

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA (PROFIAP)

IGOR BEGA DE MIRANDA

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: UM ESTUDO EM UMA UNIVERSIDADE FEDERAL

Recife
2025

IGOR BEGA DE MIRANDA

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: UM ESTUDO EM UMA UNIVERSIDADE FEDERAL

Dissertação apresentada ao Mestrado Profissional em Administração Pública (PROFIAP) da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Administração Pública.

Orientadora: Profa. Dra. Angela Cristina Rocha de Souza

Coorientadora: Profa. Dra. Maria Iraê de Souza Corrêa.

Recife

2025

IGOR BEGA DE MIRANDA

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: UM ESTUDO EM UMA UNIVERSIDADE FEDERAL

Dissertação apresentada ao Mestrado Profissional em Administração Pública (PROFIAP) da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Administração Pública.

Aprovada em: _____/_____/_____

BANCA EXAMINADORA

_____
Profa. Dra. Angela Cristina Rocha de Souza – Orientadora
Universidade Federal Rural de Pernambuco (UFRPE)

_____
Profa. Dra. Maria Iraê de Souza Corrêa - Coorientadora
Universidade Federal Rural de Pernambuco (UFRPE)

_____
Prof. Dr. Jorge da Silva Correia Neto - Examinador Interno
Universidade Federal Rural de Pernambuco (UFRPE)

_____
Profa. Dra. Telma Lúcia de Andrade Lima - Examinadora Externa
Universidade Federal Rural de Pernambuco (UFRPE)

_____
Prof. Dr. Luiz Gustavo de Sena Brandão Pessoa - Examinador Externo
Universidade Federal da Paraíba (UFPB)

Inserir dedicatória

AGRADECIMENTOS

Inserir epígrafe

RESUMO

O crescente uso das tecnologias tem gerado discussões globais sobre a criação de legislações que tratem da proteção de dados pessoais e da privacidade no âmbito digital. Nesse contexto, diversos países têm buscado regulamentar a proteção de dados para assegurar a privacidade e a segurança dos dados pessoais. A Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, introduziu no Brasil um regime de proteção de dados que abrange tanto o setor público quanto o privado, promovendo direitos fundamentais relacionados à privacidade e ao livre desenvolvimento da personalidade. Diante disso, este estudo buscou investigar como a LGPD vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE), avaliando as ações implementadas, os desafios enfrentados e o nível de maturidade da instituição em relação à proteção de dados, a fim de propor ações para fortalecer a proteção de dados pessoais na UFRPE. Metodologicamente, a pesquisa é caracterizada como aplicada, descritiva e estudo de caso, utilizando-se de dados documentais e de campo. Quanto à abordagem, trata-se de um estudo de natureza mista, com análise qualitativa e quantitativa. Os resultados apontaram que estão sendo realizadas ações para promover a proteção de dados pessoais, apesar da existência de desafios, sobretudo concernentes a restrições orçamentárias. Nesse contexto, foi possível constatar um nível intermediário de maturidade em relação à LGPD, o que demandará investimentos a longo prazo para consolidar uma cultura de proteção de dados pessoais na UFRPE. Conclui-se que a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da UFRPE com esforços consistentes da instituição para adequar-se à normativa. Tais iniciativas demonstram um comprometimento da autarquia na construção de uma cultura de privacidade e proteção de dados pessoais.

Palavras-chave: LGPD; instituições de ensino superior; proteção de dados; privacidade; segurança da informação.

ABSTRACT

The increasing use of technology has sparked global discussions on the creation of legislation addressing the protection of personal data and privacy in the digital sphere. In this context, several countries have sought to regulate data protection to ensure privacy and security of personal data. Brazil's General Data Protection Law (LGPD), inspired by the European Union's General Data Protection Regulation (GDPR), introduced a data protection framework that applies to both the public and private sectors, promoting fundamental rights related to privacy and the free development of personality. Against this backdrop, this study aimed to investigate how the LGPD has been implemented at the Federal Rural University of Pernambuco (UFRPE), evaluating the actions taken, the challenges faced, and the institution's level of maturity regarding data protection, in order to propose measures to strengthen personal data protection at UFRPE. Methodologically, the research is characterized as applied, descriptive, and a case study, using documentary and field data. As for its approach, the study is of a mixed nature, combining qualitative and quantitative analysis. The results indicated that actions are being taken to promote personal data protection, despite existing challenges, especially those related to budgetary constraints. In this context, an intermediated level of maturity in relation to the LGPD was identified, which will require l long-term investments to consolidate a culture of personal data protection at UFRPE. It is concluded that the General Data Protection Law (LGPD) is being applied at UFRPE with consistent efforts by the institution to comply with the regulation. These initiatives demonstrate the institution's commitment to building a culture of privacy and personal data protection.

Keywords: LGPD; higher education institutions; data protection; privacy; information security.

LISTA DE ILUSTRAÇÕES

Quadro 1 - Controles do *framework* do PPSI 37
Quadro 2 - Seções do *framework* de proteção de dados 38
Quadro 3 - Documentos institucionais consultados na pesquisa 49
Quadro 4 - Classificação de privacidade e proteção de dados 51
Quadro 5 - Elementos de análise dos documentos consultados na pesquisa 52
Quadro 6 - Estrutura da pesquisa 56
Quadro 7 - Documentos externos analisados na pesquisa 61
Quadro 8 - Objetivos relativos à gestão das TDIC na UFRPE 66
Quadro 9 - Alcance das metas relativas à gestão das TDIC na UFRPE 68
Quadro 10 - Ações de proteção de dados no âmbito da UFRPE 69
Quadro 11 - Matriz SWOT 73
Quadro 12 - Categorias da análise temática ou categorial 75
Quadro 13 - Análise da categoria Recursos Humanos 76
Quadro 14 - Análise da categoria Universidade 82
Quadro 15 - Análise da Categoria Legislação 89
Quadro 16 - Análise da Categoria Orçamento 95
Figura 1 - Logotipo do Programa Previna-se! 70
Figura 2 - Layout de vídeos sobre segurança da informação 71
Figura 3 - Fascículos da Cartilha de Segurança para Internet 72
Gráfico 1 - Nível de maturidade e classificação dos controles de proteção de dados 98

LISTA DE TABELAS

Tabela 1 - Segurança para Privacidade 99
Tabela 2 - Estrutura de Privacidade 100
Tabela 3 - Inventário de Dados Pessoais 102
Tabela 4 - Legitimidade do Tratamento 103
Tabela 5 - Atendimento a Requisições 104
Tabela 6 - Conformidade de Terceiros 106
Tabela 7 - Avaliação Geral 107

LISTA DE ABREVIATURAS E SIGLAS

AGU	Advocacia-Geral da União
ANPD	Autoridade Nacional de Proteção de Dados
CAEE	Certificado de Apresentação de Apreciação Ética
CCPA	*California Consume Privacy Act*
CEP	Comitê de Ética em Pesquisa
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CF	Constituição Federal
CGD	Comitê de Governança Digital
CGI.br	Comitê Gestor da Internet no Brasil
CGPPD	Comitê Gestor de Privacidade e Proteção de Dados
CGSI	Comitê Gestor de Segurança da Informação
CNPJ	Cadastro Nacional da Pessoa Jurídica
CNS	Conselho Nacional de Saúde
CONEP	Comissão Nacional de Ética em Pesquisa
CONSU	Conselho Universitário
CPF	Cadastro de Pessoa Física
CTDA	Comitê de Transparência e Dados Abertos
DPO	*Data Protection Officer*
E-Ciber	Estratégia Nacional de Segurança Cibernética
E-Digital	Estratégia Brasileira para a Transformação Digital
e-SIC	Serviço de Informação ao Cidadão
EGD	Estratégia de Governança Digital
EPD	Encarregado de Proteção de Dados
ETIR	Equipe de Tratamento e Respostas a Incidentes Cibernéticos
FGV	Fundação Getúlio Vargas
GDPR	*General Data Protection Regulation*
IBGE	Instituto Brasileiro de Geografia e Estatística
IES	Instituições de Ensino Superior
IFES	Instituições Federais de Ensino Superior
IND	Infraestrutura Nacional de Dados
	INEP Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
LAI	Lei de Acesso à Informação

LGPD	Lei Geral de Proteção de Dados Pessoais
LIA	Legítimo Interesse da Organização
MS	Ministério da Saúde
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
ONU	Organização das Nações Unidas
PCTIC	Plano de Contingência de Tecnologia da Informação e Comunicação
PDA	Plano de Dados Abertos
PDI	Plano de Desenvolvimento Institucional
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PLS	Projeto de Lei do Senado
PNSI	Política Nacional de Segurança da Informação
POSIC	Política de Segurança da Informação e Comunicação
PPPDP	Política de Privacidade e Proteção de Dados Pessoais
PPSI	Programa de Privacidade e Segurança da Informação
PROPLAN	Pró-Reitoria de Planejamento e Gestão Estratégica
PTT	Produto Técnico-Tecnológico
RAIS	Relação Anual de Informações Sociais
REGIC	Rede Federal de Gestão de Incidentes Cibernéticos
RIPD	Relatório de Impacto à Proteção de Dados
RGPD	Regulamento Geral sobre a Proteção de Dados
RNP	Rede Nacional de Ensino e Pesquisa
SIC	Segurança da Informação e Comunicação
SIPAC	Sistema Integrado de Administração, Patrimônio e Contratos
SIAPE	Sistema Integrado de Administração de Pessoal
SSIC	Subcomitê de Segurança da Informação e Comunicação
STD	Secretaria de Tecnologias Digitais
STF	Supremo Tribunal Federal
TCU	Tribunal de Contas da União
TCLE	Termo de Consentimento Livre e Esclarecido
TDIC	Tecnologias Digitais da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação
UFRPE	Universidade Federal Rural de Pernambuco

SUMÁRIO

1 INTRODUÇÃO 13
1.1 PROBLEMA DE PESQUISA 14
1.2 OBJETIVOS 17
1.2.1 Objetivo Geral 18
1.2.2 Objetivos Específicos 18
1.3 JUSTIFICATIVA 18
1.3.1 Justificativa teórica 18
1.3.2 Justificativa prática 19
1.4 ESTRUTURA DA DISSERTAÇÃO 20
2 REVISÃO DA LITERATURA **22**
2.1 PROTEÇÃO DE DADOS NO SETOR PÚBLICO 22
2.2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 28
2.3 LGPD NO SETOR PÚBLICO 34
3 PROCEDIMENTOS METODOLÓGICOS **48**
3.1 CARACTERIZAÇÃO DO ESTUDO 48
3.2 COLETA DE DADOS 49
3.3 ANÁLISE DE DADOS 51
3.4 ASPECTOS ÉTICOS 54
3.5 ESTRUTURA DA PESQUISA 56
4 RESULTADOS E DISCUSSÕES **57**
4.1 AÇÕES REALIZADAS NA PROMOÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA UFRPE 57
4.2 DESAFIOS PARA IMPLEMENTAR PRÁTICAS DE PROTEÇÃO DE DADOS NA UFRPE 73
4.3 NÍVEL DE MATURIDADE DA PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA UFRPE COM BASE NO *FRAMEWORK* PROPOSTO POR SANTANA E MENDONÇA (2023) 98
4.4 DIAGNÓSTICO E PROPOSIÇÃO DE AÇÕES PARA FORTALECER A PROTEÇÃO DE DADOS PESSOAIS NA UFRPE (PTT) 107
5 CONSIDERAÇÕES FINAIS **109**
REFERÊNCIAS **112**
APÊNDICE A – RELATÓRIO TÉCNICO-CONCLUSIVO E RECOMENDAÇÕES **124**
APÊNDICE B – ROTEIRO DE ENTREVISTA SEMIESTRUTURADO **141**
ANEXO – *FRAMEWORK* DE PROTEÇÃO DE DADOS **147**

1 INTRODUÇÃO

A proteção de dados tem suscitado inúmeras discussões mundiais sobre a criação de diplomas legais que tratam do direito à privacidade no âmbito digital, incluindo a real necessidade de instituir marcos regulatórios para a governança no ciberespaço, bem como verificar o modo e em que medida os instrumentos normativos são capazes de assegurar a proteção jurídica do direito à privacidade e à inviolabilidade dos dados pessoais.

Nesse sentido, conforme estudo realizado por Melo (2015), no ano de 1995, a União Europeia aprovou a diretiva 95/46/EC sobre este tema. O Canadá, por sua vez, regulamentou a matéria em meados dos anos 2000, no documento intitulado "*Personal Information Protection and Eletronic Documents Act*". No ano de 2014, a Organização das Nações Unidas (ONU), por meio de sua Assembleia Geral, aprovou a resolução denominada "O direito à privacidade na Era Digital", cujo teor recomendava que os Estados tomassem medidas concretas para proteção de seus cidadãos contra a utilização de dados por empresas.

Já o Brasil, apenas em 2014, debruçou-se sobre o assunto, incluindo no Marco Civil da Internet elementos que versavam sobre o tratamento de dados pessoais, de forma bastante específica, representando um avanço, em termos de segurança jurídica, para o ciberespaço no país (Boff; Fortes, 2014; Sarlet; Ruaro, 2021). Naquele mesmo ano, foi apresentado o Projeto de Lei do Senado (PLS) 181/2014, que visava estabelecer "princípios, garantias, direitos e obrigações para a proteção de dados no Brasil" (Melo, 2015, p. 185).

Posteriormente, no ano de 2018, com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, o Brasil conferiu aos cidadãos um maior poder em relação à sua privacidade. Essa normativa brasileira dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, visando à tutela dos direitos fundamentais de liberdade e privacidade, e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018b).

Nesse sentido, segundo Mendes (2019), a LGPD garantiu, de forma inédita, um regime geral de proteção de dados pessoais no Brasil, sendo um marco normativo na sociedade da informação. Além disso, foi essencial para consolidar as normativas esparsas existentes sobre o tema, que se mostravam insuficientes para a tutela dos cidadãos (Silva; Melo; Kfouri, 2019). Outro desdobramento positivo relaciona-se ao entendimento de que todas as informações são relevantes, inclusive aquelas a que não se concedia qualquer importância, uma vez que,

interpretadas em conjunto com outras, podem causar danos aos indivíduos (Silva; Melo; Kfouri, 2019).

Ao explorarem os reflexos da LGPD no cenário digital, Almeida e Soares (2022) ressaltam a heterogeneidade da matéria, que se relaciona à governança, ao tratamento de dados e à segurança da informação. Os autores asseveram que as organizações públicas e privadas ainda carecem de um maior amadurecimento em relação à implementação da norma, envolvendo a criação de políticas internas e a disponibilização de treinamentos (Almeida; Soares, 2022). Por sua vez, Sarlet e Ruaro (2021) destacam que, geralmente, os dados pessoais são tratados sem uma preocupação com a segurança, o que demanda atenção, já que, no âmbito público, auxiliam o desenvolvimento de políticas no bojo do aparelho estatal, ao passo que, no setor privado, contribuem para gerar lucro.

Nesse contexto, torna-se essencial discutir os efeitos da LGPD no âmbito público, considerando que a lei trata de uma nova acepção relacionada a um direito fundamental, reservando ao Estado alguns tratamentos não extensíveis às organizações privadas, desde que caracterizado o regime de finalidade pública (Rosso, 2019). Além disso, a própria Lei nº 12.527/2011, que trata do acesso à informação, constitui-se como um fator importante, haja vista a integração que deverá existir entre essas duas normas (Brasil, 2011). Apesar dessa interlocução, os direitos e as tutelas da primeira são mais abrangentes, uma vez que recaem sobre todos os tipos de dados pessoais, inclusive os regimes de transparência e de acesso à informação, configurando-se um desafio para o Poder Público assegurar uma efetiva proteção desses dados (Barbosa *et al*., 2021).

No tocante às instituições públicas de ensino, Barbosa *et al.* (2021) identificaram desafios que estão relacionados à implementação da LGPD: necessidade de aportes financeiros, capacitação profissional e técnica, incentivo à cultura de proteção de dados e criação de políticas institucionais. Nesse contexto, visualiza-se que essa lei representa um desafio no âmbito das organizações, uma vez que novas diligências deverão ser adotadas pelas instituições para que os direitos dispostos na norma sejam assegurados. Por outro lado, evidencia-se o avanço da LGPD em proporcionar empoderamento e segurança aos indivíduos, a fim de que possam opinar sobre o compartilhamento de suas informações (Ghisleni, 2022).

1.1 PROBLEMA DE PESQUISA

Dados pessoais são valiosos e precisam ser tratados com a devida responsabilidade, priorizando a privacidade e a proteção dos seus titulares, o que justifica a importância da criação

de normas e regulamentos. Na visão de Crespo (2021), uma lei que tenha como objetivo a proteção de dados é um marco na instituição de direitos para os indivíduos, não importando a natureza da organização responsável pela coleta, guarda e tratamento. Assim, esses direitos devem resguardar a pessoa natural, propiciando-lhe os instrumentos para assegurar o controle efetivo de seus dados pessoais. É nesse contexto que foi publicada a Lei Geral de Proteção de Dados Pessoais (LGPD).

Para além de aspectos jurídicos, essa normativa contempla também aspectos técnicos relacionados à segurança da informação e à governança, regulamentando várias questões que devem ser observadas para garantir a proteção de dados pessoais, dentre as quais a composição de equipes técnicas nas instituições (Barbosa *et al*., 2021). Kanagusku e Lahr (2022) pontuam que um desses aspectos consiste na necessidade de estruturar um ambiente seguro de *backup* e armazenamento de dados. Na seara pública, essas questões adquirem uma maior relevância, pois compete ao Estado controlar, ainda que indiretamente, os dados relativos à saúde, educação e finanças, por exemplo (Rosso, 2019).

Ao referir-se à gestão eficiente desses dados, Montolli (2020) destaca a importância da organização, estruturação e uso estratégico desde a coleta até o tratamento. Segundo a autora, ao gerir de forma eficiente as informações produzidas, a organização demonstra a preocupação com a governança de dados, o que irá auxiliar o planejamento e o processo decisório. Na visão de Cristóvam, Bergamini e Hahn (2021), a publicação da LGPD configurou-se como um avanço importante para subsidiar essa governança, tutelando os direitos e garantias fundamentais de liberdade e de privacidade em busca da utilização mais segura e transparente dos dados pessoais, além de servir como mecanismo de prevenção a fraudes.

No âmbito educacional e, mais precisamente, nas universidades públicas, o debate sobre a proteção de dados tem se intensificado, sobretudo devido à utilização de recursos tecnológicos para subsidiar as atividades de ensino, pesquisa, extensão e gestão (UFRPE 2021c; Barbosa *et al.*, 2021). Para Almeida e Soares (2022), um dos principais desafios atrelados ao contexto universitário consiste na necessidade de estabelecer um programa de boas práticas de governança e de proteção de dados.

Ainda no âmbito dessas organizações, cabe pontuar que a LGPD não se aplica ao tratamento de dados para fins exclusivamente acadêmicos (Brasil, 2018b). No entanto, isso não quer dizer que essas instituições estejam isentas de responsabilidade pelo tratamento de dados de discentes, egressos, servidores ou qualquer outro titular, registrados em suportes digitais ou físicos (Rojas, 2020). Desse modo, essas entidades têm procurado adequar os seus sistemas e

processos, ao passo que têm buscado fortalecer uma cultura de tratamento de dados pessoais (Rojas, 2020).

Em que pese isso, alguns trabalhos já realizados no âmbito dessas instituições apontaram a importância de que sejam intensificadas pesquisas nesta área. Ao realizar um estudo de caso numa dessas entidades, Rojas (2020) concluiu que não há uma conformidade plena em relação à LGPD, destacando a necessidade de algumas ações, dentre as quais a criação de plano de ação, a definição dos responsáveis por gerir todo o processo e o mapeamento de sistemas que manipulam dados pessoais ou sensíveis, com vistas a permitir a adoção de critérios para proteção desses dados.

Por seu turno, Tenório Filho *et al.* (2021) identificaram as iniciativas que têm sido adotadas por universidades públicas brasileiras para implementar a LGPD. Apesar do estudo ter se restringido geograficamente ao Nordeste do país, foi possível concluir que, ao se analisar o grau de conformidade à normativa, boa parte delas encontram-se num estágio incipiente, convergindo com o trabalho de Rojas (2020).

Nessa mesma linha, Souza, Belda e Arima (2022) realizaram uma pesquisa cujo objetivo consistiu em analisar o arcabouço normativo de uma instituição pública de ensino em atendimento aos requisitos abordados na LGPD. Assim, detectou-se a necessidade de maior observância, por parte da entidade, dos direitos do titular de dados, permitindo-lhe o efetivo exercício das prerrogativas conferidas, tais como a "revogação do consentimento", anonimização" e "bloqueio ou eliminação dos dados pessoais" (Souza; Belda; Arima, 2022, p. 1867). Como desdobramento, foi sugerida a criação de um programa de privacidade interno, compatível com a política de segurança da própria instituição.

Além dos aspectos abordados nos trabalhos citados, a análise do nível de maturidade em relação à LGPD se mostra fundamental uma vez que, caso essa legislação não seja observada, poderão ser aplicadas sanções administrativas (Tenório Filho *et al.*, 2021). Segundo Nascimento e Silva (2023), não cumprindo as disposições contidas na lei, as universidades estão suscetíveis a sanções administrativas impostas pela Autoridade Nacional de Proteção de Dados (ANPD), além de processos jurídicos impetrados pelos titulares de dados. Outra consequência apontada pelas autoras refere-se à perda de credibilidade em episódios de vazamentos de dados, o que pode comprometer a imagem da organização perante a sociedade (Nascimento; Silva, 2023).

Para aprimorar a maturidade, o Governo Federal instituiu o Programa de Privacidade e Segurança da Informação (PPSI), que disponibiliza um *framework* para auxiliar as instituições a identificarem, acompanharem e preencherem lacunas de privacidade e segurança da

informação (Brasil, 2023). Com base no exposto, pode-se destacar a necessidade de aprofundar o conhecimento acerca da forma como as instituições públicas, em especial as universidades, têm se adequado ao regramento relativo à proteção de dados.

Assim, na direção do cumprimento dessas normas, essas instituições têm incluído ações visando assegurar a prestação de serviços à comunidade acadêmica sem comprometer a segurança da informação. É o caso da Universidade Federal Rural de Pernambuco (UFRPE), que estabeleceu como objetivos atrelados à Tecnologia da Informação e Comunicação (TIC) a melhoria da segurança dos dados e dos serviços digitais; a conscientização e a capacitação dos usuários em segurança da informação e comunicação; e a adequação dos serviços prestados à LGPD (UFRPE, 2021c).

Apesar desses esforços, a UFRPE, de acordo com o levantamento anual divulgado pelo Tribunal de Contas da União (TCU), encontra-se no estágio considerado "inexpressivo" no que tange à governança e à gestão de segurança e de tecnologia da informação (Brasil, 2021c). Esse levantamento é subsidiado por meio do questionário eletrônico enviado pelo órgão de controle às entidades públicas, incluindo as universidades federais, a fim de coletar dados sobre diversas áreas e, após sistematizá-los, publicizar os indicadores de desempenho de cada uma delas. Nesse sentido, ao constatar-se a inexpressividade da UFRPE em relação à gestão e segurança em tecnologia da informação na proteção de dados, corrobora-se a importância de que sejam realizadas pesquisas científicas que busquem compreender as ações, os desafios e o nível de maturidade da instituição no que se refere à privacidade, proteção de dados e segurança da informação.

Nesse sentido, tem-se a seguinte questão de pesquisa: **como a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE)?**

1.2 OBJETIVOS

A seguir, serão apresentados os objetivos geral e específicos que nortearam a condução deste estudo.

1.2.1 Objetivo Geral

Esta pesquisa teve como objetivo geral investigar como a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE).

1.2.2 Objetivos Específicos

A fim de atingir esse objetivo, foram propostos os objetivos específicos a seguir relacionados:

- Identificar as ações realizadas na promoção da proteção de dados pessoais no âmbito da Universidade Federal Rural de Pernambuco (UFRPE);
- Identificar os desafios enfrentados pela UFRPE na implementação das práticas de proteção de dados pessoais;
- Analisar o nível de maturidade da proteção de dados pessoais no âmbito da UFRPE com base no *framework* proposto por Santana e Mendonça (2023);
- Elaborar um diagnóstico e propor ações para fortalecer a proteção de dados pessoais na UFRPE.

1.3 JUSTIFICATIVA

Nesta seção serão apresentadas as justificativas teórica e prática que embasaram a realização deste estudo.

1.3.1 Justificativa teórica

Ao analisar a produção científica acerca da LGPD, encontram-se alguns autores que salientam haver ainda lacunas a serem preenchidas por estudos na área. Barbosa *et al*. (2021), por exemplo, identificaram a ausência de estudos científicos sobre as dificuldades enfrentadas por organizações de ensino públicas no tratamento de dados sensíveis, tais como aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, dados referentes à saúde ou à vida sexual, entre outros, que “envolvem questões de cunho totalmente íntimo e individual” (Flôres; Silva, 2020, p. 2) e carecem de um maior aprofundamento.

Já Rocha *et al.* (2023) constataram um aumento significativo no portfólio de artigos nacionais e internacionais sobre o tema. Porém, por meio de um estudo bibliométrico, evidenciou-se um predomínio de trabalhos publicados em periódicos europeus e no âmbito jurídico. Segundo os autores, 46% das publicações versavam sobre a área do Direito, ao passo que apenas 7% tratavam das peculiaridades da Administração Pública, o que reforça a importância da efetivação de estudos com este enfoque. Essa constatação coaduna-se com a pesquisa de Carvalho, Freitag e Santos (2022), cujos resultados revelaram a produção constante nas bases *Scopus, Web of Science, SciELO* e Portal de Periódicos Capes, entre os anos de 2018 e 2021, de estudos que expunham, predominantemente, questões relativas às áreas de saúde, direito e tecnologia.

Em que pese a importância do tema, Rojas (2020) registra a escassez de estudos relativos à aplicação desta Lei em instituições de ensino, públicas ou privadas, o que corrobora a importância de pesquisas como esta, com o fito de ampliar o conhecimento acadêmico sobre a aplicação da Lei em universidades públicas.

Desta forma, este estudo se justifica, pois seus resultados irão contribuir para preencher lacunas apontadas pelos autores acima, tendo em vista que se trata de um estudo sobre a LGPD desenvolvido no Brasil, na perspectiva da gestão pública e em uma instituição federal de ensino superior. Nesse sentido, estima-se que esta pesquisa possibilitará o aprofundamento do tema na esfera pública, ampliando o conhecimento sobre as ações, desafios e nível de maturidade relacionados à implementação da LGPD em uma universidade federal de ensino.

1.3.2 Justificativa prática

As instituições da área educacional vêm adotando novas tecnologias de informação, de comunicação e de ensino em seu cotidiano, adaptando-as à proposta pedagógica, aos processos administrativos e ao próprio fluxo comunicacional, com o objetivo de modernizar e otimizar os processos institucionais (Barbosa *et al*., 2021). Nesses processos, são utilizados cada vez mais dados pessoais de alunos, servidores e terceirizados. Desse modo, tais organizações devem estar atentas aos riscos e às consequências do compartilhamento ou vazamento de dados pessoais constantes em bancos de dados, o que poderá acarretar prejuízos que ultrapassam a violação do direito à privacidade dos indivíduos.

Nesse contexto, a Lei Geral de Proteção de Dados surge para exigir das organizações um tratamento adequado dos dados pessoais dos indivíduos, orientando-as quanto ao que precisa ser atendido por elas para estar em conformidade com a referida Lei. Sob o ponto de

vista prático, essa adequação pode ser avaliada pela análise do nível de maturidade, que se mostra fundamental para que as organizações possam adequar suas rotinas e sistemas, a fim de assegurar a conformidade prevista na normativa e promover a gestão de privacidade e o uso de dados pessoais (Brasil, 2020b).

No que se refere às universidades federais, Tenório Filho *et al.* (2021) pontuam o desafio para efetivar essa adequação, que não é discricionária, uma vez que, caso não ocorra, poderão ser aplicadas sanções administrativas, corroborando a importância dessa análise da maturidade. Some-se a isto que a normativa elenca, dentre seus fundamentos, o desenvolvimento econômico e tecnológico, além da inovação (Brasil, 2018b), indo ao encontro da missão das universidades. Desse modo, tais instituições devem se adequar totalmente à LGPD, re(estruturando) processos e sistemas, para promover uma cultura de tratamento de dados.

Cabe ainda ressaltar que Oliveira (2024) realizou uma pesquisa cujo objetivo foi analisar a proteção de dados no âmbito dos processos eletrônicos que tramitam na UFRPE. De maneira geral, os resultados apontaram que assegurar a conformidade do nível de acesso à informação é um desafio para a gestão da Universidade, destacando a necessidade de que sejam realizados outros trabalhos que investiguem a temática de proteção de dados numa dimensão aplicada, contemplando as práticas adotadas na entidade. Assim, identifica-se uma convergência com este estudo, que possibilitará um aprofundamento sobre o tema.

Assim, os resultados deste trabalho poderão contribuir para que a instituição objeto da pesquisa, a UFRPE, alcance um dos seus objetivos estratégicos, a adequação integral dos seus serviços à LGPD até o ano de 2025 (UFRPE, 2021c). Tal contribuição envolve o conhecimento acerca de como a Lei vem sendo aplicada na Instituição, salientando-se as ações implementadas, os desafios enfrentados e o nível de maturidade, com perspectiva de que sejam apontadas áreas específicas que requerem uma maior atenção da gestão institucional, com vistas a fomentar treinamentos, revisão de procedimentos e adoção de novas tecnologias. Afora isso, conjectura-se que esses resultados poderão servir de *insights* para incentivar que outras instituições de ensino superior fortaleçam as suas políticas de proteção de dados pessoais e de segurança da informação.

1.4 ESTRUTURA DA DISSERTAÇÃO

A estrutura da dissertação abrange várias seções e cada uma apresenta uma parte do trabalho concluído. Sendo assim, o capítulo 1 - Introdução delimita o tema de pesquisa, que corresponde à proteção de dados pessoais e à aplicabilidade da Lei Geral de Proteção de Dados

Pessoais (LGPD) no setor público. Para tanto, é realizada uma breve contextualização histórica, contemplando as normativas pioneiras sobre a proteção de dados pessoais e privacidade. Além disso, foram abordados alguns aspectos relacionados à LGPD, a fim de destacar a complexidade dessa norma brasileira, bem como foram apresentadas algumas conclusões de outros trabalhos que exploraram a implementação dessa Lei em organizações públicas.

O referido capítulo abrange também os objetivos e as justificativas teórica e prática desta pesquisa. Desse modo, almeja-se contribuir para o aumento de publicações científicas sobre o tema na Administração Pública e propor ações para fortalecer a proteção de dados pessoais no âmbito da instituição que foi objeto do estudo.

No capítulo 2, é apresentado o referencial teórico da pesquisa. Nele, são levantadas as bases conceituais acerca do tema estudado, abrangendo a proteção de dados e a Lei Geral de Proteção de Dados Pessoais, discutindo a aplicabilidade dessa norma no setor público em geral e, especificamente, no contexto universitário.

No capítulo subsequente, são apresentados os procedimentos metodológicos adotados para a realização do estudo, incluindo-se as seguintes técnicas para coleta dos dados: pesquisa documental, entrevista e aplicação de *framework* estruturado no formato de questionário. O capítulo 3 também apresenta a sistemática utilizada na análise e na interpretação desses dados, que compreendeu: análise documental; análise de conteúdo, segundo Bardin (2016); e análise com base na média aritmética das respostas, a fim de medir o nível de maturidade da entidade em proteção de dados.

No capítulo 4 são apresentados os resultados da pesquisa e sua interpretação. A análise e a interpretação respondem aos objetivos definidos e, para tal, foram utilizados os resultados analisados com base nas teorias presentes na fundamentação teórica. Por fim, apresentam-se as considerações finais, com as limitações do estudo e as propostas de novas pesquisas, incluindo-se as referências bibliográficas na última parte.

2 REVISÃO DA LITERATURA

Neste capítulo serão expostos os pressupostos teóricos relacionados à proteção de dados no setor público, à Lei Geral de Proteção de Dados Pessoais e à LGPD e o setor público, considerando as contribuições proporcionadas por investigações anteriores.

2.1 PROTEÇÃO DE DADOS NO SETOR PÚBLICO

O compartilhamento de dados tem crescido à medida que a tecnologia evolui. A substituição dos suportes físicos pelos digitais e o uso progressivo da rede mundial de computadores para diversos fins resultaram em maior praticidade e comodidade, bem como na criação de um novo espaço do qual os indivíduos fazem parte: o digital (Lima; Alcassa; Pappert, 2022). Ao referirem-se a este *lócus*, Boff e Fortes (2014, p. 110) utilizam o termo "ciberespaço", que consiste numa rede aberta e interativa, na qual os sujeitos produzem dados, navegam e estabelecem relações.

Sarlet e Ruaro (2021) pontuam que esse ambiente apresenta facetas peculiares, tendo em vista que suas dimensões não se limitam ao tempo e espaço. Some-se a isto que o avanço tecnológico conduz, inevitavelmente, a uma impermanência deste *lócus,* o que tem contribuído para a proposição de parâmetros jurídicos, a fim de tutelar direitos fundamentais previstos constitucionalmente (Sarlet; Ruaro, 2021). Segundo Silva, Melo e Kfouri (2019), um deles refere-se à privacidade, caracterizado como um direito da personalidade. Assim, considerando que os dados de caráter pessoal, após sistematização, traduzem-se em informações que podem relevar as idiossincrasias dos sujeitos a que se referem, vem se intensificando o debate sobre proteção de dados, ainda que não sejam dotados de sigilo.

Apesar de serem empregados de forma intercambiável, inclusive neste trabalho, Doneda (2011) adverte que os termos "dado" e "informação" são distintos. Segundo o autor, "o dado apresenta uma conotação um pouco mais primitiva e fragmentada, [...] e estaria associado a uma espécie de pré-informação, anterior à interpretação e ao processo de elaboração", ao passo que "a informação [...] alude a algo além da apresentação contida no dado, chegando ao limiar da cognição" (Doneda, 2011, p. 94). Assim, a partir de um processo de combinação, a exemplo de dados biométricos e senhas, seria possível singularizar o usuário, de modo que é viável ter acesso à sua individualidade e privacidade apenas cruzando as informações que lhe pertencem (Cella; Copetti, 2017).

De acordo com Doneda (2011), essas informações que pertencem a um indivíduo estão correlacionadas à sua privacidade, numa lógica inversamente proporcional. Desse modo, quanto maior a privacidade, menor será o compartilhamento de informações pessoais, e vice-versa. Para o autor, essa relação demonstra que a proteção de dados ingressou no ordenamento jurídico brasileiro "como um desdobramento da tutela do direito à privacidade" (Doneda, 2011, p. 94)

Na visão de Finkelstein e Finkelstein (2019), o conceito de privacidade é amplo. Na Constituição Federal, por exemplo, há uma relação com o direito à inviolabilidade da correspondência, intimidade e vida privada, garantindo aos indivíduos a prerrogativa de não terem divulgado os fatos de maneira alheia à sua vontade (Brasil, 1988). Por seu turno, o Código Civil tutela, ainda que de forma abrangente, a divulgação de escritos e a transmissão da palavra, bem como a utilização da imagem de pessoa física ou jurídica, incluindo a honra, fama e respeitabilidade (Brasil, 2002). Visualiza-se, portanto, que "a privacidade figura como gênero na qual a intimidade atua como espécie" (Finkelstein; Finkelstein, 2019, p. 286).

Contemporaneamente, a definição do termo privacidade encontra-se relacionada à evolução tecnológica, abrangendo novas dimensões relativas à coleta e ao tratamento de dados. Para Doneda (2011, p. 97), tem se consolidado o direito à "autodeterminação informativa", consubstanciada na prerrogativa de que os indivíduos devem estabelecer limites para a utilização de seus dados, já que, na sociedade da informação, qualquer conteúdo poderá adquirir relevância, ou seja, não existem dados insignificantes. Desse modo, a proteção dos dados equipara-se à tutela da pessoa humana, sobretudo quanto ao desenvolvimento da personalidade (Sarlet; Ruaro, 2021).

Diante de tal cenário, visualiza-se uma evolução no conceito de privacidade, que passa a abranger não somente a proteção contra a interferência de terceiros, mas também confere aos sujeitos a titularidade "de um direito ao consentimento quanto à circulação de dados pessoais, reconhecendo-se ser uma violação à dignidade da pessoa humana a utilização de suas informações pessoais sem a anuência, em atenção à autonomia privada" (Silva; Melo; Kfouri, 2019, p. 356). Assim, sob este novo prisma, os titulares tornam-se responsáveis pelo controle de suas informações, de modo que haja o exercício pleno da privacidade. Apesar dessa nova roupagem, Silva, Melo e Kfouri (2019) advertem que o conceito clássico subsiste, coexistindo com a concepção contemporânea.

No Brasil, a preocupação com a proteção de dados remonta ao século XIX. No ano de 1852, durante a Guerra dos Marimbondos, levante popular ocorrido no estado de Pernambuco, o governo suspendeu a aplicação de lei que determinava o registro de nascimentos e óbitos, pois

a “população temia que informações obtidas com base na nova legislação, que ficou conhecida como “Lei do Cativeiro”, fossem usadas para discriminar os mais pobres” (Carvalho, 2023, p. 141).

Outro fato semelhante aconteceu na Bahia, durante a Guerra dos Canudos, ocorrida entre 1896 e 1897. Na ocasião, o censo imposto pela República, que fora recentemente instalada, afligiu a população, receosa da utilização discriminatória de seus dados, notadamente os raciais, que poderiam ser utilizados com o fim de restabelecer a escravidão (Carvalho, 2023).

A discussão trouxe à tona o debate acerca dos dados não apenas no Brasil, mas também em outras partes do globo. Nos anos 70, o Tribunal da Alemanha debruçou-se sobre o tema, ao julgar questões relativas à privacidade e ao censo. Na oportunidade, decidiu-se, com base no direito à personalidade, em síntese, que o que atualmente se considera tratamento de dados só poderia ocorrer com a autorização do titular (Cella; Copetti, 2017).

