas **Inst.1** e **Inst.3**, a PPDP é abrangente e detalhada, pois engloba uma vasta gama de elementos essenciais para garantir a conformidade com a LGPD. A política de proteção de dados da **Inst.2** é estruturada com ênfase em elementos fundamentais como objetivos, público-alvo, princípios e definições, mas inclui a avaliação de impacto à proteção de dados pessoais

demonstra um enfoque preventivo, buscando identificar e mitigar riscos antes que ocorram violações de dados. Já o modelo de PPDPA política do MGI é estruturado de maneira a cobrir tanto aspectos operacionais quanto estratégicos da proteção de dados. Mas deixa de lado a figura do comitê gestor. A presença de um comitê gestor nas três IFES indica a busca de um nível de governança adequado, proporcionando supervisão e coordenação das atividades de proteção de dados.

Em análise dos elementos das políticas de proteção de dados das IFES e do modelo do MGI, revela-se a intenção de compromisso com a conformidade legal e a proteção dos direitos dos titulares de dados. Embora existam variações na forma como cada instituição aborda a proteção de dados, todas as IFES demonstram uma preocupação abrangente com a segurança, governança em relação à privacidade de dados.

Figura 23. Comparativo dos elementos de Políticas de Proteção de Dados Pessoais

ELEMENTOS	Modelo PPDP - MGI	PPDP - INST1	PPDP - INST2	PPDP - INST3
Objetivo/Propósito	✔	✔	✔	✔
Escopo/Abrangência	✔	✔	✔	✔
Princípios	✔	✔	✔	✔
Termos e definições/Glosssário	✔	✔	✔	✔
Diretrizes gerais	✔			
Destinatários e figuras legais		✔		✔
Bases legais para o tratamento de dados pessoais		✔		✔
Tratamento de dados pessoais	✔	✔	✔	✔
Compartilhamento de de dados pessoais		✔		✔
Transferência internacional dados pessoais		✔		✔
Contratos, convênios, acordos e instrumentos congêneres	✔			
Direito do titular		✔	✔	✔
Violação e descumprimento		✔		✔
Funções e Responsabilidades	✔		✔	
Comitê gestor de proteção de dados		✔	✔	✔
Conscientização, capacitação e sensibilização	✔			
Segurança e boas práticas	✔	✔		✔
Auditoria, fiscalização e conformidade	✔	✔		✔
Penalidades	✔			
Disposições finais	✔	✔	✔	✔

Fonte: Elaborado pelo autor com base em Brasil, 2023 e Inst.1, Inst.2, Inst.3, 2024.

Já o MGI inova em se tratando de educação contínua. A inclusão de seções sobre conscientização, capacitação e sensibilização reflete uma abordagem holística que reconhece a importância de educar e envolver todos os membros da instituição. Aborda também segurança e boas práticas, assim como auditoria e conformidade, o que é crucial para garantir que a política não apenas exista no papel, mas seja efetivamente implementada e monitorada. Funções e responsabilidades são claramente especificadas, o que facilita a governança e a gestão dos dados

pessoais. A atenção a contratos, convênios, acordos e instrumentos congêneres assegura que terceiros que lidam com dados da instituição também estejam em conformidade com a LGPD.

Ressalta-se novamente que a implementação de políticas detalhadas e bem estruturadas é essencial para garantir a conformidade com a LGPD e promover uma cultura institucional que valorize a privacidade e a proteção de dados pessoais.

Portanto, as políticas de proteção de dados das instituições analisadas incorporam, em diferentes graus, os critérios estabelecidos pela LGPD conforme apontados por Basan (2021). Em geral, todos os critérios são abordados, embora algumas instituições sejam mais explícitas em suas políticas do que outras. A presença de elementos como unidade e generalidade, hipóteses autorizativas, princípios e direitos do titular, obrigações dos agentes de tratamento, e responsabilização refletem um compromisso claro com a conformidade legal e a proteção dos dados pessoais, demonstrando um alinhamento significativo com os princípios da LGPD.

Finalmente, com base na análise das políticas de proteção de dados das Instituições Federais de Ensino Superior (IFES) e do modelo do MGI, alinhadas aos eixos estabelecidos por BASAN e embasada pelo referencial teórico desta pesquisa, este pesquisador elaborou uma minuta de Política de Proteção de Dados para as IFES. Essa minuta visa integrar as melhores práticas observadas nas diferentes instituições, atendendo aos princípios e diretrizes fundamentais da Lei Geral de Proteção de Dados (LGPD) e garantindo a proteção dos dados pessoais no contexto acadêmico.

Por fim os elementos da minuta proposta encontram-se no subtópico a seguir. Trata-se de um modelo abrangente e adaptável para aplicação em diversas instituições de ensino superior.

4.3.1 Minuta de política de proteção de dados pessoais para IFES

CAPÍTULO I

DISPOSIÇÕES GERAIS

Seção XX

Dos objetivos

Art. Z A presente Política de Proteção de Dados Pessoais (PPDP) estabelece diretrizes e reponsabilidades no tratamento de dados pessoais realizado pela [Universidade/Instituto] com o objetivo de proteger a privacidade e os dados pessoais sob sua custódia.

[Acrescente aqui mais objetivos da Política de Proteção de Dados Pessoais que julgue necessárias.]

Seção XX

Da abrangência

Art. Z1 Esta Política dispõe sobre o tratamento de dados pessoais nos meios físicos e digitais por qualquer pessoa que realize operações de tratamento de dados pessoais custodiados pela [Universidade/Instituto].

Parágrafo único. O disposto neste artigo, aplica-se a todos os servidores docentes e técnicos-administrativos em educação, estagiários, consultores externos, prestadores de serviço ou quem de alguma forma atua para ou em nome da [Universidade/Instituto].

Art. Z Esta Política, suas normas complementares e procedimentos abrange toda estrutura universitária: unidades administrativas e acadêmicas, além de entidades vinculadas à [Universidade/Instituto].

Art. Z Todos aqueles mencionados no parágrafo único do art. Z1 são responsáveis pela proteção dos dados pessoais custodiados pela [Universidade/Instituto], e devem estar comprometidos com o cumprimento desta política, normas e procedimentos complementares.

[Acrescente aqui mais definições sobre o escopo/abrangência da Política de Proteção de Dados Pessoais que julgue necessárias.]

Seção XX

Dos Conceitos e Definições

[Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política (Recomenda-se utilizar como referência as definições apresentadas no Art. 5 da LGPD e no guia Glossário de Proteção de Dados Pessoais e Privacidade da ANPD)]

Art. Z Para os fins desta [Resolução] considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, entre outros;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

XV - Relatório de Impacto de Proteção de Dados - RIPD: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVI - autodeterminação informativa: confere à pessoa titular de dados o direito de controlar seus próprios dados pessoais, com base nos preceitos da boa-fé e da transparência;

XVII - Autoridade Nacional de Proteção de Dados (ANPD): Autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, em todo o território nacional;

XVIII - controladoria conjunta: determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD;

XIX - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XX - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XXI - Lei Geral de Proteção de Dados Pessoais (LGPD): Lei Federal n. 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

XXII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XXIII - violação de dados pessoais: violação de segurança que provoque acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

XXIV - pseudoanonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (titular), senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

[Exclua, ou acrescente os termos-chave, siglas ou conceitos que podem ser utilizados na política]

Sessão XX

Dos princípios

Art. Z2 Em todas as ações de tratamento de dados pessoais na Universidade, deverão ser observados os seguintes princípios:

I - boa-fé: convicção de agir com correção e em conformidade com as normas legais;

II - finalidade: o tratamento dos dados deve possuir propósitos legítimos, específicos, explícitos e informados;

III - adequação: o tratamento dos dados deve ser compatível com a finalidade pela qual são tratados;

IV - necessidade: limitação do tratamento ao mínimo necessário para o alcance da finalidade, considerados apenas os dados pertinentes, proporcionais e não excessivos;

V - livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais bem como sobre a integralidade deles;

VI - qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados de acordo com a necessidade e para o cumprimento da finalidade do respectivo tratamento;

VII - transparência: garantia aos titulares de informações claras, precisas e acessíveis sobre o tratamento de seus dados pessoais e sobre os agentes de tratamento;

VIII - segurança e prevenção: utilização de medidas técnicas e administrativas que garantam a proteção dos dados pessoais contra acessos não autorizados e a prevenção contra situações acidentais ou ilícitas que gerem destruição, perda, alteração, comunicação ou difusão desses dados;

IX - não discriminação: vedação de realizar o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos; e

X - responsabilização e prestação de contas: demonstração de que os agentes de tratamento da instituição são responsáveis pelo tratamento de dados e adotam medidas eficazes para o cumprimento das normas de proteção de dados pessoais.