Naquele contexto, firmou-se um entendimento no sentido de que o direito ao pleno desenvolvimento da personalidade inclui a capacidade do indivíduo de escolher, por conta própria, quando, quais e até que ponto suas informações pessoais serão processadas e reveladas (Schwabe, 2005).

Apesar dessa discussão revestir-se de uma dimensão histórica, Flôres e Silva (2020) destacam o caráter tardio da publicação de normas brasileiras adequadas de proteção de dados pessoais, sobretudo quando se analisa outros países, a exemplo da Alemanha. De acordo com as autoras, o marco normativo deu-se com a previsão do *habeas data*, na Constituição Federal, e com a inclusão do banco de dados dos consumidores, previsto no Código de Defesa do Consumidor, instituído pela Lei nº 8.078/1990 (Flôres; Silva, 2020).

Convém ressaltar também a publicação do Marco Civil da Internet, materializado por intermédio da Lei nº 12.965/2014, estabelecendo princípios, garantias e deveres para o uso da internet no país (Brasil, 2014). Embora seja possível reconhecer a importância dessa lei para assegurar os direitos humanos e fundamentais, é oportuno destacar o seu caráter incipiente no que se refere à tutela de dados pessoais (Flôres; Silva, 2020).

No ano de 2016, as discussões sobre a proteção de dados no setor público brasileiro voltaram-se à publicação do Decreto Federal nº 8.789/2016, que tratava do compartilhamento de bases de dados na Administração Pública (Brasil, 2016). Sob o argumento de assegurar a eficiência e simplificar as atividades administrativas, o Decreto buscou facilitar a transferência de dados, criando uma base única em nível federal. Apesar de uma aparente conotação positiva,

a proteção à privacidade foi, de certo modo, negligenciada pela normativa, já que mencionou apenas a tutela a dados concernentes aos sigilos fiscal e bancário (Cella; Copetti, 2017).

O fato é que, ao quebrar as barreiras entre os diferentes órgãos e entidades do Estado, os dados compartilhados podem adquirir um novo propósito para além do que foram coletados inicialmente (Cella; Copetti, 2017). Além disso, para Carvalho (2023, p. 143), atrelado ao setor público, encontra-se o efeito do "excedente comportamental", que resulta da ampliação de capacidade de processamento hodierna, caracterizada por uma espécie de "sobrevalor, que transcende os propósitos originais da operação de coleta". Para o autor, mesmo após finalizado o uso inicialmente pretendido, os dados têm capacidade de gerar valor, seja público, político ou econômico para aqueles que os detêm, sem a necessidade de grandes esforços (Carvalho, 2023).

Esse debate, ao longo dos anos, vem adquirindo notoriedade também devido à mudança de paradigmas na atuação da Administração Pública. Para Nemetz (2004), o arcaico pensamento que a Administração Pública deve unicamente abster-se de agir, proporcionando, por simples inércia, liberdades civis e políticas aos cidadãos, evoluiu para a necessidade de garantir os direitos de segunda geração, tidos como aqueles relacionados à educação e saúde, por exemplo, que exigem ação para serem efetivados. Desse modo, segundo Carvalho (2023), a fim de ampliar e conceder plena efetividade a esses direitos, o Estado utiliza-se dos dados coletados para execução de políticas públicas. Ao analisar o uso desses dados, Rodotà (2008, p. 28) destaca que:

> [...] o enorme aumento da quantidade de informações pessoais coletada por instituições públicas e privadas visa sobretudo a dois objetivos: a aquisição dos elementos necessário à preparação e gestão de programas de intervenção social, por parte dos poderes públicos, o desenvolvimento de estratégias empresariais privadas; e o controle da conformidade dos cidadãos à gestão política dominante ou aos comportamentos prevalecentes.

Entretanto, o controle de determinadas autoridades públicas sobre bancos de dados nem sempre permite que essa utilização ocorra de maneira legítima, o que poderá desembocar em intervenção para manutenção no acesso a esses dados (Carvalho, 2023). Por seu turno, Aguilera e Di Biase (2021) advertem que o risco desse uso inadequado tem suscitado discussões sobre o tratamento adequado em instituições públicas, consubstanciado a partir de vários casos que vêm reafirmando a importância de robustecer a proteção de dados nessas entidades, dentre os quais o episódio que culminou no vazamento de dados, no ano de 2021, de 223 milhões de brasileiros, vivos ou falecidos.

Para além da problemática que envolve o compartilhamento ilícito de dados de posse do Poder Público, Carvalho (2023) pontua que o debate sobre esse tratamento é mais complexo, tendo em vista que pode haver controvérsias quanto à legitimidade em disponibilizar tais dados no âmbito da própria administração. Segundo o autor, esses conflitos fundamentam-se na falta de clareza da legislação, na fragilidade das justificativas para acessar dados ou no risco de haver desvio de finalidade na execução de políticas públicas, o que vai de encontro à LGPD (Carvalho, 2023; Brasil, 2018b). Como desdobramento, tem-se a necessidade de manifestação do Supremo Tribunal Federal (STF), conforme evidenciado a seguir:

> o STF se manifestou contrariamente ao compartilhamento de dados pessoais obtidos pelo Instituto Brasileiro de Geografia e Estatística (IBGE) e pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). Os dados em questão, que haviam sido coletados para fins estatísticos, seriam utilizados, respectivamente, para permitir que o Ministério Público Federal identificasse crianças não registradas na cidade de Bauru (SP) e que o TCU realizasse uma auditoria no Programa Bolsa Família. Ainda que, em ambos os casos, o compartilhamento de dados fosse destinado para atender finalidades públicas, a Corte entendeu que, no caso concreto, deveria prevalecer o sigilo estatístico e a finalidade original da coleta, sob pena de violação à privacidade e à intimidade dos titulares. Ademais, caso realizado, o compartilhamento poria em risco a confiança depositada nos órgãos de pesquisa pelos entrevistados e a própria continuidade dessas atividades (Carvalho, 2023, p. 144).

Visualiza-se, portanto, que - no bojo do próprio Estado - o compartilhamento de dados pessoais não tem caráter absoluto, dada a possibilidade de interferência nos direitos individuais fundamentais, incluindo-se a privacidade. Nesse sentido, é ilegítimo que os agentes públicos se apropriem dos bancos de dados armazenados por outras instituições, públicas ou privadas, com total discricionariedade, valendo-se do argumento de que o objetivo corresponde à execução de políticas públicas (Carvalho, 2023).

Nesse contexto, Doneda (2011) aponta que há alguns princípios inerentes à proteção de dados pessoais, cujo objetivo é salvaguardar os indivíduos a mitigar a utilização ilegítima por parte de terceiros, que são:

a) Princípio da publicidade (ou da transparência): a criação de um banco de dados requer autorização prévia e comunicação à autoridade competente, prezando-se pela transparência;
b) Princípio da exatidão: deve-se assegurar a fidedignidade e verossimilhança, o que demanda que os dados sejam coletados e tratados com correição, além de serem atualizados periodicamente;

c) Princípio da finalidade: refere-se ao estrito cumprimento das razões transmitidas ao titular antes da coleta, funcionando também como um balizador da utilização dos dados, bem como um limitador para o compartilhamento com terceiros;
d) Princípio do livre acesso: relativo ao acesso que o titular deve possuir ao banco de dados, propiciando-lhe um controle efetivo, com possibilidade de eventuais atualizações;
e) Princípio da segurança física e lógica: abrange aspectos concernentes à proteção contra risco de perda, alteração, destruição ou acesso sem permissão.

Nesse contexto, diante das normas incipientes sobre proteção de dados que, até então, haviam sido publicadas no Brasil, restou evidente a importância de lei específica, com respaldo internacional, tendo em vista que, à medida que os dados evoluem por meio da tecnologia, com processamento em curto espaço de tempo, maior deve ser a regulação sobre o tema, incluindo-se a privacidade, a fim de que seja possível garanti-la aos indivíduos, de modo a diminuir a sua vulnerabilidade (Cella; Copetti, 2017).

Desse modo, no ano de 2010, o Ministério da Justiça realizou uma consulta pública, a fim de coletar a opinião popular sobre os limites da privacidade e proteção de dados no país (Finkelstein; Finkelstein, 2019). Os desdobramentos do processo culminaram com o início da tramitação, perante o Congresso Nacional, do Projeto de Lei nº 5.276/2016, que dispunha sobre o tema (Cella; Copetti, 2017), cuja sanção ocorreu no ano de 2018, instituindo-se a Lei Geral de Proteção de Dados Pessoais. Outro marco normativo ocorreu no ano de 2019, quando foi publicado o Decreto Federal nº 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal, instituindo o Cadastro Base do Cidadão e o Comitê de Governança de Dados, revogando também o Decreto nº 8.789/2016 (Brasil, 2019b).

Essa evolução cronológica, sob a ótica normativa, corrobora a opinião de Finkelstein e Finkelstein (2019), no sentido de que a proteção de dados deve acompanhar as dinamicidades da sociedade da informação. A despeito do Código de Defesa do Consumidor, da Lei de Acesso à Informação e do Marco Civil da Internet, ainda que de modo incipiente, conferirem tutela ao titular de dados, o Brasil carecia de uma normativa específica e com maior amplitude, o que conduziu à publicação da LGPD (Finkelstein; Finkelstein; 2019).

Apesar disso, Carvalho (2023, p. 135) aponta que, durante a tramitação desta última, houve tentativas de excluir o Poder Público da incidência das normas de proteção de dados sob a justificativa “de que num ambiente digital, o fluxo de dados não pode ter muitas amarras”. Na

prática, o argumento foi refutado, subsistindo a necessidade de que as organizações públicas observem o estrito cumprimento dos princípios atrelados à proteção de dados, dentre os quais aqueles referidos por Doneda (2011). O fato é que há um elemento cultural que pode criar uma resistência em efetivar a proteção de dados pessoais no setor público, fundada em "velhas e bem conhecidas práticas administrativas", caracterizadas pela total discricionariedade e pela falta de transparência (Carvalho, 2023, p. 136).

Quanto à transparência, identifica-se sua correlação com o controle que os cidadãos devem possuir em relação à atuação das entidades públicas, que deve abranger o fluxo das informações sistematizadas a partir dos seus dados pessoais (Carvalho, 2023). Desse modo, visualiza-se que esses dados, sobretudo no âmbito público, constituem-se como "fonte de poder", já que quanto mais conhecimento uma instituição detiver sobre um indivíduo, maior a possibilidade de exercer certa dominação sobre ele, o que implica um conceito de privacidade para além da relação "sigilo-publicidade" (Carvalho, 2023, p. 156).

Nesse sentido, visualiza-se o avanço da legislação brasileira em reconhecer a proteção de dados como consectária do direito à privacidade, fato corroborado pela elevação do *status* deste último como um direito fundamental constitucional, incluído por meio da Emenda nº 115, de 10 de fevereiro de 2022 (Brasil, 2022a). Na próxima seção, serão discutidos os principais elementos abordados pela LGPD, que, como já relatado, configurou-se como um grande avanço para a proteção de dados.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dados pessoais, ainda que não pareçam relevantes ou não remetam diretamente a um indivíduo, são importantes e demandam tutela jurídica. Com base nisso, foi instituída a Lei Geral de Proteção de Dados Pessoais (LGPD), que visa proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018b). Nesse sentido, esse diploma legal apresenta como finalidade precípua a proteção de dados no que tange à sua captação, armazenamento e tratamento, nos meios físicos e digitais, havendo maior discussão em relação ao suporte digital devido à maior facilidade de captação (Finkelstein; Finkelstein, 2019).

Seu advento se deu na esteira do Regulamento Geral sobre a Proteção de Dados da União Europeia, vigente desde o ano de 2018. No entanto, o assunto é debatido com mais ênfase, no Velho Continente, desde meados de 1995, ano em que surgiu a Diretiva de Proteção de Dados (Mulholland, 2018). Apesar disso, o assunto ganhou notoriedade a partir do avanço

tecnológico, que possibilitou a manipulação e análise de informações de forma intensa, especialmente pelos riscos decorrentes de procedimentos constantes na lei, os quais, muitas vezes, envolvem dados pessoais sensíveis (Finkelstein; Finkelstein, 2019).

Nesse contexto, a LGPD possibilitou à pessoa natural uma proteção contra a utilização indevida de seus dados, estabelecendo padrões mínimos para seu tratamento e manipulação, bem como garantindo autonomia e consentimento ao usuário sobre o uso de suas informações. Alguns conceitos fundamentais são enunciados pela normativa, dentre os quais o "dado pessoal", "dado pessoal sensível" e "dado anonimizado". O primeiro refere-se à informação de pessoa natural identificada ou identificável, abrangendo, por exemplo, o nome, endereço ou estado civil (Finkelstein; Finkelstein, 2019). O segundo, numa dimensão estrita, consiste em dados relativos à origem racial ou étnica, religião, opinião política, orientação sexual, dentre outros, quando vinculados à pessoa natural (Brasil, 2018b). Por seu turno, o último relaciona-se com o dado do titular que não possa ser identificado, tendo em vista a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento (Brasil, 2018).

Ao analisar esses conceitos, Finkelstein e Finkelstein (2019) ressaltam que os "dados anonimizados" não são considerados "dados pessoais", exceto se for possível descobrir a sua autoria, razão pela qual os que forem "indeterminados" e "indetermináveis" não são amparados pela LPGD. Outro termo presente no dispositivo legal é a "pseudonimização", 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 em ambiente controlado e seguro (Brasil, 2018b).

É oportuno destacar a definição sobre tratamento de dados, que engloba toda a operação de "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, 2018b, p. 60). O dispositivo legal define também as atribuições dos agentes responsáveis por esse tratamento, que podem ser pessoa física ou jurídica, de direito público ou privado (Finkelstein; Finkelstein, 2019; Brasil, 2018b). Nesse sentido, emergem os papéis de controlador e operador.

Compete ao controlador tomar decisões referentes ao tratamento dos dados, ao passo que a efetivação propriamente dita cabe ao operador, que o faz em nome daquele (Brasil, 2018b). Finkelstein e Finkelstein (2019) destacam a importância desses agentes em subsidiar a proteção dos dados, numa perspectiva de evitar acessos não autorizados, sob pena de

responsabilização. Por sua vez, Rocha, Fontes e Machado (2023) destacam que, durante esse tratamento, devem ser considerados os princípios norteadores da LGPD, a saber:

- Princípio da finalidade: os objetivos devem ser legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de modo diverso. Os setores de marketing e atendimento são os mais afetados, tendo em vista que os dados dos clientes não poderão ser divulgados em dissonância com a finalidade pré-estabelecida;
- Princípio da adequação: relaciona-se com a convergência entre o tratamento e a finalidade repassada ao titular, devendo haver uma compatibilidade entre o dado solicitado e o contexto de negócio. Assim, uma empresa do ramo de comércio eletrônico não poderá solicitar, por exemplo, dado relativo à saúde do cliente;
- Princípio da necessidade: o tratamento deverá ser necessariamente compatível e proporcional às finalidades pretendidas, devendo-se evitar excessos;
- Princípio do livre acesso: aos titulares, deverá ser assegurada consulta à forma, duração do tratamento e totalidade de seus dados, o que conduzirá a modelação de processos, que deverão estar alinhados à política de segurança da informação;
- Princípio da qualidade dos dados: refere-se à clareza, exatidão, relevância e atualização dos dados, em compatibilidade com a sua necessidade, visando ao cumprimento da finalidade. Assim, as organizações devem investir em *softwares* e fomentar a cultura de sigilo e proteção à privacidade;
- Princípio da transparência: concernente à garantia de que os titulares dispõem em obter informações precisas e acessíveis em relação ao tratamento de seus dados, incluindo-se os agentes responsáveis. Do ponto de vista organizacional, demandará a criação de políticas e diretrizes de segurança da informação que visem impedir o compartilhamento de dados com terceiros;
- Princípio da segurança: requer a adoção de medidas que almejem proteger os dados pessoais de acessos não autorizados e de situações acidentais/ilegais. As empresas deverão investir na qualificação dos profissionais de tecnologia e de segurança da informação, bem como em técnicas de criptografia e *softwares* modernos;
- Princípio da prevenção: atrelado à importância de ações profiláticas que visem prevenir incidentes e danos críticos no tratamento de dados. As organizações devem realizar *backups* periódicos, investir na qualificação das equipes e criar planos e diretrizes relativos à segurança da informação;

- Princípio da não discriminação: deve-se abolir o tratamento para fins abusivos ou discriminatórios. Neste caso, o impacto maior relaciona-se às equipes de gestão de pessoas, que dispõem de vários dados sensíveis dos titulares. Além disso, deve-se evitar situações que possam ocasionar constrangimentos, dentre as quais solicitar dados sobre religião e orientação sexual;
- Princípio da responsabilização e proteção de contas: o agente deverá apresentar as medidas que utiliza para assegurar a proteção de dados, bem como a eficácia delas. Na prática, as empresas deverão aperfeiçoar os protocolos de segurança, bem como poderão contratar consultorias especializadas.

Desse modo, visualiza-se que esses princípios visam assegurar aos titulares que suas informações pessoais sejam tratadas em consonância com os propósitos a que se destinam. Na visão de Teffé e Viola (2020, p. 5), tais princípios "têm grande parte de seu centro gravitacional baseado no ser humano", o que corrobora a "preocupação do legislador com a participação do indivíduo no fluxo de suas informações". Assim, surge a necessidade de haver o consentimento, que será realizado por escrito ou por outro meio que ateste a manifestação da vontade, com possibilidade de revogação a qualquer tempo (Brasil, 2018b).

Quanto ao consentimento, Teffé e Viola (2020) destacam a sua importância em razão do panorama tecnológico contemporâneo, caracterizado pela coleta massiva de dados pessoais, pela possibilidade de mercantilização desses dados e por situações de pouca transparência e informação em relação ao seu tratamento. A despeito disso, há casos previstos na norma que dispensam essa autorização, dentre os quais os que envolvem dados tornados manifestamente públicos pelo titular (Brasil, 2018b). Porém, essa exceção não isenta o agente de tratamento do dever de observar os princípios enunciados pela LGPD, tendo em vista que, ainda que sejam considerados públicos, os dados não deixam de ser pessoais (Teffé; Viola, 2020).

No que se refere à natureza jurídica do consentimento para o tratamento de dados pessoais, cuja classificação "se dá não por preciosismo acadêmico, mas sim porque a categorização em determinada natureza jurídica traz uma série de efeitos práticos que podem mudar enormemente a disciplina do instituto em questão" (Requião, 2022, p. 22), há autores, a exemplo de Doneda (2020) e Tepedino e Teffé (2020a), segundo Requião (2022), que defendem ser o consentimento um ato jurídico *stricto sensu*, o qual se caracteriza, segundo Mello (2022, p. 79), como:

> [...] o fato jurídico que tem por elemento nuclear do suporte fático manifestação ou declaração unilateral de vontade cujos efeitos jurídicos são prefixados pelas normas

> jurídicas e invariáveis, não cabendo às pessoas qualquer poder de escolha da categoria jurídica ou de estruturação de conteúdo das relações jurídicas respectivas.

Dessa forma, a categoria jurídica e a estruturação do conteúdo derivam diretamente da legislação, o que de certo modo limita a atuação das partes e se mostra relevante em face das preocupações relacionadas à mercantilização dos dados pessoais (Requião, 2022).

Por outro lado, há autores, a exemplo do próprio Requião (2022), que atribuem ao consentimento caráter de negócio jurídico, cujo conceito, conforme leciona Mello (2022, p. 87), se traduz em:

> [...] fato jurídico cujo elemento nuclear do suporte fático consiste em manifestação ou declaração consciente de vontade, em relação à qual o sistema jurídico faculta às pessoas, dentro de limites predeterminados e de amplitude vária, o poder de escolha de categoria jurídica e de estruturação do conteúdo eficacial das relações jurídicas respectivas, quanto ao seu surgimento, permanência e intensidade no mundo jurídico.

À luz desse cenário, as partes gozam de certa liberdade quando da pactuação dos termos da avença. De acordo com Requião (2022, p. 24), ao categorizar o consentimento como negocial, é possível assegurar aos titulares "um número ainda maior de tutelas protetivas", em razão das "diversas causas de invalidade e, notadamente, dos defeitos do negócio jurídico" (Requião, 2022, p. 31). Doneda (2020), todavia, alerta que a categorização do consentimento como negocial pode torná-lo apto a figurar em estruturas contratuais prejudiciais ao direito de personalidade.

Ambos - ato jurídico *stricto sensu* e negócio jurídico - são espécies do gênero ato jurídico *lato sensu* e têm como característica comum a presença da vontade (Mello, 2022). A despeito disso, independentemente da classificação, o fato é que, segundo Requião (2022), o consentimento pode trazer consigo vícios, assim como em outros negócios jurídicos. O autor sustenta que, ao conceder sua anuência, usualmente o titular encontra-se em desvantagem informacional e técnica perante o controlador, estando em situação de hipossuficiência ao permitir a intervenção em direito fundamento individual.

Portanto, evidencia-se a importância de que os indivíduos disponham das informações necessárias e suficientes para avaliar corretamente o tratamento de seus dados, afinal, há riscos imbricados a esse processo (Teffé; Viola, 2020). De acordo com Doneda (2011, p. 92), esses riscos se materializam na "possibilidade de exposição e utilização indevida ou abusiva [...], na eventualidade desses dados não serem corretos e representarem erroneamente seu titular e em sua utilização por terceiros sem o conhecimento deste", o que corrobora a importância do papel

do controlador e do operador de dados. Além destes, destaca-se a atuação do encarregado de dados, cuja indicação é realizada pelos agentes de tratamento (Brasil, 2018b).

Nesse sentido, o tratamento de dados pessoais só poderá ocorrer quando a organização designar seu encarregado, que deverá manter uma comunicação entre o controlador, o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No Brasil, compete à ANPD fiscalizar e regular a LGPD. Esse órgão foi criado por intermédio da Lei nº 13.853, de 8 de julho de 2019, a fim de orientar as organizações, públicas e privadas, quanto à aplicação do dispositivo legal e, posteriormente, fiscalizar e advertir, sendo a punição aplicada somente após essas etapas (Brasil, 2019a). As atribuições do encarregado de dados poderão sofrer alterações propostas pela ANPD, a partir de normas complementares, com possibilidade de deliberação pela ausência do encarregado, a depender da natureza, porte da instituição ou quantidade de operações de tratamento de dados pessoais (Brasil, 2018b).

A ANPD também poderá estabelecer que o controlador elabore o Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados (Brasil, 2018b). Esse documento deverá conter, no mínimo: o detalhamento dos tipos de dados que serão coletados; a metodologia utilizada para a coleta e garantia da segurança das informações; e, finalmente, a análise do controlador no que concerne às medidas, proteção e mecanismos para atenuação de riscos observados (Brasil, 2018b). Como requisito prévio indispensável para sua constituição, exige-se que ao menos tenha sido iniciado o inventário de dados pessoais da instituição (Souza, 2022; Almeida, 2024).

Ao avaliarem o tratamento de dados no âmbito clínico-hospitalar, Zaganelli e Binda Filho (2022) constataram a imprecisão da LGPD quanto a esses relatórios, tendo em vista que o dispositivo legal não detalha os casos em que será necessária a elaboração desse documento. Além disso, o estudo possibilitou a identificação de outras lacunas e fragilidades constantes na referida norma, dentre elas:

- Alto custo para assegurar a conformidade;
- Ausência de menção quanto à necessidade de formalizar a relação existente entre operador e controlador;
- Ausência de detalhamento de prazos referentes à comunicação de incidentes de segurança que possam ocasionar riscos ou danos aos titulares dos dados;
- Ausência de detalhamento de prazos quanto à notificação do risco de vazamento de dados à autoridade competente;

- Presença da expressão genérica “nível razoável” ao referir-se à proteção para dados pessoais, o que concede aos reguladores uma elevada discricionariedade na avaliação de multas por violações de dados ou não conformidade.

Em que pese essas lacunas, o não cumprimento das normas relativas ao tratamento de dados acarretará penalidades ao agente de tratamento de dados (Brasil, 2018b). Conforme o dispositivo legal, a Autoridade Nacional poderá aplicar sanções administrativas, que variam desde a aplicação de advertência, multa, suspensão do exercício das atividades relacionadas com o tratamento de dados ou, até mesmo, proibição parcial ou total dessas atividades (Brasil, 2018b; Finkelstein; Finkelstein, 2019).

No entanto, Mulholland (2018) destaca que há algumas exceções relativas à aplicação da LGPD, em rol taxativo: (i) tratamento por pessoas naturais para fins particulares e não econômicos; (ii) tratamento para fins exclusivamente jornalísticos, artísticos ou acadêmicos; (iii) tratamento para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; e (iv) tratamento de dados 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 na LGPD (Brasil, 2018b).

Na prática, é possível afirmar que a publicação da LGPD se constitui como um marco legal, na perspectiva de consolidar uma cultura de proteção de dados no país, considerando o seu propósito em implementar instrumentos para tutelar e garantir a dignidade humana (Teffé; Viola, 2020). Em linhas gerais, essa lei visa facilitar o controle desses dados; impor deveres e responsabilidades aos agentes de tratamento; e proporcionar segurança aos titulares. Além das organizações privadas, as instituições públicas também devem atentar-se aos dispositivos da referida lei, o que será discutido na seção subsequente.

2.3 LGPD NO SETOR PÚBLICO

O estudo da LGPD no setor público perpassa por ações implementadas por órgãos e entidades a fim de mitigar os desafios enfrentados para assegurar o cumprimento da lei. As disposições para aplicação da LGPD à Administração Pública estão contidas no Capítulo IV da norma que rege a proteção de dados pessoais tratados pelos órgãos públicos da administração direta e pelas entidades da administração indireta, além dos serviços notariais e de registro

exercidos em caráter privado, devendo-se incluir a Defensoria Pública (Brasil, 2018b; Aguilera; Di Biase, 2021).

Nesse sentido, o art. 24 da norma estabelece que as empresas públicas e sociedades de economia mista que operam em regime de concorrência, nos termos da Constituição Federal (CF), terão o mesmo tratamento destinado às pessoas jurídicas de direito privado particulares. O parágrafo único, por sua vez, determina que as empresas públicas e sociedades de economia mista, ao operacionalizarem políticas públicas, sujeitam-se ao tratamento previsto para os órgãos e entidades do Poder Público (Brasil, 2018b).

Contudo, Aguilera e Di Biase (2021) apontam que essa distinção, pautada apenas na subjetividade do agente de tratamento, não se mostra a mais adequada, haja vista a linha tênue existente entre o público e o privado na ordem administrativa e econômica atual, a exemplo de concessionárias, permissionárias e autorizatárias, entes privados que prestam serviço público. Assim, os autores defendem que o âmbito de aplicabilidade da LGPD deve ser analisado à luz da "finalidade e a natureza da manipulação dos dados e com o propósito para o qual o tratamento está sendo realizado" (Aguilera; Di Biase, 2021, p. 9).

Na visão de Magacho e Trento (2021), a inserção do setor público na LGPD representa um avanço na Administração Pública, implicando o investimento em políticas de segurança e uma atuação efetiva dos órgãos e entidades, no sentido de evitar a utilização de dados pessoais em dissonância com os propósitos informados ao titular. Para Philippi (2023), ainda que haja um constante avanço tecnológico, há possibilidade de vazamentos e compartilhamento indevido dos dados coletados. Assim, é imperativo que o Poder Público invista em tecnologia que possa conferir segurança e proteção a esses dados, bem como promova mudanças culturais, a fim de conscientizar os agentes de tratamento quanto à utilização dentro de padrões éticos (Philippi, 2023).

Por sua vez, Crespo (2021) aponta que, independentemente da esfera, o Estado necessita promover medidas direcionadas para assegurar a conformidade com a LGPD. Essa demanda justifica-se, dentre outras razões, pelo quantitativo de dados pessoais constantes nas bases de dados dos órgãos e entidades públicos, seja por obrigações legais, para fins de pesquisa, para emissão de documentos ou atendimento em hospitais, por exemplo. Na visão desse autor, o Brasil precisa consolidar uma cultura de transparência em relação à proteção de dados pessoais e privacidade, sendo primordial que haja conscientização dos agentes públicos nesse processo (Crespo, 2021).

Percebe-se que Philippi (2023) e Crespo (2021) são uníssonos quanto à importância de se consolidar uma cultura de proteção de dados no setor público. Esse reconhecimento também é compartilhado pelo Tribunal de Contas União (TCU), que ressalta a importância de estimular a implantação de uma cultura de segurança da informação e de proteção de dados (Brasil, 2022). Nesse sentido, o órgão de controle disponibilizou um questionário *online* para 382 organizações públicas federais, a fim de avaliar a adequação à LGPD. Os principais resultados apontam que 58,9% delas estão em um nível intitulado como "inicial", ao passo que 17,8% encontram-se no nível "inexpressivo" (Brasil, 2022c). Dentre as demais, a atividade de auditoria revelou que 20,4% situam-se no nível "intermediário" e, finalmente, apenas 2,9% foram consideradas no nível "aprimorado" (Brasil, 2022c).

Numa dimensão estrita, o órgão de controle apontou também que somente 14% dessas instituições identificaram os dados pessoais que são objeto de tratamento em seus processos, incluindo aqueles compartilhados com terceiros; 11% identificaram e documentaram todas as finalidades dos tratamentos; e 82% não têm um registro instituído para consolidar informações relacionadas com as características das atividades de tratamento de dados pessoais, bem como não possuem política de proteção de dados (Brasil, 2022c). Ao destacar a baixa implementação de medidas básicas visando à conformidade dessas instituições com a LGPD, Carvalho (2023, p. 140-141) frisou:

> Muitas dessas organizações sequer realizaram o mapeamento de processos e a identificação de quais dados são tratados e para quais finalidades, o que indica que esses processos são desconhecidos ou são realizados de forma discricionária e desestruturada, isto é, sem a devida avaliação e motivação quanto à sua adequação à LGPD. Por sua vez, a opacidade das operações realizadas com dados pessoais é atestada pelo reduzido índice de organizações que elaboraram e publicaram política de privacidade ou que instituíram mecanismos para atender aos direitos dos titulares. Em suma, as informações levantadas pelo TCU revelam a existência e o predomínio de uma postura reativa no setor público federal em face da implementação da LGPD, o que pode ter sido incentivado pelas sucessivas postergações de vigência da lei ou, ainda, pela concepção de que a legislação de proteção de dados pessoais representa um entrave à inovação e à eficiente execução de políticas e serviços públicos.

Nesse contexto, com o propósito de elevar a maturidade relacionada à implementação da LGPD nesses órgãos e entidades, têm sido adotadas ações por parte do Poder Público, dentre as quais a instituição do Programa de Privacidade e Segurança da Informação (PPSI), formalizado por intermédio da Portaria nº 852, de 28 de março de 2023, contemplando os órgãos e entidades da administração pública federal direta, autárquica e fundacional, com unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (Brasil, 2023a).

O PPSI contempla um conjunto de projetos e de processos distribuídos nas áreas de governança, maturidade, metodologia, pessoas e tecnologia, cujas iniciativas perpassam, dentre outras, o diagnóstico do grau de implementação dos controles de privacidade e segurança da informação, bem como a disponibilização de guias, processos, modelos e procedimentos, incluindo um *framework*[1] (Brasil, 2023a). Este auxiliará os entes a identificarem, acompanharem e preencherem possíveis lacunas de privacidade e segurança da informação (Brasil, 2023a).

Ao implementar esse *framework*, por meio de uma autoavaliação, será possível avaliar a maturidade do órgão ou entidade, identificando as lacunas, a fim de possibilitar a adoção de novas medidas ou aperfeiçoamento das já existentes, bem como realizar o planejamento visando subsidiar essa execução (Brasil, 2023a). A ferramenta é composta por 32 controles, que estão alinhados com a Política Nacional de Segurança da Informação (PNSI), a própria LGPD, os normativos emitidos pela Autoridade Nacional de Proteção de Dados (ANPD) e pelo Gabinete de Segurança Institucional, bem como as recomendações de órgãos federais de controle. O Quadro 1 ilustra esses controles, bem como suas respectivas categorias.

Quadro 1 - Controles do *framework* do PPSI

Categoria	Controle
Estruturação básica de gestão em privacidade e segurança da informação	0. Controle de estruturação básica de gestão em privacidade e segurança da informação
Segurança cibernética	1. Inventário e controle de ativos institucionais
	2. Inventário e controle de ativos de *software*
	3. Proteção de dados
	4. Configuração segura de ativos institucionais e *software*
	5. Gestão de contas
	6. Gestão de controle de acesso
	7. Gestão contínua de vulnerabilidades
	8. Gestão de registros de auditoria
	9. Proteções de e-mail e navegador web
	10. Defesas contra *malware*
	11. Recuperação de dados
	12. Gestão da infraestrutura de rede
	13. Monitoramento e defesa da rede
	14. Conscientização e treinamento de competências sobre segurança
	15. Gestão de provedor de serviços
	16. Segurança de aplicações
	17. Gestão de resposta a incidentes
	18. Testes de invasão
Privacidade	19. Inventário e mapeamento
	20. Finalidade e hipóteses legais

[1] Em tradução literal, quer dizer “estrutura”. No contexto desta pesquisa, o termo foi empregado como “estrutura conceitual”.

Categoria	Controle
	21. Governança
	22. Políticas, processos e procedimentos
	23. Conscientização e treinamento
	25. Gestão do tratamento
	26. Acesso e qualidade
	27. Compartilhamento, transferência e divulgação
	28. Supervisão em terceiros
	29. Abertura, transparência e notificação
	30. Avaliação de impacto, monitoramento e auditoria
	31. Segurança aplicada à privacidade

Fonte: Elaborado pelo autor (2024), com base no *framework* do PPSI.

Além desse *framework*, cabe destacar a estrutura conceitual idealizada por Santana e Mendonça (2023). Este último foi estruturado num formato de questionário, elaborado a partir do estudo da Lei Geral de Proteção de Dados (LGPD), da *General Data Protection Regulation* (GDPR) e da *California Consume Privacy Act* (CCPA), bem como do *NIST Privacy Framework* e ISO 27701, que consistem em *frameworks* e normas de boas práticas de privacidade e proteção de dados. Esse questionário busca avaliar a adequação e adesão às leis e às boas práticas de privacidade e proteção de dados e contém seis seções, com 49 perguntas, conforme disposto no Quadro 2.

Quadro 2 - Seções do *framework* de proteção de dados

Nº	Seção	Conteúdo
1	Segurança para Privacidade	Estabelecimento de medidas de segurança técnicas e administrativas para proteção dos dados pessoais, de acordo com o tratamento e a estrutura técnica e organizacional, a fim de prevenir o acesso não autorizado a dados pessoais e situações acidentais ou ilegais de destruição, perda, alteração, comunicação ou difusão.
2	Estrutura de Privacidade	Estabelecimento de uma estrutura de governança de privacidade, incluindo-se a definição de pessoas responsáveis pela cultura de privacidade na organização (encarregado e Comitê de Privacidade) e a elaboração de políticas, procedimentos e programas de conscientização, para auxiliar a construção da maturidade em privacidade.
3	Inventário de Dados Pessoais	Identificação e mapeamento dos processos que realizam o tratamento dos diversos tipos de dados (dados pessoais, dados pessoais sensíveis, dados de menores de idade, dados de estrangeiros), registro das finalidades de tratamento, ciclo de vida dos dados pessoais, tempo de retenção, forma de destruição, declaração de bases legais e análise dos demais princípios da LGPD, de acordo com o art. 6º (minimização, segurança, transparência e afins).
4	Legitimidade do Tratamento	Atribuição de bases legais ao tratamento de dados pessoais mapeados de acordo com as finalidades especificadas, a fim de garantir aos titulares o livre acesso aos seus dados pessoais, bem como o tratamento adequado.

5	Atendimento a Requisições	Elaboração de Relatórios de Impacto à Proteção de Dados (RIPD), desenvolvimento de procedimentos para permitir o atendimento às requisições da Autoridade Nacional de Proteção de Dados (ANPD) e das solicitações de titulares.
6	Conformidade de Terceiros	Definição e implementação de cláusulas específicas de privacidade em contratos com terceiros, bem como elaboração de procedimentos com diretrizes sobre o tratamento adequado dos dados pessoais compartilhados com terceiros.

Fonte: adaptado de Santana e Mendonça (2023).

Desse modo, por meio do *framework*, será possível analisar o nível de maturidade considerando-se a classificação obtida em termos do *compliance* quanto à privacidade e proteção de dados no âmbito de uma organização. Segundo Garbaccio, Vadell e Torchia (2022, p. 213), o *compliance* abrange "um conjunto de medidas através das quais se busca cumprir a ordem vigente, observando os princípios da ética e integridade corporativa, se constituindo de procedimentos internos que objetivam evitar práticas ilícitas no âmbito de uma estrutura organizada". Para os autores, o *compliance* deve contribuir para a cultura de respeito às normas e à ética e, em se tratando de dados pessoais, encontra-se relacionado ao cumprimento dos direitos dos titulares desses dados (Garbaccio; Vadell; Torchia, 2022).

Nessa perspectiva, identifica-se a necessidade de se realizar estudos direcionados para compreender, além do nível de maturidade, as ações e desafios do processo de implementação e adequação da LGPD na Administração Pública.

Ademais, Aguilera e Di Biase (2021, p. 11) ressaltam que os dados pessoais em posse do Poder Público "devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral". Para Cristóvam, Bergamini e Hahn (2021, p. 96), isso evita "que o mesmo dado seja coletado inúmeras ocasiões por diversos órgãos".

Entretanto, sabe-se que, em não raras situações, a infraestrutura para manutenção de dados de órgãos e entidades públicas são deficientes, principalmente em estados e municípios dos rincões do país, o que se configura um desafio para aplicação efetiva da norma, uma vez que não se garante a interoperabilidade dos dados, tampouco seu compartilhamento de forma segura quando o ente receptor não possui condições para tratá-los de forma adequada, em desacordo com a LGPD (Aguilera; Di Biase, 2021).