Parágrafo único. Serão observados ainda, sem prejuízo dos demais, outros princípios constitucionais que regem a Administração Pública Federal, zelando pela transparência pública e o dever de acesso à informação.

[Acrescente aqui mais princípios da Política de Proteção de Dados Pessoais que julgue necessárias.]

CAPÍTULO II

DIRETRIZES GERAIS

Seção XX

Das Hipóteses Autorizativas para o Tratamento de Dados Pessoais

Art. Z3 A realização de operações de tratamento de dados pessoais pela Universidade/Instituto], poderá ser realizada nas seguintes hipóteses:

I - para o cumprimento de obrigação legal ou regulatória;

II - para a realização de estudos por órgão de pesquisa;

III - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular de dados pessoais;

IV - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

V - para a proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;

VI - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde.

VII - mediante o fornecimento de consentimento pelo titular de dados pessoais;

Seção XX

Do Tratamento e Dados Pessoais

Art. Z. A aplicação desta Política é pautada pela observância dos princípios previstos no **art. Z2**.

Art. Z O tratamento de dados pessoais pela [Universidade/Instituto] deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os

procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, conforme art. Z4 desta Resolução;

II - realizem o tratamento mínimo de dados pessoais, necessário e imprescindível à garantia do interesse público e à execução de suas atividades acadêmicas e administrativas.

Art. Z É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela [Universidade/Instituto] ou por pessoa não autorizada formalmente por esta.

Art. Z4 A [Universidade/Instituto] deverá publicar, de modo claro e atualizado, em lugar de fácil acesso e visualização em seu site, o aviso de privacidade contendo no mínimo as seguintes informações sobre o tratamento de dados pessoais:

I - as hipóteses que fundamentam a realização do tratamento de dados pessoais na instituição;

II - a previsão legal, a finalidade e os procedimentos para tratamento de dados pessoais;

III - a identificação do controlador (instituição) com o respectivo contato;

IV - o nome do encarregado e o respectivo contato;

V - as responsabilidades dos operadores envolvidos no tratamento e os direitos do titular com menção expressa ao art. 18 da Lei nº 13.709, de 2018; e

VI - outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

Art. Z. O tratamento de dados pessoais sensíveis deverá ser realizado somente nos termos da seção II do capítulo II da LGPD e devem ser estabelecidos procedimentos de segurança no tratamento destes dados conforme a LGPD e demais normativos.

Art. Z Os dados pessoais de crianças e adolescentes serão tratados com o mesmo nível de cuidado exigido e oferecido aos dados pessoais sensíveis e estarão sujeitos às disposições próprias estabelecidas no art.14 da LGPD, entre outras normas específicas aplicáveis.

Parágrafo único. Se a hipótese para tratamento for o Inciso VII do art. Z3 desta política, é necessário o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Art. Z Nas situações em que o tratamento ofertar riscos às liberdades civis e aos direitos fundamentais, bem como em casos indicados pela ANPD, ou decididos pelo Comitê Gestor de Proteção de Dados Pessoais, aquele deverá ser precedido do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

[Exclua, ou acrescente outras regras para tratamento de dados pessoais que julgar necessárias].

Seção XX

Do compartilhamento dos Dados Pessoais

Art. Z O compartilhamento de dados pessoais pela [Universidade/Instituição] somente será permitido para o cumprimento de suas obrigações legais ou para atendimento de políticas públicas aplicáveis, observado o princípio da necessidade e dos procedimentos de segurança, ficando o tratamento de dados pessoais sempre contíguo ao desenvolvimento de atividades autorizadas pela Instituição.

Art. Z A [Universidade/Instituição], somente poderá fazer o compartilhamento de dados pessoais nas seguintes hipóteses:

I - entre as unidades e setores da [Universidade/Instituição]: O compartilhamento de dados pessoais entre as unidades e setores somente será permitido para o cumprimento das suas obrigações legais.

II - para a realização de estudos por órgão de pesquisa: O compartilhamento de dados pessoais para fins de pesquisa deve atender às normas institucionais, garantindo, sempre que possível, a anonimização dos dados pessoais.

III - entre Órgãos e entidades públicas: O compartilhamento de dados pessoais pelo [Universidade/Instituição] entre os órgãos públicos deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no artigo 6º da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e a legislação especial sobre o tema, entre elas o Decreto 10.046/2019;

IV - entre entidades privadas: A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a entidades privadas será informado à autoridade nacional e dependerá de consentimento do titular, exceto nas hipóteses previstas no artigo 26º e 27º da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

Parágrafo único. O tratamento de dados na hipótese em que o consentimento é requerido, caso a [Universidade/Instituição] necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas em lei.

Seção XX

Da Transferência Internacional de Dados Pessoais

Art. Z A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 da LGPD;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD.

Parágrafo único. Para os fins do inciso I deste artigo, a [Universidade/Instituto], no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Seção XX

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. Z Os contratos, convênios, acordos e instrumentos congêneres com operadores, atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, devem incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e que contemplem:

I. requisitos mínimos de segurança da informação;

III. requisitos de proteção de dados pessoais;

II. determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador;

IV. condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador;

V. diretrizes especificas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais.

[Liste as demais diretrizes que julgarem pertinentes sobre os contratos, convênios, acordos e instrumentos congêneres que devem estar presentes nesta Política de Proteção de Dados Pessoais]

Obs:. A Secretaria de Governo Digital disponibiliza em seu portal o Guia de Requisitos e Obrigações quanto à Privacidade e Segurança da Informação que orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de privacidade e segurança dos dados.

Seção XX

Do Direito do Titular

Art. Z O titular dos dados pessoais tem direito a obter da [Universidade/Instituto], em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - Direito à confirmação da existência do tratamento: o titular de dados pessoais, a qualquer momento, poderá confirmar se há operações de tratamento relativo aos seus dados pessoais;

II - Direito de acesso: o titular de dados pessoais poderá solicitar o acesso aos seus dados que são mantidos pela instituição;

III - Direito de correção: o titular de dados pessoais poderá solicitar a alteração do seu respectivo dado pessoal que estejam incompletos, inexatos ou desatualizados. A [Universidade/Instituto] poderá solicitar documentação comprobatória da alteração, providenciará a alteração em período pré-estabelecido e notificará o titular quando a solicitação estiver atendida;

IV - Direito de eliminação: o titular de dados pessoais pode requisitar à [Universidade/Instituto], a exclusão de seus dados pessoais tratados com o consentimento, salvo exceto nas hipóteses previstas no

art. 16 da LGPD. A [Universidade/Instituto] poderá escolher o procedimento de eliminação a ser empregado, comprometendo-se utilizar meio que garanta a segurança e evite a recuperação dos dados;

V - Direito de solicitar a suspensão de tratamento ilícito de dados pessoais: o titular de dados pessoais poderá solicitar a qualquer momento a anonimização, bloqueio ou eliminação de seus dados pessoais, que tenham sido reconhecidos por autoridade competente como desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

VI - Direito à portabilidade dos dados: o titular de dados pessoais poderá solicitar a portabilidade dos seus dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; bem como os limites técnicos de sua infraestrutura;

VII - Direito de oposição a um tratamento de dados pessoais: informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

VIII - Direito à revogação do consentimento: O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular;

IX- Direito de obter informação das entidades públicas e privadas com as quais a [Universidade/Instituto] realizou uso compartilhado de dados.

Parágrafo único. É imprescindível que a verificação da identificação do titular seja confirmada pela [Universidade/Instituto] antes do atendimento de qualquer solicitação feita pelo titular do dado.

CAPÍTULO III

GOVERNANÇA E BOAS PRÁTICAS

Seção XX

Funções e Reponsabilidades

Subseção XX

Do Controlador

Art. Z A [Universidade/Instituto] é o Controlador dos Dados Pessoais por ele tratados, nos termos das suas competências legal e institucional.

Art. Z Compete ao Controlador:

I. observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos.

II - indicar um encarregado pelo tratamento de dados pessoais por meio de ato formal, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional;

III - cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando à proteção de dados pessoais e sua governança e boas práticas;

IV - manter o registro das operações que envolva o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em seus sítios eletrônicos;

V - elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis e de crianças e adolescentes, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial;

VI - orientar o operador quanto ao tratamento de dados pessoais segundo instruções internas, legislação vigente e das regulamentações da Autoridade Nacional de Proteção de Dados (ANPD);

VII - disseminar a cultura da proteção de dados;

VIII - garantir a proteção, integridade, disponibilidade, confidencialidade e autenticidade dos dados pessoais sobre sua guarda;

IX - comprovar que o consentimento obtido do titular atende às exigências legais do art. 8º, § 2º da LGPD;

X - comunicar à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidentes de segurança.

XI - prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos recursos humanos, técnicos e administrativos;

XII - proporcionar ao encarregado autonomia técnica e acesso à alta administração da [Universidade/Instituto], para o melhor desempenho de suas atividades;

XIII - prover meios de atendimento humanizados do encarregado com o titular de dados e com a ANPD.

Art. Z O controlador é o responsável pela conformidade do tratamento dos dados pessoais, nos termos da Lei nº 13.709, de 2018.

[Exclua, ou acrescente outras competências para o controlador de dados pessoais que julgar necessárias]

Subseção XX

Do Operador

Art. Z Considera-se operador de dados pessoais as pessoas naturais ou jurídicas de direito público ou privado, que realizam operações de tratamento de dados pessoais em nome do controlador.

Parágrafo único. Qualquer fornecedor de produtos ou serviços, que por algum motivo, realiza o tratamento de dados pessoais a eles confiados, são considerados operadores e devem seguir as diretrizes estabelecidas nesta Política.

Art. Z Compete ao operador:

I - observar os princípios estabelecidos no Art. 6º da LGPD, ao realizar tratamento de dados pessoais;

II - realizar tratamento de dados pessoais segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Parágrafo único. É vedada a decisão unilateral do operador quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

[Exclua, ou acrescente outras regras e competências para o operador de dados pessoais que julgar necessárias]

Subseção XX

Do Encarregado pelo Tratamento de Dados Pessoais

Art. Z O encarregado pelo tratamento de dados pessoais será designado dentre os servidores estáveis, devendo este ser detentor de reputação ilibada, por meio de portaria emitida pelo Reitor da [Universidade/Instituto].

Art. Z5 Compete ao encarregado pelo tratamento de dados pessoais:

I - receber as solicitações e reclamações dos titulares de dados, devendo responder sobre as operações de tratamento de dados, somente aos titulares cujo os dados tenham sido objeto de tratamento pelo [Universidade/Instituto];

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os servidores da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

V - monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas da [Universidade/Instituto];

VI - prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes;

VII - orientar todos os destinatários desta Política e acompanhar no tratamento de dados referente a eliminação dos dados pessoais;

VIII - implementar o Plano de Conformidade e Melhoria Contínua da LGPD na [Universidade/Instituto];

IX - auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;

Art. Z A indicação do encarregado pelo [Reitor] deverá observar as suas qualidades profissionais, e, principalmente, seus conhecimentos relativos à disciplina de privacidade e proteção de dados, bem como aqueles necessários para o desempenho das atribuições previstas neste Regulamento.

Art. Z O encarregado deverá declarar ao [Reitor] qualquer situação que possa configurar conflito de interesse, responsabilizando-se pela veracidade das informações prestadas.

Art. Z Presume-se conflito de interesses o acúmulo da função de encarregado com aquela em que haja competência para decisões referentes ao tratamento de dados pessoais, em nome do agente de tratamento.

Art. Z O [Reitor], ao indicar o encarregado, deve atentar para que este não esteja ocupando ou não passe a ocupar posição que acarrete conflito de interesses.

Parágrafo único. Uma vez constatada a possibilidade de conflito de interesses, o [Reitor] não deverá prosseguir com a indicação ou deverá proceder a sua substituição.

Art. Z Nas ausências, impedimentos e vacâncias do encarregado, a função será exercida por substituto formalmente designado.

Parágrafo único. As situações de afastamento do encarregado referidas no caput não poderão consistir em obstáculos para o exercício dos direitos dos titulares ou para o atendimento às comunicações da ANPD.

Art. Z O desempenho das atividades e das atribuições dispostas no art. Z5 não confere ao encarregado a responsabilidade pela conformidade do tratamento dos dados pessoais.

Subseção XX

Do Comitê Gestor de Proteção de Dados Pessoais

Art. Z O Comitê Gestor de Proteção de Dados Pessoais é de caráter permanente e vinculado administrativamente à Reitoria, com atribuições de apoio à governança em privacidade e proteção de dados pessoas, possuindo natureza consultiva e propositiva nas políticas e ações em sua área de competência no âmbito da [Universidade/Instituto].

Art. Z São competências do Comitê Gestor de Proteção de Dados Pessoais:

I - assessorar o Encarregado de Dados da [Universidade/Instituto] em suas atividades descritas no Art. Z5.

I – auxiliar na elaboração da comunicação de incidente de segurança com dados pessoais;

II - auxiliar na elaboração do registro das operações de tratamento de dados pessoais;

III - auxiliar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais;

IV – realizar a identificação e análise de risco relativo ao tratamento de dados pessoais;

V - definir 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;

VI – promover a implementação da Lei nº 13.709, de 2018, dos regulamentos da ANPD e na adoção de melhores práticas para proteção de dados pessoais;

VII - analisar cláusulas contratuais com terceiros que versem sobre proteção de dados pessoais;

VIII – analisar as transferências internacionais de dados, realizadas nos termos desta Política e do art. 33, da Lei nº 13.709, de 2018;

IX - formular e implementar regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 2018.

X - promover ações de conscientização, sensibilização e capacitação sobre a aplicação desta Política e normas relacionadas à proteção de dados pessoais;

XI - aprovar pareceres técnicos e revisão de documentos no que se refere à proteção de dados.

XII - avaliar os procedimentos de tratamento e proteção dos dados pessoais existentes e propor estratégias e metas em observância a LGPD;

XIII - acompanhar a implantação dos planos e o cumprimento das ações regulamentadoras no [Universidade/Instituto].

XIV - revisar a Política de Proteção de Dados Pessoais e as instruções normativas a cada 1(um) ano, ou no caso de alterações de legislações relevantes;

Art. Z O Comitê Gestor de Proteção Dados Pessoais do [Universidade/Instituto] será composto por:

I - Encarregado pelo Tratamento de Dados Pessoais;

II - Gestor da Segurança da Segurança de Informação

III - Gestor do Serviço de Informação ao Cidadão (SIC); (ou um representante do Ouvidoria Pública da instituição)

IV - Um representante do Gabinete – Reitoria;

V - Um representante da Pró-Reitoria de Gestão de Pessoas;

VI - Um representante da Pró-Reitoria de Administração;

VII - Um representante da Pró-Reitoria de Graduação;

VIII- Um representante da Pró-Reitoria de Pós-Graduação;

IX - Um representante da Pró-Reitoria de Extensão;

X – Um representante do Colégio de Aplicação (se houver)

XI – Um representante do Núcleo de Desenvolvimento/Educação Infantil (se houver)

XII - Um representante do Arquivo Central

XIII - Um representante da Comissão Permanente de Avaliação de Documentos

[Exclua, ou acrescente outros representantes]

Art. Z Anualmente o Comitê emitirá cronograma de reuniões para a efetivação de suas obrigações estabelecidas no artigo anterior.