Ademais, atecnias[2], contradições e incongruências são fatores que constituem um entrave para a implementação da LGPD em instituições públicas, conforme apontado a seguir:

> Uma leitura mais atenta dos arts. 26, §1º, e 27 da LGPD permite constatar que o legislador não foi feliz na escolha de alguns termos e expressões-chave desses dispositivos, tampouco na sua estrutura organizacional. Em primeiro lugar, é possível notar uma falta de organização e coesão na construção dos referidos artigos de Lei, ao se observar que (i) o caput do art. 26 trata do uso compartilhado de dados entre órgãos e entidades do próprio Poder Público, enquanto seu §1º trata da transferência de dados envolvendo o Poder Público e particulares (ou seja, matéria totalmente diversa); ao passo que (ii) o art. 27 volta a tratar da matéria do compartilhamento de dados entre Poder Público e particulares. Por óbvio, não foi utilizada a melhor técnica legislativa na organização e redação desses dispositivos da LGPD. Diante da disciplina diversa dada a essas matérias, o mais correto teria sido destinar um artigo para o compartilhamento de dados pessoais no âmbito do Poder Público; e um outro artigo para a relação entre o Poder Público e particulares, com a subsunção dos parágrafos ao conteúdo normativo dos respectivos caputs (Aguilera; Di Biase, 2021, p. 18).

É fato que os dispositivos podem suscitar interpretações conflitantes acerca do tema, prejudicando o entendimento do agente responsável por aplicar a lei e, por conseguinte, do órgão ou ente a que está vinculado, constituindo-se, por essa razão, um desafio para o âmbito público. Numa perspectiva mais ampla, Montolli (2020) pontua que um dos principais dilemas se refere à própria atuação desses agentes públicos, que devem conciliar as exigências constantes na LGPD com o direito à privacidade dos cidadãos, a fim de construir uma relação de confiança com eles. Por sua vez, outro desafio relaciona-se à disparidade tecnológica visualizada na Administração Pública, uma vez que "existem entidades e órgãos com melhores condições de aparelhamento e capacitação digital", ao passo que outras "têm condições precárias de instalações, [...] de acesso à internet e tecnologias" (Philippi; 2023, p. 14).

Especificamente, no âmbito das Instituições de Ensino (IES), um dos principais desafios relaciona-se ao elevado volume de dados efetivamente tratados pelas IES, o que corrobora a importância de que sejam implementadas ações para assegurar a conformidade no tratamento dos dados (Santos Filho; Jesus, 2023). Segundo esses autores, ao adotar tais ações, é possível "aperfeiçoar a gestão acadêmica, otimizar processos, [...], desenvolver pesquisas e inovações, fortalecer a comunicação e o relacionamento com a comunidade acadêmica, além de promover a segurança e a confiabilidade da instituição" (Santos Filho; Jesus, 2023, p. 275). Assim, esses autores destacam que devem ser adotadas algumas ações, dentre as quais:

[2] Na linguagem jurídica, ocorre quando o legislador erra ao escrever uma palavra impropriamente no texto da lei.

- Designação de um *Data Protection Officer* (DPO): a quem compete supervisionar a implementação e o cumprimento da política institucional de proteção de dados, a fim de assegurar a conformidade com a LGPD;
- Análise pormenorizada dos dados: consiste em identificar as fontes, os fluxos de processamento, o armazenamento e as finalidades, com vistas a detectar potenciais vulnerabilidades ou riscos à privacidade;
- Instituição de políticas e procedimentos claros: devem abordar aspectos como obtenção de consentimento do titular, segurança da informação e descarte seguro de informações, por exemplo;
- Adoção de medidas técnicas para garantir a segurança dos dados: engloba a criptografia, controle de acesso, *backups*, anonimização ou pseudonimização de informações sensíveis, dentre outros;
- Capacitação funcional: contempla a necessidade de treinamentos, bem como a elaboração e disponibilização de materiais educativos, a fim de auxiliar que os colaboradores compreendam sua responsabilidade em assegurar a proteção de dados pessoais;
- Avaliações de conformidade e auditorias internas: cujo objetivo é verificar se as políticas e procedimentos estão sendo adequadamente cumpridos.

Outra pesquisa sobre a implementação da LGPD em instituições de ensino foi realizada por Gomes, Cunha Filho e Luccas (2023). Os autores fizeram um estudo no âmbito da Fundação Getúlio Vargas (FGV) e constataram que a organização estruturou sua metodologia de implementação da norma de acordo com os tipos de vínculo que mantinha com os discentes. A partir disso, concluiu-se que a natureza do relacionamento era fator determinante para a especificação da finalidade do tratamento de dados, alterando-se o regime de aplicabilidade da LGPD em cada caso.

Assim, de acordo com Gomes, Cunha Filho e Luccas (2023), a fim de dar efetividade ao tratamento de acordo com as categorias, o passo inicial deve ser o de mapeamento de processos. Isso permite que sejam identificados os dados relacionados à categoria de ensino, excluindo-se aqueles referentes às interações não condizentes com essa categoria. Desse modo, ainda segundo os autores, os processos identificados como decorrentes dessa relação são divididos em quatro categorias, sendo aplicável, “para cada grupo de operações de tratamento pertencentes a cada categoria, [...] uma base legal cabível, uma finalidade, etc.”, identificando-

se, desse modo, “problemas de adequação característicos de cada categoria”, de modo a “encontrar solução para cada um deles” (Gomes; Cunha Filho; Luccas, 2023, p. 407).

Para tanto, foram observados os tratamentos realizados como “preliminares à prestação de serviços acadêmicos, como forma de prestar serviço propriamente, ou, ainda, em decorrência, jurídica ou não, de tal prestação” (Gomes; Cunha Filho; Luccas, 2023, p. 407), tendo sido identificadas quatro categorias, a saber:

> 1) Interessados: são os titulares de dados que manifestam, direta ou indiretamente, o interesse de participar, como alunos de cursos, de disciplinas ou de eventos promovidos pela IES.
> 2) Inscritos: são os titulares que se inscrevem em processos seletivos para cursos ou disciplinas avulsas de graduação, de pós-graduação ou de extensão, ou para eventos promovidos pela IES.
> 3) Matriculados: são os titulares matriculados em cursos ou disciplinas avulsas de graduação, de pós-graduação ou de extensão oferecidos pela IES, incluindo aqueles com matrícula trancada ou suspensa.
> 4) Ex-alunos: são os titulares com matrícula encerrada, seja por conclusão ou por abandono, em cursos ou disciplinas avulsas de graduação, de pós-graduação ou de extensão oferecidos pela IES (Gomes; Cunha Filho; Luccas, 2023, p. 408).

Não obstante a distinção apresentada, é possível que os titulares pertençam a mais de uma categoria, como, por exemplo, um ex-aluno de curso de graduação pode ser discente de um curso de pós-graduação. Nessas situações, “os dados do titular [...] devem seguir, apenas, as operações de tratamento, as bases legais e as finalidades apontadas para [...] a categoria específica” (Gomes; Cunha Filho; Luccas, 2023, p. 409).

Nesse sentido, tem-se como exemplo o caso de ex-aluno da instituição, cujos dados foram coletados durante o período em que possuía vínculo. Nesse caso, não poderá a instituição usá-los em momento posterior ao fim da relação, uma vez que está adstrita à finalidade inicial, qual seja, a prestação do ensino. Desse modo, a categorização da finalidade mostrou-se efetiva e exitosa para a aplicação da LGPD na organização, de modo a subordiná-la ao atendimento dos ditames legais.

Ainda no âmbito dessas instituições, Nascimento e Silva (2023) analisaram a adequação à LGPD dos repositórios institucionais, que reúnem as produções científicas de uma entidade. Ao solicitar a publicação de um trabalho naquela plataforma, o usuário deverá fornecer dados pessoais, o que justifica a importância de que sejam protegidos. Assim, as autoras pontuam que deverão ser adotadas algumas ações para assegurar a conformidade desses repositórios, dentre as quais:

- Cadastramento: identificar os dados pessoais ou sensíveis relativos ao cadastro do perfil dos usuários, buscando-se solicitar apenas os considerados essenciais;

- Capacitação: promover treinamentos junto às equipes para orientar quanto aos novos procedimentos e fluxos de trabalho para a proteção dos dados pessoais;
- Gestão de risco: identificar e analisar possíveis riscos, a partir da probabilidade e do impacto de cada um deles. A partir de então, definir estratégias para prevenir e mitigá-los, bem como proceder nos casos de incidentes;
- Gestão documental: mapear o ciclo de vida dos dados pessoais nos arquivos físico e digital: coleta, uso, armazenamento, eliminação, dentre outros;
- Gestão institucional: participar das discussões relativas ao estabelecimento de processos e fluxos que compreendam o ciclo do tratamento dos dados pessoais e sensíveis; bem como apropriar-se da política institucional de privacidade ou de proteção de dados, caso a instituição já disponha; caso não, contribuir junto a uma equipe multidisciplinar com a sua elaboração.

Barbosa *et al*. (2021) reforçam a importância de que as instituições de ensino busquem consolidar uma cultura para o tratamento de dados. Nesse sentido, esses autores ressaltam a importância de estudos que explorem as ações e os desafios inerentes ao processo. O fato é que, no âmbito público, há peculiaridades quanto aos objetivos e finalidades desse tratamento, que demandam uma atenção dos agentes em estrita observância ao interesse público (Aguilera; Di Biase, 2021), o que é extensível às instituições públicas de ensino (Rojas, 2020).

Outra particularidade refere-se à existência de hipóteses em que o tratamento de dados dar-se-á com fulcro em outros fundamentos previstos na LGPD (Blum; López, 2020; Crespo, 2021). Nesse sentido, embora a regra preveja o consentimento do titular (Requião, 2022; Blum; López, 2020) – de forma autônoma, prévia, livre de vícios e específica, instrumentalizando a autodeterminação informativa (Doneda, 2011; Tepedino; Teffé, 2020b) – há situações nas quais essa anuência é dispensada (Brasil, 2018).

De qualquer modo, com a anuência do titular ou com fundamento em outra base legal, é essencial preservar todos os direitos assegurados pela LGPD, não havendo legalmente a possibilidade de o controlador extrapolar, em regra, a finalidade prevista inicialmente no consentimento, quando este for exigido. Dessa forma, para que haja o tratamento, é necessário que sejam asseguradas todas garantias inerentes à proteção de dados (Dias, 2022).

É cediço que o princípio da legalidade em sentido estrito norteia o Poder Público em suas ações. Ademais, os tratamentos efetuados pelas pessoas jurídicas de direito público devem ser realizados “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" (Brasil, 2018b, p. 62).

Tal submissão, contudo, não significa que os tratamentos realizados no âmbito da Administração Pública serão, necessariamente, fundamentados em obrigação legal ou cumprimento de dever, sendo possível a aplicação de outras bases legais (Blum; López, 2020), as quais também são aplicáveis ao tratamento realizado por particulares, salvo quando para execução de políticas públicas (Brasil, 2018b).

Esses dispositivos autorizadores estão elencados no inciso II do art. 11 da LGPD (Brasil, 2018b) e não guardam relação de hierarquia com o consentimento do titular previsto no inciso I do mesmo artigo (Tepedino; Teffé, 2020b). São eles:

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude ou à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Brasil, 2018b, p. 61).

É certo que as bases legais têm como condão evitar tratamentos discriminatórios para com indivíduos, tal como grupos em desvantagem sistêmica e sub-representados, que podem, exemplificativamente, ter o acesso ao crédito e ao emprego tolhidos (Tepedino; Teffé, 2020b). Por outro lado, a existência de outras hipóteses para tratamento que não apenas o consentimento também tem como fundamento coibir abusos de particulares. Cravo (2021) ilustra enfatizando o contrassenso que seria a necessidade de consentimento do titular para dar andamento a cobranças fiscais ou para o exercício de poder de polícia em seu desfavor.

Especificamente no que se refere ao cumprimento de obrigação legal ou regulatória pelo controlador, esta pode ocorrer de diferentes maneiras. A título de exemplo, pode-se citar o preenchimento da Relação Anual de Informações Sociais (RAIS) pelo empregador com os dados do empregado (Meireles, 2022), a divulgação da remuneração de servidores públicos (Paranhos, 2022) e a manutenção de dados pessoais e transacionais de indivíduos por instituições financeiras e afins por um período de cinco anos (Brasil, 1998).

Ademais, em relação à Administração Pública, a LGPD não será aplicada nos casos de tratamento para fins exclusivos de: segurança pública; defesa nacional; defesa do Estado; e atividades de investigação e de repressão de infrações penais (Brasil, 2018b; Crespo, 2021). Nessas hipóteses, Blum e López (2020, p. 173) defendem a inaplicabilidade da normativa apenas de forma aparente, uma vez que a ANPD "emitirá opiniões técnicas ou recomendações sobre essas exceções e poderá solicitar relatório de impacto à proteção de dados pessoais", não se exigindo, entretanto, para o tratamento, a subsunção do fato a uma das bases legais previstas no art. 7º (Blum; López, 2020).

Ainda fora do âmbito privado, Crespo (2021, p. 22) aponta a necessidade de maior transparência quanto à proteção dos dados em posse do Poder Público, face às "massivas quantidades de dados pessoais e dados pessoais sensíveis, em virtude da obrigatoriedade da entrega dessas informações pelos cidadãos" e devido ao desequilíbrio existente nessa relação. Conforme destacado por Montolli (2020), a relação entre a Administração Pública e os cidadãos deve ser pautada pela confiança, o que requer uma atuação responsiva por parte dos agentes públicos, em conformidade com a LGPD.

Essas constatações enunciadas por Crespo (2021) e Montolli (2020) vão ao encontro do estudo realizado por Oliveira (2024) no âmbito da mesma universidade objeto desta dissertação. A partir da análise de processos administrativos eletrônicos que tratam sobre a concessão de pensão civil, foi possível identificar inconsistências na natureza dos documentos constantes nos processos, tipificando-os como ostensivos, quando, na verdade, deveriam ser classificados como restritos (ou vice-versa). Dos 79 processos que tramitaram no período de 2020 a 2022, 73 apresentaram desconformidade em relação à LGPD, o que representa um percentual de 92,4% (Oliveira, 2024). Segundo a autora, "constatou-se a ocorrência de exposição integral de documentos digitalizados de dados bancários, certidões de casamento, contracheques e cartão bancário, inclusive com o código de segurança", o que poderá "permitir o acesso a uma quantidade substancial de dados pessoais por parte de terceiros, aumentando a vulnerabilidade dos indivíduos a possíveis violações de privacidade e fraudes" (Oliveira, 2024, p. 71).

Na UFRPE, a abertura de processo eletrônico é centralizada no setor de Protocolo da instituição. Além disso, no decorrer da tramitação, a inclusão de novos documentos é realizada pelos servidores do setor responsável pela análise processual, o que é um indicativo de que as falhas estão ocorrendo devido à atuação dos operadores internos durante o tratamento de dados (Oliveira, 2024). Uma dessas falhas consiste na exposição do número do Cadastro de Pessoa Física (CPF) dos operadores, que consiste num dado desnecessário, "uma vez que sua matrícula

já é suficiente para respeitar o princípio da transparência e publicidade, bem como resguardar seus dados pessoais" (Oliveira, 2024, p. 72), em consonância com o posicionamento da Advocacia-Geral da União (AGU) (Brasil, 2021a).

De acordo com a AGU, é possível substituir o CPF pelo número da matrícula Siape[3] do representante legal da pessoa jurídica de direito público em "lavratura de contratos, termos aditivos e instrumentos congêneres, [...] acordos de cooperação técnicas, portarias de designação ou mesmo em relatórios e documentos relacionados às atividades finalísticas" (Brasil, 2021a, p.1). Desse modo, "embora se enquadre na definição de dado pessoal, à luz da LGPD", a matrícula Siape "não possui repercussões para além da vida pública do servidor, não havendo razões para que esse dado tenha restrição de acesso" (Brasil, 2021a, p. 1).

Quanto ao número do CPF, a AGU destacou sua relevância, advertindo que esse dado cumula a natureza jurídica de "Informação pessoal relativa à intimidade" e de "Dado pessoal não-sensível", devendo ser tutelado pela LGPD, "observando os princípios da necessidade, segurança e prevenção" (Brasil, 2022b, p. 14). Apesar disso, o órgão ressalta a possibilidade da divulgação do CPF, nos casos de representantes legais de pessoas jurídicas contratadas pelo Poder Público, desde que descaracterizado (Brasil, 2021a; Brasil 2024a; Brasil, 2024b), independentemente do consentimento expresso do titular, com amparo, entre outras, nas seguintes razões:

> A publicação em transparência ativa do número do CPF deve ser feita de forma descaracterizada, mediante ocultação dos três primeiros dígitos e dos dois últimos dígitos verificadores, uma vez que: tal procedimento enquadra-se no conceito de técnica de anonimização do dados da LGPD (art. 5º, XI, e 12); deriva sua juridicidade também da analogia ao art. 149 da LDO, e consagração na jurisprudência administrativa de pedidos de acesso à informação e no costume administrativo do Portal da Transparência; e atende concomitantemente aos requisitos de restrição de acesso à informação do art. 31 da LAI; aos requisitos de proteção de dados pessoais da LGPD, notadamente aos princípios da necessidade, segurança e prevenção; e às obrigações legais e às necessidades da política pública de transparência e de governo aberto, possibilitando o controle social e prevenindo homonímias (Brasil, 2022b, p. 14).

Por outro lado, a ANPD entende que "o nome completo e o número do CPF são dados indispensáveis no âmbito dos contratos administrativos e sua publicidade se impõe" (Brasil, 2023d). Além disso, a autarquia aponta que em "casos de dados públicos ou compartilhados,

[3] A matrícula no Sistema Integrado de Administração de Pessoal (Siape) identifica o servidor público Federal no órgão em que desempenha suas atividades.

como não há um padrão para o mascaramento[4], é possível que partes distintas dos dados estejam visíveis e por consequência os dados originais sejam reconstruídos" (Brasil, 2023c, p. 22).

Nesse contexto, visualiza-se a necessidade da implantação e propagação de uma cultura de dados na Administração Pública, a fim de que os agentes tenham ciência da importância do tratamento correto dos dados armazenados, visando incrementar a segurança e o compromisso ético, bem como mitigar a ocorrência de vazamentos e compartilhamentos indevidos e ilegais (Philippi, 2023). Assim, será possível assegurar o direito à proteção de dados pessoais de forma ampla e efetiva.

[4] "A técnica consiste em substituir uma parte dos caracteres dos dados por um caractere símbolo (por exemplo * ou x) (Brasil, 2023c, p. 21)".

3 PROCEDIMENTOS METODOLÓGICOS

Este capítulo trata das estratégias metodológicas que foram empregadas neste estudo. Barros e Lehfeld (2007) destacam que a metodologia consiste no estudo da abordagem mais apropriada para investigar um problema; é a aplicação do método, com o objetivo de assegurar a legitimidade científica do conhecimento adquirido.

3.1 CARACTERIZAÇÃO DO ESTUDO

No que tange à natureza, esta pesquisa tipifica-se como aplicada, uma vez que pretendeu obter "conhecimento com vistas à aplicação numa situação específica" (Gil, 2017, p. 33). Para Barros e Lehfeld (2007), nesse tipo de pesquisa, o conhecimento gerado subsidiará a resolução mais ou menos imediata de problemas que, porventura, possam existir numa organização.

No tocante aos objetivos, esta pesquisa classifica-se como descritiva. Gil (2017, p. 33) destaca que "as pesquisas descritivas têm como objetivo a descrição das características de determinada população ou fenômeno". Desse modo, almejou-se investigar como a LGPD vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE).

Em relação aos métodos, trata-se de uma pesquisa documental, de campo e estudo de caso. Segundo Gil (2017), a pesquisa documental constitui-se como um dos delineamentos mais utilizados no âmbito das ciências sociais, abrangendo documentos físicos e eletrônicos. Para Cellard (2008, p. 296), nesse método, "a informação [...] circula em sentido único, pois, embora tagarela, o documento permanece surdo", o que justifica a importância de que o pesquisador tenha cautela ao interpretar as informações, tendo em vista que não poderá "exigir precisões suplementares" do documento. Nesse sentido, a pesquisa documental compreendeu as normas institucionais relacionadas à proteção de dados pessoais, a fim de subsidiar a investigação do problema do estudo. Por sua vez, tipifica-se como uma pesquisa de campo, que "não deve ser confundida com a simples coleta de dados (esta última corresponde à segunda fase de qualquer pesquisa); é algo mais que isso, pois exige contar com controles adequados e objetivos preestabelecidos que discriminam suficientemente o que deve ser coletado" (Trujillo, 1982, p. 229). Trata-se também de um estudo de caso instrumental, segundo Stake (2000). Para o autor, este tipo de caso é utilizado quando, por meio dele, é possível ter um entendimento geral sobre determinado tema, problema de pesquisa, que pode ser solucionado a partir do caso específico. Nesta pesquisa, o caso específico é a UFRPE.

De acordo com Marconi e Lakatos (2003), a pesquisa de campo compreende algumas fases. Na primeira delas, deverá ser realizada uma pesquisa bibliográfica, a fim de aprofundar o conhecimento sobre o tema, verificar trabalhos realizados e elaborar o plano geral de pesquisa. Na segunda etapa, serão determinadas as técnicas que serão utilizadas na coleta de dados e, na última fase, antes de realizar tal coleta, "é preciso estabelecer tanto as técnicas de registro desses dados como as técnicas que serão utilizadas em sua análise posterior" (Marconi; Lakatos, 2003).

Quanto à abordagem do estudo, trata-se de uma pesquisa mista, já que os dados foram analisados de forma quantitativa, com o tratamento estatístico dos dados relativos ao nível de maturidade em relação à LGPD, e qualitativa, quanto à análise das entrevistas e documentos. A esse respeito, Martins e Theóphilo (2007) advogam que as abordagens qualitativa e quantitativa devem ser visualizadas como complementares e não como opostas. Além de corroborar esse posicionamento, Creswell (2010) destaca que o pesquisador deve basear a investigação na suposição de que a coleta de diversos tipos de dados proporciona uma melhor compreensão do problema de pesquisa.

Sendo assim, tal estratégia revelou-se apropriada para identificar as ações realizadas na promoção da proteção de dados no âmbito da UFRPE; identificar os desafios enfrentados pela UFRPE na implementação das práticas de proteção de dados; analisar o nível de maturidade da proteção de dados no âmbito da UFRPE com base no *framework* proposto por Santana e Mendonça (2023); e propor ações para fortalecer a política de proteção de dados no contexto da organização.

3.2 COLETA DE DADOS

A primeira etapa da coleta de dados consistiu na pesquisa documental no âmbito da UFRPE, voltada para o levantamento de documentos referentes à LGPD. O Quadro 3, disposto abaixo, enumera os documentos que foram consultados nesta pesquisa, com vistas a atender ao primeiro objetivo específico deste estudo. Para subsidiar a elaboração do Quadro 3, foi utilizado o critério cronológico, ou seja, os documentos foram listados com base no ano de publicação:

Quadro 3 - Documentos institucionais consultados na pesquisa

(continua)

Documento	Ano
Resolução Nº 031/2020-CONSU/UFRPE	2020
Cartilha LGPD da UFRPE	2021
Resolução Nº 103/2021-CONSU/UFRPE	2021
Plano de Desenvolvimento Institucional (PDI) da UFRPE Vigência 2021-2030	2021
Plano de Dados Abertos (PDA)	2022

Documento	Ano
Política de Segurança da Informação e Comunicação (POSIC)	2022
Constituição da Equipe de Tratamento e Respostas a Incidentes Cibernéticos (ETIR)	2022
Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)	2023
Plano de Contingência de Tecnologia da Informação e Comunicação (PCTIC)	2023
Painel de Monitoramento do PDI UFRPE 2021-2030	2025

Fonte: Elaborado pelo autor (2025).

Na segunda fase, foram realizadas entrevistas com o Encarregado da LGPD na entidade, o Diretor da Secretaria de Tecnologias Digitais (STD) e o Coordenador de Governança Digital, para subsidiar o alcance do segundo objetivo específico desta pesquisa. A STD é o setor responsável por prover serviços de Tecnologia da Informação e Comunicação (TIC) no âmbito da UFRPE, incluindo governança digital, serviços computacionais, sistemas de informação, serviços de conectividade e segurança da informação e comunicação.

Como critério de inclusão, a escolha desses participantes se deu em razão da relevância de suas funções para subsidiar a implementação da LGPD na instituição. Em consonância com a Norma Operacional nº 001/2013, do Conselho Nacional de Saúde (CNS), esses participantes foram recrutados por meio de mensagem eletrônica enviada ao e-mail institucional, contendo as informações básicas da pesquisa, a fim de agendar a entrevista no formato presencial, na própria instituição. Os encontros foram realizados nos meses de fevereiro e março do ano de 2025. Porém, dois deles foram realizados virtualmente, por meio da ferramenta *Google Meet*, devido à solicitação dos participantes, não havendo prejuízo para a coleta de dados.

Para tanto, foi utilizado um roteiro semiestruturado (ver Apêndice B), que permitiu que novas questões fossem abordadas no decorrer do diálogo, a fim de ampliar e aprofundar a coleta de informações durante esta fase. Os dados demográficos constantes no roteiro de entrevista (área de formação, cargo, função, tempo de trabalho na instituição e tempo de atuação como responsável pela implementação da LGPD) possuem correlação com o objetivo da pesquisa, auxiliando as inferências resultantes da análise dos dados pelo pesquisador.

A terceira fase da coleta consistiu na aplicação do *framework* desenvolvido por Santana e Mendonça (2023), constante no Anexo, a fim de atender ao terceiro objetivo desta pesquisa. Tal *framework* foi enviado à instituição investigada por meio do Fala.BR, plataforma que integra a Ouvidoria e o Acesso à Informação do Poder Executivo Federal. A escolha foi motivada pela obrigatoriedade de as instituições responderem às solicitações no prazo de 20 dias, prorrogáveis por mais 10 dias, possibilitando o acesso aos dados que necessitavam ser coletados, nos termos da Lei de Acesso à Informação (Brasil, 2011).

Para avaliar a adesão dos controles de proteção de dados[5], foram incluídas quatro opções de resposta, a saber: I) sim; II) não; III) parcialmente; e IV) não aplicável. Para cada uma delas, foram concedidas notas, que variam de 4 a 0 (4 para cada resposta positiva; 2 para parcial; e 0 para negativa), a fim de subsidiar o cômputo do resultado de cada seção, bem como a avaliação global. Quanto à categoria de resposta "não aplicável", esta será desconsiderada.

Com base nesses resultados, foi possível efetuar a classificação de privacidade e de proteção de dados, após o cálculo da média aritmética de cada seção. Com vistas a possibilitar tal classificação, foram estabelecidas faixas de variação, de acordo com os parâmetros definidos no Quadro 4, constante abaixo.

Quadro 4 - Classificação de privacidade e proteção de dados

Nível de maturidade	Entre 0 e 1,9	Entre 2 e 2,5	Entre 2,6 e 4
Classificação	Não *compliance*	*Compliance* parcial	*Compliance*

Fonte: adaptado de Santana e Mendonça (2023).

Finalizada a coleta, os dados foram organizados e tabulados numa planilha do *Microsoft Excel*. Com o objetivo de facilitar a visualização dos dados, foram elaborados tabelas e gráfico, que serão apresentados no capítulo sobre os resultados.

3.3 ANÁLISE DE DADOS

Após a etapa de coleta, procedeu-se à análise dos dados. Inicialmente foi realizada uma análise dos documentos dispostos no Quadro 5, de modo a atender ao primeiro objetivo específico desse trabalho, ou seja, identificar as ações realizadas na promoção da proteção de dados pessoais no âmbito da Universidade Federal Rural de Pernambuco (UFRPE).

Consoante Cellard (2008), é necessário que o investigador adote algumas precauções antes de iniciar a análise documental, dentre as quais selecionar textos pertinentes à temática, bem como avaliar sua credibilidade e representatividade, com vistas a assegurar a validade e a solidez das inferências. Com base nisso, selecionaram-se documentos ostensivos, publicizados

[5] Refere-se ao conjunto de "atividades de gestão de privacidade e proteção de dados que devem ser presentes nas organizações que precisam se adequar às legislações de proteção de dados aplicáveis" (Santana; Mendonça, 2023, p. 31). Ao analisar essas atividades, será possível medir o nível de maturidade da organização. Nesta dissertação, as expressões "controles de proteção de dados" e "nível de maturidade" são intercambiáveis.

pela UFRPE, que, direta ou indiretamente, tratam das TDIC, e, consequentemente, da proteção de dados, da segurança da informação e da privacidade na instituição, conforme o Quadro 5.

Quadro 5 - Elementos de análise dos documentos consultados na pesquisa

Documento	Elementos
Plano de Desenvolvimento Institucional (PDI) da UFRPE Vigência 2021-2030	Diretrizes, os objetivos e as metas referentes à gestão das TDIC na UFRPE
Painel de Monitoramento do PDI UFRPE 2021-2023	Alcance das metas referentes à gestão das TDIC, a fim de identificar as ações realizadas para promover a proteção de dados na organização
Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)	Necessidades corporativas e o diagnóstico de TI da entidade, com vistas a identificar os desafios para promover a proteção de dados
Política de Segurança da Informação e Comunicação (POSIC)	Diretrizes estratégicas sobre segurança da informação e comunicação
Plano de Dados Abertos (PDA)	Diretrizes estratégicas sobre o processo de abertura de dados
Plano de Contingência de Tecnologia da Informação e Comunicação (PCTIC)	Procedimentos que devem ser adotados em caso de incidentes cibernéticos que envolvam dados
Constituição da Equipe de Tratamento e Respostas a Incidentes Cibernéticos (ETIR)	Responsabilidades da ETIR da entidade
Resolução Nº 031/2020-CONSU/UFRPE	Procedimentos de restrição à divulgação de dados pessoais no âmbito da UFRPE
Resolução Nº 103/2021-CONSU/UFRPE	Diretrizes da Política de Privacidade e Proteção de Dados Pessoais (PPPDP) da UFRPE
Cartilha LGPD da UFRPE	Procedimento para o tratamento de dados pessoais no âmbito da instituição

Fonte: Elaborado pelo autor (2025).

A análise das entrevistas foi realizada para atender ao segundo objetivo específico, identificar os desafios enfrentados pela UFRPE na implementação das práticas de proteção de dados pessoais. Para subsidiar a transcrição das entrevistas, foi utilizado o *Whisper*, modelo de aprendizado de máquina criado pela *OpenAI*, lançado como *software* de código aberto no ano de 2022. Após a transcrição, o pesquisador recorreu à análise de conteúdo como método de investigação. Segundo Bardin (2016), esse método corresponde a um conjunto de instrumentos metodológicos de análise das comunicações, que são aplicados ao conteúdo das mensagens para inferir os significados. Neste estudo, foi utilizada a técnica da análise temática ou categorial, cujo objetivo é transformar os dados brutos em categorias, facilitando a inteligibilidade e discussão do tema (Bardin, 2016). Frise-se que foram cumpridas todas as etapas associadas a esse método.

Na primeira etapa da análise de conteúdo, teve início a pré-análise, que consistiu na organização do material bruto, constituído por três documentos referentes às entrevistas, que

totalizaram 67 páginas. Nessa oportunidade, buscou-se a sistematização e a seleção do conjunto de dados, enquanto ocasionalmente foram observadas as primeiras pré-inferências e possíveis categorizações. Em relação à seleção do *corpus*[6], esta foi balizada pelas seguintes regras fundamentais, estabelecidas por Bardin (2016):

- Exaustividade: integram o *corpus* os documentos necessários para análise, que devem ser suficientes para responder o objetivo de pesquisa. As não inclusões e exclusões devem ser justificadas;
- Representatividade: o conjunto de dados escolhido deve ser apto a permitir a generalização dos resultados dentro do contexto estudado;
- Homogeneidade: os documentos selecionados devem guardar semelhança entre si. A heterogeneidade compromete a eficácia do processo analítico, sobretudo quando comparações são exigidas;
- Pertinência: o *corpus* deve ser adequado para elucidar as questões relacionadas à pesquisa. Os documentos irrelevantes devem ser excluídos com as respectivas justificativas.

Dessa maneira, foi realizada uma leitura "flutuante", para estabelecer o primeiro contato com o conteúdo, "deixando-se invadir por impressões e orientações" (Bardin, 2016, p. 126). Em seguida, simultaneamente com a reprodução dos áudios das entrevistas, o pesquisador realizou uma nova leitura do conjunto de dados, a fim de identificar e corrigir eventuais inconsistências na transcrição, tendo elaborado posteriormente a referenciação das unidades do *corpus*, numerando-as de 1 a 3, dado o quantitativo de entrevistados.

Na segunda etapa, com vistas a delimitar as unidades de análise, o plexo documental foi decodificado (ou unitarizado), sendo estabelecidas as unidades de registro e de contexto. De acordo com Bardin (2016, p. 134), a unidade de registro "corresponde ao segmento de conteúdo considerado unidade de base, visando à categorização e à contagem frequencial". Por sua vez, a unidade de contexto concede significado e contextualiza a unidade de registro, consistindo numa dimensão maior (Bardin, 2016). Sendo assim, definiu-se o "tema" como unidade de registro e o "parágrafo" como unidade de contexto.

Nesse sentido, após estabelecer as unidades de registro, o pesquisador agrupou-as em categorias, reunindo-as sob um título único, o que permitiu a generalização dos elementos internos (Bardin, 2016). Neste trabalho, utilizou-se o critério "semântico", compilando-se os

[6] Segundo Bardin (2016, p. 126), "o *corpus* é o conjunto dos documentos tidos com conta para serem submetidos aos procedimentos analíticos", sendo utilizadas algumas regras fundamentais para tal, dentre as quais a exaustividade, representatividade, homogeneidade e pertinência.

temas correlacionados entre si (Bardin, 2016). Essa categorização foi realizada na última etapa do método e pautou-se pelas seguintes regras (Bardin, 2016):

- Regra de exclusão mútua: veda a categorização dupla de uma unidade de registro. Isso significa que uma unidade de registro pode figurar em não mais que uma categoria;
- Regra da homogeneidade: determina que as categorias estejam relacionadas entre si e com o escopo da pesquisa;
- Regra da pertinência: preconiza a adequação das categorias à investigação proposta;
- Regra da exaustividade: estatui que as informações relevantes devem compor alguma categoria;
- Regras da objetividade e fidelidade: exigem clareza quanto às razões das associações de unidades de registro às suas respectivas categorias, de modo a evitar incongruências e ambiguidades.

Como consequência, foram identificadas quatro categorias como causas dos desafios enfrentados na implementação das práticas de proteção de dados pessoais na UFRPE, cuja exposição será realizada no capítulo dos resultados.

A última etapa de análise deste estudo foi analisar o nível de maturidade da proteção de dados no âmbito da UFRPE com base no *framework* proposto por Santana e Mendonça (2023). Nesse sentido, tal fase foi fundamental para propor ações, com vistas a fortalecer a política de proteção de dados no contexto da instituição.

Com base nos resultados encontrados nos três objetivos específicos, foi desenvolvido um produto técnico-tecnológico (PTT), com um diagnóstico da situação da UFRPE no que tange à implementação da LGPD e com propostas de ações para fortalecer a política de proteção de dados no contexto da organização, atendendo ao quarto objetivo específico da pesquisa.

3.4 ASPECTOS ÉTICOS

A apreciação ética foi realizada pelo Comitê de Ética em Pesquisa com Seres Humanos (CEP) da UFRPE, subordinado às diretrizes do Conselho Nacional de Saúde do Ministério da Saúde (CNS/MS) e da Comissão Nacional de Ética em Pesquisa (CONEP), a fim de obter o termo de anuência. Após análise, via Plataforma Brasil, houve a aprovação, conforme Parecer Consubstanciado nº. 7.359.001 e Certificado de Apresentação de Apreciação Ética (CAEE) nº.

84217124.2.0000.9547. Quanto aos procedimentos éticos, o estudo orientou-se pela Resolução nº 510/2016, do CNS/MS.

No tocante aos riscos, destacam-se a possibilidade de desconforto com alguma pergunta e de identificação do entrevistado. Em relação ao primeiro, o formulário de pesquisa apresentou um Termo de Consentimento Livre e Esclarecido (TCLE), indicando que as informações serão utilizadas exclusivamente para o desenvolvimento do estudo, bem como que a coleta de dados não possui fins financeiros nem serão repassadas a terceiros, em consonância com a LGPD. Por sua vez, para mitigar a ocorrência do segundo risco, não foi atribuído o conteúdo diretamente a qualquer participante, o que diminui a possibilidade de identificação.

Quanto aos benefícios, destaca-se: i) contribuir para que a UFRPE alcance um dos seus objetivos estratégicos, a adequação integral dos seus serviços à LGPD até o ano de 2025. Essa contribuição envolve o conhecimento acerca de como a Lei vem sendo aplicada na Instituição, salientando-se as ações implementadas, os desafios enfrentados e o nível de maturidade, com perspectiva de que sejam apontadas áreas específicas que requerem uma maior atenção da gestão institucional, com vistas a fomentar treinamentos, revisão de procedimentos e adoção de novas tecnologias; e ii) possibilidade de os resultados servirem de *insights* para incentivar que outras instituições de ensino superior fortaleçam as suas políticas de proteção de dados pessoais e de segurança da informação.

Durante a pesquisa, os dados coletados foram armazenados em computador protegido por senha, *firewall* e antivírus, com a realização periódica de *backups* dos dados em dispositivo USB e disco rígido externo. Esses cuidados foram adotados para contornar os riscos inerentes ao mundo virtual e às limitações dos equipamentos eletrônicos utilizados.

Todas as informações do estudo são confidenciais e serão divulgadas apenas em eventos ou publicações científicas. Após a conclusão do trabalho, o pesquisador armazenará os dados coletados em dispositivo eletrônico local, HD externo e computador pessoal, apagando todo e qualquer registro que esteja ao seu alcance de qualquer plataforma virtual, ambiente compartilhado ou "nuvem", nos termos da Carta Circular nº 1/2021-CONEP/MS.

Os dados coletados ficarão armazenados no endereço residencial do investigador pelo período mínimo de cinco anos, sendo garantida a divulgação dos resultados aos participantes e à instituição em cujos dados foram coletados, conforme disposições da Resolução n. 510/2016 e da Norma Operacional nº 001/2013, ambas do CNS/MS.