Seção XX

Da Segurança da Informação

Art. Z As normas de segurança da informação e prevenção contra incidentes de dados pessoais estarão contidas na Política de Segurança da Informação (POSIN) da [Universidade/Instituto] e nas normas internas e documentos correlatos ao tema.

Art. Z A prevenção da violação de dados é de responsabilidade de todos os destinatários desta Política.

Art. Z É dever de todos os servidores notificarem o Encarregado sempre que observadas suspeitas de irregularidade em relação às atividades de tratamento de dados pessoais ou da ocorrência efetiva das seguintes condutas:

I - tratamento de dados pessoais sem a autorização por parte da [Universidade/Instituto] no propósito das atividades que desenvolve;

II - operação de tratamento de dados pessoais realizada sem base legal que a justifique;

III - operação de tratamento de dados pessoais que seja realizada em desconformidade com a Política de Segurança da Informação (POSIN) da [Universidade/Instituto], com os normativos internos e documentos correlatos ao tema.

IV - eliminação, alteração ou destruição não autorizada pela [Universidade/Instituto] de dados pessoais de plataformas digitais ou de acervos físicos;

V - qualquer outra violação desta Política ou de qualquer um dos princípios de proteção de dados previstos no art. 6º da Lei 13.709/18.

Seção XX

Da Fiscalização

Art. Z O Encarregado juntamente com o Comitê Gestor de Proteção de Dados Pessoais (CGPDP), deverá definir, os procedimentos e mecanismos de fiscalização do cumprimento desta Política.

Art. Z As denúncias ou reclamações sobre ilegalidades no tratamento de dados pessoais ou incidente de segurança que possa acarretar risco ou dano relevante aos titulares, devem ser recebidas pelo Encarregado de dados pessoais, que apoiado pelo Comitê Gestor de Proteção de Dados Pessoais, poderá tomar as providências cabíveis como:

I - identificar o impacto do dano ou da violação à legislação de proteção de dados pessoais

e elaborar medidas técnicas para a proteção dos dados pessoais.

II - notificar o Reitor;

III - notificar o titular do dado;

IV - notificar à Autoridade Nacional de Proteção de Dados (ANPD);

III - notificar ao órgão correcional da [Universidade/Instituto] para apuração dos fatos por meio de procedimento administrativo disciplinar cabível;

III – notificar, quando cabível, à Comissão de Ética Pública da [Universidade/Instituto] para apuração ética de conduta em desacordo com as normas éticas pertinentes;

Parágrafo único. O canal institucional para recebimento de denúncias ou reclamações é o sistema Fala.Br, sob responsabilidade da Ouvidoria Pública da [Universidade/Instituto].

Seção XX

Do Descumprimento e Responsabilização

Art. Z Ações no tratamento de dados pessoais pelos servidores, ou quem de alguma forma atua para ou em nome da [Universidade/Instituto] será irregular quando violarem dados pessoais, ou esta Política e legislação aplicável.

Parágrafo único. As violações de dados pessoas poderão acarretar, isolada ou cumulativamente, nos termos das normativas internas e da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. Z As sanções administrativas aos servidores, ou quem de alguma forma atua para ou em nome da [Universidade/Instituto], em caso de descumprimento de termos estabelecidos por este documento, serão aplicadas com base na legislação vigente e nas regulamentações internas da [Universidade/Instituto].

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. Z As solicitações de informações pelos titulares, os pedidos voluntários de revogação do consentimento ou eliminação de dados onde existiu consentimento, deverão ser realizadas através da plataforma Fala.BR e encaminhadas ao Encarregado de Dados da [Universidade/Instituto].

Art. Z As dúvidas sobre a Política de Proteção de Dados Pessoais e seus documentos devem ser submetidas ao Comitê Gestor de Proteção de Dados Pessoais**.**

Art. Z Os casos omissos serão resolvidos pelo Comitê Gestor de Proteção de Dados Pessoais.

Art. Z A presente política deverá ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, ou quando houver alteração de legislação, a partir do início de sua vigência.

Art. Z Esta Resolução entrará em vigor na data de sua publicação.

[Liste, caso necessário, as diretrizes finais da Política de Proteção de Dados Pessoais]

5 CONSIDERAÇÕES FINAIS

A implementação de uma política de governança para a proteção de dados pessoais nas Instituições Federais de Ensino Superior (IFES) é uma demanda urgente, devido à crescente importância da proteção de dados em um contexto de rigorosa regulação e às auditorias anuais realizadas pelo Tribunal de Contas da União (TCU) sobre o tema. Com base no arcabouço legal estabelecido pela LGPD é essencial que as IFES ajustem seus processos e políticas de tratamento de dados pessoais para assegurar a conformidade legal e resguardar direitos fundamentais, como a privacidade e a liberdade individual.

Nesse viés, essa pesquisa teve como objetivo principal propor diretrizes para a implementação de políticas de governança para proteção de dados pessoais em IFES. Foram analisadas as políticas já em vigor nas IFES participantes do estudo, bem como o modelo de Política de Proteção de Dados elaborado pelo Ministério da Gestão e Inovação (MGI), complementado por entrevistas com Encarregados pela Proteção de Dados Pessoais dessas instituições, almejando alinhá-las aos critérios estabelecidos pela LGPD.

Os objetivos específicos, como verificar diretrizes e boas práticas de proteção de dados, identificar processos de elaboração e implementação dessas políticas, e elaborar um modelo de minuta de política de proteção de dados para as IFES, foram alcançados por meio de uma análise detalhada das práticas em curso. A investigação permitiu identificar elementos fundamentais para uma política eficaz, como a definição clara de responsabilidades, o tratamento adequado dos dados, a segurança da informação e a capacitação contínua dos envolvidos.

A análise dos fluxos de elaboração dessas políticas em diversas instituições revelou similaridades nas fases de aprovação e publicação, mas também divergências nos estágios iniciais, onde algumas priorizam diagnósticos institucionais, enquanto outras se concentram na compatibilidade normativa. Essas diferenças reforçam a necessidade de um fluxo mais eficiente, adaptável à realidade das diversas IFES, especialmente aquelas com estruturas mais enxutas. A proposta de fluxo sugerida na pesquisa visa justamente essa eficiência, incluindo a análise institucional inicial e a participação de comitês de governança digital e da procuradoria, promovendo uma abordagem abrangente e robusta.

Além disso, a criação de um comitê permanente para a governança de proteção de dados e segurança da informação, em vez de grupos de trabalho temporários, mostrou-se uma estratégia crucial para garantir a continuidade e a preservação do conhecimento adquirido durante o processo de adequação. A composição sugerida desse comitê, abrangendo áreas como jurídico, segurança da informação, tecnologia da informação e comunicação, auditoria interna,

ouvidoria e representações das pró-reitorias, reflete a necessidade de uma abordagem integrada e multidisciplinar.

Ferramentas metodológicas como PDCA, SWOT e 5W2H foram destacadas como importantes no processo de implementação dessas políticas, mas o benchmarking emergiu como uma ferramenta fundamental para instituições que estão iniciando o processo, permitindo a comparação e a adoção de práticas bem-sucedidas de outras IFES.

Assim, conclui-se que a criação de políticas de governança para a proteção de dados pessoais nas IFES deve seguir uma abordagem integrada e adaptável, sustentada por comitês permanentes, garantindo a continuidade e eficiência das ações. A pesquisa destaca a importância da conformidade com a LGPD e o papel central das IFES na promoção da proteção de dados, assegurando a segurança e privacidade de dados no contexto educacional.