3.5 ESTRUTURA DA PESQUISA

Com o objetivo de apresentar a estrutura do estudo, foi elaborado o Quadro 6, disposto a seguir.

Quadro 6 - Estrutura da pesquisa

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: UM ESTUDO EM UMA UNIVERSIDADE FEDERAL

PERGUNTA DE PESQUISA
Como a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE)?

OBJETIVOS	
Geral	Investigar como a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE)
Específicos	1. Identificar as ações realizadas na promoção da proteção de dados pessoais no âmbito da Universidade Federal Rural de Pernambuco
	2. Identificar os desafios enfrentados pela UFRPE na implementação das práticas de proteção de dados pessoais
	3. Analisar o nível de maturidade da proteção de dados pessoais no âmbito da UFRPE com base no *framework* proposto por Santana e Mendonça (2023)
	4. Propor ações para fortalecer a proteção de dados pessoais no âmbito da organização

REFERENCIAL TEÓRICO	
Proteção de Dados no Setor Público	Doneda (2011), Cella; Copetti (2017), Flôres; Silva (2020), Carvalho (2023)
Lei Geral de Proteção de Dados Pessoais	Brasil (2018b), Finkelstein; Finkelstein (2019), Teffé; Viola (2020)
LGPD no Setor Público	Aguilera; Di Biase (2021), Philippi (2023), Santos Filho; Jesus (2023), Gomes, Cunha Filho e Luccas (2023)

METODOLOGIA			
Caracterização	Pesquisa aplicada, descritiva, mista, documental, de campo e estudo de caso		
Coleta de dados	Objetivo específico 1: pesquisa documental	Objetivo específico 2: entrevistas semiestruturadas	Objetivo específico 3: *framework* de proteção de dados
Análise de dados	Objetivo específico 1: análise documental	Objetivo específico 2: análise de conteúdo	Objetivo específico 3: análise com base na média aritmética

RESULTADOS
Desenvolver um produto técnico-tecnológico (PTT), com um diagnóstico da UFRPE no que tange à implementação da LGPD e proposição de ações para fortalecer a política de proteção de dados e de segurança da informação.

Fonte: Elaborado pelo autor (2025).

No próximo capítulo, serão apresentados os resultados e as discussões.

4 RESULTADOS E DISCUSSÕES

Neste capítulo, foram explorados os resultados obtidos no estudo, a partir da análise dos documentos institucionais que tratam sobre o tema, das entrevistas realizadas e do *framework* elaborado por Santana e Mendonça (2023). Os participantes foram denominados apenas como "entrevistado", seguido de um número "n" (1- ≤ n ≤ 3), a fim de preservar-lhes a identidade. Por questões didáticas, optou-se por estruturar este capítulo em quatro seções, em consonância com os objetivos específicos propostos na pesquisa.

4.1 AÇÕES REALIZADAS NA PROMOÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA UFRPE

Nesta seção serão apresentadas as ações desenvolvidas na UFRPE para a promoção da proteção de dados pessoais em consonância com a LGPD. Inicialmente, foram analisados os documentos institucionais que orientam a proteção de dados pessoais nessa Universidade.

Assim, em seu Plano de Desenvolvimento Institucional (PDI) 2021-2030, a UFRPE inseriu a proteção de dados na gestão das Tecnologias Digitais da Informação e Comunicação (TDIC). De acordo com o entendimento da instituição, as TDIC visam garantir "uma melhor qualidade de interação entre os indivíduos e ambientes, facilitando a comunicação e o armazenamento de dados e informações que irão apoiar as atividades acadêmicas e administrativas da organização" (UFRPE, 2021c, p. 286).

Nesse sentido, atribuiu-se à área de governança da Tecnologia da Informação a incumbência de planejar e executar políticas públicas, estratégias e soluções digitais, abrangendo todos os serviços prestados pela Universidade, levando-se em consideração a proteção de dados e a segurança da informação (UFRPE, 2021c). A fim, de concretizar essa missão, "a gestão institucional buscará fortalecer a governança da Tecnologia da Informação (UFRPE, 2021c, p. 291), o que corrobora a relação entre governança e gestão, tendo em vista que essa última consiste no instrumental daquela, possibilitando a concretização dos objetivos estabelecidos no plano estratégico da entidade.

Na UFRPE, além da LGPD, a proteção de dados coaduna-se com outros documentos do Governo Federal, que foram utilizados para subsidiar a elaboração do PDI, dentre eles: a Estratégia Brasileira para a Transformação Digital (E-Digital); a Política Nacional de

Segurança da Informação (PNSI); a Estratégia Nacional de Segurança Cibernética (E-Ciber); e a Estratégia de Governo Digital (EGD), conforme disposto no plano estratégico da instituição (UFRPE, 2021c).

A E-Digital foi instituída pelo Decreto nº 9.319, de 21 de março de 2018 (Brasil, 2018a). No ano de 2022, esse documento foi atualizado, apresentando um novo diagnóstico acerca dos desafios a serem enfrentados para a transformação digital no país, bem como as ações a serem implementadas no âmbito do Poder Executivo Federal no quadriênio 2022-2026. Um dos eixos norteadores é a confiança no ambiente digital, com aprimoramento dos mecanismos de proteção de dados pessoais. Para tal, foram propostas algumas ações, dentre elas (Brasil, 2022d, p. 38):

> a) Promover o fortalecimento da cultura de proteção de dados pessoais, por meio de ações estratégicas voltadas à prevenção e à detecção de infrações à LGPD, assim como as ações dirigidas à capacitação e à orientação dos agentes de tratamento e da sociedade quanto às normas de proteção de dados pessoais;
> b) Estabelecer mecanismos eficazes de monitoramento e de detecção de violações à LGPD;
> c) Instrumentalizar a Autoridade Nacional de Proteção de Dados com os meios adequados para que possa exercer as suas competências definidas pela LGPD, de modo a garantir estabilidade e segurança jurídica ao ambiente regulatório e fiscalizatório relacionado à proteção de dados;
> d) Fomentar campanhas educacionais amplas para expandir a conscientização da população sobre o tema da segurança da informação.

Por seu turno, a Política Nacional de Segurança da Informação (PNSI) foi instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018, no âmbito da Administração Pública Federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional (Brasil, 2018c). A política, além de elencar princípios, objetivos e instrumentos, criou o Comitê Gestor de Segurança da Informação (CGSI), constituído por membros indicados por Ministérios, pela AGU e pela ANPD, a quem compete assessorar a Chefia do Executivo nas atividades relacionadas à segurança da informação. A PNSI é de observância obrigatória por parte dos órgãos e entidades, que, dentre outras ações, deverão designar gestores internos, elaborar políticas de segurança da informação, instituir comitês e destinar recursos orçamentários para ações de segurança da informação (Brasil, 2018c).

Um dos instrumentos da PNSI é a Estratégia Nacional de Segurança da Informação, que contém as ações estratégicas propriamente ditas, em consonância com as políticas públicas e os programas do governo (Brasil, 2018c). Essa estratégia foi dividida em módulos, sendo um deles a E-Ciber, instituída por meio do Decreto nº 10.222, de 05 de fevereiro de 2020 (Brasil, 2020a). A finalidade é direcionar as ações na área de segurança cibernética, auxiliando as instituições

na prevenção de ações maliciosas no ciberespaço, o que fragiliza a proteção de dados pessoais e a privacidade (Brasil, 2020a).

Outro documento externo é a Estratégia de Governo Digital (EGD), aprovada pelo Decreto nº 10.332, de 28 de abril de 2020 (2020b). A EGD 2020-2022 foi utilizada para subsidiar a elaboração do atual PDI da UFRPE. Posteriormente, a EGD foi alterada, sendo ajustado seu período de vigência para o quadriênio 2020-2023, consoante o Decreto nº 11.260, de 22 de novembro de 2022 (Brasil, 2022e).

A EGD encontra-se estruturada em princípios, objetivos e iniciativas, cuja finalidade é nortear a transformação da gestão pública por meio das tecnologias digitais. De acordo com esse documento, a mudança visa promover a evolução das políticas e serviços públicos, a fim de maximizar a qualidade e atender às expectativas da sociedade, contribuindo para um governo mais confiável, que se caracteriza por um equilíbrio entre a inovação e a eficiência - proporcionadas pelas tecnologias digitais - com a proteção dos direitos e da privacidade dos cidadãos (Brasil, 2020b).

Dentre os objetivos da EGD, estabeleceu-se a implementação da LGPD no âmbito do Governo Federal, devendo ser criados métodos de adequação e conformidade dos órgãos com os requisitos da norma, bem como plataforma de gestão da privacidade e uso dos dados pessoais dos cidadãos (Brasil, 2020b). O marco temporal para efetivar essas iniciativas foi o ano de 2020 (Brasil, 2020b).

Atualmente, encontra-se vigente a Estratégia Federal de Governo Digital[7] para o período 2024-2027, instituída pelo Decreto nº 12.198, de 24 de setembro de 2024 (Brasil, 2024c). Esse Decreto criou também a Infraestrutura Nacional de Dados (IND), que "constitui um conjunto de normas, políticas, arquiteturas, padrões, ferramentas tecnológicas e ativos de informação, com vistas a promover o uso estratégico dos dados em posses dos órgãos e entidades do Poder Executivo Federal" (Brasil, 2024c, p. 1). Nesse sentido, foram definidas iniciativas para aperfeiçoar a governança de dados, dentre as quais (Brasil, 2024d):

> a) Alcançar uma economia de seis bilhões com a utilização do Programa Conecta GOV.BR, reduzindo as exigências de documentos do cidadão na utilização dos serviços públicos digitais, no âmbito da Infraestrutura Nacional de Dados - IND, até 2026;
> b) Impulsionar a integração das plataformas digitais de governo por meio da integração de, pelo menos, dois sistemas estruturantes ao Conecta GOV.BR, no âmbito da Infraestrutura Nacional de Dados - IND, até 2027;
> c) Estimular as decisões do Poder Executivo Federal baseadas em dados, por meio da elevação da média do índice de maturidade de dados, de dois para três pontos

[7] Esse documento revogou a Estratégia de Governo Digital (EGD) 2020-2023.

> em escala de cinco pontos, no âmbito da Infraestrutura Nacional de Dados - IND, até 2026;
> d) Aumentar a transparência e estimular o reuso de dados, disponibilizando dois mil conjuntos de dados catalogados na ferramenta central de metadados, no âmbito da Infraestrutura Nacional de Dados - IND até 2026 (Brasil, 2024d, p. 28).

O Programa Conecta GOV.BR é uma iniciativa que visa promover a troca automática e segura de informações entre os sistemas utilizados por órgãos e entidades do Poder Executivo Federal, a fim de que os cidadãos não necessitem reapresentar informações constantes na base de dados do Governo (Brasil, 2025). Essa integração é denominada "interoperabilidade", cujo objetivo é proporcionar economia ao erário e simplificar a prestação dos serviços, contribuindo para a eficiência pública (Brasil, 2025). Além disso, há um compromisso em estimular decisões estratégicas baseadas em dados, a partir do aumento do índice de maturidade, bem como em elevar a transparência e estimular a reutilização desses dados.

Uma das principais normativas que norteiam as ações do Conecta GOV.BR é o Decreto nº 10.046/2019, que instituiu o Cadastro Base do Cidadão (Brasil, 2019b). Esse Cadastro possui uma base integradora, que congrega o "número de inscrição no CPF, nome completo, nome social, data de nascimento, sexo, filiação, nacionalidade e naturalidade", por exemplo (Brasil, 2019b, p. 4). A essa base, poderão ser acrescidos outros dados provenientes de bases temáticas de determinadas políticas públicas, permitindo a "criação de meio unificado de identificação do cidadão para a prestação de serviços públicos" (Brasil, 2019b, p. 4).

Desse modo, percebe-se que essa iniciativa do Governo Federal converge com Aguilera e Di Biase (2021, p. 11), que advogam que os dados pessoais em posse do Poder Público "devem ser mantidos em formato interoperável e estruturado para o uso compartilhado". A despeito disso, os autores destacam que, de maneira geral, a infraestrutura dos órgãos e das entidades públicos é deficitária, o que pode comprometer a interoperabilidade desses dados (Aguilera; Di Biase, 2021).

Além do mais, ainda que o Cadastro Base do Cidadão vise aprimorar a gestão pública, é importante refletir sobre a possibilidade de que os dados pessoais, ao serem compartilhados por vários órgãos e entidades do Poder Executivo Federal, podem adquirir um novo propósito para além do que foram coletados inicialmente (Cella; Copetti, 2017). Carvalho (2023, p. 143) adverte também que não se pode olvidar do "excedente comportamental", ou seja, os dados pessoais têm capacidade de gerar valor para aqueles que os detêm, mesmo após serem utilizados para a finalidade inicialmente pretendida. Esses aspectos, pois, não podem ser negligenciados pelos operadores de tratamento de dados.

A fim de sintetizar os documentos externos que nortearam a elaboração do PDI da UFRPE, foi elaborado o Quadro 7, constante a seguir, no qual constam os respectivos elementos de análise.

Quadro 7 - Documentos externos analisados na pesquisa

Documento	Elementos
Estratégia Brasileira para a Transformação Digital (E-Digital)	Ações propostas pelo Governo Federal para aprimorar os mecanismos de proteção de dados
Política Nacional de Segurança da Informação (PNSI)	Diretrizes da administração pública federal no tocante à segurança da informação
Estratégia Nacional de Segurança Cibernética (E-Ciber)	Disposições do Poder Executivo Federal no âmbito da segurança cibernética
Estratégia de Governo Digital (EGD)	Princípios, objetivos e iniciativas propostas pelo Governo Federal para aperfeiçoar a gestão pública por meio das tecnologias digitais, sem desconsiderar a proteção de dados

Fonte: Elaborado pelo autor (2025).

Do ponto de vista interno, além do PDI, os documentos que respaldam a proteção de dados são: o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC); a Política de Segurança da Informação e Comunicação (POSIC); e o Plano de Dados Abertos (PDA).

O PDTIC visa auxiliar o direcionamento, o planejamento e o monitoramento das ações relativas à gestão das TDIC (UFRPE, 2023b). Conforme esse documento, após o levantamento das necessidades corporativas e do diagnóstico da capacidade da instituição, contemplando a força de trabalho, a organização deve planejar ações e definir metas, aprovando-as e divulgando-as à comunidade, a fim de assegurar o comprometimento dos responsáveis pela efetivação e o acompanhamento periódico dos resultados obtidos (UFRPE, 2023b).

Com base no PDTIC, foi criado o Programa "UFRPE Digital", cujo objetivo é promover uma transformação digital na Universidade a partir de eixos habilitadores, dentre os quais: a gestão assertiva baseada em dados; a transparência e o acesso à informação; e a segurança e a privacidade (UFRPE, 2023b). Esses eixos têm caráter transversal, devendo permear as áreas de atuação do ente (UFRPE, 2023b). O monitoramento e a manutenção desse Programa competem ao Comitê de Governança Digital (CGD), que deve direcionar as prioridades (UFRPE, 2023a).

O CGD é um órgão colegiado estratégico, de natureza deliberativa, composto por várias instâncias, dentre elas a Reitoria, a Vice-Reitoria, as Pró-Reitorias e a STD, com a participação do EPD da entidade (UFRPE, 2023a). Esse órgão possui atuação permanente, sendo realizadas reuniões trimestrais, com vistas a "coordenar e implementar políticas, diretrizes e normas que assegurem a adoção de boas práticas de governança digital e da segurança da informação e

comunicação" (UFRPE, 2023a, p. 2). As atas dessas reuniões são divulgadas no sítio virtual da STD, para que a comunidade acadêmica possa acompanhar as ações e as estratégias direcionadas à gestão das TDIC.

Por sua vez, o principal objetivo da Política de Segurança da Informação e Comunicação (POSIC) da Universidade é "formalizar o direcionamento estratégico institucional acerca da Segurança da Informação e Comunicação (UFRPE, 2022b, p. 5). Para tanto, devem ser definidas "normas relativas à implementação dos sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados", bem como devem ser criados e implementados "programas destinados à conscientização e à capacitação dos recursos humanos e da comunidade universitária" (UFRPE, 2022b, p. 5-6). A Política possui um escopo holístico, abrangendo qualquer indivíduo, agente público ou não, que desempenha alguma atividade vinculada à instituição (UFRPE, 2022b).

Dentre os princípios que fundamentam a POSIC, podem-se citar: obrigatoriedade de tratar as informações produzidas ou recebidas como patrimônio da instituição, salvo em casos excepcionais; utilização dos recursos de comunicação e computacionais apenas para realização dos objetivos finais; responsabilidade de cada usuário pela segurança dos ativos de informação que estão sob sua custódia; e criação de planos de contingência para os principais serviços e sistemas institucionais (UFRPE, 2022b).

A POSIC da UFRPE previu a realização de atividades de auditoria, a partir do trabalho de equipes responsáveis por fiscalizar e por avaliar a segurança das TDIC (UFRPE, 2022b). Ademais, definiu o papel dos setores de gestão de pessoas e de registro/controle acadêmico. Ambos deverão disponibilizar um Termo de Compromisso, a fim de que os servidores e discentes, respectivamente, assumam o compromisso de tratar o dado e a informação como um patrimônio da instituição e, como tal, devem ter seu sigilo preservado, caso necessário (UFRPE, 2022b). A Política possui diretrizes para nortear a realização de "ações contínuas de conscientização", com o objetivo de consolidar uma "cultura organizacional consciente em Segurança da Informação e Comunicação" (UFRPE, 2022b, p. 13).

Compete ao Gestor de Segurança da Informação assessorar a alta administração na implementação da POSIC (UFRPE, 2022b). Além do mais, esse gestor deverá coordenar o Subcomitê de Segurança da Informação e Comunicação (SSIC), que atua no escopo tático, bem como estimular ações de capacitação em temas relacionados à segurança da informação, promover a divulgação das normas internas e acompanhar o trabalho da Equipe de Tratamento

da Respostas e Incidentes Cibernéticos (ETIR), que constitui o nível operacional da estrutura de segurança da informação (UFRPE, 2022c).

Em linhas gerais, o trabalho dessa Equipe "consiste em identificar, filtrar, classificar, responder e registrar os alertas e as notificações dos incidentes de segurança, procurando obter informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências" (UFRPE, 2022c, p. 5). Em consonância com a POSIC e com os processos de gestão de riscos de segurança da informação, a ETIR deverá:

> a) monitorar, receber e registrar eventos, elaborar relatórios de incidentes de segurança e alertas;
> b) categorizar e priorizar incidentes de segurança;
> c) analisar os impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos;
> d) oferecer resposta eficiente, adequada e proporcional aos incidentes cibernéticos que apresentem risco à integridade, disponibilidade ou confidencialidade das informações hospedadas nos sistemas ou redes de computadores da UFRPE;
> e) apoiar a manutenção da segurança de todo o ambiente computacional;
> f) atender os usuários dos serviços de tecnologia fornecidos pela UFRPE que comunicarem eventos que possam ser relacionados a incidentes de segurança cibernética;
> g) participar de reuniões semanais; e
> h) implementar e desempenhar os serviços de: tratamento de incidentes de segurança cibernética; tratamento de vulnerabilidades técnicas no ambiente computacional; e coleta e preservação de evidências digitais em acidentes cibernéticos penalmente relevantes (UFRPE, 2022c, p. 7-8).

Nesse sentido, é evidente a amplitude do trabalho desenvolvido pela ETIR, atuando de maneira preventiva e reativa em todo o processo de gerenciamento de incidentes, isto é, desde o planejamento até a execução de ações, estabelecendo uma comunicação com os usuários das TDIC, que são atores-chave para reduzir ou, até mesmo, evitar investidas maliciosas no âmbito da instituição.

Por seu turno, o Plano de Dados Abertos (PDA) visa orientar as ações de implementação e promoção da abertura de dados da instituição, com vistas a facilitar a publicação, o acesso, a compreensão e a reutilização desses dados, contemplando não apenas os usuários internos, mas também os cidadãos que tenham interesse em obtê-los (UFRPE, 2022a). Assim, foram definidas diretrizes que devem ser consideradas no processo de abertura, priorizando, dentre outros, a divulgação de dados (UFRPE, 2022a):

- Relacionados às demandas encaminhadas por meio do sistema utilizado pelo Serviço de Informação ao Cidadão (e-SIC), ou seja, transparência passiva;
- Decorrentes de obrigatoriedade legal ou compromisso assumido pela entidade;
- Com maior relevância para o cidadão, de acordo com consultas públicas;

- Relativos a um sistema estruturante ou utilizado por vários órgãos;
- Com capacidade de fomentar o desenvolvimento sustentável e novos negócios na sociedade.

Segundo o PDA, foi firmado um compromisso da entidade em assegurar a prestação de informações à sociedade, com valorização da transparência e com estímulo à participação e ao controle social, tendo suporte do Comitê de Transparência e Dados Abertos (CTDA) do próprio ente (UFRPE, 2022a).

Além desses documentos, especificamente no âmbito da proteção de dados pessoais, há duas resoluções: a Resolução nº 31/2020 e a Resolução nº 103/2021, aprovadas pelo Conselho Universitário (CONSU) da entidade. A primeira trata da restrição à divulgação de documentos que contenham dados pessoais de pessoa natural no âmbito da UFRPE. A título exemplificativo, é dado pessoal: "número de telefone de contato pessoal; endereço residencial; endereço de correio eletrônico pessoal; data de nascimento; RG; CPF; título de eleitor; estado civil" (UFRPE, 2020. p. 2).

A aprovação da Resolução nº 31/2020 constitui-se como um marco legal na proteção de dados pessoais. No ano de 2020, foi implementado o Sistema Integrado de Administração, Patrimônio e Contratos (SIPAC), ferramenta que instituiu o processo eletrônico, razão pela qual foi necessária a definição de diretrizes internas para nortear a atuação dos usuários, tais como:

> Art. 3º - Quando da criação ou inserção de documentos no SIPAC, os servidores da UFRPE devem observar a presença de informações que contenham dado pessoal ou dado pessoal sensível, selecionando as opções de restrição de acesso às peças documentais que contenham tais características, restringindo o seu acesso às unidades administrativas ou servidores que necessitem de tais dados, para o desempenho de suas atividades funcionais.
> Art. 4º - Na elaboração de modelos de documentos a serem cadastrados no SIPAC, somente devem neles constar solicitação de dado e dado pessoal sensível indispensável para o andamento do processo e, somente, se tal dado não puder ser obtido em bancos de dados de sistemas de livre acesso da UFRPE.
> Art. 5º Além dos documentos referenciados no art. 3º, devem ser selecionadas as opções de restrição de acesso às peças documentais que tenham seu caráter reservado, conforme legislação específica [...] (UFRPE, 2020, p. 2).

Em contrapartida, a Resolução nº 103/2021 instituiu o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) e a Política de Privacidade e Proteção de Dados Pessoais (PPPDP) no âmbito da organização. O CGPPD atua em caráter permanente, sendo constituído por representantes de vários setores da instituição e pelo EPD, que o preside (UFRPE, 2021c). O colegiado exerce um papel consultivo e deliberativo, atuando na implementação de programa de privacidade; na avaliação dos procedimentos de tratamento e proteção de dados, incluindo

propostas de melhoria com base na LGPD; e na proposição de normativas para regulamentar a privacidade e a proteção de dados pessoais (UFRPE, 2021c).

Uma dessas normativas é a PPPDP, que, em caráter complementar à POSIC, estabeleceu regras direcionadas ao tratamento de dados pessoais, definindo processos e responsabilidades (UFRPE, 2021c). De acordo com a PPPDP, a UFRPE é a controladora, tomando decisões relativas a esse tratamento, ao passo que o operador é "qualquer pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (UFRPE, 2021c, p. 9).

Em relação ao registro de tratamento de dados pessoais - sensíveis ou não - a PPPDP estabeleceu que a organização disponibilizasse, no mínimo, em seu sítio eletrônico: "finalidade do tratamento; base legal; descrição dos titulares; categorias de destinatários; transferência internacional[8]; e início e término do tratamento e prazo de conservação" (UFRPE, 2021c, p. 10).

Nos termos da PPPDP, a proteção de dados pessoais deverá ser concebida de maneira ampla, ou seja, "*privacy by design*", que, em tradução literal, significa "privacidade desde o *design*". Assim, deve ser "pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais" (UFRPE, 2021c, p. 13). Outrossim, "os bancos de dados [...] não podem estar disponíveis para acesso direto pela internet, devendo estar em rede segregada da rede exposta à internet e protegida por *software* ou *hardware* especializado em segurança de rede", sendo "vedado o armazenamento de dados pessoais fora dos repositórios oficiais" (UFRPE, 2021c, p. 13).

Em linhas gerais, constatou-se a complexidade da gestão das TDIC na instituição com vários documentos que devem nortear as ações estratégicas na área de governança, privacidade, proteção de dados e segurança da informação. Dessa forma, observa-se que a universidade tem buscado definir as formas de atuação em seu ambiente digital, inserindo-as em instrumentos de planejamento de órgãos e de entidades, almejando consolidar uma maturidade na utilização da tecnologia, o que perpassa a atenção com a proteção de dados pessoais, a privacidade e a segurança da informação.

Nesse contexto, de acordo com o PDI da Universidade, foram estabelecidos 14 objetivos relativos à gestão das TDIC na UFRPE, a saber:

1) Adequar os serviços da UFRPE à LGPD (Lei nº 13.709/2018);

[8] Consiste na "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". (Brasil, 2018b, p. 60). Ao mencionar o termo país, a LGPD se refere ao Brasil.

2) Conscientizar e capacitar usuário(s) da UFRPE em segurança da informação e comunicação;
3) Melhorar a segurança dos dados e serviços digitais ofertados na Universidade;
4) Aprimorar a segurança da informação;
5) Adequar a instituição às normas de dados abertos definidas pelas EGD e LGPD;
6) Avaliar e adotar sistemas de informação de acordo com diretrizes estabelecidas pelo governo digital;
7) Ampliar o quantitativo de processos de negócio transformados digitalmente;
8) Adequar infraestrutura para garantia de uso das soluções digitais;
9) Adequar infraestrutura para garantia de continuidade de uso das soluções digitais;
10) Gerir os ativos de TIC;
11) Estabelecer um programa único de *campus* inteligente como projeto de desenvolvimento institucional;
12) Implantar um sistema computacional único de gestão de serviços;
13) Aumentar o nível de maturidade de governança de TI aplicada na UFRPE;
14) Implementar e formalizar plano orçamentário de TI anual. (UFRPE, 2021c, p. 287-293).

Com base nesses objetivos, pode-se visualizar a complexidade da gestão das TDIC na instituição, contemplando ações nas áreas de proteção de dados, segurança da informação, governança, processos de negócio e infraestrutura de TI. Dada essa amplitude e tendo em vista o escopo deste estudo, optou-se por aprofundar a análise dos objetivos nº 1 ao nº 4, incluindo as respectivas metas, conforme ilustra o Quadro 8.

Quadro 8 - Objetivos relativos à gestão das TDIC na UFRPE

(continua)

Nº	Objetivo	Unidade responsável	Meta 2022	Meta 2023	Meta 2024	Meta 2025
1	Adequar os serviços da UFRPE à LGPD	Comitê Gestor de Privacidade e Proteção de Dados	------	50% dos serviços em conformidade	75% dos serviços em conformidade	100% dos serviços em conformidade
2	Conscientizar e capacitar usuário(s) da UFRPE em segurança da informação e comunicação	Subcomitê de Segurança da Informação e Comunicação	Realizar 05 treinamentos sobre segurança	Realizar 02 treinamentos sobre segurança	Realizar 02 treinamentos sobre segurança	Realizar 02 treinamentos sobre segurança
			Realizar treinamentos com alcance de, no mínimo, 30% dos servidores	Realizar treinamentos com alcance de, no mínimo, 50% dos servidores	Realizar treinamentos com alcance de, no mínimo, 70% dos servidores	Realizar treinamentos com alcance de, no mínimo, 90% dos servidores
3	Melhorar a segurança dos dados e serviços digitais ofertados na Universidade	Subcomitê de Segurança da Informação e Comunicação	Analisar os riscos de, pelo menos, 20% dos sistemas	Analisar os riscos de, pelo menos, 40% dos sistemas	Analisar os riscos de, pelo menos, 50% dos sistemas	Atingir o nível 3 de maturidade
						Analisar os riscos de, pelo menos, 60% dos sistemas
				Monitorar 20% dos riscos de	Monitorar 30% dos riscos de	Monitorar 50% dos riscos de

Nº	Objetivo	Unidade responsável	Meta 2022	Meta 2023	Meta 2024	Meta 2025
				segurança cibernética	segurança cibernética	segurança cibernética
						Reduzir em 10% os incidentes de segurança cibernética
4	Aprimorar a segurança da informação	Subcomitê de Segurança da Informação e Comunicação	Formalizar e executar 02 iniciativas de segurança da informação	Formalizar e executar 02 iniciativas de segurança da informação	Formalizar e executar 02 iniciativas de segurança da informação	Formalizar e executar 02 iniciativas de segurança da informação

Fonte: Elaborado pelo autor com base em UFRPE (2021c) e UFRPE (2023b).

No que tange ao primeiro objetivo, constatou-se que não foi definida meta para o ano de 2022. Acredita-se que tal ausência esteja relacionada à complexidade para atingir esse objetivo, o que converge com pesquisas já realizadas, que evidenciaram que as organizações carecem de um maior amadurecimento em relação à implementação da LGPD (Almeida; Soares, 2022). Desse modo, seria difícil estimar uma meta factível para um intervalo curto, uma vez que o PDI passou a viger no ano de 2021. Frise-se que a instituição vislumbra adequar todos os serviços à norma até o final de 2025.

O segundo objetivo envolve a conscientização e a oferta de treinamentos aos servidores da UFRPE na área de segurança da informação e comunicação. Nesse caso, ficou perceptível a preocupação da entidade em, inicialmente, ofertar um quantitativo maior de treinamentos, a fim de despertar o interesse dos usuários em relação ao tema e, à medida que esse processo de sensibilização avançar, ampliar o percentual mínimo de servidores capacitados. Essa estratégia, novamente, conduziu à reflexão de que a instituição tem noção da complexidade de adequação à LGPD, que perpassa, dentre outros aspectos, a disponibilização de treinamento (Almeida; Soares, 2022).

Por sua vez, o terceiro objetivo correlaciona-se à melhoria da segurança dos dados e dos serviços digitais ofertados na entidade. Neste caso, firmou-se a importância de gerenciar riscos que, nos termos da política institucional, consiste na "possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos" (UFRPE, 2019, p. 9). Assim como ocorrera no objetivo nº 2, foram estabelecidas metas mais robustas, que contemplam o monitoramento e a redução de incidentes de segurança cibernética, cujo gerenciamento é realizado pelo SSIC.

O último objetivo consistiu no aprimoramento da segurança da informação, com metas estabelecidas para o período 2022-2025. Nessa linha, Magacho e Trento (2021) reforçam a importância de que sejam realizados investimentos em políticas de segurança em organizações públicas.

A fim de monitorar o planejamento estratégico, a Pró-Reitoria de Planejamento e Gestão Estratégica (PROPLAN) tem coletado, semestralmente, dados junto aos setores, divulgando-os por meio de um painel criado no *Microsoft Power BI* (UFRPE, 2025a). O Quadro 9 apresenta o *status* das metas referentes ao triênio 2022-2024.

Quadro 9 - Alcance das metas relativas à gestão das TDIC na UFRPE

Nº	Ano	Meta	Status
1	2022	------	------
	2023	50% dos serviços em conformidade com a LGPD	Não atingida
	2024	75% dos serviços em conformidade com a LGPD	Parcialmente atingida
2	2022	Realizar 05 treinamentos sobre segurança	Atingida
		Realizar treinamentos com alcance de, no mínimo, 30% dos servidores	Não atingida
	2023	Realizar 02 treinamentos sobre segurança	Atingida
		Realizar treinamentos com alcance de, no mínimo, 50% dos servidores	Parcialmente atingida
	2024	Realizar 02 treinamentos sobre segurança	Atingida
		Realizar treinamentos com alcance de, no mínimo, 70% dos servidores	Parcialmente atingida
3	2022	Analisar os riscos de, pelo menos, 20% dos sistemas	Não atingida
	2023	Analisar os riscos de, pelo menos, 40% dos sistemas	Não atingida
		Monitorar 20% dos riscos de segurança cibernética	Não atingida
	2024	Analisar os riscos de, pelo menos, 50% dos sistemas	Não atingida
		Monitorar 30% dos riscos de segurança cibernética	Não atingida
4	2022	Formalizar e executar 02 iniciativas de segurança da informação	Superada
	2023	Formalizar e executar 02 iniciativas de segurança da informação	Superada
	2024	Formalizar e executar 02 iniciativas de segurança da informação	Não atingida

Fonte: Dados da pesquisa (2025), com base em UFRPE (2025a).

Com base no Quadro 9, constatou-se que, no que tange à gestão das TDIC, cinco metas foram alcançadas, das quais duas delas superaram o quantitativo estabelecido; três metas foram parcialmente atingidas; e oito metas não foram alcançadas pela UFRPE. Nesse contexto, a partir da análise das metas do Quadro 9, foi possível identificar as ações que vêm sendo realizadas para promover a proteção de dados na entidade.

O Quadro 10, constante a seguir, caracteriza essas ações institucionais, organizadas em três categorias definidas no Painel de Monitoramento do PDI (UFRPE, 2025a), a saber: normatização interna e estruturação organizacional; sensibilização; e treinamento. O critério adotado para definir essas categorias foi o tema atrelado a cada ação, buscando identificar a correlação com os objetivos estratégicos de nº 1 ao nº 4, listados no Quadro 8.

Quadro 10 - Ações de proteção de dados no âmbito da UFRPE

Categoria	Ações realizadas	Objetivo estratégico
Normatização interna e estruturação organizacional	Criação do Subcomitê de Segurança da Informação e Comunicação (SSIC) no ano de 2022	Adequar os serviços da UFRPE à LGPD Aprimorar a segurança da informação
	Atualização da Política de Segurança da Informação e Comunicação (POSIC) no ano de 2022	
	Criação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no ano de 2022, com participação de servidores indicados pelas Unidades Acadêmicas, para descentralizar as ações de Segurança da Informação e Comunicação (SIC)	
	Adesão à Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), instituída pelo Decreto nº 10.748, de 16 de julho de 2021	
	Atualização do Plano de Contingência de Tecnologia da Informação e Comunicação (PCTIC)	
Sensibilização	Disponibilização de área específica sobre SIC no portal UFRPE Digital, com orientações à comunidade acadêmica para garantir a confidencialidade, integridade e disponibilidade de dados	Conscientizar e capacitar usuário(s) da UFRPE em segurança da informação e comunicação
	Lançamento do programa "Previna-se!" no ano de 2023, com disponibilização de cursos, cartilhas e vídeos relevantes sobre SIC no portal UFRPE Digital e nas mídias sociais	
Treinamento	Participação de servidores que atuam na área de SIC nos seguintes cursos promovidos pela Rede Nacional de Ensino e Pesquisa (RNP): ● Gestão da Segurança da Informação e Privacidade; ● Gestão de Riscos de Segurança da Informação e Privacidade; ● Infraestrutura e Segurança com *Firewalls* Fortinet; ● Tratamento de Incidentes de Segurança; ● Teste de Invasão de Aplicações Web; ● PenTest.	Conscientizar e capacitar usuário(s) da UFRPE em segurança da informação e comunicação
	Participação de servidores que atuam na área de SIC nos seguintes cursos: ● LGPD na Prática e *Oficial* EXIN PDPF – *Privacy & Data Protection Foudation*; ● *Oficial* EXIN ISFS – *Information Security Foundation* ISO/IEC 27001; ● *Oficial* EXIN PDPE – *Privacy & Data Protection Essentials*; ● Administração de *Firewalls* FortiGate Avançado; ● Cibersegurança EAD (parceria oficial Ascend).	

Fonte: Dados da pesquisa (2025), com base em UFRPE (2025a).

No tocante à normatização interna e à estrutura organizacional, ficou evidente que têm sido efetivadas ações importantes para adequar os serviços da UFRPE à LGPD e aprimorar a segurança da informação, dentre as quais a instituição de comitês e elaboração de políticas, conforme definido na PNSI (Brasil, 2018c). A adesão à Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) foi um avanço importante para subsidiar o fortalecimento da proteção de dados em nível nacional. Essa Rede, formalizada pelo Decreto nº 10.748, de 16 de julho de 2021, tornou obrigatória a participação de órgãos e entidades da administração federal direta, autárquica e fundacional nessa iniciativa, com vistas a "aprimorar e manter a coordenação [...] para prevenção, tratamento e resposta a incidentes [...], de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação" (Brasil, 2021b, p. 2).

Outra ação consistiu na atualização do Plano de Contingência de Tecnologia da Informação e Comunicação (PCTIC). A proposta é "fornecer diretrizes e procedimentos para lidar com possíveis incidentes e interrupções nos serviços", apresentando "medidas, estratégias de resposta e planos de recuperação para manter a estabilidade operacional, minimizando o impacto negativo à comunidade" (UFRPE, 2023c, p. 4). Assim, os usuários internos e externos, ao constatarem um possível ataque cibernético que possa comprometer o desempenho, os dados ou a configuração dos serviços prestados na Universidade, deverão notificar a ETIR, por meio de serviço *web*, telefone ou *e-mail*, divulgados pela equipe de TIC (UFRPE, 2023c; UFRPE, 2022c).

Quanto à sensibilização, a pesquisa evidenciou que a instituição criou uma área no Portal UFRPE Digital[9], dividido em sete abas, dentre elas a que trata sobre a estruturação da área de tecnologia, que abrange a governança e a transformação digitais, bem como a segurança da informação e comunicação[10] (UFRPE, 2025b). Quanto a esta última, a pesquisa revelou que a instituição lançou, no ano de 2023, o Programa "Previna-se!", cujo logotipo encontra-se retratado na Figura 1.

Figura 1 - Logotipo do Programa Previna-se!



Fonte: Dados da pesquisa (2025), disponibilizado em UFRPE (2025b).

[9] https://digital.ufrpe.br/
[10] https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/

O objetivo do “Previna-se!” é promover conhecimento e desenvolver uma cultura em segurança, que perpassa a aplicação de boas práticas na manipulação de informações institucionais, convergindo com o objetivo estratégico relativo à conscientização dos usuários da instituição (UFRPE, 2025b). Para tanto, o Programa contempla a indicação de fontes de informação, a realização de campanhas de conscientização e a oferta de treinamentos sobre proteção de dados pessoais no setor público, segurança da informação e uso responsável das TICs (UFRPE, 2025b).

Uma dessas fontes consiste nos vídeos disponibilizados pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br)[11], instituído para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil (CGI.br). Compete a esse Comitê coordenar e integrar as iniciativas e os serviços da internet no país. Os vídeos são curtos e, por meio de uma linguagem acessível, buscam orientar os usuários em diversos temas, dentre os quais a criação de senhas seguras, o armazenamento de dados apenas em equipamentos de uso individual e a desconfiança com *links* suspeitos (UFRPE, 2025b), conforme ilustra a Figura 2.

Figura 2 - Layout de vídeos sobre segurança da informação



Fonte: Dados da pesquisa (2025), com base em UFRPE (2025b).

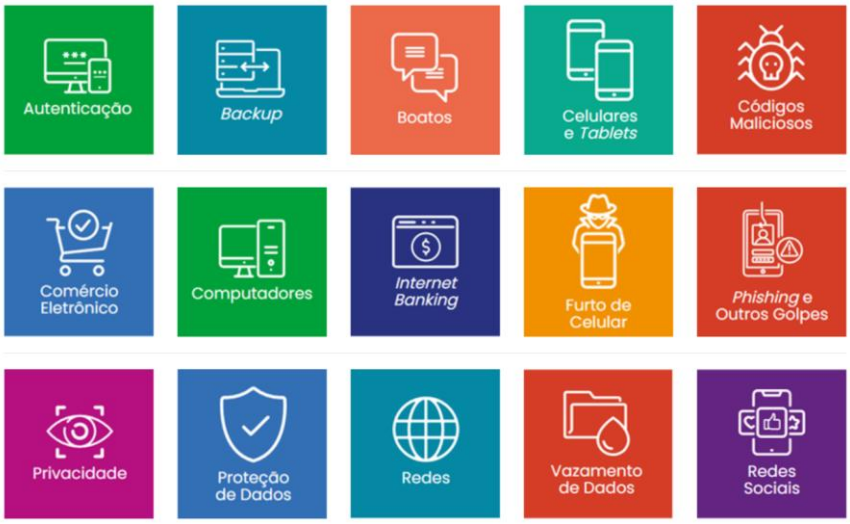
Outra fonte é a Cartilha de Segurança para Internet[12], produzida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br), disponível no *site* UFRPE Digital. A cartilha é composta por fascículos, com recomendações e dicas para aumentar a segurança dos usuários na internet, protegendo-os de eventuais ameaças. Assim, são

[11] https://nic.br/quem-somos/

[12] Essa cartilha poderá ser consultada no site do CERT.br, cujo link encontra-se disponibilizado no UFRPE Digital (2025b): https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/

explorados diversos temas, que englobam, por exemplo: a proteção e o vazamento de dados; a privacidade; e os golpes a que os usuários estão vulneráveis. A Figura 3 ilustra esse recurso de informação.

Figura 3 - Fascículos da Cartilha de Segurança para Internet



Fonte: Dados da pesquisa (2025), com base em UFRPE (2025b).

Além dessas fontes informacionais, a UFRPE dispõe também de uma cartilha, publicada no ano de 2021, que apresenta alguns conceitos da LGPD, os princípios de tratamento de dados e as sanções administrativas previstas para os órgãos e as entidades (UFRPE, 2021a).

Por fim, este estudo revelou que têm sido disponibilizados treinamentos voltados à equipe da STD que atua na área de segurança da informação e comunicação, o que é positivo, dada a importância de que sejam constituídas equipes técnicas nas organizações para assegurar a proteção de dados pessoais (Barbosa *et al.*, 2021). Entretanto, os dados divulgados pela PROPLAN não contemplam as capacitações realizadas pelos demais servidores da entidade. Um dos motivos que pode justificar essa ausência é que os cursos divulgados ao público em geral, por meio do "Previna-se!", são promovidos por instituições externas, sem um controle por parte da Universidade, diferentemente dos oferecidos aos profissionais de TI, cujo custeio é realizado pela própria instituição.

Outrossim, segundo o painel de monitoramento do PDI, "o direcionamento institucional é estruturar [...] a segurança da TIC e capacitar equipes diretamente responsáveis pela segurança dos serviços digitais" (UFRPE, 2025, p. 1), o que pode conduzir à reflexão de que, embora seja fundamental que a organização qualifique seu corpo técnico especializado, é necessário ampliar

esse horizonte, haja vista a relevância em sensibilizar todos os usuários sobre proteção de dados e segurança da informação.

Nesse contexto, este estudo evidenciou que têm sido efetivadas ações para promover a proteção de dados pessoais na UFRPE, indo ao encontro dos documentos elaborados pela entidade e pelo Governo Federal. No entanto, em que pesem os esforços e os avanços, há metas estratégicas relacionadas à gestão das TDIC ainda não alcançadas, o que é um indicativo de que há desafios a serem superados, cuja discussão será realizada na próxima seção.

4.2 DESAFIOS PARA IMPLEMENTAR PRÁTICAS DE PROTEÇÃO DE DADOS NA UFRPE

Considerando que a proteção de dados está inserida no escopo da gestão das TDIC, antes de explorar os desafios enunciados pelos entrevistados, optou-se por analisar o diagnóstico da TIC na UFRPE. Para tanto, recorreu-se à análise SWOT[13], que consiste numa "ferramenta utilizada para realizar análise de ambientes, fornecendo uma base para a gestão organizacional e a compreensão de cenários para planejamento" (UFRPE, 2023b). O Quadro 11 ilustra a etapa.

Quadro 11 - Matriz SWOT

	Forças	**Fraquezas**
Fatores Internos	- Prioridade da alta gestão para o avanço da tecnologia digital; - TIC entendida como estratégica; - Receptividade e interesse por soluções digitais; - Comitê de Governança Digital (CGD) com participação ativa da alta gestão.	- Competências limitadas em gestão e áreas específicas de TIC; - Equipe reduzida; - Compartilhamento precário de boas práticas de TIC; - Infraestrutura computacional insuficiente.
	Oportunidades	**Ameaças**
Fatores Externos	- Estratégia de Governo Digital (EGD); - Momento favorável para a transformação digital; - Colaboração com outras IFES; - Possibilidade de integração com órgãos governamentais de TIC.	- Perda de profissionais para o mercado e outros órgãos; - Limitações orçamentárias; - Rigidez em processos, estruturas e legislações; - Gastos para infraestrutura tecnológica inflacionados.

Fonte: Dados da pesquisa, com base em UFRPE (2023b).

A análise SWOT apresentada revela um cenário que, apesar de contar com importantes forças estruturais e estratégicas, evidencia que a instituição enfrenta desafios significativos, sobretudo relacionados à capacidade operacional e à sustentabilidade tecnológica. Ao analisar

[13] SWOT é um acrônimo na Língua Inglesa para: *Strengths, Weakness, Opportunities, Threats*. Em tradução para a Língua Portuguesa, significa: Forças, Fraquezas, Oportunidades e Ameaças.

os fatores internos, visualiza-se que a Universidade elencou como forças: a prioridade da alta gestão para o avanço da tecnologia digital; a concepção estratégica da TIC; a receptividade e o interesse por soluções digitais; e a participação de gestores do alto escalão no Comitê de Governança Digital. A criação do CGD, que, consoante já explorado, é o comitê responsável por gerenciar o programa que visa promover uma transformação digital na UFRPE, com a participação da Reitoria e das Pró-Reitorias, é um reflexo dessa postura (UFRPE, 2023a).

Essa percepção institucional converge com as normativas do Governo Federal debatidas na seção 4.1, que têm buscado estabelecer diretrizes para auxiliar os órgãos e as entidades a institucionalizarem suas políticas de gestão de TDIC e, por conseguinte, implementar ações voltadas à proteção de dados, à privacidade e à segurança.

A despeito dessas potencialidades, a entidade entende que há elementos internos que podem comprometer a execução dessas ações, dentre as quais: a limitação de competências em gestão e áreas específicas de TIC; o quantitativo reduzido de pessoal; a precariedade na difusão de boas práticas de TIC; a infraestrutura computacional insuficiente; e a baixa capacidade para aquisição de TIC (UFRPE, 2023b). Na prática, essas fraquezas podem maximizar os desafios para assegurar a conformidade no tratamento de dados, tendo em vista que, de acordo com Santos Filho e Jesus (2023), as instituições de ensino têm um trabalho relativamente complexo, dado o volume considerável de dados que são tratados por elas.

Do ponto de vista externo, a percepção da entidade é de que há oportunidades que podem ser exploradas para aprimorar a gestão das TDIC, num contexto caracterizado pela formalização da Estratégia de Governo Digital e pela necessidade de promover uma transformação na gestão pública com o auxílio das tecnologias digitais. Além do mais, há uma tendência em fortalecer a integração entre os órgãos e as entidades do Poder Executivo Federal no âmbito da TIC, como é o caso da REGIC, que, conforme já discutido, consiste num avanço importante para subsidiar o fortalecimento da proteção de dados a nível nacional.

Quanto às ameaças, a entidade compreende que a perda de servidores para o mercado e para outros órgãos públicos; as limitações orçamentárias; a rigidez em processos, estruturas e legislações; e a inflação dos gastos com infraestrutura tecnológica podem comprometer a gestão das TDIC. Esses fatores externos podem agravar alguns desafios enfrentados pelas instituições públicas de ensino durante a implementação da LGPD, dentre os quais a necessidade de aportes financeiros e de capacitação profissional e técnica (Barbosa *et al.*, 2021).

Tais obstáculos restringem a capacidade de execução de projetos tempestivamente e expõem a organização a uma série de riscos (UFRPE, 2023b, p. 23), quais sejam:

- Limitação na possibilidade de automatização de processos internos;
- Perda do conhecimento técnico, por vezes irrecuperável, sobre os sistemas existentes, devido à saída de servidores por pedido de vacância por posse inacumulável;
- Sobrecarga de chefias na área de TI, trazendo-lhes, ainda, óbices em exercer mais eficazmente as funções de planejamento, direção, coordenação e avaliação dos respectivos trabalhos, assim como exercer a liderança administrativa eficaz e eficiente perante suas equipes. Isso compromete não somente a gestão, mas, também, a governança de TI;
- Impossibilidade de lançamento de novos serviços públicos digitais disponíveis ao cidadão devido à escassez de pessoal.

Com base nesse diagnóstico, realizado pela própria instituição, foi possível analisar os desafios elencados pelos atores-chave da organização para subsidiar a implementação da LGPD na UFRPE. Para sistematizar esses desafios, foram criadas quatro categorias, escolhidas em razão da recorrência de citações, pela pertinência com o tema e pela relação com o objetivo da pesquisa. O Quadro 12, constante a seguir, contém as categorias temáticas e as respectivas definições.

Quadro 12 - Categorias da análise temática ou categorial

Categoria	Definição
Orçamento	Inclui as unidades de registro que identificaram a necessidade de investimento e a restrição de recursos financeiros/orçamentários como desafios enfrentados durante a implementação de práticas de conformidade com a proteção de dados
Recursos Humanos	Agrupa as unidades de registro que apontaram a restrição de pessoal, a sobrecarga de trabalho e a falta de interesse no setor público como desafios para a implementação de medidas de conformidade com a proteção de dados pessoais
Legislação	Agrupa as unidades de registro em que os entrevistados apontaram o conflito aparente entre normas, a ausência de uniformização, a dificuldade de interpretação e o caráter incipiente da legislação como desafios para a implementação eficaz de práticas de proteção de dados
Universidade	Contém as unidades de registro que apontaram a visão limitada da instituição, a necessidade de educar os titulares e os operadores de dados, a complexidade universitária e o engajamento da comunidade acadêmica como desafios a serem superados

Fonte: Elaborado pelo autor (2025).

As categorias com maior frequência de ocorrência foram Recursos Humanos, com 35 menções (33,33%), seguida de Universidade, com 34 citações (32,38%). Em terceiro lugar, a categoria Legislação foi mencionada em 21 unidades de contexto (20,00%), e, por fim, a categoria Orçamento apresentou 15 menções (14,29%). Ao lado de cada uma das unidades de

contexto, foi incluído o entrevistado que realizou a ponderação, utilização a letra “E” seguida de um número “n” (1≤n≤3), a fim de preservar a identidade de cada um deles.

No tocante à categoria “Recursos Humanos”, as entrevistas revelaram o predomínio da sobrecarga de trabalho (57,14%) como desafio para implementar práticas de proteção de dados pessoais na organização. Consoante o Quadro 13, além desse fator, os participantes apontaram também a restrição de pessoal (37,14%) e a falta de interesse no setor público (5,71%).

Quadro 13 - Análise da categoria Recursos Humanos

(continua)

Nº de citação e frequência (%)	**Unidade de registro**	**Unidade de contexto**
35 (33,33%)	Restrição de pessoal 13 (37,14%)	Foi aprovado o plano de dados abertos e junto com a aprovação desse plano foi divulgado o portal de dados abertos da UFRPE, mas, assim, muito incipiente, tem poucos dados lá, até porque por falta de alguém que realmente assumisse esse trabalho [...] E1
		É, recursos humanos e financeiros, né? Infelizmente os dois estão difíceis hoje, né? E1
		E as pessoas... a própria instituição [...] eu acho que isso é uma realidade da... de vários órgãos da Administração Pública Federal, têm uma dificuldade muito grande de pessoas [...]. Então, você atender à legislação, [...] ao mesmo tempo que você tem uma restrição de pessoas [...] E2
		Então, eu acho que esse é o principal fator que vem influenciando nessa dificuldade de engajamento, restrição de pessoal, de recursos [...] E2
		Então, eu diria que há um conjunto, tanto... o investimento, o engajamento [...] como também você ter mais pessoas pra atuar nessas questões operacionais [...] E2
		Já estou com formulários em mãos para propor um curso da LGPD. [...] O desafio é tornar isso sistemático, que esbarra também nessa restrição. [...] De pessoal, porque você tem poucas pessoas com expertise na área para ofertar esse curso. E2
		Eu mencionaria também a realização de eventos, que é algo que como eu já mencionei está limitado em relação à carência que a gente tem de pessoas [...] E2
		Eu acho que a principal seria essa questão de restrição de pessoal [...], essa é uma realidade de toda a instituição, eu me compadeço, inclusive, com a gestão da universidade que tem […] E2
		[...] o desafio principal seria em relação à... à escassez de pessoas e recursos financeiros, né, porque só pelos exemplos que eu dei aqui [...] tudo isso exige pessoas e recursos para que seja feito um planejamento [...] completo da Lei Geral de Proteção de Dados em âmbito institucional, né? E esse desafio financeiro, orçamentário e de pessoal ele é gigante, não só LGPD, mas em todas as áreas, né? Então eu acho que esse seria, se eu pudesse colocar como principal, seria ele [...] E2
		Acho que a grande dificuldade é de pessoal, porque aí você acaba tendo várias demandas urgentes e prioritárias. [...] Então assim, precisa de mais recursos a nível [...] de pessoal. Porque hoje a gente atua muito mais no apagar incêndio e no que a gente consegue apagar, porque também como a gente tem [...] poucas pessoas, então isso dificulta. E3
		Então, você tem que ter equipe para ter capacitação para conhecer sobre aquela solução, realizar os procedimentos necessários e fazer um acompanhamento. [...] a gente precisaria ter uma equipe de tratamento só dedicada a isso [...] E3

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		Então, tudo isso precisa [...] de pessoas... Financeiro, tecnológico e pessoal. E3
		E aí também precisa de pessoas para estar monitorando ou realizando... porque tem algumas ferramentas, digamos, que você permite "escanear" a rede e você identificar alguns desses ativos de rede. E3
	Sobrecarga de trabalho 20 (57,14%)	[...] a proteção de dados, desde a promulgação da lei, já era para a instituição estar trabalhando nesse sentido. Hoje existe, como eu falei, [...] um comitê que trabalha, antigamente era uma pessoa só [...] E1
		E, no geral, acredito que a instituição está fazendo, que foi criado esse setor, um setor específico para tratar da LGPD, infelizmente [...] só tem uma pessoa e somente uma pessoa para fazer isso. Eu acredito que era para ser uma equipe maior [...]. Mas, assim, infelizmente só tem uma pessoa e para [...] sozinho, acho que é difícil a atuação [...] na LGPD. E1
		E não é raro você ver pessoas que acumulam [...] essa função com outras e não têm uma função comissionada, designada para isso, e nem ocupa um cargo específico. E2
		[...] todas essas previsões da política de privacidade se tornaram tão complexas, que exigia que uma pessoa só ficasse responsável por isso [...] tornou complexa, né, essa aplicação, por isso necessitaria de uma pessoa específica para fazer isso [...] E2
		Então, você atender à legislação, tendo a quantidade de trabalho expressiva [...] E2
		[...] essa autoavaliação, essa adequação à legislação, trazendo uma carga de trabalho adicional, [...] E2
		[...] acumula outras duas funções [...] então não há, pelo menos atualmente, uma pessoa que especificamente atue nessas metas relacionadas à adequação da instituição à Lei Geral de Proteção de Dados, então seria mais ou menos isso. E2
		[...] porque atualmente quem faria esse trabalho dentro da própria instituição seria o encarregado, mas como ele acumula tantas outras funções, é difícil você planejar uma política pública e você, de forma operacional, atuar elaborando, por exemplo, vias, formulários etc., e fazendo esse treinamento junto aos setores, entende? Então eu creio que é de fato um desafio [...]. É um desafio que eu creio que seja... superável num curto prazo [...] E2
		Então, é difícil porque o encarregado é quem lidera todas essas medidas, mesmo que tenha a ajuda do comitê. [...] é um desafio grande [...] por ter a figura do encarregado tendo que liderar todas essas questões. E2
		Ano passado eu ofertei um curso na área de [...]. Só eu estava disponível para ofertar esse curso e foi uma exigência de um órgão de controle, em relação a... aos colegas da área de gestão de pessoas. E2
		Já estou com formulários em mãos para propor um curso da LGPD. [...] O desafio é tornar isso sistemático, que esbarra também nessa restrição. [...] eu tenho um trabalho operacional muito grande [...] E2
		Eu mencionaria também a realização de eventos, que é algo que como eu já mencionei está limitado [...], bem como [...] por eu estar acumulando com outras funções, [...] é um desafio muito grande [...] E2
		Esbarra sempre nessa questão, são muitas questões e o encarregado tem muitas atribuições, não consegue fazer tudo [...] E2
		[...] mas há outros, como por exemplo o engajamento dos setores que realizam esses tratamentos de dados pessoais, como eu disse, a lei ela traz consigo, mesmo que de forma implícita, uma obrigação de você revisar seus processos institucionais (inaudível), isso traz um trabalho para os setores que muitas vezes já têm uma carga de trabalho, uma demanda muito grande [...] E2

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		[...] então o desafio seria realizar esse engajamento, né, porque como eu disse, é uma, entre aspas, um trabalho a mais para aqueles setores que eventualmente já têm uma demanda, uma carga de trabalho grande... e é isso. E2
		[...] seria o atual cenário de acúmulo de funções, porque tanto são demandas muito complexas e laborosas [...] E2
		[...] com toda a complexidade que eu venho mencionando ao longo de todas as perguntas, [...] Então, sem dúvida nenhuma, seria algo relacionado a esse acúmulo de funções [...] E2
		[...] mesmo a gente tendo acesso ao código do sistema para poder fazer alguns ajustes ou algumas melhorias, a gente não tem condições técnicas e capacidade operacional para isso, porque nossa equipe é muito pequena, e aí requer muito conhecimento e uma equipe de desenvolvimento muito ampla para poder fazer essas melhorias do sistema. E3
		Da mesma forma, como eu falei aqui, que a gente também tem uma equipe que atende várias áreas, vários contextos, [...] colocou essa questão lá que só é [...] pra tudo [...] E3
		E como a gente, de uma forma geral, são muitas demandas institucionais e equipes pequenas, acaba atropelando um pouco e acredito que dificulta o avanço dessas ações. E3
	Falta de interesse no setor público 2 (5,71%)	Tanto o recurso humano, a gente tem ciência disso, né? Que a instituição abre concurso para a área de TI e não consegue, infelizmente não está conseguindo preencher as vagas. Enfim, o desinteresse das pessoas em querer trabalhar com tecnologia na instituição. [...] Eu estou dizendo tecnologia no geral. E1
		É, está pagando melhor o mercado hoje. Ninguém sabe se vai ser uma onda, uma moda. Mas é basicamente isso, você paga bem melhor do que trabalhar aqui na instituição. [...] E aqui, infelizmente, é o salário de servidor público. [...] Pode ter o currículo que for, vai ser aquilo ali e pronto. E1

Fonte: Dados da pesquisa (2025)

Nessa categoria, foram identificados óbices que influem no planejamento da instituição, em função da restrição de pessoal. Segundo Almeida (2024), constitui-se como um entrave para as atividades de adequação à LGPD a restrição de profissionais capacitados, imprescindíveis em todas as fases desse processo.

A escassez de recursos humanos dificulta a atuação voltada à proteção de dados, na medida em que obriga os profissionais da área de tecnologia da informação a concentrarem seus esforços em demandas mais urgentes. Conforme ponderou o entrevistado nº 3, a atuação do corpo técnico se dá predominantemente no âmbito reativo, que, na linguagem conotativa, está relacionada com a expressão “apagar incêndio”:

> Acho que a grande dificuldade é de pessoal, porque aí você acaba tendo várias demandas urgentes e prioritárias. [...] Então, assim, precisa de mais recursos a nível [...] de pessoal. Porque hoje a gente atua muito mais no apagar incêndio e no que a

> gente consegue apagar, porque também como a gente tem [...] poucas pessoas, então isso dificulta (Entrevistado 3).

Tal cenário acaba por restringir a atuação a medidas imediatas e contingenciais. Essas limitações repercutem diretamente na capacidade de planejamento da instituição, visto que os profissionais mantêm-se mobilizados para a solução de demandas prioritárias, em detrimento de uma atuação no planejamento tático e estratégico relacionado à proteção de dados, o que demandaria tempo, organização e maior disponibilidade técnica.

Na visão de outro participante, a restrição de servidores resulta na incapacidade institucional de promover capacitações internas, assim como de torná-las sistemáticas:

> Já estou com formulários em mãos para propor um curso da LGPD. [...] O desafio é tornar isso sistemático, que esbarra nessa restrição. [...] De pessoal, porque você tem poucas pessoas com expertise na área para ofertar esse curso (Entrevistado 2).

Ainda que não de forma explicitada, percebe-se que a limitação do quadro de pessoal também repercute na carência de expertise técnica específica, fator que, embora não seja único, compromete a consolidação de iniciativas de capacitação regulares. Para além disso, também se compromete a implementação de práticas contínuas e planejadas de aperfeiçoamento, impondo limites à difusão do conhecimento entre os diversos setores da universidade e, por consequência, à efetivação dos dispositivos da LGPD.

Outro ponto que merece destaque é a sobrecarga de trabalho, que revela uma disparidade entre a estrutura organizacional e a capacidade operacional. A designação de apenas um agente público para responder por todas as demandas relacionadas ao tratamento de dados pessoais é insuficiente, evidenciando outro desafio que dificulta a implementação plena da norma, conforme se depreende da fala de um dos respondentes e em consonância com os apontamentos de Almeida (2024) sobre a restrição de servidores:

> E, no geral, acredito que a instituição está fazendo, que foi criado esse setor, um setor específico para tratar da LGPD, infelizmente [...] só tem uma pessoa e somente uma pessoa para fazer isso. Eu acredito que era para ser uma equipe maior [...]. Mas, assim, infelizmente só tem uma pessoa e para [...] sozinho, acho que é difícil a atuação [...] na LGPD (Entrevistado 1).

Essa percepção também foi relatada por outro entrevistado no que se refere aos demais setores da instituição:

> [...] mas há outros, como, por exemplo, o engajamento dos setores que realizam esses tratamentos de dados pessoais, como eu disse, a lei ela traz consigo, mesmo que de forma implícita, uma obrigação de você revisar seus processos institucionais (inaudível), isso traz um trabalho para o setores que muitas vezes já têm uma carga de trabalho, uma demanda muito grande [...] (Entrevistado 2).

> [...] então o desafio seria realizar esse engajamento, né, porque como eu disse, é uma, entre aspas, um trabalho a mais para aqueles setores que, eventualmente, já têm uma demanda, uma carga de trabalho grande… e é isso (Entrevistado 2).

Além da sobrecarga de trabalho, caracterizada pelo acúmulo de demandas do próprio setor, essas ponderações evidenciaram que a implementação da LGPD possui uma dimensão cultural, tal como apontado por Barbosa *et al.* (2021), Crespo (2021) e Philippi (2023). Nesse sentido, é fundamental que haja conscientização dos operadores de que a proteção de dados pessoais não é uma demanda dissociada das suas atividades. Ao contrário disso, a preocupação com os dados pessoais de terceiros e dos próprios servidores deverá permear todo o contexto laboral, o que implica a necessidade de promover uma cultura de proteção de dados.

De acordo com o terceiro respondente, essa sobrecarga pode manifestar-se tanto no volume de tarefas quanto em sua complexidade técnica:

> [...] mesmo a gente tendo acesso ao código do sistema para poder fazer alguns ajustes ou algumas melhorias, a gente não tem condições técnicas e capacidade operacional para isso, porque nossa equipe é muito pequena, e aí requer muito conhecimento e uma equipe de desenvolvimento muito ampla para poder fazer essas melhorias do sistema (Entrevistado 3).

Assim, é possível concluir que a deficiência no quantitativo de recursos humanos não apenas sobrecarrega os servidores, mas também compromete a capacidade operacional da organização e o planejamento na área de proteção de dados pessoais. Segundo Tavares (2015), essa sobrecarga pode refletir na percepção da insatisfação em relação ao ambiente de trabalho. Além disso, é importante mencionar que, na visão de um dos entrevistados, esse desafio não é exclusivo da organização objeto da pesquisa, mas de âmbito nacional, que foge do alcance da administração superior:

> Eu acho que a principal seria essa questão de restrição de pessoal [...], essa é uma realidade de toda a instituição, eu me compadeço, inclusive, com a gestão da universidade que tem [...] (Entrevistado 2).

> E as pessoas… a própria instituição [...] eu acho que isso é uma realidade da… de vários órgãos da Administração Pública federal, têm uma dificuldade muito grande de pessoas [...]. Então, você atender à legislação [...] ao mesmo tempo que você tem uma restrição de pessoas [...] (Entrevistado 2).

Outro aspecto relevante refere-se à baixa atratividade do setor público para profissionais da área de tecnologia da informação. Conforme estudo realizado pela Fecomércio-SP, com base nos dados da RAIS, o mercado de trabalho do segmento apresentou um crescimento expressivo de 741,2% entre os anos de 2012 e 2021 (Fecomercio-SP, 2024). Isso evidencia um cenário de destaque do setor e de escassez de profissionais qualificados, intensificando a competição entre os diversos agentes empregadores e impactando diretamente a elevação da média salarial da categoria.

Essa conjuntura repercute sobre a universidade especialmente no que diz respeito à dificuldade de retenção de servidores e preenchimento de cargos vagos. Um dos entrevistados destacou os entraves enfrentados para o provimento de tais cargos, atribuindo-lhes, sobretudo, à limitação da remuneração oferecida no setor público:

> Tanto o recurso humano, a gente tem ciência disso, né? Que a instituição abre concurso para a área de TI e não consegue, infelizmente não está conseguindo preencher as vagas. Enfim, o desinteresse das pessoas em querer trabalhar com tecnologia na instituição. [...] Eu estou dizendo de tecnologia no geral (Entrevistado 1).

> É, está pagando melhor o mercado hoje. Ninguém sabe se vai ser uma onda, uma moda. Mas é basicamente isso, você paga bem melhor do que trabalhar aqui na instituição. [...] E aqui, infelizmente, o salário de servidor público. [...] Pode ter o currículo que for, vai ser aquilo ali e pronto (Entrevistado 1).

Nas IFES, a remuneração dos servidores técnico-administrativos em educação é disciplinada pela Lei nº 11.091, de 12 de janeiro de 2005, que instituiu o Plano de Carreira dos Cargos Técnico-Administrativos em Educação (PCCTAE) (Brasil, 2005). Trata-se, portanto, de uma estrutura remuneratória cuja modificação depende de fatores externos às instituições, sobretudo de iniciativa e deliberação em âmbito federal, o que limita a autonomia das IFES para tratar da valorização de seus quadros funcionais e contribui para a configuração do cenário descrito. Para além disso, conforme aponta Tavares (2015), a remuneração, assim como a distribuição equitativa da carga de trabalho, constitui elemento de prevenção da insatisfação no ambiente organizacional.

A partir dessas ponderações, foi possível notar que a carência em recursos humanos é um fator que perpassa por diversas dimensões da aplicação da LGPD e se constitui, na visão dos entrevistados, em razão da recorrência de citações, como o maior entrave para a adequada aplicação da norma e o efetivo fomento a políticas de proteção de dados pessoais. O descumprimento de algumas das metas relativas a essa proteção pode, em alguma medida, ser

compreendido como reflexo dos obstáculos mencionados, uma vez que a limitação e a capacitação profissionais impactam diretamente a efetividade das ações.

Quanto à segunda categoria com maior frequência, Universidade, os respondentes apontaram que um dos princípios desafios para implementar a LG PD na entidade está atrelado à própria complexidade universitária (35,29%). Em seguida, constatou-se um equilíbrio entre os fatores "educação do titular/operador de dados" (26,74%) e "engajamento da comunidade universitária" (23,53%). Por fim, o último desafio relaciona-se à visão institucional limitada (14,71%). O Quadro 14 sintetiza os resultados dessa categoria.

Quadro 14 - Análise da categoria Universidade

(continua)

Nº de citação e frequência (%)	**Unidade de registro**	**Unidade de contexto**
34 (32,38%)	Visão institucional limitada 5 (14,71%)	[...] foi colocado no PDI a LGPD, e aí colocou a STD como responsável por isso, que é um dos eixos tecnológicos lá [...]. E, no nosso entendimento, a LGPD não pode recair somente na área de tecnologia. Veja, nós temos que estar envolvidos, ponto. E1
		[...] tudo que era relacionado à tecnologia mandava tudo para cá. E, assim, nem sempre, tudo que é relacionado à tecnologia é a STD que é responsável. E1
		[...] eu creio que essa meta já havia sido estabelecida pela própria instituição, o que traz um desafio muito grande [...]. Existem formas de você avaliar a maturidade [...], a adequação [...] à Lei Geral de Proteção de Dados, que talvez não se encaixem exatamente em um único critério, que é o que prevê o PDI. E2
		[...] acredito que foi um pouco mal dimensionado essas metas em termos da LGPD. [...] Porque é algo que não é uma coisa pontual da STD [...] eu acredito que deve ter ações mais assim, no sentido de melhor dimensionar essa meta, porque uma meta que ela não é muito bem quantificada, você não consegue atingir. [...] a STD não é responsável pela LGPD da instituição, ela é mais um ente que faz parte de um contexto. Então, acho que isso acaba dificultando [...] E3
		[...] eu acho que cada vez mais integrar essas áreas para que elas possam, em conjunto, realizar essas ações. E não ficar uma coisa assim: ah, isso é do encarregado, isso aqui é da TI [...] eu acho que no PDI ficou muito além da nossa capacidade, algumas coisas difíceis de mensurar. E até dele no planejamento de cada setor: na PROGEPE, [...] TI, os setores acadêmicos... Enfim, porque é algo que permeia toda a instituição [...] E3
	Educação do titular/operador dos dados 9 (26,74%)	[...] a gente tenta tratar da forma educacional, né, porque, hoje, observando em uma forma geral, o elo mais fraco da segurança é o usuário. [...] a melhor forma que a gente encontrou foi essa, a partir... é educar o usuário [...] E1
		Mas eu não me preocupo com isso, não, porque, quando eu trabalhava na [....], que divulgava os editais, o meu CPF ia lá. [....] Na época eu entendia [...] porque tem que ir meu CPF, mas pra dar uma, vamos dizer, assim, uma autenticidade. [...] Eu acho que isso, se colocar na internet aí, pega meu CPF facinho. E1
		A RNP também tem um programa de cursos voltado para a LGPD. Então assim, cursos sempre tem. Cabe a cada servidor ter interesse de fazer. A gente até recomenda, mas forçar [...] a fazer curso não. E1

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		Acredito também que a capacitação dos usuários aqui, da comunidade como um todo, acho que vai ajudar bastante. E1
		Você tem lá o Google *Docs*, o Google Planilha, enfim. Mas muita gente não sabe utilizar. Então, por isso que eu falo e repito: a capacitação é importante...para toda a comunidade. E1
		E aí você esbarra muitas vezes numa... numa restrição de nível de maturidade mesmo institucional das pessoas que atuam nessa área [...]. Eu entendo que algo assim vai ser melhorado ao longo do tempo, mas é um desafio grande por ser novo. E2
		Então, eu entendo que a gente oferece essa capacitação já, há cursos correlatos... já foram ofertados cursos relacionados à LGPD, como também a gente atua de forma a conscientizar a [...] comunidade da UFRPE [...]. Porém, a gente tem um desafio de tornar isso de forma mais sistemática. Como eu disse a você, são desafios... E2
		[...] quando algum formulário é criado por algum setor que usa o Google *Forms* [...]. Então, a gente não tem um controle no sentido assim de como que o usuário solicita dados que são sensíveis, ou como ele trata esse dado, como é que ele guarda esse dado. E3
		[...] a gente não consegue controlar um dado quando ele não é gerenciado totalmente aqui pela STD. [...] Os órgãos aqui podem ter acesso a partir do e-mail institucional, e ele pode criar alguns formulários [...]. Então, fica muito, às vezes, do usuário daquele setor, como é que ele está atendendo ou não aos requisitos da LGPD. E3
	Complexidade universitária 12 (35,29%)	A gente sabe que uma universidade pública federal atua em diversas frentes. São muitas unidades, são muitas pró-reitorias e cada uma tem uma (inaudível) diferente. E2
		Então, é uma função relativamente complexa nesse sentido, porque envolve todas essas questões com todas as diferenças que a própria instituição detém pela sua natureza, né, de ser uma instituição que atua em várias frentes, apesar de ter o objetivo educacional, né, de ensino, pesquisa e extensão. E2
		E todos os desafios derivam exatamente [...] de você adequar os seus processos institucionais, bem como a cultura organizacional da instituição. E aí é que está o nosso desafio, né? E2
		O primeiro anexo é o que estabelece o Comitê Gestor de Privacidade e Proteção de Dados, e nele a gente já vê que a própria concepção do Comitê já permite a gente identificar a complexidade do desafio [...] na instituição, porque ela prevê a participação de todas as pró-reitorias e de todas as unidades acadêmicas, com a adição, se eu não me engano, de alguns outros setores [...] E2
		Então, é uma atuação bem ampla, bem complexa, porque, como eu disse, a instituição ela atua em diversas frentes. Cada frente tem um tipo de atuação bem específica. [...] o tratamento que é realizado no Departamento de Qualidade de Vida é bem diferente do que é realizado na Pró-Reitoria de Graduação, por exemplo, ou na própria Pró-Reitoria de Planejamento [...] E2
		[...] há pessoas que trabalham com análises de relatórios financeiros, [...] com contratos administrativos, [...] com a parte de gestão de pessoas que têm um sistema específico para isso, [...] com qualidade de vida, enfim, a atuação da universidade, como eu disse, é muito ampla. E isso necessitaria de uma revisão, porque apesar de eles terem um sistema institucional, a gente sabe que alguns dados são tratados por meio de formulários físicos, são tratados por meio de dispositivos que não são [...] vinculados a contas institucionais [...] E2

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		A gente está em um processo de revisão agora dessa meta de 75%, porque ela é muito ampla e, como eu disse, são muitas questões relacionadas... muitos setores, né, muitas unidades. Então ela vai necessitar de uma revisão... muito provavelmente para baixo [...] e eu entendo que é uma questão relativamente complexa, digamos assim, né? E2
		[...] porque a Universidade já poderia, [...] ter evoluído em um guia, em um manual nesse sentido, né, porque a operação de anonimização de um dado ela é relativamente simples. Talvez a gente não tenha a melhor ferramenta ou a ferramenta adequada para fazer isso em alguns setores que tratam de um volume muito grande de informações. [...] Então, eu acho que sim, que é um desafio, mas talvez seja fácil corrigir. E2
		[...] O PPSI ele prevê, se eu não me engano, 311 medidas, 310 medidas, né? Só pra você ter uma noção, uma medida, uma só, é a revisão de todos os formulários institucionais. Então pense você: é relativamente simples você realizar um... um planejamento, fazer um guia, em que você demonstra a toda a comunidade como é que um formulário deve ser elaborado. [...] O difícil é [...] fazer isso ao longo de toda a complexidade da instituição, entende? [...] E eu poderia dar outros exemplos, mas só esses você já entende que a complexidade é gigante. E2
		Eu dei o exemplo dos formulários, né, que é outra que exigiria atuação cada vez maior de cada um deles. Eu dou outros, por exemplo, como a gestão de cookies no site institucional. [...] os próprios setores [...] poderiam fazer, mas é difícil você... adequar sem a orientação específica do encarregado [...]. Então eu quis fazer esse aparte só pra você ter a noção da complexidade. E2
		[...] como eu disse, a universidade é muito plural e muito ampla, então normalmente a gente atua na parte do planejamento por meio de (inaudível) processos ou por meio de setores específicos. E2
		Então, é um desafio grande, porque quando você fala de inventário, você tem que fazer uma revisão dos processos institucionais e fazer um inventário de todos aqueles dados que são tratados [...]. Eu não preciso repetir da complexidade de fazer isso, porque envolve todos os agentes e atores das mais diversas áreas da instituição, né? E2
	Engajamento da comunidade universitária 8 (23,53%)	[...] e o Comitê Gestor ter uma participação de todos os setores, já tem uma importância grande, [...] o Comitê Transparência de Dados Abertos [...] não tem participação de todos os setores, só de alguns setores-chaves, e aí você percebe que há uma dificuldade de engajamento dessas pessoas [...] E2
		[...] eu diria que seria a dificuldade de você engajar, né, os próprios setores e servidores nessa tarefa, porque para você fazer uma adequação à Lei Geral de Proteção de Dados, você necessita revisar os seus processos, fazer uma análise de lacuna, fazer um planejamento e implementar medidas. E2
		[...] essa talvez seja a principal influência de não atingimento da própria meta do PDI, né, porque é um desafio muito grande você... levar toda essa adequação, essa autoavaliação, a todos os setores da instituição. [....] Então, eu acho que esse é o principal fator que vem influenciando nessa dificuldade de engajamento. E2
		Porém, eu diria que é um desafio conjunto [...] se houvesse um engajamento institucional de 90% a 80% dos servidores em relação à Lei Geral de Proteção de Dados, você já diminuiria a ocorrência de incidentes de privacidade que ocorre em âmbito operacional. [...] Então, eu diria que há um conjunto, tanto... o investimento, o engajamento [...] E2
		[...] só que a gente tem uma dificuldade de engajamento muito grande, né, porque quando você traz [...] muitas vezes para participar de decisões

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		coletivas, é que você acumula experiência de vários setores. Mas a dificuldade é você engajar todas essas pessoas na construção, por exemplo, de um instrumento. Até porque as pessoas que participam do comitê, elas têm uma formação diversa, elas têm uma atuação diversa dentro da instituição, que nem sempre é vinculada à parte de proteção de dados. E2
		[...] mas há outros, como por exemplo o engajamento dos setores que realizam esses tratamentos de dados pessoais, como eu disse, a lei ela traz consigo, mesmo que de forma implícita, uma obrigação de você revisar seus processos institucionais (inaudível), isso traz um trabalho para os setores [...] E2
		[...] então o desafio seria realizar esse engajamento, né, porque como eu disse, é uma, entre aspas, um trabalho a mais para aqueles setores que eventualmente já têm uma demanda, uma carga de trabalho grande... e é isso. E2
		[...] a nível institucional, é esse engajamento de todas as áreas da Universidade, no sentido de cada vez mais melhorar esses aspectos de segurança e de tratamento de dados. E3

Fonte: Dados da pesquisa (2025).