Adicionalmente, foi constatado que os regulamentos exigem mudanças significativas nos processos de governança organizacional, revisão de procedimentos e transformações culturais voltadas à proteção de dados pessoais. Contudo, a ausência de um guia específico para a criação de políticas de proteção de dados no contexto das IFES indica a necessidade de diretrizes claras e adaptadas à complexidade organizacional dessas instituições, que lidam com grandes volumes e diversidade de dados pessoais.

Nesse diapasão, por meio da análise realizada, foi possível, portanto, elaborar uma minuta de Política de Proteção de Dados para as IFES, baseada nos resultados da análise comparativa das políticas existentes e no referencial teórico da pesquisa. Este modelo oferece uma base que pode ser adaptada por outras instituições para garantir a conformidade com a LGPD e assegurar a proteção eficaz dos dados pessoais.

Por fim, esta pesquisa contribui para o desenvolvimento de políticas institucionais de proteção de dados nas IFES, oferecendo diretrizes e práticas que podem ser adotadas para assegurar o cumprimento da legislação e fortalecer a cultura de proteção de dados nas instituições de ensino superior. Recomenda-se que pesquisas futuras continuem a explorar a implementação dessas políticas, considerando as particularidades e desafios dos diferentes contextos organizacionais e culturais. Esses guias poderiam oferecer um passo a passo detalhado para que as IFES possam criar e implementar políticas de proteção de dados mais eficazes, alinhadas tanto à LGPD quanto às necessidades internas de governança. A criação de frameworks adaptáveis, que levem em consideração as diferenças estruturais e de recursos entre as diversas IFES, também seria um aspecto importante a ser tratado nessas pesquisas.

Recomenda-se também explorar a interseção entre a Lei Geral de Proteção de Dados (LGPD) e o tratamento de dados históricos e sensíveis, como os que emergem da Comissão da

Verdade e de outros esforços de justiça de transição. A Comissão da Verdade, que investigou violações dos direitos humanos durante o período da ditadura militar no Brasil, gerou um vasto acervo de dados históricos sensíveis, incluindo testemunhos e informações pessoais. A relação entre esses dados e a LGPD abre um campo de investigação relevante, pois é necessário balancear a proteção da privacidade e os direitos dos indivíduos com o interesse público e a preservação da memória histórica.

REFERÊNCIAS

ARCOVERDE, L; RAMOS, M.V; ZANATTA, R S. **Transparência sob ataque:** LGPD está sendo utilizada indevidamente para cercear o acesso a informações públicas. Folha de São Paulo, 4 de nov. de 2021. Disponível em: https://www1.folha.uol.com.br/opiniao/2021/11/transparencia-sob-ataque.shtml. Acesso em 25 de jul. de 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT **NBR ISSO/IEC 27002:2005** Tecnologia da informação - Técnicas de segurança - Código de Prática para de segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT **NBR ISSO/IEC 27002:2013**: Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT **NBR ISO/IEC 29100:2020**: Tecnologia da informação-técnicas de segurança-estrutura de privacidade. Rio de Janeiro, 2020.

AVELINO, D. P. DE; POMPEU, J. C.; FONSECA, I. F. DA. TD 2624 - Democracia digital: mapeamento de experiências em dados abertos, governo digital e ouvidorias públicas. **Texto para Discussão**, p. 1–52, 2021.

BASAN, A. P. **Publicidade digital e proteção de dados pessoais:** o direito ao sossego. Editora Foco, São Paulo, 2021.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. Forense Rio de Janeiro, 2019.

BIONI, B. R; RIELLI, M. M. A. **A Construção Multissetorial da LGPD:** História e Aprendizados, in: Proteção de dados: contexto, narrativas e elementos fundantes [livro eletrônico]. (Organização Bruno Ricardo Bioni), B. R. Bioni Sociedade Individual de Advocacia, 2021.

BIONI, B. R; ZANATTA, R. A. F. **A Infraestrutura Jurídica da Economia dos Dados:** dos princípios de justiça às leis de dados pessoais, in: Proteção de dados: contexto, narrativas e elementos fundantes [livro eletrônico]. (Organização Bruno Ricardo Bioni), B. R. Bioni Sociedade Individual de Advocacia, 2021.

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: Coletânea de artigos da pós-graduação em ouvidoria pública**, v. 1, n. 1, p. 8–19, 2022.

BRASIL. ANPD. Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte. Brasília: ANPD, 2021.

BRASIL. ANPD. Guia de elaboração de programa de governança em privacidade: Lei Geral de Proteção da dados. Brasília: ANPD, 2020.

BRASIL. ANPD. **Guia de elaboração de termo de uso e política de privacidade para serviços públicos**. Brasília: ANPD, 2022.

BRASIL. ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 20 de jul. de 2022b.

BRASIL. ANPD. **Guia orientativo de tratamento de dados pessoais pelo poder público**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 24 fev. 2023.

BRASIL. ANPD. **Texto para discussão nº 1/2022 - Estudo técnico**: A LGPD e o tratamento de dados pessoais para fins acadêmicos e para realização de estudos por órgão de pesquisa. Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_2022_17.pdf. Acesso em 06/03/2023.

BRASIL. ENAP. **Governo aberto: transparência e dados abertos**. Brasília: Fundação Escola Nacional de Administração Pública, 2022.

BRASIL. MGI. **Modelo de Política de Proteção de Dados Pessoais:** Programa de Privacidade e Segurança da Informação (PPSI). Brasília: MGI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modeloppdp.pdf. Acesso em: 24 de abr. de 2024.

BRASIL. SGD. **Programa de Privacidade e Segurança da Informação (PPSI).** Brasília: MGI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 08 de ago. de 2024.

BRASIL. Casa Civil da Presidência da República. **Guia da política de governança pública**. Brasília. Casa Civil da Presidência da República, 2018.

BRASIL. Comitê Central de Governança de Dados. **Guia de boas práticas - Lei Geral de Proteção de Dados Pessoais**. Brasília: Ministério da Economia., 2020b.

BRASIL. Constituição (2022). **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais… Brasília: Presidência da República, 10 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 09 jul. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 04 de jul. 2022.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Programa Nacional de Gestão Pública – GesPública**: Instruções para avaliação da gestão pública. Brasília: Prêmio Nacional de Gestão Pública – PQGF**,** 2009.

BRASIL. **Proteção de Dados Pessoais agora é um direito fundamental**. 2022. ANPD. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental. Acesso em: 09 jul. 2022.

BRASIL. Tribunal de Contas da União. **Dez passos para a boa governança**. Tribunal de Contas da União. 2 ed. Brasília: TCU, Secretaria de Controle Externo da Administração do Estado, 2021a.

BRASIL. Tribunal de Contas da União. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD) No Âmbito das Contratações do TCU**. Brasília: TCU, 2021b.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU**. Tribunal de Contas da União. 3 ed. Brasília: TCU, Secretaria de Controle Externo da Administração do Estado, 2020a.

BRASIL. Câmara dos Deputados. Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas. **Agência Câmara de Notícias**. Publicado em 18/11/2021. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de--protecao-de-dados-dizem-especialistas/. Acesso em 09 fev. 2023.

BRASIL. **Decreto nº 10.046/2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília: Presidência da República. 09 out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Decreto/D10046.htm. Acesso em 06 mar. 2023.

BRASIL. **Lei nº 9.610/1988**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília: Presidência da República. 19 de fevereiro de 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm.Acesso em 06 mar. 2023.

BRASIL. **Lei nº 9.394/1996**. Estabelece as diretrizes e bases da educação nacional. Brasília: Presidência da República. 20 dez. de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em 06 mar. 2023.

BRASIL, **Lei nº 12.527/2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República. 18 nov. de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06 mar. 2023.

BRASIL. **Lei nº 11.892/2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Brasília: Presidência da República. 29 dez. de 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Acesso em: 06 mar. 2023.

BRASSCOM. **Manifesto pela aprovação da lei de proteção de dados pessoais**. Disponível em: https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/. Acesso em: 04 de junho de 2022.

BUSKIRK, H. **Business and Administrative Policy**: text, cases, incidents and readings. New York: Wiley, 1971.