Na categoria Universidade, que envolve a complexidade da estrutura organizacional, bem como a pluralidade de perfis da comunidade, os entrevistados relataram dificuldades de coesão, entendimento e, sobretudo, de engajamento da comunidade universitária, além de desafios relacionados à divisão das responsabilidades. Em seu estudo, Almeida (2024) também observou a complexidade da estrutura e da cultura administrativa como um entrave para a correta implementação da LGPD, dificultando a celeridade de ações nas unidades.

De acordo com o PDTIC, a UFRPE dispõe de infraestrutura acadêmica e administrativa composta por mais de 1,2 mil docentes, mais de mil técnicos administrativos, mais de 500 trabalhadores terceirizados e cerca de 17 mil discentes. Além disso, atende diversos cidadãos por meio de projetos de ensino, pesquisa, extensão e inovação (UFRPE, 2023b, p. 13).

Nas unidades de registro, a universidade é apontada como plural e multifuncional, com estrutura diversificada, formada por unidades acadêmicas e pró-reitorias:

> A gente sabe que uma universidade pública federal atua em diversas frentes. São muitas unidades, são muitas pró-reitorias e cada uma tem uma (inaudível) diferente (Entrevistado 2).

Devido às idiossincrasias de cada setor, bem à multiplicidade de tarefas, a complexidade da instituição por si só é vista como um entrave à aplicação da LGPD, por exigir atuação individualizada. Esse desafio, porém, é potencializado quando a divisão das atribuições

relativas à norma não se dá de forma efetiva. Ao ser entrevistado, um dos respondentes destacou que a falta de clareza nas responsabilidades institucionais obstaculiza a atuação para a aplicação da norma, notadamente as metas previstas no PDI da instituição:

> [...] acredito que foram um pouco mal dimensionadas essas metas em termos da LGPD. [...] Porque é algo que não é uma coisa pontual da STD [...] eu acredito que deve ter ações mais assim, no sentido de melhor dimensionar essa meta, porque uma meta que ela não é muito bem quantificada, você não consegue atingir. [...] a STD não é responsável pela LGPD da instituição, ela é mais um ente que faz parte de um contexto. Então, acho que isso acaba dificultando [...] (Entrevistado 3).

Esse relato aponta um desacerto na formulação estratégica quanto à responsabilidade de adequação à LGPD e reforça a tese de que a proteção de dados pessoais deve ser pensada de forma transversal e colaborativa, tal como preconizam os *frameworks* de proteção de dados, como é o caso do PPSI, que contempla um conjunto de processos e projetos distribuídos nas áreas de governança, maturidade, metodologia, pessoas e tecnologia (Brasil, 2023a). Desse modo, é incoerente atribuir a um setor exclusivo a competência de promover aquela adequação, tendo em vista a necessidade do envolvimento de toda a gestão institucional, que deverá participar das discussões sobre o ciclo de tratamento de dados pessoais e sensíveis, bem como apropriar-se da política de privacidade da organização (Nascimento; Silva, 2023).

Outro ponto relevante diz respeito à necessidade de educação tanto dos titulares quanto dos operadores de dados. Rojas (2020, p. 13) sustenta que, para fins de conformidade com a LGPD, uma das recomendações consiste na "necessidade de educação dos alunos, para cuidar da informação (proteção à privacidade) em acessos à internet".

Nesse sentido, o Entrevistado 1 enfatizou que os usuários[14] configuram o elo mais vulnerável na cadeia de proteção de dados, o que exige a adoção de estratégias pedagógicas voltadas à sensibilização dos titulares, a fim de evitar ou ao menos reduzir os danos de eventual violação de dados pessoais:

> [...] a gente tenta tratar da forma educacional, né, porque, hoje, observando em uma forma geral, o elo mais fraco da segurança é o usuário. [...] a melhor forma que a gente encontrou foi essa, a partir… é educar o usuário [...] (Entrevistado 3).

[14] De acordo com a POSIC, compreendem: "servidores, estudantes e docentes contratados e voluntários. Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, estudantes, consultores e colaboradores internos, assim como prestadores de serviços aposentados, visitantes e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais" (UFRPE, 2022b, p. 7).

A abordagem educacional é um dos pilares para a eficácia de uma política de segurança da informação e proteção de dados, de modo que a educação e a conscientização dos membros da comunidade acadêmica são imprescindíveis. Esses direcionamentos são representados pelas diversas iniciativas e ações da instituição, a exemplo da criação de uma aba específica no Portal UFRPE Digital sobre segurança da informação e do lançamento do Programa "Previna-se!", cuja análise foi realizada na seção 4.1.

A fala ainda destaca que a contribuição para a proteção de dados não é papel exclusivo da instituição e apresenta maior probabilidade de ser efetiva quando há o interesse do usuário, revelando a importância de se "difundir a cultura de proteção de dados para que todos os cidadãos, e não só os servidores que fazem o tratamento de dados, consigam entender melhor a legislação" (Souza, 2022, p. 100).

Esse processo educacional, no entanto, esbarra em outra dificuldade, representada pelo "engajamento da comunidade universitária". A recorrência de citações dessa unidade de registro revela a preocupação dos entrevistados em relação à falta de engajamento dos usuários, o que poderá comprometer o tratamento correto dos dados a que eles têm acesso e, consequentemente, aumentar a probabilidade de vazamentos e compartilhamentos indevidos e ilegais (Philippi, 2023). Esse risco de segurança da informação poderá conduzir à perda da credibilidade da UFRPE, fragilizando sua imagem perante a sociedade (Nascimento; Silva, 2023).

Outrossim, os vídeos e cursos disponibilizados possuem caráter meramente facultativo e, na falta de iniciativa voluntária por parte do usuário em dedicar-se às ações de capacitação, torna-se improvável a obtenção de quaisquer resultados concretos, conforme pontuou um dos partícipes:

> A RNP também tem um programa de cursos voltado para a LGPD. Então, assim, cursos sempre tem. Cabe a cada servidor ter interesse de fazer. A gente até recomenda, mas forçar [...] a fazer curso não (Entrevistado 1).

Além de corroborar essa falta de engajamento dos usuários em participarem de ações voltadas à proteção de dados, um dos respondentes destacou também a necessidade de revisar os processos de cada unidade organizacional.

> [...] eu diria que seria a dificuldade de você engajar, né, os próprios setores e servidores nessa tarefa, porque, para fazer uma adequação à Lei Geral de Proteção de Dados, você necessita revisar os seus processos, fazer uma análise de lacuna, fazer um planejamento e implementar medidas (Entrevistado 2).

Isso evidencia o caráter técnico e multifásico do processo de adequação à LGPD, o qual demanda um conjunto de etapas, como a revisão de processos, a identificação de lacunas, o planejamento e a implementação de medidas, especialmente de controle. Para Souza (2022, p. 75), "o mapeamento de processos é essencial para auxiliar as IFES no diagnóstico de melhor disposição de estrutura física e de trâmites processuais para propiciar a adequada proteção dos dados pessoais".

Cada uma daquelas etapas pressupõe não apenas conhecimento técnico específico sobre as rotinas setoriais, mas também a articulação entre as áreas administrativas e acadêmicas da instituição, o que termina por ser inviabilizado diante da inércia e falta de comprometimento da comunidade acadêmica, bem como pelo déficit de servidores. Na opinião de um dos entrevistados, essa pode ser a razão pela qual as metas do PDI relacionadas à adequação á LGPD não foram atingidas:

> [...] essa talvez seja a principal influência do não atingimento da própria meta do PDI, né, porque é um desafio muito grande você… levar toda essa adequação, essa autoavaliação, a todos os setores da instituição. [...] Então, eu acho que esse é o principal fator que vem influenciando nessa dificuldade de engajamento (Entrevistado 2).

Nesse contexto, a necessidade de autoavaliação e de revisão de processos da instituição impacta diretamente a capacidade da Universidade de alcançar as metas estratégicas, revelando como a proteção de dados pessoais está atrelada à governança. Essa relação já foi ressaltada por outros autores, como Barbosa *et al*. (2021), cujo estudo revelou que a LGPD não se resume a aspectos jurídicos, contemplando também fatores técnicos relacionados à segurança da informação e à governança. Outros autores que compartilham desse entendimento ressaltam que a publicação da referida lei foi essencial para subsidiar a governança de dados (Bergamini; Hahn, 2021) e que, no âmbito universitário, um dos principais desafios é estruturar um programa de boas práticas de governança e proteção de dados (Almeida; Soares, 2022).

Dessa forma, consoante a análise das unidades de contexto da categoria Universidade, verifica-se que os desafios derivam, sobretudo, da complexidade organizacional da instituição, em face da sua natureza plural.

As ponderações dos entrevistados revelaram a heterogeneidade da atuação de uma instituição federal de ensino superior, sobretudo no que se refere à complexidade para a mobilização da comunidade acadêmica, incluindo-se servidores e setores, em torno da temática da proteção de dados. Na visão de Souza (2022, p. 74), é importante "o envolvimento de todos

que fazem parte das IFES e uma cultura orientada para a gestão de dados, com destaque para aspectos de segurança e privacidade".

Conforme debatido, a LGPD, enquanto marco legal, impõe obrigações técnicas e exige uma mudança de paradigma quanto à forma como os dados pessoais são compreendidos, tratados e protegidos no cotidiano da instituição. Essa transformação, contudo, tem sido limitada em virtude do contexto organizacional, acentuando-se por desafios relacionados ao ordenamento jurídico, representado pela categoria Legislação.

Essa categoria refere-se às unidades de registro que evidenciam dificuldades relacionadas às normas jurídicas concernentes à proteção de dados, publicidade e afins, notadamente os conflitos aparentes entre normas, a ausência de diretrizes uniformes, a complexidade interpretativa e o caráter ainda embrionário da legislação específica. Esses elementos são percebidos como fatores que comprometem a efetividade e a segurança jurídica dos processos institucionais relacionados à proteção de dados. A categoria encontra-se representada no Quadro 15:

Quadro 15 - Análise da Categoria Legislação

(continua)

Nº de citação e frequência (%)	**Unidade de registro**	**Unidade de contexto**
21 (20,00%)	Conflito aparente entre normas 7 (33,33%)	[...] no meu ponto de vista, existe uma linha tênue entre o que é dados abertos e o que é LGPD. Se por um lado, a gente tem que dar transparência aos atos da Administração Pública, por outro, a gente tem que proteger, e aí fica esse dilema. Então gera muitas dúvidas dentro da instituição pública, quais os limites, o que é dado aberto e o que é protegido pela LGPD. E1
		Existe muita dúvida [...] chegou uma solicitação de uma pesquisadora [...] pedindo todos os endereços eletrônicos, e-mail dos docentes [...]. A gente não divulgou, porque entendeu que o e-mail, mesmo sendo domínio UFRPE, tendo o nome da pessoa, ele é pessoal [...]. Você quer conversar com alguém do setor X, entre em contato com o e-mail da coordenação, da direção, do setor, enfim, mas não da pessoa. Aí você vem, aí tem outra questão, muitas pessoas estão em PGD, aí foi divulgado o e-mail pessoal e o telefone, e aí você fica, o que que é, o que não é. Então gera muito conflito na cabeça das pessoas, realmente é um pouco polêmico. E1
		[...] essa linha tênue que existe entre dados abertos e LGPD. Em algum momento pode ter, a própria UFRPE ter divulgado alguma listagem, sei lá, de alunos, ou de servidores, que não deveria e passou despercebido e foi. E1
		É uma linha tênue entre dados abertos e a LGPD, né? Sempre vai ser esse, vamos dizer, esse cabo de guerra aí, um puxando pro lado, outro puxando pro outro, enfim. E1
		Existe uma dicotomia [...] sobre a transparência e a privacidade, que são duas leis diferentes, dois princípios diferentes, mas que trata dessas mesmas questões, né, da gestão dos dados por meio da instituição. [...] Então... existem nuances de acordo com essas legislações que exigem

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		que a gente tenha um nível de... de compreensão acerca da necessidade de tornar os processos cada vez mais transparentes e mais públicos, por uma... por uma questão de um exercício de controle social, mas ao mesmo tempo cumprindo o que prevê a Lei Geral de Proteção de Dados. [...] Então, existem muitas dúvidas por conta dessas dicotomias das várias legislações [...] E2
		[...] são duas políticas que, em tese, exigiriam que uma pessoa ficasse responsável por cada uma delas, inclusive porque em determinados casos, [...] há um conflito entre normas, [...] E2
		Então, por exemplo, no sentido do acesso aos dados... Porque tem a questão da lei de acesso aos dados, a informação da LAI, e tem a LGPD. Têm algumas coisas que até parecem um pouco conflitantes, né? Porque da mesma forma que a LAI prega essa questão da transparência, a LGPD tem um pouco um sentido da segurança, do dado, enfim. E3
	Ausência de uniformização 4 (19,05%)	A gente sabe que não pode divulgar o número do CPF, mas se você for pesquisar, tem algumas bases de dados que fazem o quê? Eles suprimem os cinco números do meio, já outras botam os números dos cantos, dos extremos, e aí você confronta, chega no CPF [...] da pessoa [...]. Aí você tem que ter uma regra, uma padronização, ou você vai anonimizar os cinco números do meio ou os dados da extremidade [...] E1
		[...] não há uma uniformização. É o nosso entendimento, o meu entendimento é dessa forma. Não existe uma linha de raciocínio única. E1
		Como eu estou dizendo, não tem uma uniformidade, né? Não tem um padrão para a gente seguir. E aí cabe a interpretação de cada setor, de cada órgão. E1
		E ainda tem a questão do padrão, né? E aí você vai anonimizar, beleza, mas qual? Os cinco do meio, os quatro da extremidade... E1
	Dificuldade de interpretação 2 (9,52%)	[...] Tanto a gente tem essa dificuldade da interpretação da lei, quanto pode acontecer também vazamento da instituição, né? E1
		Primeiro, a gente precisa conhecer a fundo a lei. Eu confesso que eu tenho essa dificuldade de entender algumas situações lá da lei. No meu ponto de vista, ela não é fácil de entender, de interpretar. E1
	Caráter incipiente 8 (38,10%)	Então eu entendo que sim, deveria existir, mas eu entendo que é uma questão que vai amadurecer junto com a própria legislação, que é uma legislação relativamente nova. E2
		Eu repito até pela questão da incipiência da legislação, né? E2
		Já a proteção de dados, ela é um conceito mais novo. A própria legislação, que é de 2018, né? [...] Então é algo muito novo, muito incipiente. E todos os desafios derivam exatamente dessa incipiência da legislação. E2
		Então, a gente toma isso como base, a própria lei é um norte em relação a isso, né, [...] e, até agora, como eu disse, como a legislação é incipiente [...] E2
		Como a legislação é nova, ainda é muito incipiente no sentido de você atribuir, por exemplo, ao comitê, sem que o encarregado lidere especificamente essa questão, a atribuição de fazer essa... esses guias, esses manuais etc. Porém, [...] é um desafio superável. E2
		E aí você esbarra muitas vezes numa... [...] incipiência, digamos assim, da própria legislação. Eu entendo que algo assim vai ser melhorado ao longo do tempo, mas é um desafio grande por ser novo [...] E2
		A ANPD começou há pouco tempo a... fazer decisões, a expedir decisões no sentido de penalizar algumas instituições, tanto privadas como públicas, em relação ao descumprimento da Lei Geral de Proteção de Dados, tá? Eu acho que a gente está, como eu disse, num ambiente de maturidade, num ambiente tão incipiente [...]. Num segundo momento é

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		que a gente vai passar a responder legalmente por eventuais omissões, né? [...] mas até agora não aconteceu. E2
		[...] com toda a complexidade que eu venho mencionando ao longo de todas as perguntas, no sentido do planejamento institucional, de ser uma legislação incipiente, [...] tanto porque a legislação é nova [...] E2

Fonte: Dados da pesquisa (2025).

Nessa categoria, a terceira com maior frequência de citações, apresentando 21 menções, têm-se as unidades de registro em que os entrevistados apontaram o caráter incipiente (38,10%) e conflito aparente entre normas (33,33%), como desafios para a implementação eficaz de práticas de proteção de dados, havendo um equilíbrio entre ambos. Além desses, a ausência de uniformização (19,05%) e a dificuldade de interpretação da LGPD (9,52%) também foram apontadas como óbices.

Uma das unidades de registro criadas para abarcar as citações dos respondentes nessa categoria é o caráter incipiente da norma. Segundo o entrevistado 2, a natureza ainda embrionária da consolidação da LGPD representa um elemento que dificulta sua efetiva implementação:

> [...] Já a proteção de dados, ela é um conceito mais novo. A própria legislação, que é de 2018, né? [...] Então é algo muito novo, muito incipiente. E todos os desafios derivam exatamente dessa incipiência da legislação (Entrevistado 2).

Segundo Doneda (2021, p. 16), a LGPD se estrutura "a partir de um instrumental jurídico que é, em boa parte, novo para o nosso ordenamento". Com efeito, diferentemente da União Europeia, onde o RGPD vigora há mais tempo, o arcabouço jurídico relacionado à proteção de dados pessoais no Brasil ainda experimenta uma fase de amadurecimento (FONTE, ANO). A inexperiência no tratamento dos dados dificulta a construção e a aplicação de políticas associadas ao tema, bem como exige, conforme exposto anteriormente, um processo de mudança cultural, com o envolvimento de gestores, servidores e discentes em ações de conscientização, com o fito de consolidar uma cultura organizacional orientada à privacidade.

Para além dessa incipiência - e talvez em razão dela -, a LGPD também apresenta como desafio a sua própria exegese, representada pela unidade de registro "dificuldade de interpretação". Acerca disso, o entrevistado 2 afirmou:

> Primeiro, a gente precisa conhecer a fundo a lei. Eu confesso que eu tenho essa dificuldade de entender algumas situações lá da lei. No meu ponto de vista, ela não é fácil de entender, de interpretar (Entrevistado 2).

O texto da norma, por mais que busque ser abrangente e protetivo, traz conceitos jurídicos que, embora definidos na própria LGPD, exigem, eventualmente, interpretação sistemática e contextualizada. Para Aguilera e Di Biase (2021), a lei contém dispositivos que não foram redigidos e organizados com a melhor técnica legislativa. Soma-se a esse contexto a ausência de normativas específicas, por parte do Governo Federal e da ANPD, que estabeleçam diretrizes acerca do tratamento de dados pessoais no âmbito das IFES, o que contribui ainda mais para o cenário de adversidades enfrentado por estas instituições no processo de adequação à LGPD (Souza, 2022).

Nesse sentido, um dos respondentes ressaltou a ausência de uniformidade no que se refere a aspectos sobre os quais a norma é silente, apontando a inexistência de padronização quanto aos procedimentos operacionais, notadamente aqueles atinentes à anonimização e à pseudonimização. Segundo ele, um desses exemplos é a divulgação do CPF dos titulares dos dados:

> Como eu estou dizendo, não tem uma uniformidade, né? Não tem um padrão para a gente seguir. E aí cabe a interpretação de cada setor, cada órgão (Entrevistado 1)

> A gente sabe que não pode divulgar o número do CPF, mas se você for pesquisar, tem algumas bases de dados que fazem o quê? Eles suprimem os cinco números do meio, já outras botam os números dos cantos, dos extremos, e aí você confronta, chega no CPF [...] da pessoa [...]. Aí você tem que ter uma regra, uma padronização, ou você vai anonimizar os cinco números do meio ou os dados da extremidade [...] (Entrevistado 1).

Em estudo acerca dos processos de anonimização, a ANPD, corroborando a fala do respondente, reconhece que, em relação à supressão de caracteres do CPF, em "casos de dados públicos ou compartilhados, como não há um padrão para o mascaramento, é possível que partes distintas dos dados estejam visíveis e por consequência os dados originais sejam reconstruídos" (Brasil, 2023c, p. 22).

Com efeito, as orientações acerca do fato a que se referiu o entrevistado não são plenamente elucidativas. Para ilustrar essa ambiguidade, tem-se as manifestações da CGU e da ANPD acerca da divulgação de dados pessoais de servidores em contratos e convênios dos quais façam parte o Poder Público.

O órgão de controle interno do Poder Executivo, em resposta a consultas sobre a divulgação de contratos, convênios e afins nas páginas de transparência e órgãos e entidades da

Administração Pública, entendeu que em tais casos hão de ser divulgados apenas os dados estritamente necessários à identificação das partes, limitando-se aos nomes e números do CNPJ/CPF, este último de forma descaracterizada, no caso de representantes legais das pessoas jurídicas contratadas, com vistas a evitar uso indevido. No que concerne aos representantes da Administração Pública, sugeriu-se a substituição do número do CPF pelo número de matrícula funcional, tal como o número Siape no âmbito federal (Brasil, 2021a; Brasil 2024a; Brasil, 2024b).

Por outro lado, em resposta a consulta sobre conflito de entendimentos acerca do tratamento a ser dispensado aos dados dos servidores públicos federais quanto à substituição do CPF dos servidores em contratos administrativos e outros documentos organizacionais pelo número Siape, a ANPD concluiu pela inexistência de óbice para a divulgação do número da inscrição no CPF de servidores públicos federais nos contratos administrativos, bem como a de outros dados pessoais relacionados, assinalando que a matrícula Siape "não se mostra suficiente para as finalidades de cumprir o dever de transparência da Administração Pública ou garantir o direito à informação, pois não facilita ou tem utilidade direta para o exercício facilitado do controle social pelo cidadão" (Brasil, 2023d).

Esse desencontro normativo expõe a instituição a riscos evitáveis e compromete a efetividade da proteção de dados pessoais, ensejando ocasionalmente decisões improvisadas e dissonantes entre os múltiplos setores do ente, bem como entre órgãos e entidades da Administração Pública. A ausência de parâmetros uniformes, além de eventualmente permitir a reconstrução do dado pessoal, restringe, e por vezes inviabiliza, a atuação técnica dos servidores, gerando insegurança operacional e decisória, com reflexos potenciais sobre a credibilidade institucional e a segurança jurídica no contexto da organização.

Nesse contexto, mostra-se essencial a edição de orientações específicas por parte da ANPD, como uma que verse sobre o mascaramento do número do CPF, com o objetivo de colmatar lacunas legais que hoje dificultam a proteção plena dos dados pessoais. Registre-se que uma regulamentação isolada pela UFRPE teria eficácia limitada, considerando que não raro os cidadãos mantêm registros em múltiplas bases de dados da Administração Pública. Dessa forma, conforme já exposto, uma suposta divergência de entendimento entre controladores seria suficiente para permitir a reidentificação dos dados mascarados através da reconstrução dos fragmentos.

Ainda na categoria Legislação, ao referir-se à compreensão do texto legal, entrevistado 2 mencionou a última unidade de registro, o aparente conflito entre normas, notadamente em

relação à LGPD e à LAI. São leis que apresentam enfoques distintos, muito embora se destinem a finalidades igualmente relevantes no ordenamento jurídico: a transparência, tutelada pela LAI, e a privacidade, assegurada pela LGPD.

Segundo Almeida (2024, p. 58), a "Lei 13.709/18 trouxe muitos conceitos até então desconhecidos, com pontos não regulamentados ou esclarecidos, criando um ambiente de dúvida na relação da LGPD com outras legislações, em especial a relação com a Lei de Acesso à Informação (LAI)". Acerca dessa questão, um dos respondentes mencionou a dicotomia envolvendo ambas as legislações:

> Existe uma dicotomia [...] sobre a transparência e a privacidade, que são duas leis diferentes, dois princípios diferentes, mas que tratam dessas mesmas questões, né, da gestão dos dados, por meio da instituição. [...] Então… existem nuances de acordo com essas legislações que exigem que a gente tenha um nível de compreensão acerca das necessidades de tornar os processos cada vez mais transparentes e mais públicos, por uma… por uma questão de um exercício de controle social, mas ao mesmo tempo cumprindo o que prevê a Lei Geral de Proteção de Dados. [...] Então, existem muitas dúvidas por conta dessas dicotomias das várias legislações [...] (Entrevistado 2).

O termo dicotomia parece evidenciar a controvérsia existente sobre o tema, a aparente carência de integração entre as duas normas, prejudicando a compreensão e a compatibilidade entre seus princípios, ainda que ambas devam ser interpretadas de forma harmônica (Barbosa *et al.*, 2021). De fato, os contornos que envolvem a publicidade e a privacidade são formados por uma linha tênue. Para Almeida (2024, p. 58), contudo, a "LGPD não se sobrepõe à LAI, as leis necessitam coexistir, sendo divulgado o necessário para a transparência sem exceder o razoável quanto à quantidade de dados divulgados, bem como à necessidade de estarem totalmente visíveis".

Diante de tais complexidades, repise-se, é importante que os órgãos reguladores, notadamente a ANPD, ampliem gradualmente o escopo de sua atuação orientadora. Ainda que ações nesse sentido tenham sido registradas, percebe-se que a consolidação de práticas administrativas mais uniformes e seguras dependerá de um acompanhamento mais presente e de diretrizes que contribuam para mitigar as incertezas hermenêuticas e operacionais.

Por fim, apresenta-se a categoria Orçamento, que obteve 15 citações no estudo. Esse eixo temático agrega as unidades de registro que destacam a necessidade de investimento e as restrições orçamentárias como desafios críticos na implementação de práticas de conformidade com a legislação de proteção de dados. Nessa categoria, as entrevistas revelaram um equilíbrio entre os desafios para implementar práticas de proteção de dados pessoais sob a ótica dos partícipes. Consoante o Quadro 16, os temas inerentes às ponderações de cada um deles foram

registrados em duas unidades: necessidade de investimento (53,33%) e restrição de recursos financeiros e orçamentários (46,67%).

Quadro 16 - Análise da Categoria Orçamento

(continua)

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
15 (14,29)	Necessidade de investimento 8 (53,33%)	[...] os investimentos que a instituição está fazendo, na medida do possível, [...] que incluem tanto segurança como tecnologia de uma forma geral são caros, são tantos serviços e equipamentos dolarizados, então, assim, requer um certo investimento. [...] a gente tem uma certa dificuldade em relação a investimento. E1
		Outra coisa também, investimento. Não adianta você querer fazer tecnologia sem investimento. Acho que são duas coisas indissociáveis, tecnologia e investimento. Tem que ser feito investimento em equipamento [...]. Fortalecer esse setor que trabalha com a LGPD e o investimento em proteção [...] E1
		E a questão de investimento também. Como que eu posso dizer... os recursos de tecnologia, eles... Poxa, eu esqueci o nome da palavra agora. Eles vão perdendo valor ao longo do tempo [...]. Então, o ideal seria, a cada cinco anos, a instituição estar trocando os seus equipamentos. E1
		Então, eu diria que há um conjunto, tanto... o investimento, o engajamento [...] como também você ter mais pessoas pra atuar nessas questões operacionais [...] E2
		Então assim, precisa de mais recursos a nível de investimento, [...] como também no sentido de investimento. [...] Então, a gente teria que ter investimento a nível de *firewall* [...] Porque hoje a gente atua muito mais no apagar incêndio e no que a gente consegue apagar, porque também como a gente tem pouca ferramenta tecnológica [...], então isso dificulta. Então, eu acho que é investimento de uma forma geral, olhando um pouco mais para TI. E3
		Tecnológicos e financeiros, porque assim, esse tecnológico você precisa ter recursos financeiros para isso. E3
		Então, tudo isso precisa de investimentos financeiros [...] Financeiro, tecnológico [...]. E3
		[...] é uma das pendências que a gente tem, mas porque também requer uma ferramenta que possibilite esse inventário. Então, a gente, primeiro, tem que adquirir uma solução dessa que permita a gente fazer esse levantamento. [....] Mas como a gente não tem uma rede autenticada, também isso já vai dificultando [...] isso tudo depende de ferramenta tecnológica para ser adquirida e implantada dentro da instituição. E3
	Restrição de recursos financeiros e orçamentários 7 (46,67%)	É, recursos humanos e financeiros, né? Infelizmente os dois estão difíceis hoje, né? E1
		[...] a própria instituição [...] eu acho que isso é uma realidade da... de vários órgãos da Administração Pública Federal, têm uma dificuldade muito grande de [....] recursos financeiros. Então, você atender à legislação, [...] ao mesmo tempo que você tem uma restrição de [....] orçamento grande [...] E2
		Então, eu acho que esse é o principal fator que vem influenciando nessa dificuldade de engajamento, restrição de pessoal, de recursos [...] E2
		Já estou com formulários em mãos para propor um curso da LGPD. [...] O desafio é tornar isso sistemático, que esbarra também nessa

Nº de citação e frequência (%)	Unidade de registro	Unidade de contexto
		restrição. Orçamentária, porque esses cursos normalmente remuneram, no mínimo, o instrutor do curso, né? E2
		Eu mencionaria também a realização de eventos, que é algo que como eu já mencionei está limitado em relação à carência que a gente tem de [...] recursos financeiros [...] E2
		Eu acho que a principal seria essa questão de [...] restrições financeiras orçamentárias, essa é uma realidade de toda a instituição, eu me compadeço, inclusive, com a gestão da universidade que tem […] E2
		[...] o desafio principal seria em relação à... à escassez de pessoas e recursos financeiros, né, porque só pelos exemplos que eu dei aqui [...] tudo isso exige pessoas e recursos para que seja feito um planejamento [...] completo da Lei Geral de Proteção de Dados em âmbito institucional, né? E esse desafio financeiro, orçamentário e de pessoal ele é gigante, não só LGPD, mas em todas as áreas, né? Então eu acho que esse seria, se eu pudesse colocar como principal, seria ele [...] E2

Fonte: Dados da pesquisa (2025).

Ao analisar essa categoria, constatou-se que uma das unidades de contexto revela um obstáculo recorrente na Administração Pública: a demanda por investimentos contínuos em tecnologia e segurança da informação, conforme explicitado no seguinte depoimento:

> [...] os investimentos que a instituição está fazendo, na medida do possível, [...] que incluem tanto segurança como tecnologia de uma forma geral são caros, são tantos serviços e equipamentos dolarizados, então, assim, requer um certo investimento [...] a gente tem uma certa dificuldade em relação a investimento (Entrevistado 1).

A referência à dolarização dos insumos tecnológicos evidencia um fator macroeconômico extrínseco que impacta a capacidade de aquisição das instituições federais. Tais investimentos raramente são pontuais, dada a acelerada obsolescência tecnológica e a necessidade de atualização constante dos sistemas de segurança. Nesse contexto, mesmo havendo total comprometimento da instituição e conhecimento técnico para atender às exigências legais, é possível que a efetiva operacionalização da LGPD não se concretize, devido à fragilidade do suporte técnico e financeiro.

Outro ponto importante relaciona-se à restrição de recursos financeiros e orçamentários. De acordo com um dos entrevistados, em que pesem os múltiplos desafios enfrentados, a restrição orçamentária, ao lado da restrição de pessoal, são os principais entraves à implementação da LGPD:

> [...] o desafio principal seria em relação à… à escassez de pessoas e recursos financeiros, né, porque só pelos exemplos que eu dei aqui [...] tudo isso exige pessoas e recursos para que seja feito um planejamento [...] completo da Lei Geral de Proteção de Dados, em âmbito institucional, né? E esse desafio financeiro, orçamentário e de

> pessoal ele é gigante, não só LGPD, mas em todas as áreas, né? Então eu acho que esse seria, se eu pudesse colocar como principal, seria ele [...] (Entrevistado 2).

A escassez orçamentária afeta desde a aquisição de ferramentas tecnológicas - como sistemas de gestão de dados, *firewalls*, soluções de inventário e autenticação de rede - até a contratação de serviços especializados, treinamentos e consultorias externas, impactando diretamente a capacidade de resposta institucional frente às exigências legais e eventuais vazamentos de dados.

O entrevistado 2 evidenciou com clareza o peso da restrição orçamentária, revelando a dicotomia entre as obrigações legais impostas pela LGPD e a realidade fiscal das universidades públicas federais, ante a cobrança para que as instituições cumpram uma legislação complexa, sem que haja, contudo, a contrapartida orçamentária suficiente para garantir a sua efetividade.

Nesse sentido, as unidades de contexto dessa categoria revelaram dificuldades generalizadas de financiamento para cursos de capacitação, realização de eventos, aquisição de soluções tecnológicas, manutenção de infraestrutura e planejamento institucional. Há o reconhecimento da interdependência entre tecnologia e investimento, de modo que o cumprimento da legislação exige não apenas boas intenções, mas recursos concretos para a aquisição de equipamentos, ferramentas de segurança, treinamentos, capacitações e estruturação de equipes especializadas.

Nesse contexto, a análise do conteúdo das entrevistas apontou uma convergência entre os desafios apontados pelos participantes para a implementação da LGPD com algumas das fraquezas e das ameaças constantes da análise SWOT do PDTIC, constantes no Quadro 11. Apesar de preocupante, esse fato reforça que a entidade possui conhecimento das dificuldades para assegurar a conformidade à LGPD, o que é essencial para que sejam adotadas estratégias efetivas, em consonância com os dispositivos legais.

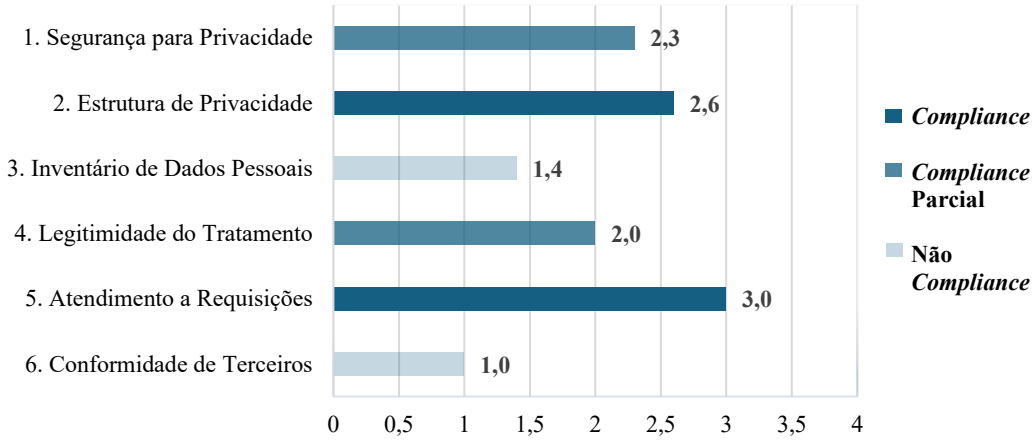
Por fim, a análise das quatro categorias revelou um panorama abrangente dos principais desafios enfrentados pela instituição na implementação da LGPD. Diante de tais evidências, torna-se fundamental medir o nível de maturidade institucional em relação à proteção de dados, o que será realizado na próxima seção, pois essa mensuração não apenas pode orientar o planejamento de ações corretivas e preventivas, como também tem o condão de subsidiar decisões estratégicas para garantir a conformidade legal e a efetividade da governança da informação.

4.3 NÍVEL DE MATURIDADE DA PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA UFRPE COM BASE NO *FRAMEWORK* PROPOSTO POR SANTANA E MENDONÇA (2023)

Os resultados obtidos a partir da aplicação do *framework,* adaptado da pesquisa desenvolvida por Santana e Mendonça (2023), contendo 31 questões, permitiram calcular o nível de maturidade da proteção de dados na UFRPE, a fim de avaliar "a adequação às legislações de privacidade (com foco na LGPD) e a adesão de boas práticas de proteção de dados pessoais" (Santana; Mendonça, 2023, p. 30).

As perguntas estão organizadas em seis seções temáticas, estruturadas conforme as principais áreas de gestão de privacidade e da proteção de dados pessoais (Santana; Mendonça, 2023, p. 31). No Gráfico 1 são apresentados os resultados das seis seções do questionário:

Gráfico 1 - Nível de maturidade e classificação dos controles de proteção de dados



Fonte: Dados da pesquisa (2025).