CABELLA, D. **Guia Prático de Governança em Privacidade**. Rio de Janeiro. Zoox Smart Data, 2020.

CAMPOS, V. F. **Gerenciamento da rotina do trabalho do dia-a-dia**. 8. ed. Belo Horizonte: Editora de Desenvolvimento Gerencial, 2004.

CANCELIER, M. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência:** Estudos Jurídicos e Políticos, Florianópolis, v. 76, n. 38, p. 213-239, 20 set. 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213. Acesso em: 05 jul. 2022.

CARPINETTI, L. C. R; GEROLAMO, M. C. **Gestão da Qualidade ISO 9001: 2015**: requisitos e integração com a ISO 14001:2015. 1. ed. São Paulo: Atlas, 2016.

CASTRO, C. A. P.de; FALCÃO, L. P. Ciência política: uma introdução. São Paulo - SP: Atlas, 2004.

CHIZZOTTI, A. **Pesquisa qualitativa em ciências humanas e sociais**. 3. ed. Petrópolis: Vozes, 2010.

CRISTÓVAM, J. S.; HAHN, T. M. Revista de Direito Administrativo. **Revista de Direito Administratico e Gestão Pública**, v. 6, n. 11, p. 0, 2020.

COTS, M. **Como incentivar um comportamento em prol da proteção de dados?** Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/cultura-privacidade-lgpd-governanca: acesso em 12 set. 2022.

CRAVO, D. C. Perspectivas gerais sobre os direitos do titular dos dados no poder público. In: CRAVO, D. C; CUNDA, D. Z.G; RAMOS, R. (Orgs.). **Lei Geral de Proteção de Dados e o Poder Público.** Porto Alegre: Tribunal de Contas do Estado do Rio Grande do Sul, 2021.

DATA PRIVACY BRASIL. **Privacidade e Proteção de Dados: Teoria e Prática** - Data Privacy Brasil. ago. de 2023. Disponível em: https://dataprivacy.com.br/cursos/curso-privacidade-e-protecao-de-dados-teoria-e-pratica/. Acesso em 25 de jul. de 2024.

DENHARDT, R. B. **Teorias da Administração Pública**. São Paulo: Cengage Learning, 2012.

DONEDA, D. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. [livro eletrônico] 2. ed. Revista dos Tribunais, São Paulo, 2020.

DYE, T. D. Mapeamento dos Modelos de Análise de políticas públicas. In: HEIDEMANN, F. G.; SALM, J. F. (Orgs.). **Políticas públicas e desenvolvimento:** bases epistemológicas e modelos de análise. 2. ed. [S.l.]: Universidade de Brasília, 2010. p. 99-127. cap. 3.

DYE, T. D. **Understanding Public Policy.** Englewood Cliffs, N.J.: PrenticeHall. 1984.

FERNANDES, I. F.; ALMEIDA, L. A. **Teorias E Modelos De Políticas Públicas**: Uma Revisão Das Theories and Models of Public Policies : a Review of the. p. 122–146, 2019.

FERREIRA, M. C. **Qualidade de vida no trabalho**: uma abordagem centrada no olhar dos trabalhadores. 2. ed. Brasília-DF: Paralelo 15, 2012.

FINKELSTEIN, M. E.; FINKELSTEIN, C. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284, 2020.

FONTES, E. L. G. **Políticas e normas para a segurança da informação**: Como desenvolver implantar e manter a regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FRANÇA, G. F. F; MARTINS, P. B. L (orgs.). Entrelinhas: **Explorando a Privacidade e Proteção de Dados em comunidade**. São Paulo: Data Privacy Brasil. 2024. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2024/01/entrelinhas-vf. pdf. Acesso em: 31 de jul. de 2024.

FRAZÃO, A. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO. G; FRAZÃO, A; OLIVA M. D. (Coords.). **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro**. [livro eletrônico] São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte I, cap. 1. p. 10-25.

FUNG, A. Varieties of participation in complex governance. **Public Administration Review**, v. 66, n. SUPPL. 1, p. 66–75, 2006.

GODOI, C. K; MELLO, R. B; SILVA, A. B. **Pesquisa qualitativa em estudos organizacionais: paradigmas, estratégias e métodos.** São Paulo: Saraiva, 2006.

HEIDEMANN, F. G. Do sonho de progresso às políticas de desenvolvimento. In: HEIDEMANN, F. G.; SALM, J. F. **Políticas públicas e desenvolvimento:** bases epistemológicas e modelos de análise. Brasília: Universidade de Brasília, 2014, p. 23-49.

HEIDEMANN, F. G. Do sonho do progresso às políticas de desenvolvimento. In: HEIDEMANN, F. G.; SALM, J. F. (Orgs.). **Políticas públicas e desenvolvimento:** bases epistemológicas e modelos de análise. 2. ed. Brasilia: Universidade de Brasília, 2010. p. 23-40. cap. 1.

IDESP. Instituto Daryus de Ensino Superior Paulista. **Manual LGPD para PME pequenas e médias empresas**. (Ebook) São Paulo. IDESP, 2021.

INSTITUTO BRASILEIRO DE GOVERNANÇA PUBLICA. IBGP. **Desafios da Governança e da Gestão Pública Brasileira**. 1. ed. Brasília: IBGP, 2002.

KONDER, C. N. O Tratamento dos dados pessoais sensíveis à luz da lei 13.709/2018? In: FRAZÃO, A, TEPEDINO. G; OLIVA, M. (Coords.) **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro**. [livro eletrônico] São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte II, cap. 1. p. 261-272.

LEONTIADES, Milton. **Management Policy, Strategy and Plans**. Boston: Little, Brown and Company, 1982.

LIMA, A D; ALVES, D. Normativos internos para demonstrar governança em privacidade. In: LIMA, A; SAMANIEGO, D; BARONOVSKY, T. (Orgs.). **LGPD para contratos: adequando contratos e documentos à Lei Geral de Proteção de Dados.** São Paulo: Expressa, 2021.

LIMA, A. P. M. C; ALMEIDA D; MAROSO, E. P. **Lei geral de proteção de dados:** Sua empresa está pronta? São Paulo: Literare Books International, 2020.

LIMA, C. C. Capítulo II - Do Tratamento de Dados Pessoais: Seção I - Dos requisitos para tratamento de dados pessoais: In: MALDONADO, V. N; BLUM, R. O. (Orgs.). **Lei Geral de Proteção de Dados**: comentada. [livro eletrônico] 2. ed. São Paulo: Revista dos Tribunais, 2019. Cap. 2. p. 201-241.

LIMBERGER, T. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI): um diálogo (im)possível? As influências do direito europeu. **Revista de Direito Administrativo**, v. 281, n. 1, p. 113–144, 2022.

LGPD no Setor Público. [*S. l.: s. n.*], 2022. 1 vídeo (1:55 h). Publicado pelo canal anpdgov. Disponível em: https://youtu.be/tyWsgCReG98. Acesso em: 28 fev. 2023.

LYNN, L. E. **Designing Public Policy:** A Casebook on the Role of Policy Analysis. Santa Monica, California: Goodyear, 1980.

MALDONADO, V. N. Capítulo III – Dos Direitos do Titular: In: MALDONADO, V. N; BLUM, R. O. (Orgs.). **Lei Geral de Proteção de Dados**: comentada. [livro eletrônico] 2. ed. São Paulo: Revista dos Tribunais, 2019. Cap. 2.

MARTINS, P. CRUZ, S. Presente e Futuro da Proteção de Dados nas Organizações Brasileiras. Revista Data, São Paulo, v. 1, n. 1. p. 4-1, mar. 2022.

MATOS, A. C. H; RUZYK, C. E. P. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: FRAZÃO, TEPEDINO. G; FRAZÃO A; OLIVA M. D. (Coords.). **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro**. [livro eletrônico] São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte I, cap. 7. p. 106-117.

MAYER-SCHOENBERGER, V.; CUKIER, K. **Big Data:** a revolution that will transform how we live, work, and think. Londres: John Murray, 2013.