No geral, os resultados mostraram-se equilibrados, com duas seções classificadas como em *compliance* (Estrutura de Privacidade e Atendimento a Requisições), duas como em *compliance* parcial (Segurança para Privacidade e Legitimidade do Tratamento) e as duas

restantes como em não *compliance* (Inventário de Dados Pessoais e Conformidade de Terceiros).

Na primeira seção (Segurança para Privacidade), que contém 14 perguntas, a entidade apresentou média 2,3 de nível de maturidade, posicionando-se no patamar de *compliance* parcial. A Tabela 1 sintetiza as perguntas e as respostas, assim como as notas que lhes foram atribuídas:

Tabela 1 - Segurança para Privacidade

(continua)

1. Segurança para Privacidade	**Resposta**	**Nota**
1.1 A equipe de trabalho ou organização possui inventário de ativos sistêmicos[15] centralizado e atualizado?	Não	0
1.2 Os sistemas em que são armazenados dados pessoais possuem *backup*?	Sim	4
1.3 A organização ou equipe de trabalho conta com normativos de segurança da informação publicados e comunicados?	Sim	4
1.4 Os ativos sistêmicos da organização contam com recursos que controlem acesso físico e lógico?	Parcialmente	2
1.5 Os dados pessoais processados nos ativos sistêmicos da organização são criptografados em trânsito e em repouso?	Não	0
1.6 A organização ou a equipe de trabalho conta com plano de continuidade de negócios e recuperação de desastres?	Sim	4
1.7 Os *data centers* físicos gerenciados pela organização possuem infraestrutura de segurança nos termos da ISO27001?	Parcialmente	2
1.8 Regras de gestão de acessos aos sistemas de acordo com a necessidade e adequação de cada colaborador (controle de acessos e segregação de funções)?	Parcialmente	2
1.9 É mantida trilha de auditoria de acesso, edição, cópia ou deleção de dados em todos os ativos da empresa que possuem dados pessoais?	Parcialmente	2
1.10 São aplicadas regras de anonimização, pseudonimização e/ou mascaramento aos dados pessoais?	Parcialmente	2
1.11 A organização ou equipe de trabalho possui Comitê de Segurança da Informação?	Sim	4
1.12 A companhia estabeleceu regras para a utilização de dispositivos eletrônicos corporativos ou pessoais?	Parcialmente	2
1.13 A organização ou equipe de trabalho conta com medidas de controle de segurança para acesso à rede da empresa?	Parcialmente	2
1.14 A organização utiliza plataformas colaborativas seguras para fins de comunicações profissionais?	Parcialmente	2
	Nível de Maturidade	**2,3**
	Classificação: *Compliance* parcial	

Fonte: Dados da pesquisa (2025).

[15] No âmbito da segurança da informação e proteção de dados, definem-se como ativos sistêmicos quaisquer recursos, físicos ou lógicos, que detenham valor para uma organização e que demandem proteção contra ameaças. Esses ativos abrangem desde dados e informações sigilosas até a infraestrutura de TI, incluindo servidores, computadores, *softwares* e redes.

Nessa seção, verifica-se que a organização atende, ao menos parcialmente, à maioria dos aspectos relacionados à Segurança para Privacidade. No entanto, merece destaque a resposta ao item 1.5, isto é, a ausência de criptografia no processamento dos dados pessoais, denotando relativa fragilidade em relação a aspectos de segurança importantes da proteção de dados.

Uma vez que o art. 46 da LGPD determina aos agentes de tratamento a adoção de "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 [...] ou qualquer outra forma de tratamento inadequado ou ilícito", recomenda-se o investimento em mecanismos de criptografia, caso tais recursos estejam ao alcance da instituição, uma vez que sua ausência pode ensejar vulnerabilidade à segurança, à disponibilidade e à integridade dos dados pessoais sob custódia da organização. Essa recomendação coaduna-se com as orientações de Santos Filho e Jesus (2023, p. 285), que destacam a necessidade de medidas técnicas e organizacionais, que incluem "a criptografia de dados, controle de acesso, anonimização ou pseudonimização de informações sensíveis e realização de *backups* regulares".

Na segunda seção, Estrutura de Privacidade, composta por dez perguntas, atribuiu-se ao ente a média 2,6, correspondente à classificação de *compliance*, conforme detalhado na Tabela 2, a qual apresenta as respostas fornecidas para cada item e suas respectivas pontuações:

Tabela 2 - Estrutura de Privacidade

2. Estrutura de Privacidade	**Resposta**	**Nota**
2.1 Há uma estrutura organizacional de governança para privacidade?	Parcialmente	2
2.2 Um programa de privacidade foi estabelecido?	Parcialmente	2
2.3 Há uma matriz de riscos de privacidade ou alguma identificação dos possíveis riscos?	Não	0
2.4 Foi nomeado um DPO (Encarregado pelo Tratamento de Dados)?	Sim	4
2.5 A organização conta com equipe/comitê de privacidade?	Sim	4
2.6 A equipe de trabalho é constantemente conscientizada acerca da proteção de dados e privacidade?	Parcialmente	2
2.7 Há algum canal para contato e interação entre titular e encarregado?	Sim	4
2.8 Foram estabelecidas políticas, normas e procedimentos de privacidade?	Sim	4
2.9 A organização ou equipe já possui políticas de privacidade (interna e externa) publicadas e comunicadas?	Sim	4
2.10 A organização ou equipe estabeleceu matriz RACI para distribuição dos papéis e responsabilidades em privacidade?	Não	0

Nível de Maturidade	**2,6**
Classificação: *Compliance*	

Fonte: Dados da pesquisa (2025).

A criação de um comitê de segurança da informação, representado pelo Subcomitê de Segurança da Informação (SSIC), de um comitê de privacidade, formalizado pelo Comitê Gestor de Privacidade de Proteção de Dados (CGPPD); e de uma política de privacidade interna, consubstanciada na Política de Privacidade e Proteção de Dados Pessoais (PPPDP), representa um ponto relevante na governança de dados. Quanto a essa última, dado que um dos desafios das instituições públicas de ensino corresponde à elaboração de políticas de proteção de dados (Barbosa *et al*., 2021), a UFRPE evidencia uma certa maturidade nesse item, haja vista a edição de diversas normativas nesse sentido, conforme constatado na análise documental debatida na Seção 4.1. Para Santos Filho e Jesus (2023), é importante que sejam instituídas políticas que abordem aspectos como consentimento do titular e segurança da informação., haja vista a edição de diversas normativas nesse sentido, conforme constatado na análise documental debatida na Seção 4.1. Para Santos Filho e Jesus (2023), é importante que sejam instituídas políticas que abordem aspectos como consentimento do titular e segurança da informação.

Outro fator positivo se refere à nomeação do EPD. Para Santos Filho e Jesus (2023, p. 285), "a designação de um Encarregado de Proteção de Dados (DPO) é essencial" no processo de adequação à LGPD. Em contrapartida, a Universidade ainda não dispõe de uma matriz de riscos de privacidade, bem como de uma matriz RACI[16] para a distribuição dos papéis e das responsabilidades naquele processo. Sem esses instrumentos, os esforços organizacionais voltados à responsabilização e à prevenção e mitigação de vulnerabilidades internas podem ser prejudicados, o que tende a enfraquecer a eficácia de medidas de controle. Além do mais, essa ausência poderá comprometer algumas ações importantes para subsidiar a conformidade à LGPD, dentre elas a criação de um plano de ação, a definição dos responsáveis por gerir o processo e o mapeamento de sistemas que manipulam dados pessoais ou sensíveis (Rojas, 2020).

[16] A Matriz RACI, igualmente denominada Matriz de Responsabilidades, consiste em um instrumento visual empregado na gestão de projetos, com a finalidade de delimitar e comunicar as funções e responsabilidades atribuídas a cada integrante da equipe em relação às atividades e entregas previstas. O acrônimo RACI corresponde aos quatro papéis principais: *Responsible* (Responsável), *Accountable* (Responsável/Aprovador), *Consulted* (Consultado) e *Informed* (Informado).

Na terceira seção, Inventário de Dados Pessoais, que reúne sete perguntas e cuja média foi 1,4, a instituição foi enquadrada na classificação de não *compliance*. Na Tabela 3 constam as perguntas, suas respectivas respostas e as notas delas decorrentes:

Tabela 3 - Inventário de Dados Pessoais

3. Inventário de Dados Pessoais	**Resposta**	**Nota**
3.1 Todos os dados pessoais tratados foram identificados e classificados ou pelo menos há mecanismo para fazê-los?	Parcialmente	2
3.2 Todos os dados sensíveis tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	Parcialmente	2
3.3 Todos os dados pessoais de menores de idade tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	Parcialmente	2
3.4 Todos os dados pessoais de estrangeiros tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	Parcialmente	2
3.5 O inventário de dados pessoais já foi estabelecido?	Não	0
3.6 A equipe conta com mecanismos, já implementados, para o gerenciamento do ciclo de vida dos dados pessoais?	Parcialmente	2
3.7 Existe regra de temporalidade definida para a retenção de dados pessoais, incluindo a retenção embasada em legislações específicas?	Não	0
	Nível de Maturidade	**1,4**
	Classificação: Não *compliance*	

Fonte: Dados da pesquisa (2025).

A identificação e a classificação dos dados são etapas essenciais para o processo de adequação à LGPD. Elas viabilizam o conhecimento sobre quais dados estão sendo tratados, em que sistemas estão armazenados, quem a eles tem acesso e com qual finalidade. A resposta "parcialmente" indica que a instituição possui algum nível de mapeamento de dados, mas ainda não de forma completa e abrangente.

Santos Filho e Jesus (2023, p. 285) enfatizam a necessidade do detalhamento dos dados tratados pela instituição, o que inclui "identificar suas fontes, fluxos de processamento, armazenamento e finalidades", de modo que seja "possível mapear todo o ciclo de vida dos dados, identificando potenciais vulnerabilidades ou riscos à privacidade".

Para além disso é importante que se observe que a universidade não dispõe de dois instrumentos essenciais, citados nos itens 3.5 e 3.7, da Tabela 3, quais sejam: um inventário de dados pessoais e uma regra de temporalidade definida para a retenção de dados pessoais. Quanto ao primeiro, representa um dos pontos de maior atenção. O inventário é a base sobre a qual se constroem outras práticas de governança, como definição de base legal, controle de

acesso, gestão de riscos e compartilhamento de dados (Brasil, 2023b). Isso compromete diretamente os esforços da organização e a expõe a sanções administrativas passíveis de aplicação pela ANPD.

Em sua pesquisa, Souza (2022, p. 119) verificou que grande parte das IFES ainda não desenvolveu o inventário de dados pessoais, sendo comum a compreensão de que se trata de uma atividade complexa e que demanda elevada carga de trabalho, o que converge para os desafios já documentados na seção 4.2 deste estudo.

No que se refere ao segundo instrumento, a regra de temporalidade, o art. 16 da LGPD determina a eliminação dos dados pessoais após o fim da sua finalidade, salvo nas hipóteses legais de conservação, ao passo que o princípio da necessidade preceitua que o tratamento deve ser limitado ao mínimo indispensável para atingir a finalidade pretendida (Brasil, 2018b).

Nesse sentido, a falta de uma política de retenção, de modo que porventura não se saiba até quando e para qual finalidade os dados pessoais estão sendo armazenados, além de destoar do princípio da necessidade, fragiliza a estrutura de governança informacional, contribuindo para a elevação do risco institucional de exposição a vazamentos e de uso indevido dos dados pessoais não eliminados.

Por sua vez, na quarta seção, Legitimidade do Tratamento, em que foram respondidas dez perguntas, atribuiu-se ao ente a média 2,0, alcançando-se a classificação de *compliance* parcial. A Tabela 4 detalha as respostas obtidas para cada questão, com as respectivas notas atribuídas a cada item:

Tabela 4 - Legitimidade do Tratamento

4. Legitimidade do Tratamento	**Resposta**	**Nota**
4.1 Foram atribuídas bases legais a todas as operações de tratamento de forma adequada?	Não	0
4.2 A organização possui meios de garantir que os dados pessoais são tratados de acordo com finalidades adequadas?	Parcialmente	2
4.3 A organização dispõe de meios para garantir que apenas dados pessoais necessários são tratados?	Parcialmente	2
4.4 A organização possui meios para comprovar a coleta do consentimento para o tratamento de dados que necessitem de tal base legal?	Parcialmente	2
4.5 A organização coleta o consentimento dos responsáveis para o tratamento de dados de crianças?	Parcialmente	2
4.6 A organização possui critério para avaliar o legítimo interesse da organização (LIA - Avaliação de Legítimo Interesse[17])?	Não	0

[17] Contempla a necessidade de que o "controlador somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas", devendo, por exemplo, proteger "em relação ao titular, o exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais" (Brasil, 2018b, p.60-61)

4.7 A organização possui meios de assegurar que o titular tenha livre acesso a seus dados pessoais?	Sim	4
4.8 A organização possui entendimento acerca da sua atuação como operadora e/ou controladora de dados?	Sim	4
	Nível de Maturidade	**2,0**
	Classificação: *Compliance* parcial	

Fonte: Dados da pesquisa (2025).

Embora a UFRPE também tenha atendido à maioria dos critérios nesse segmento, ainda que parcialmente, observam-se duas respostas negativas, referentes aos itens 4.1 (atribuição de bases legais a todas as operações de tratamento) e 4.6 (critérios para avaliar o legítimo interesse da organização).

O art. 7º e o art. 11º da LGPD estabelecem, respectivamente, as bases legais para o tratamento de dados pessoais e de dados pessoais sensíveis, tais como o consentimento, obrigação legal, execução de políticas públicas e outras. A ausência dessa designação viola os referidos dispositivos e impossibilita a demonstração de conformidade, podendo tornar o tratamento ilegal. Assim, a fim de se adequar, a organização precisa conduzir um mapeamento de suas atividades de tratamento e, para cada uma, vincular a base legal adequada, devendo tratar tal ponto com prioridade.

Por outro lado, são sinais positivos de maturidade institucional as respostas afirmativas aos itens 4.7 (meios de assegurar que o titular tenha livre acesso a seus dados pessoais) e 4.8 (entendimento da organização acerca de sua atuação como operadora e/ou controladora de dados). No primeiro caso, tem-se a manifestação concreta de cumprimento do preceito contido no art. 18, II, da LGPD, o que pode vir a contribuir para um maior índice de confiança do usuário na UFRPE. Quanto ao segundo, o reconhecimento do papel institucional no tratamento de dados pessoais, além de ser crucial para o planejamento, é fundamental para a delimitação de obrigações, fluxos e riscos no âmbito da segurança da informação e da proteção de dados.

Já na quinta seção, Atendimento a Requisições, composta por oito perguntas, a universidade atingiu a média 3,0, estabelecendo-se na classificação de *compliance*. Na Tabela 5, a seguir, são apresentadas as respostas e as notas relativas a cada questão:

Tabela 5 - Atendimento a Requisições

5. Atendimento a Requisições	**Resposta**	**Nota**
5.1 A organização de trabalho possui mecanismo para realizar o atendimento a requisições de titulares de dados?	Sim	4

5.2 A organização já realizou atendimento a requisições de titulares de dados?	Sim	4
5.3 A organização já eliminou dados pessoais a pedido do titular?	Sim	4
5.4 A organização possui meios para registrar e evidenciar que o atendimento às requisições de direitos dos titulares dos dados pessoais foi realizado?	Sim	4
5.5 A organização de trabalho já elaborou um modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?	Não	0
5.6 A organização já realizou um Relatório de Impacto à Proteção de Dados?	Não	0
5.7 A organização possui meios de identificar, registrar e tratar violações de privacidade?	Sim	4
5.8 A organização de trabalho possui mecanismos para informar ao titular e à ANPD acerca de violações à privacidade?	Sim	4
	Nível de Maturidade	**3,0**
	Classificação: *Compliance*	

Fonte: Dados da pesquisa (2025).

Em relação a essa seção, a entidade mais uma vez respondeu afirmativamente à maioria das indagações, o que indica um nível avançado de maturidade nesse domínio. Como pontos positivos, destacam-se: a existência de mecanismos para atender a requisições dos titulares; o efetivo atendimento a essa requisições; a eliminação de dados a pedido dos titulares; os meios de comprovação do atendimento às requisições; a existência de meios para identificar; registrar e tratar as violações de privacidade e a existência de mecanismos para informar ao titular e à ANPD sobre episódios de violações à privacidade; todos fatores que contribuíram para o bom desempenho nesse segmento.

Em contraponto, a instituição não elaborou um modelo de Relatório de Impacto à Proteção de Dados Pessoais, tampouco produziu o próprio RIPD. Este documento, contudo, não é de confecção obrigatória, sendo exigido apenas em situações específicas (Brasil, 2018b). Assim, embora digna de atenção, a resposta negativa não configura, à primeira vista e por si só, um indicativo de criticidade elevada, salvo se sua apresentação já houver sido formalmente demandada pela ANPD em momento anterior.

É importante destacar, porém, que, na hipótese de ser exigido, é imprescindível que, ao menos, tenha sido iniciado o processo de elaboração do inventário de dados pessoais, haja vista que, de acordo com Souza (2022), a confecção do RIPD pressupõe a constituição - ou, no mínimo, o início - de um inventário de dados.

Por fim, na sexta e última seção, formada por apenas duas perguntas, a nota obtida foi 1,0, com classificação de não *compliance*. A Tabela 6, a seguir, apresenta as perguntas, as respostas e a suas respectivas notas:

Tabela 6 - Conformidade de Terceiros

6. Conformidade de Terceiros	**Resposta**	**Nota**
6.1 A equipe elaborou cláusula de privacidade e atualizou contratos padrões?	Parcialmente	2
6.2 A equipe aditou contratos existentes com cláusulas de privacidade?	Não	0
	Nível de Maturidade	**1,0**
	Classificação: Não *compliance*	

Fonte: Dados da pesquisa (2025).

Nessa seção, foi atribuída à instituição a pior avaliação relacionada ao nível de maturidade, com uma resposta parcialmente afirmativa e outra negativa. De acordo com Santos Filho e Jesus (2023, p. 282), "os agentes de tratamento são responsáveis por garantir que seus contratados e parceiros de negócios também cumpram com as disposições da LGPD. Isso pode ser feito por meio da inclusão de cláusulas específicas relacionadas à proteção de dados nos contratos firmados com terceiros". Desse modo, a formalização contratual clara e específica é relevante para delimitar responsabilidades, prever obrigações de segurança, confidencialidade e mecanismos de resposta a incidentes.

Na questão 6.1, a resposta "Parcialmente" revela que a instituição começou a adequar seus contratos padrões à LGPD, incluindo cláusulas de privacidade, mas ainda não concluiu essa atualização. Trata-se de uma iniciativa fundamental, considerando que o art. 42 da norma estabelece a responsabilidade solidária entre o controlador e o operador em casos de danos decorrentes do tratamento irregular de dados (Brasil, 2018b).

Já a resposta do item 6.2 evidencia a inexistência de aditamento dos contratos existentes. Mesmo que novos contratos estejam sendo atualizados com cláusulas de proteção de dados (como indicado no item anterior), os contratos em vigor, notadamente aqueles com duração prolongada e com operadores de dados externos à instituição, devem ser adequados à LGPD, estabelecendo-se obrigações e critérios mínimos para tratamento seguro, a fim de evitar que se tornem fontes de riscos legais.

Por fim, como avaliação geral, os resultados demonstraram que a organização atingiu a média 2,05, situando-se atualmente no nível intermediário de maturidade em relação à LGPD, isto é, *compliance* parcial. Esse fato demanda atenção por parte da instituição, pois o *compliance* contribui para o respeito às normas e à ética e, especificamente na seara dos dados pessoais, relaciona-se ao cumprimento dos direitos dos titulares desses dados (Garbaccio; Vaddel; Torchia, 2022). Desse modo, esse nível mediano de maturidade, embora revele

avanços, conduz à conclusão de que, na prática, tais direitos não estão sendo plenamente assegurados, o que contraria os dispositivos da LGPD.

Na Tabela 7, estão representadas as médias de cada seção, bem como a média global atribuída ao ente.

Tabela 7 - Avaliação Geral

Controles de proteção de dados	Nível de maturidade	Classificação
1. Segurança para Privacidade	2,3	Compliance parcial
2. Estrutura de Privacidade	2,6	Compliance
3. Inventário de Dados Pessoais	1,4	Não compliance
4. Legitimidade do Tratamento	2,0	Compliance parcial
5. Atendimento a Requisições	3,0	Compliance
6. Conformidade de Terceiros	1,0	Não compliance
Nível de Maturidade	**2,05**	***compliance* parcial**

Fonte: Dados da pesquisa (2025).

Conforme previamente assinalado, destaca-se, de forma particularmente relevante e positiva, o nível de maturidade alcançado nas seções Estrutura de Privacidade e Atendimento a Requisições, cujas médias foram, respectivamente, 2,6 e 3,0. Em sentido oposto, contudo, observou-se um desempenho insatisfatório nas seções Inventário de Dados Pessoais e Conformidade de Terceiros, face às médias 1,4 e 1,0, respectivamente, demandando maior atenção da entidade.

Diante dos pontos de fragilidade identificados ao longo da análise dos dados obtidos mediante a aplicação do *framework* proposto por Santana e Mendonça (2023), será apresentado, na próxima seção, um produto técnico-tecnológico, com vistas a fomentar o fortalecimento da proteção de dados no contexto da instituição.

4.4 DIAGNÓSTICO E PROPOSIÇÃO DE AÇÕES PARA FORTALECER A PROTEÇÃO DE DADOS PESSOAIS NA UFRPE (PTT)

A partir de uma análise pormenorizada, e em consonância com a proposta deste programa de pós-graduação, foi realizado um diagnóstico das práticas institucionais da UFRPE no tocante à proteção de dados pessoais, a fim de recomendar ações na universidade *lócus* do estudo, a fim de recomendar ações na universidade lócus do estudo, identificando-se

fragilidades, riscos e possibilidades de melhoria. Com base nesse levantamento, buscou-se elaborar um produto técnico-tecnológico, contendo recomendações voltadas ao fortalecimento da proteção de dados, para subsidiar a adequação à LGPD no âmbito da UFRPE, contemplando dimensões técnicas, organizacionais e de governança. O conteúdo integral do diagnóstico, incluindo a fundamentação teórica, bem como as propostas de ação, está reunido no Apêndice B desta dissertação, servindo como referência para a eventual implementação das medidas sugeridas.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como propósito investigar como a LGPD vem sendo aplicada no âmbito da UFRPE. Numa análise inicial, constatou-se que o planejamento estratégico da organização, com vigência para o período 2021-2030, estabeleceu a meta de adequação à LGPD até o ano de 2025. Isso despertou o interesse em realizar esta pesquisa, combinando análise documental, entrevistas e aplicação de *framework* de proteção de dados. A partir dessa tríade, foi possível compreender as ações que vêm sendo promovidas, os desafios enfrentados e o nível de maturidade da instituição, com o fito de propor recomendações para aprimoramento da proteção de dados pessoais.

Para tanto, na condução deste trabalho, buscou-se seguir todas as disposições constantes no capítulo metodológico, assim como houve a preocupação em se analisar com profundidade os resultados encontrados, explorando o quadro teórico, o que enriqueceu a dimensão interpretativa desta dissertação. Nesse sentido, todos os objetivos propostos foram atendidos.

Quanto ao primeiro objetivo específico, constatou-se que têm sido realizadas ações para promover a proteção de dados pessoais, dentre as quais: a instituição de política de privacidade; estruturação de comitê gestor, envolvendo vários setores da entidade; ações de sensibilização, contemplando a divulgação de cursos e materiais educativos; e treinamentos voltados ao corpo técnico-especializado em tecnologia.

Identificou-se que, embora os setores responsáveis pela proteção de dados tenham se dedicado com afinco, elaborando normas como a Política de Proteção de Privacidade e Proteção de Dados Pessoais e estruturas como o Comitê Gestor de Privacidade e Proteção de Dados, a efetivação das diretrizes ainda enfrenta desafios operacionais e estratégicos.

Apesar dessas ações promissoras, foi possível identificar os desafios a serem superados pela entidade, a fim de atender ao segundo objetivo específico. Nesse sentido, as dificuldades estão relacionadas, sobretudo, à complexidade universitária, à carência de recursos humanos, à limitação de investimentos e às restrições orçamentárias. Quanto a estas últimas, percebeu-se a forte influência que exercem nas ações planejadas pela instituição, dificultando o incremento do quadro de pessoal e a modernização da infraestrutura tecnológica, além de ações educativas. Além desses desafios, o caráter incipiente da legislação e as lacunas regulatórias também foram apontadas como óbices.

Ainda como desafios, a despeito da predisposição dos servidores, notadamente aqueles que atuam na área de proteção de dados, em colaborar com a adequação da organização à

norma, a indisponibilidade de tempo devido à sobrecarga de trabalho inviabiliza suas participações.

Tem-se também que o Programa "UFRPE Digital" e os diversos planos institucionais (PDI, PDTIC, PDA) revelam a intenção da Universidade em promover uma transformação digital e segura, pautada na governança de dados, alinhando-se às diretrizes da LGPD. Contudo, a existência de metas ainda não plenamente atingidas, como a conformidade total dos serviços à LGPD até 2025, indica que, apesar dos esforços, há fatores internos e externos que inviabilizam o alcance do objetivo.

Após identificar as ações e os desafios para promover a proteção de dados pessoais, foi possível analisar o nível de maturidade da instituição, o que correspondeu ao terceiro objetivo específico. Com base num *framework*, elaborado a partir de normas internacionais que tratam do tema, evidenciou-se que a UFRPE encontra-se num nível intermediário de maturidade em relação à LGPD.

Sendo assim, conclui-se que a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da UFRPE com esforços consistentes da instituição para adequar-se à normativa, implementando ações importantes como a criação de políticas, comitês, capacitações e iniciativas voltadas à conscientização da comunidade acadêmica. Tais iniciativas demonstram um comprometimento da autarquia na construção de uma cultura de privacidade e proteção de dados, conforme demonstrado na análise documental e nos depoimentos dos participantes da pesquisa.

No entanto, a consolidação completa dessa adequação ainda enfrenta desafios estruturantes e operacionais, que, em parte, ultrapassam a capacidade de gestão da própria Universidade. Dentre essas dificuldades, ressaltam-se a limitação orçamentária, a excessiva demanda sobre os servidores, a falta de infraestrutura robusta, especialmente tecnológica, e a carência de capacitação técnica continuada, fatores recorrentes em instituições públicas de ensino superior e confirmados pelos dados levantados neste estudo.

Logo, ainda que a UFRPE apresente um estágio intermediário em relação à LGPD, conforme verificado na aplicação do *framework*, o avanço para níveis mais elevados dependerá de investimentos contínuos e de apoio das instâncias superiores da Administração Pública, com a elaboração de políticas mais efetivas para auxiliar na implementação da LGPD, bem como com a destinação de dotações orçamentárias à instituição, garantindo assim a proteção dos direitos fundamentais à privacidade e à segurança dos dados pessoais.

Esta pesquisa traz como contribuição a ampliação da compreensão acerca do processo de implementação da LGPD em entidades públicas, com destaque para as universidades, dada a predominância de estudos que tratam, apenas, de aspectos jurídicos em detrimento de questões relacionadas à Administração Pública. Como contribuição prática, em consonância com o quarto objetivo específico, foi elaborado um relatório técnico com proposta de ações para aprimorar a proteção de dados pessoais na UFPE. Além disso, os resultados da pesquisa podem servir de *insights* para outras universidades ou instituições públicas que buscam fortalecer suas políticas de proteção de dados pessoais, de privacidade e de segurança da informação.

Como limitações desta pesquisa, tem-se as inerentes ao método do estudo de caso, que impede a generalização dos resultados, bem como as subjetividades envolvidas nas respostas dos entrevistados. No tocante a recomendações para estudos futuros, sugere-se a realização de trabalhos voltados à aplicação da LGPD em outras universidades, instituições públicas ou ainda que sejam realizados sob o prisma dos usuários.

REFERÊNCIAS

AGUILERA, Daniel Fortes; DI BIASE, Nicholas Furlan. Dificuldades Interpretativas no regime de tratamento de dados pelo Poder Público: lacunas, contradições e atecnias na LGPD. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro – PGE-RJ**, Rio de Janeiro, v. 4, n. 2, p. 1-30, maio/ago. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238. Acesso em: 14 ago. 2024.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, n. 3, p. 26-45, jul./set. 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc. Acesso em: 14 ago. 2024.

ALMEIDA, Willdson Gonçalves de. **Implementação de compliance à LGPD em instituições federais de ensino superior**: proposta de um processo estruturado para conformidade. 2024. 133 f. Dissertação (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação Profissional em Engenharia de Produção, Universidade Federal de São Carlos, São Carlos, 2024. Disponível em: https://repositorio.ufscar.br/items/2802852a-482e-4f98-9ca3-17e263287180. Acesso em: 08 jul 2025.

BARBOSA, Tatiane Santos; LOPES, Jerisnaldo Matos; PIAU, Deise Danielle Neves Dias; SILVA, Marcelo Santana; TELES, Eduardo Oliveira. A Lei Geral de Proteção de Dados (LGPD) nas Instituições Públicas de Ensino: Possíveis Impactos e Desafios. **Anais do VII Encontro Nacional de Propriedades Intelectuais (ENPI)**, Aracaju, v. 07, n. 1, p. 2114-2123, set. 2021. Disponível em: https://api.org.br/conferences/ENPI2021/ENPI2021/paper/view/1455. Acesso em: 14 ago. 2024.

BARDIN, Laurence. **Análise de conteúdo.** São Paulo: Edição 70, 2016.

BARROS, Aidil Jesus da Silveira; LEHFELD, Neide Aparecida de Souza. **Fundamentos de metodologia científica.** 3. ed. São Paulo: Pearson Prentice Hall, 2007.

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no Setor Público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos jurídicos**, São Paulo, ano 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2020/05/ii_7_cadernos_juridicos_epm.pdf. Acesso em: 01 fev. 2025.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção de dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência**, Florianópolis, n. 68, p. 109-127, jun. 2014. Disponível em: https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/abstract/?lang=pt. Acesso em: 14 ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 abr. 2023.

BRASIL. **Lei nº 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. 1998. Disponível em:https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 02 fev. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 28 abr. 2023.

BRASIL. **Lei nº 11.091, de 12 de janeiro de 2005**. Dispõe sobre a estruturação do Plano de Carreira dos Cargos Técnico-Administrativos em Educação, no âmbito das Instituições Federais de Ensino vinculadas ao Ministério da Educação, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11091.htm. Acesso em: 09 jul 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20112014/2011/lei/l12527.htm. Acesso em: 28 abr. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 ago. 2024.

BRASIL. **Decreto nº 8.789, de 29 de junho de 2016.** Dispõe sobre o compartilhamento de bases de dados na administração pública federal. 2016. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 02 ago. 2024.

BRASIL. **Decreto nº 9.319, de 21 de março de 2018**. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para Transformação Digital. 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Acesso em: 18 mar. 2025.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 28 abr. 2023.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. 2018c. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 18 mar. 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. 2019a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 18 mar. 2025.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 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. 2019b. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 03 ago. 2024.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. 2020a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 20 mar. 2025.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. 2020b. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2020/decreto-10332-28-abril-2020-790138-publicacaooriginal-160559-pe.html. Acesso em: 30 maio 2024.

BRASIL. Advocacia-Geral da União. Consultoria-Geral da União. Consultoria Jurídica junto à Controladoria-Geral da União. **Parecer nº 00001/2021/CONJUR-CGU/CGU/AGU**. Trata da compatibilização entre a LGPD e a Lei de Acesso à Informação no contexto da Administração Pública. Brasília, 2021a. Disponível em:https://repositorio.cgu.gov.br/handle/1/67796. Acesso em: 13 jul. 2025.

BRASIL. **Decreto nº 10.748, de 16 de julho de 2021**. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. 2021b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm.Acesso em: 20 mar. 2025.

BRASIL. **Acórdão nº 2164, de 15 de setembro de 2021**. Acompanhamento dos índices de governança e gestão dos órgãos da Administração Pública Federal - Ciclo 2021. 2021c. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2164%2520ANOACORDAO%253A2021%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em: 08 jul. 2025.

BRASIL. Emenda Constitucional n. 115**.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União:** seção 1, Brasília, DF, ano 160, n. 30, p. 2, 11 fev. 2022a. Disponível em:https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 14 ago. 2024.

BRASIL. Advocacia-Geral da União. Consultoria-Geral da União. Consultoria Jurídica junto à Controladoria-Geral da União. **Parecer nº 00093/2022/CONJUR-CGU/CGU/AGU**. Complementa o Parecer nº 00001/2021/CONJUR-CGU/CGU/AGU no tocante à publicidade do CPF em atos administrativos, reafirmando a necessidade descaracterização parcial do dado, com base em interpretação sistemática da LGPD e da LAI. Brasília, 2022b. Disponível em:https://repositorio.cgu.gov.br/handle/1/67796. Acesso em: 13 jul. 2025.

BRASIL. **Acórdão nº 1.384, de 15 de junho de 2022**. Relatório de auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais. 2022c. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY:ACORDAO-COMPLETO-2521877/NUMACORDAOINT%20asc/0. Acesso em: 08 jul. 2025.

BRASIL. **Portaria nº 6.543, de 16 de novembro de 2022**. Aprova a Estratégia Brasileira para a Transformação Digital (E-Digital) para o ciclo 2022-2026. 2022d. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCT_n_6543_de_16112022.html#:~:text=Aprova%20a%20Estrat%C3%A9gia%20Brasileira%20para,lhes%20s%C3%A3o%20conferidas%20pelo%20art. Acesso em: 08 jul. 2025.

BRASIL. **Decreto nº 11.260, de 22 de novembro de 2022**. Dispõe sobre a elaboração e o encaminhamento da Estratégia Nacional de Governo Digital e prorroga o período de vigência da Estratégia de Governo Digital, instituída pelo Decreto nº 10.332, de 28 de abril de 2020. 2022e. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11260.htm. Acesso em: 08 jul 2025.

BRASIL. **Portaria nº. 852, de 28 de março de 2023**. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). 2023a. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 18 maio 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia de elaboração de inventário de dados pessoais**. Versão 2.0. Brasília, 2023b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 08 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Estudo técnico sobre anonimização de dados na LGPD: uma visão de processo baseada em risco e técnicas computacionais**. Versão 1.0. Brasília, 2023c. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf. Acesso em: 13 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Normatização. **Nota Técnica nº 85/2023/CGN/ANPD**. Versa sobre o tratamento de dados pessoais em contratos administrativos, especialmente quanto à substituição do CPF pela matrícula Siape. Brasília, 2023d. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sei_4801224_nota_tecnica_85-2-1.pdf. Acesso em: 13 jul. 2025.

BRASIL. Advocacia-Geral da União. Consultoria-Geral da União. Câmara Nacional de Convênios e Instrumentos Congêneres. **Parecer nº 00001/2024/CNCIC/CGU/AGU**. Trata da da aplicabilidade da LGPD aos convênios e instrumentos congêneres no âmbito da

Administração Pública. Brasília, 2024a. Disponível em: https://www.gov.br/transferegov/pt-br/comunicados/arquivos-e-imagens/parecer-n-00001-2024.pdf. Acesso em: 13 jul. 2025.

BRASIL. Advocacia-Geral da União. Consultoria-Geral da União. Consultoria Jurídica junto à Controladoria-Geral da União. **Parecer nº 00177/2024/CONJUR-CGU/CGU/AGU**. Versa sobre o tratamento e tarjamento de dados pessoais em publicações institucionais no contexto da transparência ativa, 2024b. Disponível em:https://repositorio.cgu.gov.br/bitstream/1/93365/1/Parecer_177_2024_CONJUR_CGU_AGU_tarjamento.pdf. Acesso em: 14 jul. 2025.

BRASIL. **Decreto nº 12.198, de 24 de setembro de 2024**. Institui a Estratégia Federal de Governo Digital para o período de 2024 e 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. 2024c. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2024/decreto-12198-24-setembro-2024-796286-publicacaooriginal-173095-pe.html. Acesso em: 08 jul. 2025.

BRASIL. **Portaria nº 6.618, de 25 de setembro de 2024**. Estabelece os princípios, os objetivos e as iniciativas para o alcance da Estratégia Federal de Governo Digital para o período de 2024 a 2027, no âmbito dos órgãos e das entidades da administração pública federal, direta, autárquica e fundacional. 2024d. Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-6.618-de-25-de-setembro-de-2024-586759348. Acesso em: 08 jul. 2025.

BRASIL. Infraestrutura Nacional de Dados. 2025. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados. Acesso em: 25 mar 2025.

CARVALHO, Hannibal Escobar Ramos Henriques de; FREITAG, Alberto Eduardo Besser; SANTOS, Daiane Rodrigues dos. Impactos da implantação da Lei Geral de proteção de dados pessoais no brasil: uma análise bibliométrica. **Revista de Gestão e Secretariado (GeSec)**, São Paulo, v. 13, n. 3, p. 1398-1411, set/dez. 2022. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/1412. Acesso em: 08 jul. 2025.

CARVALHO, Lucas Borges. O poder público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo.** v. 282, n. 2, p. 133-162, maio/ago. 2023. Disponível em: https://periodicos.fgv.br/rda/article/view/89347. Acesso em: 14 ago. 2024.

CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a Administração Pública brasileira. **Revista de Direito, Governança e Novas Tecnologias.** Maranhão, v3, n.2, p. 39-58, jul./dez. 2017. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/2471/0. Acesso em: 14 ago. 2024.

CELLARD, André. Análise documental na pesquisa qualitativa. *In*: POUPART, Jean; DESLAURIERS, Jean-Pierre; GROULX, Lionel-Henri; LAPERRIÈRE, Anne; MAYER, Robert; PIRES, Álvaro. **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Petrópolis, RJ: Vozes, 2008. Disponível em: https://www.studocu.com/pt-br/document/universidade-estadual-do-ceara/metodologia-da-pesquisa-i/cellard-andre-analise-documental/79955946. Acesso em: 14 jul. 2025.