MEAD, L. M. **"Public Policy: Vision, Potential, Limits"**, Policy Currents, Fevereiro: 1-4. 1995.

MENEZES, J. B; COLAÇO, H. S. Quando a lei geral de proteção de dados não aplica? In: FRAZÃO, TEPEDINO. G; FRAZÃO A; OLIVA M. D. (Coords.). **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro**. [livro eletrônico] São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte I, cap. 6. p. 77-105.

MEYER JR, V. A prática da administração universitária: contribuições para a teoria. In: MEYER, B; MELO, P. (Orgs.). **Administração universitária em de tempo de mudança**: novos rumos e desafios. 1 ed. Curitiba: Appris, 2021.

MESQUITA, H. MEIRA, M. Adequação do Setor Público à LGPD. Revista Data, São Paulo, v. 1, n. 1. p. 4-1, mar. 2022.

MICHELETTI, M; BORGES, T. T; COSTA D. G. **Descomplicando a LGPD**: O efeito prático da lei. MICHELETTI, M (Coord.). [livro eletrônico]1 ed. São Paulo: Câmara Brasileira do Livro, 2022.

MINTZBERG, H; QUINN, J. B, **O processo da estratégia**: conceitos, contextos e casos selecionados. Porto Alegre: Artmed, 2006. Tradução Luciana de Oliveira da Rocha.

MOREY, T.; KRAJECKI, K. Personalisation, data and trust: The role of brand in a data-driven, personalised, experience economy. Journal of Brand Strategy, [s. l.], v. 5, n. 2, p. 178-185, 2016. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=120015362&lang=pt-br&site=ehost-live. Acesso em: 12 de ago. 2022.

OCDE. Recommendation of the OECD Public Governance Committee Council on Open Government, 13 dez. 2017. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0438. Acesso em 16 fev. 2023.

OLIVEIRA, D, P, R. **Planejamento Estratégico**: conceitos, metodologia, práticas. 23. ed. São Paulo: Atlas, 2007.

OLIVEIRA, M. A. B; LOPES, I.M.P. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: FRAZÃO, TEPEDINO. G; FRAZÃO A; OLIVA M. D. (Coords.) **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro** [livro eletrônico]: São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte I, cap. 2. p. 26-41.

PELTIER, T. **Information Security Fundamentals**. USA: Auerbach, 2005.

PETERS, B. G. **American Public Policy.** Chatham, N.J.: Chatham House. 1986.

PINHEIRO, P. P. **Nova Lei brasileira de proteção de dados pessoais** (LGPD) e o impacto nas instituições públicas e privadas. [Revista eletrônica] Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 10, n. 97, p. 75-87, mar. 2021.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (lgpd). São Paulo: Saraiva, 2018.

PIZA, B; ASSIS, C. **LAI e LGPD**: um conflito que não existe. Controladoria Geral do Estado de Goiás. Goiânia, 08 jun. 2022. Disponível em: https://www.controladoria.go.gov.br/noticias/15934-lai-e-lgpd-um-conflito-que-n%C3%A3o-existe.html#:~:text=O%20cerne%20do%20conflito%20inexistente,completamente%20dissociados%20entre%20as%20leis. Acesso em: 07 fev. 2023.

POSSAMAI, A. J.; SOUZA, V. G. Transparency and open Government Data: Possibilities and Challenges Based on the Access to Information Law-Web of Science Core Collection. **Administracao Publica E Gestao Social**, v. 12, 2020.

REDFORD, E S. **Democracy in the Administrative State**. New York: Oxford University Press, 1969.

ROESCH, S. M. A. **Projetos de Estágio e de Pesquisa em Administração**. 3 a ed. São Paulo: Atlas, 2010.

SARAVIA, E; FERRAREZI, E. **Políticas Públicas**: Coletâneas. Brasília: ENAP, 2006.

SAUNDERS, M.; LEWIS, P.; THORNHILL, A. **Research Methods for Business Students**. 7 a ed. Harlow, England: Pearson, 2016.

SECCHI, L. **Políticas Públicas Conceitos, esquemas de análise casos práticos**. São Paulo: Cengage Learning, 2013.
SHINTAKU, M; SOUSA, R; COSTA, L; MOURA, R; MACEDO, D. Discussões sobre política de privacidade de dados em um sistema de informação governamental. **Em Questão**, Porto Alegre, v. 27, n. 4, p 39-60. 2021.

SIEBRA, S. A.; XAVIER, G. A. C. Políticas de Privacidade da Informação: caracterização e avaliação. **Biblos**: Revista do Instituto de Ciências Humanas e da Informação, Rio Grande. v. 34, n. 02, p. 72-88, jul./dez. 2020. Disponível em: https://www.seer.furg.br/biblos/article/view/11870/8428. Acesso em: 06 set. 2022.

SILVA JUNIOR, A. **Uma proposta de política de inovação para os servidores técnico-administrativos do IFSC campus Florianópolis.** 2018. 177 p. Dissertação (Mestrado profissional) - Universidade Federal de Santa Catarina, Centro Sócio-Econômico, Programa de Pós-Graduação em Administração Universitária, Florianópolis, 2018. Disponível em: http://www.bu.ufsc.br/teses/PPAU0173-D.pdf

SILVA, J. O; MELO, P. Potencializando o pensamento estratégico em universidades. In: MEYER, B; MELO, P. (Orgs.). **Administração universitária em de tempo de mudança**: novos rumos e desafios. 1 ed. Curitiba: Appris, 2021.

SMITH, G.; MAY, D. The Artificial Debate Between Rationalist and Incrementalist Models of Decision-Making', Policy and Politics, v. 8, n. 2, 1980.

SOUZA, C. A. P. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: FRAZÃO, TEPEDINO. G; FRAZÃO A; OLIVA M. D. (Coords.). **Lei Geral de Proteção de Dados e suas Repercussões no Direito Brasileiro**. [livro eletrônico] São Paulo: Thomson Reuters - Revista dos Tribunais, 2019. Parte I, cap. 15. p. 246-259.

DAVOLI, G. B; OLIVEIRA, A. A; SILVA, G. H. Afinal, que caminho preciso percorrer para me adequar à Lei Geral de Proteção de dados Pessoais? 25 maio. 2020. Disponível em: https://baptistaluz.com.br/adequacao-lei-geral-protecao-dados/. Acesso em: 13 maio. 2024.

SOUZA, C. Políticas públicas: uma revisão da literatura. **Sociologias**, n. 16, p. 20–45, 2006.

TASSO, F. Do Tratamento de Dados Pessoais pelo Poder Público. In: MALDONADO, V. N.; BLUM, R. O. (orgs.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 245–288

TEIXEIRA, I. **LGPD e LAI: uma análise sobre a relação entre elas.** 30 mar. 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd. Acesso em: 16 fev. 2023.

TEIXEIRA, T; STINGHEN, J. O Papel do DPO na orientação do projeto de adequação à LGPD. In: TEIXEIRA et al (Orgs.). **DPO (Encarregado de dados pessoais)**: Teoria e prática. São Paulo: Expressa, 2022.

THE ECONOMIST. **The world's most valuable resource**. Disponível em: https://www.economist.com/weeklyedition/2017-05-06. Acesso em: 21 de jul. 2022.

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

UFRJ. Lei Geral de Proteção de Dados Pessoais (LGPD) - A LGPD e as Universidades. Disponível em: https://ufrj.br/acesso-a-informacao/lgpd/. Acesso em 06 mar. 2023.

UFSC. Plano de Desenvolvimento Institucional. Disponível em: https://pdi.ufsc.br/. Acesso em 20 de jul. 2022.

VAINZOF, R. Capítulo I: disposições preliminares. In: MALDONADO, V. **N**; BLUM, R. O. (Orgs.). **Lei Geral de Proteção de Dados**: comentada. [livro eletrônico] 2. ed. São Paulo: Revista dos Tribunais, 2019. Cap. 1. p. 22-200.

VERGARA, S. C. **Projetos e Relatórios de Pesquisa em Administração**. 14a ed. São Paulo: Atlas, 2013.

WEIBLE, C. M.; CARTER, D. P. Advancing Policy Process Research at Its Overlap with Public Management Scholarship and Nonprofit and Voluntary Action Studies. **Policy Studies Journal**, v. 45, n. 1, p. 22–49, 2016.

ZAPPELLINI, M. B; FEUERSCHÜTTE, S. G.). O uso da triangulação na pesquisa científica brasileira em Administração. **Administração: Ensino E Pesquisa**, v16n2.238, 2015.

ZUBOFF, S. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021. 800 p. Tradutor: George Schlesinger.

APÊNDICE A - Roteiro de entrevista

Roteiro de Entrevista para Encarregados de Tratamento de Dados

Siglas:
PPDP – Política de Proteção de Dados Pessoais
LGPD – Lei Geral de Proteção de Dados Pessoais

1 PROCESSO DE ELABORAÇÃO da PPDP

a) Quem foi/foram o (os) responsável (eis) pela elaboração de PPDP na instituição?
b) Quais critérios foram adotados para a seleção das pessoas e setores/departamentos para o processo de elaboração?
c) Foi utilizada alguma metodologia, ferramenta, ou sistema durante o processo de elaboração?
d) Quais foram os critérios para a seleção da metodologia, ferramenta, ou sistema durante o processo de elaboração?
e) O processo de elaboração de PPDP foi divido por fases ou etapas?
f) Você pode descrever brevemente cada fase, ou etapa?
g) Na sua percepção, você poderia citar e descrever os erros ou desafios encontrados na fase de elaboração da PPDP?

2 QUANTO AO CONTEÚDO/ELEMENTOS DA PPDP

h) Para elaboração do texto da PPDP (conteúdo/ elementos), quais foram as fontes e referências utilizadas além da LGPD?

3 PROCESSO DE IMPLEMENTAÇÃO DA PPDP

i) Quem foi/foram o (os) responsável (eis) pela implementação de PPDP na instituição? Houve participação de pessoas externas, ou outras organizações/instituições?
j) Quais critérios foram adotados para a seleção das pessoas setores/departamentos para o processo de implementação?
k) Foi utilizada alguma metodologia, ferramenta, ou sistema durante o processo de implementação?
l) Quais foram os critérios para a seleção da metodologia, ferramenta, ou sistema durante o processo de implementação?
m) O processo de implementação de PPDP foi divido por fases ou etapas?
n) Você pode descrever brevemente cada fase, ou etapa?
o) Na sua percepção, você poderia citar e descrever os erros ou desafios encontrados na fase de implementação da PPDP?

APÊNDICE B - Termo de Consentimento Livre e Esclarecido

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - TCLE

Meu nome é Alan Ribeiro Rodrigues, sou mestrando do Programa do Programa de Pós-graduação em Administração Universitária (PPGAU) da Universidade Federal de Santa Catarina (UFSC). Estou realizando uma pesquisa sob supervisão do professor Dr. Maurício Rissi, cujo objetivo geral é propor diretrizes para implementação de política de proteção de dados pessoais em IFES.

Você está sendo convidado a participar desta pesquisa, que será realizada por meio de entrevista (com roteiro semiestruturado previamente enviado por e-mail) e será gravada em áudio e vídeo, com tempo estimado entre 30 e 50 minutos. Assim, cabe esclarecer que a participação é voluntária podendo se recusar a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem qualquer tipo de constrangimento, pelos contatos do pesquisador constante neste TCLE.

A seguir, listam-se os riscos identificados, bem como as precauções a serem tomadas pelo pesquisador para minimizar ou mitigar o risco.

Risco identificado	Precauções adotadas
Cansaço ou aborrecimento ao responder os questionamentos da entrevista	- Dar ciência ao participante da duração estimada e do procedimento envolvido; - O participante escolherá data, hora e local da entrevista; - Encaminhar previamente o TCLE e o roteiro de entrevista para que o participante tome ciência com antecedência; - O participante poderá, a qualquer tempo, interromper, adiar ou cancelar sua participação.
Desconforto ou constrangimento durante a gravação de áudio da entrevista	- O participante, pode optar por não gravar em áudio e vídeo. Contudo, neste caso, a entrevista poderá ter a duração aumentada para que se efetivem os registros manuais das falas. - Poderá, a qualquer tempo, interromper, adiar ou cancelar sua participação.
As perguntas, apesar de serem estritamente sobre a prática profissional, podem evocar memórias e mobilizar sentimentos nem sempre agradáveis	- O participante poderá, a qualquer tempo, interromper, adiar ou cancelar sua participação.
Risco de transtornos ou danos às relações pessoais e profissionais, em caso de vazamento de dados/quebra de anonimato do entrevistado (ainda que involuntário e não intencional).	- Somente o pesquisador e seu orientador terão acesso aos dados e tomarão todas as providências necessárias para manter o anonimato do participante; - Todas as falas incluídas no texto serão duplamente revisadas para evitar a identificação, mesmo que involuntária.

A pesquisa não proporcionará ao participante qualquer tipo de benefício direto, inclusive sendo vedado pela legislação brasileira qualquer tipo de compensação financeira pela sua participação. Porém, caso alguma despesa extraordinária associada à pesquisa venha a ocorrer, você será ressarcido nos termos da lei. Entretanto, espera-se, como benefício direto desta pesquisa, proporcionar futura análise acerca das práticas de gestão da informação desempenhada pelos programas de excelência da UFSC de modo a melhor compreender os aspectos favoráveis e limitadores do processo. E, como benefício indireto, esperam-se produções bibliográficas decorrentes da pesquisa, que fomentem as discussões da área proteção de dados pessoais aplicadas às IFES

É garantido ao participante, o ressarcimento de eventuais despesas diretamente decorrentes de sua participação na pesquisa. É garantida a indenização diante de eventuais danos decorrentes da pesquisa, de acordo com a legislação vigente e amplamente consubstanciada. Não será exigido do participante da pesquisa, sob qualquer argumento, renúncia ao direito de procurar obter indenização por danos eventuais.

O pesquisador compromete-se a encaminhar os resultados da pesquisa aos entrevistados (dissertação e artigos posteriores) tão logo sejam publicados.

O pesquisador responsável, que também assina este documento, compromete-se a conduzir a pesquisa de acordo com o que preconiza a Resolução CNS 510/16, que trata de preceitos éticos e da proteção aos participantes da pesquisa. Solicitamos a sua autorização para o uso de seus dados para a produção da dissertação de mestrado e de artigos técnicos e científicos. Sendo garantindo o anonimato do participante.

O acompanhamento e a assistência ao participante referente a quaisquer dúvidas, dificuldades ou necessidades relativas à pesquisa serão feitos pelo mestrando, no e-mail alan.ribeiro@ufsc.br, pelo telefone (48) 984381375 ou pelo Programa de Pós-graduação (PPGAU/UFSC) pelo telefone (48) 3721-6525 ou pessoalmente na sala do PPGAU, terceiro andar do Bloco G/CSE, Trindade, Florianópolis/SC. Você também poderá entrar em contato com o Comitê de Ética em Pesquisa com Seres Humanos da UFSC (CEPSH/UFSC) pelo telefone (48) 3721-6094, e-mail cep.propesq@contato.ufsc.br ou pessoalmente no endereço: Prédio Reitoria II. Rua: Desembargador Vitor Lima, nº 222, sala 701, Trindade, Florianópolis/SC. O CEPSH é um órgão colegiado interdisciplinar, deliberativo, consultivo e educativo, vinculado à Universidade Federal de Santa Catarina, mas independente na tomada de decisões, criado para defender os interesses dos participantes da pesquisa em sua integridade e dignidade e para contribuir no desenvolvimento da pesquisa dentro de padrões éticos.

Agradecemos a sua participação.

Alan Ribeiro Rodrigues	Dr. Maurício Rissi
Mestrando	Orientador

Participante:

Assinatura _____ Data: ____/____/__