CRAVO, Daniela Copetti. Perspectivas gerais sobre os direitos do titular dos dados no poder público. *In*: REQUIÃO, Maurício (org.). **Proteção de Dados Pessoais: novas perspectivas.** Salvador: EDUFBA, 2022. Disponível em: https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf. Acesso em: 01 fev. 2025.

CRESPO, Marcelo. Proteção de dados pessoais e o poder público: noções essenciais. *In*: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael (org.). **Lei Geral de Proteção de Dados e o Poder Público**. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena, 2021. p. 16-28. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 14 ago. 2024.

CRESWELL, John Ward. **Projeto de Pesquisa:** métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre: Artmed, 2007.

CRISTÓVAM, José Sérgio da Silva; BERGAMINI, José Carlos Loitey; HAHN, Tatiana Meinhart. Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). **Interesse Público - IP**, Belo Horizonte, ano 23, n. 129, p. 75-101, set./out. 2021. Disponível em: https://www.researchgate.net/publication/363917428_Governanca_de_dados_no_setor_publico_brasileiro_uma_analise_a_partir_da_Lei_Geral_de_Protecao_de_Dados_LGPD_Data_governance_in_the_Brazilian_government_an_analysis_of_from_the_General_Data_Protection_. Acesso em: 14 ago. 2024.

DIAS, Fernanda Rego. Limites à utilização do consentimento como base legal adequada para o tratamento de dados pessoais. *In*: REQUIÃO, Maurício (org.). **Proteção de Dados Pessoais: novas perspectivas.** Salvador: EDUFBA, 2022. Disponível em: https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf. Acesso em: 01 fev. 2025.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 14 ago. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: DONEDA, Danilo et al. (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

FEDERAÇÃO DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO DO ESTADO DE SÃO PAULO (FecomercioSP). **No Brasil, mercado de trabalho de profissões ligadas à tecnologia cresce até 740% em dez anos**. *Fecomercio.com.br*, São Paulo, 19 nov. 2024. Disponível em: https://www.fecomercio.com.br/noticia/no-brasil-mercado-de-trabalho-de-profissoes-ligadas-a-tecnologia-cresce-ate-740-em-dez-anos. Acesso em: 09 jul 2025.

FILKENSTEIN, Maria Eugenia; FILKENSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS. **Revista de Direito Brasileira**, Florianópolis, v. 23, n. 9, p.

284-301, maio/ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343. Acesso em: 14 ago. 2024.

FLÔRES, Mariana Rocha de; SILVA, Rosane Leal de. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de Direito**, Viçosa, v. 12, n. 2, p. 1-34, 2020. Disponível em:https://periodicos.ufv.br/revistadir/article/view/10327. Acesso em: 14 ago. 2024.

GARBACCIO, Grace Ladeira; VADELL, Lorenzo-Mateo Bujosa; TORCHIA, Bruno. Principais disposições da governança em privacidade à luz da Lei Geral de Proteção de Dados no Brasil. **Revista Justiça do Direito**, v. 36, n. 1, p. 204-230, jan./abr. 2022. Disponível em: https://seer.upf.br/index.php/rjd/article/view/13379. Acesso em: 14 ago. 2024.

GHISLENI, Júlia Zimmermann. A LGPD e a risk-based approach da governança corporativa: a primeira medida para o controlador aplicar os princípios. **Revista de Economia, Empresas e Empreendedores da CPLP,** v. 8, n. 1, p. 103-126, mar. 2022. Disponível em:https://revistas.ponteditora.org/index.php/e3/article/view/618/431. Acesso em: 15 ago. 2024.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2017.

GOMES, Fabricio Vasconcelos; CUNHA FILHO, Marcelo Castro; LUCCAS, Victor Nóbrega. Proteção de dados e instituição de ensino: o que fazer com dados de alunos?. **Revista Brasileira de Políticas Públicas**, Brasília, v. 13, n. 1, p. 401-420, 2023. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7996. Acesso em: 15 ago. 2024.

KANAGUSKU, Ana Rita Akayama; LAHR, Marcus Vinícius. Impactos da LGPD na Tecnologia da Informação: Desafios para os Profissionais da Área. **FatecSeg - Congresso de Segurança da Informação**, v. 1, n. 2, p. 1-16, nov. 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/69. Acesso em: 15 ago. 2024.

LIMA, Adrianne; ALCASSA, Flávia; PAPPERT, Milena. **LGPD no Direito do Trabalho**. São Paulo: Editora Saraiva, 2022. *E-book.* ISBN 9786553621954. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553621954/. Acesso em: 11 fev. 2024.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. Impacto da LGPD e compliance no setor público: necessárias adaptações culturais na Administração Pública frente a um cenário de transformação contínua para a manutenção da boa governança. *In*: PIRONTI, Rodrigo (org.). **Lei Geral de Proteção de Dados no Setor Público.** Belo Horizonte: Fórum, 2021. Disponível em: https://sumarios.org/artigo/lgpd-e-compliance-na-administra%C3%A7%C3%A3o-p%C3%BAblica-o-brasil-est%C3%A1-preparado-para-um-cen%C3%A1rio-em. Acesso em: 15 ago. 2024.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. Ed. São Paulo: Atlas, 2003.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia de investigação científica para as ciências sociais aplicadas.** São Paulo: Atlas, 2007.

MEIRELES, Edilton. Linhas básicas da Lei Geral de Proteção de Dados na relação de emprego. *In*: REQUIÃO, Maurício (org.). **Proteção de Dados Pessoais: novas perspectivas.** Salvador: EDUFBA, 2022. Disponível em: https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf. Acesso em: 01 fev. 2025.

MELO, Jussara Costa. Regulação do direito ao esquecimento no ciberespaço: heterogeneidade de lealdades no espaço público de postulação de interesses legítimos. **Revista de Direito Setorial e Regulatório**, Brasília, v. 1, n. 1, p. 171-194, maio 2015. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/19318. Acesso em: 15 ago. 2024.

MELLO, Marcos Bernardes de. **Teoria do Fato Jurídico: plano da existência**. 23 ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book.* ISBN 9786553620261. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553620261/. Acesso em: 14 jul. 2025.

MENDES, Laura Schertel. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama setorial da internet**, São Paulo, ano 11, n. 2, p. 1-7, jun./2019. Disponível em: https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: 15 ago. 2024.

MONTOLLI, Carolina. Segurança da informação e da transparência e a proteção de dados na Administração Pública: LGPD, acesso à informação e os incentivos à inovação e à pesquisa científica e tecnológica no âmbito do estado de Minas Gerais. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ**, Rio de Janeiro, v. 3, n. 3, p. 1-23, set./dez. 2020. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/176. Acesso em: 15 ago. 2024.

MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: Uma Análise à Luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 15 ago. 2024.

NASCIMENTO, Bruna Laís Campos; SILVA, Edilene Maria. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. **Em Questão**, Porto Alegre, v. 29, p. 1-27, 2023. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/127314. Acesso em: 15 ago. 2024.

NEMETZ, Erian Karina. A Evolução Histórica dos Direitos Humanos. **Revista Ciências Jurídicas e Sociais da Unipar**, Umuarama, v. 7, n. 2, p. 233-242, jul./dez. 2004. Disponível em: https://revistas.unipar.br/index.php/juridica/article/view/1332. Acesso em: 15 ago. 2024.

OLIVEIRA, Virna de Souza Godoy. **Proteção de dados pessoais**: um estudo no âmbito dos processos administrativos eletrônicos da UFRPE (2020-2022). 2024. 93 f. Dissertação (Mestrado em Gestão Pública) – Programa de Mestrado Profissional em Gestão Pública para o Desenvolvimento do Nordeste, Universidade Federal de Pernambuco, Recife, 2024. Disponível em: https://repositorio.ufpe.br/handle/123456789/56121. Acesso em: 15 ago. 2024.

PARANHOS, Daniel de Araújo. O papel do Estado na proteção de dados dos seus servidores e suas consequências para o endividamento da categoria. *In*: REQUIÃO, Maurício (org.). **Proteção de Dados Pessoais: novas perspectivas.** Salvador: EDUFBA, 2022. Disponível em: https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf. Acesso em: 01 fev. 2025.

PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 10, n. 1, p. 1-20, jan./jun. 2023. Disponível em: https://bibliotecavirtual.unl.edu.ar/publicaciones/index.php/Redoeda/article/view/12401. Acesso em: 15 ago. 2024.

REQUIÃO, Maurício. A natureza jurídica do consentimento para tratamento de dados pessoais. *In*: REQUIÃO, Maurício (org.). **Proteção de Dados Pessoais: novas perspectivas.** Salvador: EDUFBA, 2022. Disponível em: https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf. Acesso em: 01 fev. 2025.

ROCHA, Núbia Augusto de Sousa; ALMEIDA, Alexandre Nascimento; BRAGA, Tiago Emmanuel Nunes; NUNES, André. O tratamento de dados pessoais pelo poder público: um estudo bibliométrico. **Liinc em Revista.** Rio de Janeiro, v. 19, n. 2, p. 1-18, nov. 2023. Disponível em: https://revista.ibict.br/liinc/article/view/6455. Acesso em: 15 ago. 2024.

ROCHA, Roger Luz da; FONTES, Selma Velozo; MACHADO, Thiago Fontes. A segurança da informação nas organizações: um estudo sobre o impacto da Lei Geral de Proteção de Dados Pessoais na gestão. **RECH – Revista Ensino de Ciências e Humanidades – Cidadania, Diversidade e Bem Estar**. Humaitá, v. 7, n. 2, p. 463-483, jul./dez. 2023. Disponível em: https://periodicos.ufam.edu.br/index.php/rech/article/view/12923. Acesso em: 15 ago. 2024.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROJAS, Marco Antonio Torrez. **Avaliação da adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais**. 2020. 23 f. Artigo (Especialização em Gestão Pública) – Especialização em Gestão Pública na Educação Profissional e Tecnológica, Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, Santa Catarina, 2020. Disponível em: https://repositorio.ifsc.edu.br/handle/123456789/1433. Acesso em: 28 abr. 2023.

ROSSO, Angela Maria. **LGPD e setor público:** aspectos gerais e desafios. 2019. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios. Acesso em: 28 abr. 2023.

SANTANA, Guilherme Espinati; MENDONÇA, Maurício Barreto. **Metodologia para avaliação da adesão de boas práticas de proteção de dados com aplicação em estudo de caso**. 2023. 70 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Bacharelado em Sistemas de Informação, Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Rio de Janeiro, 2023. Disponível em: https://www.researchgate.net/profile/Carlos-Pantoja-3/publication/377301167_Metodologia_para_Avaliacao_da_Adesao_de_Boas_Praticas_de_Pr

otecao_de_Dados_Pessoais_com_Aplicacao_em_Estudo_de_Caso/links/659f2dfbc77ed940476ddc30/Metodologia-para-Avaliacao-da-Adesao-de-Boas-Praticas-de-Protecao-de-Dados-Pessoais-com-Aplicacao-em-Estudo-de-Caso.pdf. Acesso em: 17 mar. 2024.

SANTOS FILHO, Ronaldo Fenelon; JESUS, Victor Borges. Compliance de dados em instituições de ensino superior. **Revista de Constitucionalização do Direito Brasileiro - RECONTO**, Maringá, v. 6, n. 2, p. 274-296, jul./dez. 2023. Disponível em: https://revistareconto.com.br/index.php/reconto/article/view/115. Acesso em: 15 ago. 2024.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018. **Revista Direitos Fundamentais & Democracia**., v. 26, n. 2, p. 81-106, maio/ago. 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 15 ago. 2024.

SCHWABE, Jürgen. **50 anos de jurisprudência do tribunal federal constitucional alemão.** Traduzido por Beatriz Hennin et al. Montevidéu: Fundacion Konrad-Adenauer, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em: 09 jul. 2025.

SILVA, Lucas Gonçalves da; MELO, Bricio Luis da Anunciação; KFOURI, Gustavo. A Lei Geral de Proteção de Dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica Unicuritiba,** Curitiba, v. 3, n. 56, p. 354-377, jul./set. 2019. Disponível em:https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581. Acesso em: 09 jul. 2025.

SOUZA, Jackson Gomes Soares; BELDA, Francisco Rolfsen; ARIMA, Carlos Hideo. Análise de Aplicação da LGPD numa Instituição Pública de Ensino: um estudo de caso. **RIAEE – Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1856-1872, jul./set. 2022. Disponível em: https://periodicos.fclar.unesp.br/iberoamericana/article/view/16789. Acesso em: 15 ago. 2024.

SOUZA, Taciana Rita Santos. **A aplicação da Lei Geral de Proteção de Dados Pessoais nas Instituições Federais de Ensino Superior à luz da abordagem sociotécnica**. 2022. 152 f. Dissertação (Mestrado em Administração) - Programa de Pós-Graduação em Administração, Universidade Federal da Paraíba, João Pessoa, 2022. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/26407?locale=pt_BR. Acesso em: 09 jul 2025.

STAKE, Robert E. Case studies. *In*: DENZIN, N. K.; LINCOLN, Y. S.. **Handbook of qualitative research**. 2. ed. Thousand Oaks, CA: Sage, 2000. p. 435-454.

TAVARES, Ubênia Niájara Golzio. **Fatores motivacionais para o trabalho dos servidores públicos na rede de educação na Paraíba**: um estudo de caso. 2015. 43 f. Monografia (Especialização em Gestão Pública) - Universidade Estadual da Paraíba, João Pessoa, 2015. Disponível em:

https://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/13024/3/PDF%20-%20Ub%C3%AAnia%20%20Ni%C3%A1jara%20G%C3%B3lzio%20Tavares.pdf. Acesso em: 09 jul. 2025.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 15 ago. 2024.

TENÓRIO FILHO, Luiz; FERREIRA, Pollyana Cassia Gonzaga; MOTA, Francisca Rosaline Leite; SOUZA, Edivanio Duarte de. Os desafios da Implementação da Lei Geral de Proteção de Dados nas Universidades Públicas Federais da Região Nordeste do Brasil. *In*: **XXI Encontro Nacional de Pesquisa em Ciência da Informação – XXI ENANCIB**, Rio de Janeiro, 2021. Disponível em: https://enancib.ancib.org/index.php/enancib/xxienancib/paper/view/456. Acesso em: 09 jul. 2025.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais – e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020a.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação dos dados pessoais. **Revista Brasileira de Direito Civil - RBDCivil**, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020b. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/521/389. Acesso em: 09 jul. 2025.

TRUJILLO FERRARI, Afonso. **Metodologia da pesquisa científica**. São Paulo: McGraw-Hill do Brasil, 1982.

UFRPE. **Resolução nº 037, de 11 de abril de 2019**. Altera a Política de Gestão de Riscos da Universidade Federal Rural de Pernambuco. 2019. Disponível em: http://ww2.proplan.ufrpe.br/sites/ww2.proplan.ufrpe.br/files/Nova%20Pol%C3%ADtica%20GEST%C3%83O%20DE%20RISCOS%20-%20abril%20de%202019%20-%20vers%C3%A3o%202_1.pdf. Acesso em: 09 jul 2025.

UFRPE. **Resolução nº 031, de 11 de agosto de 2020**. Regulamenta restrição à divulgação de documentos que contenham dados pessoais de pessoa natural no âmbito desta Universidade. 2020. Disponível em: https://seg.ufrpe.br/content/res-no-0312020-0. Acesso em: 09 jul. 2025.

UFRPE. **Cartilha LGPD**. 2021a. Disponível em: http://app.ouvidoria.ufrpe.br/sites/ouvidoria.ufrpe.br/files/Files/CARTILHA_LGPD%20%282%29.pdf. Acesso em 09 jul. 2025.

UFRPE. **Resolução nº 103, de 14 de junho de 2021**. Aprova criação de Comitê Gestor de Privacidade e Proteção de Dados - CGPPD e da Política de Privacidade e Proteção de Dados Pessoais da Universidade Federal Rural de Pernambuco. 2021b. Disponível em: https://seg.ufrpe.br/content/res-no-1032021. Acesso em: 09 jul. 2025.

UFRPE. **Resolução nº 152, de 29 de novembro de 2021**. Aprova Plano de Desenvolvimento Institucional (PDI) relativo ao período 2021 - 2030 da Universidade Federal Rural de

Pernambuco. 2021c. Disponível em: https://seg.ufrpe.br/content/res-no-1522021. Acesso em: 09 jul. 2025.

UFRPE. **Resolução nº 237, de 11 de outubro de 2022**. Aprova Plano de Dados Abertos da Universidade Federal Rural de Pernambuco, para o período de vigência 2022 - 2024. 2022a. Disponível em: https://seg.ufrpe.br/content/res-no-2372022. Acesso em: 09 jul. 2025.

UFRPE. **Política de Segurança da Informação e Comunicação (POSIC)**. 2022b. Disponível em: https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/. Acesso em: 09 jul. 2025.

UFRPE. **Documento de constituição da Equipe de Tratamento e Respostas a Incidentes Cibernéticos**. 2022c. Disponível em: https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/. Acesso em: 09 jul. 2025.

UFRPE. **Resolução nº 257, de 2 de fevereiro de 2023**. Aprova Regimento Interno do Comitê de Governança Digital da Universidade Federal Rural de Pernambuco. 2023a. Disponível em: https://seg.ufrpe.br/content/res-no-2572023. Acesso em: 09 jul. 2025.

UFRPE. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)**. 2023b. Disponível em: https://digital.ufrpe.br/paginas/comite-de-governanca-digital-cgdufrpe/. Acesso em: 09 jul. 2025.

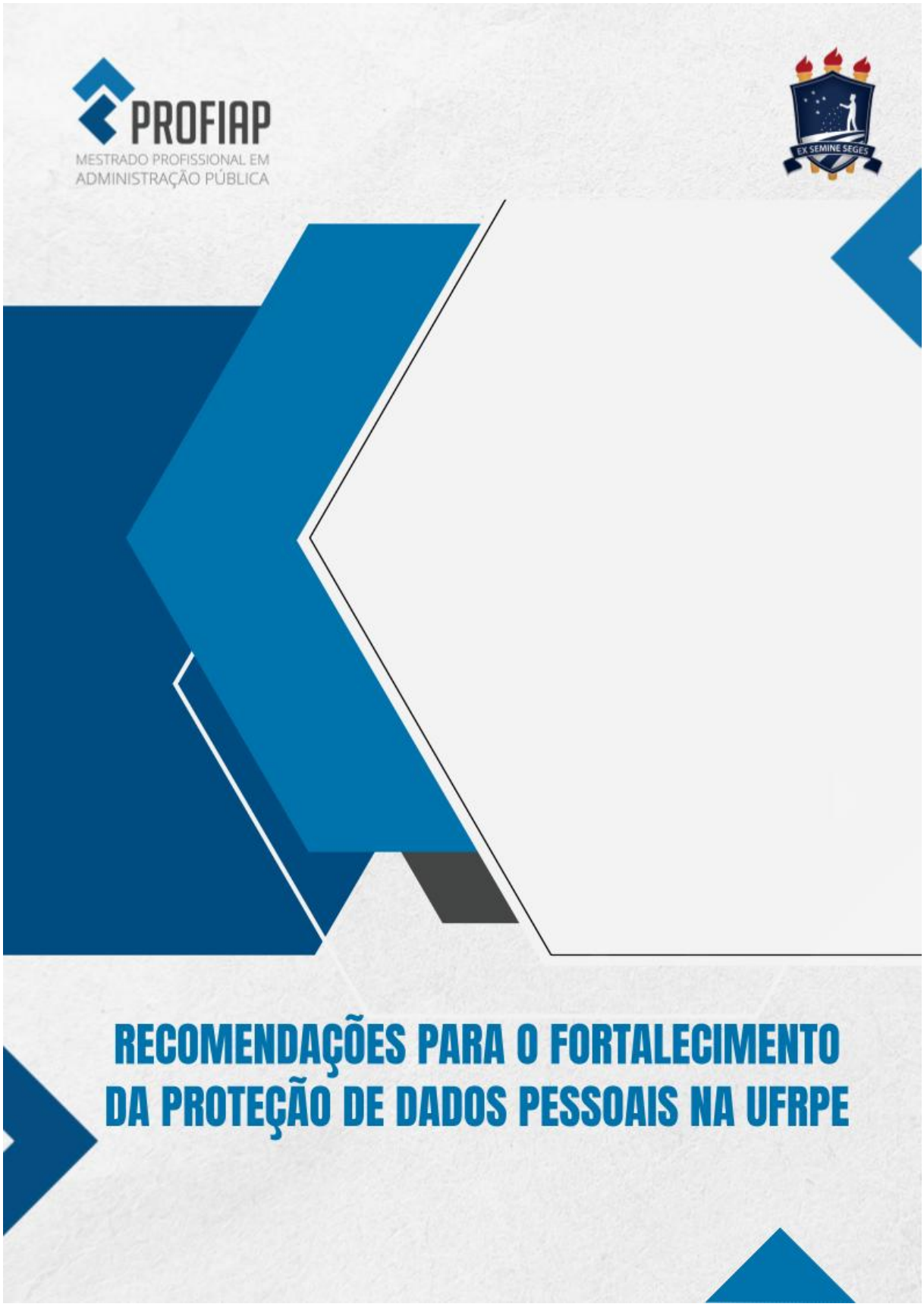
UFRPE. **Plano de Contingência em Tecnologia da Informação e Comunicação (PCTIC)**. 2023c. Disponível em: https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/. Acesso em: 09 jul. 2025.

UFRPE. **Painel de Monitoramento do Plano de Desenvolvimento Institucional 2021-2030**. 2025a. Disponível em: http://ww2.proplan.ufrpe.br/br/content/resultados-plano-de-desenvolvimento-institucional-0. Acesso em: 09 jul. 2025.

UFRPE. **Segurança da Informação e Comunicação**. *UFRPE Digital*, s.d. 2025b. Disponível em: https://digital.ufrpe.br/paginas/seguranca-da-informacao-e-comunicacao/. Acesso em: 09 jul. 2025.

ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis. A Lei Geral de Proteção de Dados e suas implicações na saúde: as Avaliações de Impacto no tratamento de dados no âmbito clínico-hospitalar. **Revista de Bioética y Derecho Perspectivas Bioéticas [online]**, n. 54, p. 215-232, 2022. Disponível em: https://scielo.isciii.es/scielo.php?pid=S1886-58872022000100013&script=sci_abstract&tlng=pt. Acesso em: 15 ago. 2024.

APÊNDICE A – RELATÓRIO TÉCNICO-CONCLUSIVO E RECOMENDAÇÕES



RECOMENDAÇÕES PARA O FORTALECIMENTO DA PROTEÇÃO DE DADOS PESSOAIS NA UFRPE

Relatório técnico apresentado pelo mestrando Igor Bega de Miranda ao Mestrado Profissional em Administração Pública em Rede (PROFIAP), sob orientação e coorientação das docentes Dra. Angela Cristina Rocha de Souza e Dra. Maria Iraê de Souza Corrêa, como parte dos requisitos para obtenção do título de Mestre em Administração Pública.

SUMÁRIO

Resumo 4

Contexto 5

Público-alvo 6

Descrição da situação-problema 7

Objetivos deste relatório 9

Diagnóstico e análise 10

Recomendações 13

Referências 15

RESUMO

Este relatório apresenta um análise estruturada sobre a implementação da LGPD na UFRPE, com base em pesquisa que examinou documentos institucionais, entrevistas e um *framework* de avaliação de maturidade.

O estudo identificou avanços na normatização interna, como a criação do Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) e a política de Privacidade e Proteção de Dados Pessoais (PPPDP), mas também revelou **desafios** relevantes, como restrições orçamentárias, escassez de recursos humanos qualificados e dificuldades relacionadas à pluralidade universitária e a aspectos da legislação, que exigem atuação da instituição.

Nesse sentido, considerando os resultados encontrados, serão apresentadas, ao final deste documento, recomendações para auxiliar a instituição no processo de adequação à LGPD.



CONTEXTO

A implementação da Lei Geral de Proteção de Dados (LGPD) na UFRPE ocorre em um cenário de profundas transformações no tratamento de informações pessoais no Brasil e no mundo. Desde sua entrada em vigor, a LGPD estabeleceu novos paradigmas para a gestão de dados, exigindo que organizações públicas e privadas revisem seus processos, políticas e infraestrutura tecnológica.

Para a UFRPE, essa adequação não se trata apenas de cumprir uma exigência legal, mas de tentar superar desafios específicos do setor público.

Como universidade federal, a UFRPE lida diariamente com um volume significativo de dados sensíveis - desde informações acadêmicas até registros administrativos e de pesquisa. Essa complexidade é agravada pela necessidade de conciliar transparência ativa (como exigido pela Lei de Acesso à Informação) com a proteção da privacidade (conforme a LGPD) (Almeida, 2024).

Ao mesmo tempo, órgãos de controle como o Tribunal de Contas da União (TCU) têm incluído a conformidade com a LGPD em suas avaliações (Brasil, 2022). Esse contexto regulatório mais rigoroso coexiste com as limitações estruturais típicas do serviço público, incluindo restrições orçamentárias, dificuldades na contratação de pessoal especializado e infraestrutura tecnológica que por vezes requer atualizações.

No entanto, esse desafio também se apresenta como um vetor de oportunidades. A adequação à LGPD pode servir como catalisador para o fortalecimento da proteção de dados. Mais do que evitar sanções, a implementação robusta da LGPD permite à UFRPE reforçar a confiança da comunidade acadêmica e da sociedade em seus processos de gestão.

É nesse contexto complexo que este documento se insere, com o objetivo de contribuir para **fortalecer a proteção de dados pessoais no âmbito da instituição.**



PÚBLICO-ALVO

- Gestores univesitários: tomadores de decisão (Reitoria, pró-reitorias, comitês).
- Equipes operacionais: tecnologia da informação, segurança da informação, jurídico e administrativo.
- Comunidade acadêmica: servidores, docentes, terceirizados e discentes que lidam com dados pessoais.

DESCRIÇÃO DA SITUAÇÃO PROBLEMA

A proteção de dados pessoais emergiu como um tema central nas discussões sobre direitos fundamentais na era digital. Embora a discussão internacional sobre o assunto remonte aos anos 1990, com legislações como a Diretiva Europeia 95/46/EC e documentos como o "Personal Information Protection and Electronic Documents Act" do Canadá, o Brasil apenas começou a estruturar normativas consistentes a partir de 2014, com o Marco Civil da Internet, culminando na aprovação da Lei Geral de Proteção de Dados em 2018.

A LGPD estabelece padrões para o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

No contexto das instituições públicas de ensino superior, sobretudo na esfera federal, como a UFRPE, a aplicação da LGPD é complexa. Essas instituições lidam com um grande volume de dados pessoais e sensíveis relacionados a servidores, discentes, egressos e usuários de seus serviços. Além disso, a LGPD, embora não se aplique ao tratamento de dados com finalidade exclusivamente acadêmica, exige das universidades o cumprimento de diversas obrigações legais quanto ao trata -

tamento, proteção e compartilhamento de informações pessoais.

Estudos recentes (Barbosa *et al.*, 2021; Rojas, 2020; Tenório Filho *et al.*, 2021; Souza, 2022) demonstram que as universidades públicas brasileiras ainda se encontram em estágios iniciais de conformidade com a LGPD. Entre os principais entraves, destacam-se a falta de recursos financeiros, a carência de pessoal capacitado, a inexistência de uma cultura institucional de proteção de dados e a ausência de orientações específicas sobre o tema.

Na UFRPE, apesar da evolução, existem metas previstas no PDI da instituição relacionadas à proteção de dados ainda não plenamente atingidas, como a conformidade total dos serviços à LGPD até 2025.

Nesse contexto, a situação problema se configura pela discrepância entre os avanços formais conquistados pela UFRPE em relação à proteção de dados pessoais e a efetividade prática das ações implementadas. Tal lacuna compromete não apenas o cumprimento da LGPD, mas também a segurança jurídica e a confiança da sociedade na gestão universitária, podendo até culminar em sanções para a instituição.

OBJETIVOS DESTE RELATÓRIO

- Contribuir para o fortalecimento da proteção de dados pessoais na UFRPE;
- Apoiar a conformidade institucional à LGPD;
- Articular a integração entre normativas, estruturas e práticas relacionadas à proteção de dados;
- Promover iniciativas para estimular o engajamento da comunidade universitária na cultura de proteção de dados;
- Propor ações para minimizar os riscos legais e técnicos decorrentes da não conformidade com a LGPD.



DIAGNÓSTICO E ANÁLISE

A análise dos dados coletados por meio de documentos institucionais, entrevistas com atores-chave relacionados à proteção de dados e aplicação do *framework* de Santana e Mendonça (2023) permitiu a identificação de desafios e avanços na implementação da LGPD na UFRPE. Os resultados indicaram que:

- O Programa Previna-se, a Política de Segurança da Informação e Comunicação (POSIC), a Política de Privacidade e Proteção de Dados Pessoais (PPPDP) e a criação do Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) representam avanços significativos no contexto da proteção de dados;
- A despeito dos esforços institucionais, a comunidade acadêmica ainda não é engajada nas questões relacionadas ao tema;
- Ainda não há a utilização de recursos de criptografia em trânsito e em repouso nos dados pessoais processados nos ativos sistêmicos da organização;
- Não foi estabelecida uma matriz RACI quanto às responsabilidades sobre a proteção de dados da instituição;
- As capacitações sobre a LGPD ainda não alcançaram todos os servidores;
- Os contratos com terceiros ainda não foram revisados para a inserção de cláusulas de proteção de dados;
- A inexistência de normas reguladoras e orientações para sanar aspectos relacionados à incipiência e obscuridade da legislação.



A Instituição apresenta instrumentos normativos referentes a políticas e comissões bem formulados, que demonstram compreensão da LGPD como um marco regulatório transversal, inserido no contexto da governança digital.

Por outro lado, a cultura de proteção de dados ainda está em formação, o que se reflete na baixa adesão da comunidade acadêmica às políticas existentes. Somam-se a isso, como fatores agravantes, limitações financeiras e de recursos humanos, inviabilizando a concretização de políticas e ações.

No plano financeiro, a insuficiência orçamentária, em um contexto recorrente de redução de despesas no âmbito federal, compromete ações relevantes, tais como a contratação de ferramentas tecnológicas, a aquisição de sistemas de segurança da informação e o oferecimento contínuo de treinamentos para a comunidade universitária, dificultando, ainda, a celebração de parcerias e o fortalecimento da proteção de dados.

Quanto aos recursos humanos, constatou-se que servidores envolvidos com a temática da LGPD acumulam múltiplas funções, muitas vezes sem dedicação exclusiva. Há, inclusive, casos de servidores dispostos a colaborar com a conformidade da instituição, mas que não dispõem de tempo ou de condições institucionais para tanto.

Essa combinação de carência de pessoal qualificado e insuficiência de recursos financeiros impacta diretamente a capacidade da UFRPE de cumprir plenamente os preceitos da LGPD.

Além disso, obstáculos relacionados à legislação também foram observados como impeditivos para a correta aplicação da LGPD. Em que pese a existência de normativas internas importantes, como a Resolução CONSU/UFRPE nº 103/2021, que institui o CGPPD e a PPPDP, ainda há carência de orientações centrais relacionadas a aspectos específicos da norma.

Essa insuficiência normativa se expressa, por exemplo, na ausência de regulamentações detalhadas sobre a anonimização dos dados e na escassez de procedimentos operacionais padronizados.

Ademais, foi identificado um ponto de aparente tensão entre a LGPD e a Lei de Acesso à Informação (LAI), também observado em outras instituições de ensino (Almeida, 2024). Enquanto a LGPD assegura proteção da privacidade e impõe restrições à divulgação de dados pessoais, a LAI se baseia no princípio da publicidade como regra e o sigilo como exceção

Como resultado, há riscos tanto de exposição indevida de informações pessoais, quanto de negação injustificada de acesso à informação pública - situações que podem violar direitos e comprometer a imagem institucional.

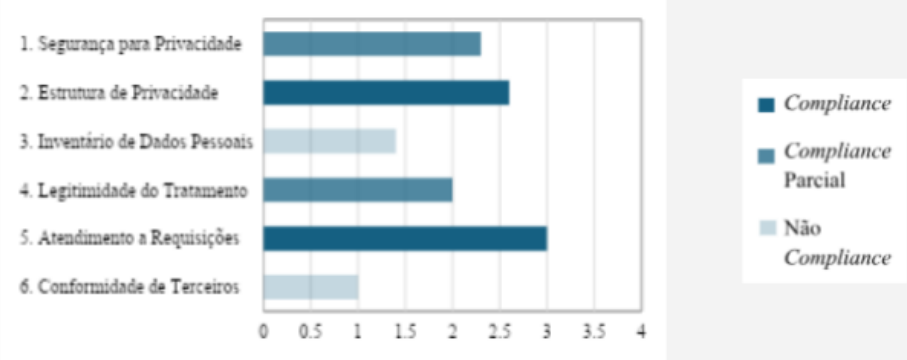
Apesar desse cenário, identificam-se condições internas favoráveis para o avanço institucional relativo à gestão das TDIC, e, como consectário, da proteção de dados pessoais, tais quais a prioridade da alta gestão para o avanço da tecnologia digital, o entendimento das Tecnologias da Informação e Comunicação como estraté -

> "[...] mas há outros , como, por exemplo, o engajamento dos setores que realizam esses tratamentos de dados pessoais, como eu disse, a lei ela traz consigo, mesmo que de forma implícita, uma obrigação de você revisar seus processos institucionais [...], isso traz um trabalho para os setores que muitas vezes já têm uma carga de trabalho, uma demanda muito grande [...]"
>
> (Entrevistado 2)

gicas e o Comitê de Governança Digital com participação ativa da alta gestão (UFRPE, 2023).

O aprimoramento institucional da UFRPE em relação à LGPD pode ser alcançado com medidas internas, mas depende sobretudo de fatores externos à instituição, como o aporte de recursos, maior liberação de códigos de vagas e o fortalecimento da ANPD como órgão de fiscalização e orientação, os quais, apesar dos notáveis avanços nos últimos anos, ainda são insuficientes.

Nesse contexto, foi aplicado o *framework* de Santana e Mendonça (2023), que classificou a instituição como *compliance* parcial, com ênfase positiva nas seções Estrutura de Privacidade e Atendimento a Requisições e negativa em Inventário de Dados Pessoais e Conformidade de Terceiros.



Fonte: Dados da pesquisa (2025)

Em vista disso, serão apresentadas na próxima seção recomendações visando aprimorar o cenário em questão.



RECOMENDAÇÕES

- **Ampliar a** divulgação interna da LGPD, bem como de todas as ações da Universidade nesse sentido, por vezes desconhecidas pela comunidade acadêmica, a fim de reforçar a cultura de proteção de dados **pessoais** na instituição.
- Estimular a participação dos diferentes usuários (discentes, servidores e docentes) nas discussões sobre a norma e implementação dela, considerando que o conhecimento sobre essa temática vai para além de grupos específicos, sendo necessário o envolvimento de todos que fazem parte da **UFRPE e** uma cultura orientada para a gestão de dados com destaque para aspectos de segurança e privacidade (Souza, 2022, p. 74).
- **Revisar os** contratos com terceiros, para inclusão de cláusulas de proteção de dados.
- Criar mecanismos que identifiquem a inclusão de um dado pessoal no processo eletrônico, de modo a notificar o usuário do sistema sobre a o eventual descumprimento da LGPD quando da não observância da norma.

- **Adotar** o *Privacy by Design*, ou Privacidade desde a concepção, para os projetos e serviços a serem desenvolvidos na instituição..
- **Criar** uma política de retenção, para que se saiba até quando e para qual finalidade os dados estão sendo tratados.
- **Desenvolver** um mapeamento completo e um inventário de dados pessoais, com a participação dos múltiplos setores da Universidade, a fim de se estabelecer quais dados são tratados, em que sistemas são armazenados, quem a eles tem acesso, com qual finalidade e sob qual base legal.
- **Estabelecer** uma matriz RACI para a distribuição e comunicação dos papéis e responsabilidades relacionados à proteção de dados.
- **Estabelecer** uma metodologia de tratamento de dados com base no relacionamento que a UFRPE possui com cada segmento universitário (docentes, discentes, técnicos), tendo em vista que a finalidade desse tratamento é fundamental para a aplicabilidade da LGPD (Gomes; Cunha Filho; Luccas, 2023).

REFERÊNCIAS

ALMEIDA, Willdson Gonçalves de. **Implementação de compliance à LGPD em instituições federais de ensino superior**: proposta de um processo estruturado para conformidade. 2024. 133 f. Dissertação (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação Profissional em Engenharia de Produção, Universidade Federal de São Carlos, São Carlos, 2024. Disponível em: https://repositorio.ufscar.br/items/2802852a-482e-4f98-9ca3-17e263287180. Acesso em: 08 jul 2025.

BARBOSA, Tatiane Santos; LOPES, Jerisnaldo Matos; PIAU, Deise Danielle Neves Dias; SILVA, Marcelo Santana; TELES, Eduardo Oliveira. A Lei Geral de Proteção de Dados (LGPD) nas Instituições Públicas de Ensino: Possíveis Impactos e Desafios. **Anais do VII Encontro Nacional de Propriedades Intelectuais (ENPI)**, Aracaju, v. 07, n. 1, p. 2114-2123, set. 2021. Disponível em: https://api.org.br/conferences/ENPI2021/ENPI2021/paper/view/1455. Acesso em: 14 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 28 abr. 2023.

BRASIL. **Acórdão nº 1.384, de 15 de junho de 2022**. Relatório de auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais. 2022. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY:ACORDAO-COMPLETO-2521877/NUMACORDAOINT%20asc/0. Acesso em: 08 jul. 2025.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: DONEDA, Danilo et al. (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

GOMES, Fabricio Vasconcelos; CUNHA FILHO, Marcelo Castro; LUCCAS, Victor Nóbrega. Proteção de dados e instituição de ensino: o que fazer com dados de alunos?. **Revista Brasileira de Políticas Públicas**, Brasília, v. 13, n. 1, p. 401-420, 2023. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7996. Acesso em: 15 ago. 2024.

ROJAS, Marco Antonio Torrez. **Avaliação da adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais**. 2020. 23 f. Artigo (Especialização em Gestão Pública) – Especialização em Gestão Pública na Educação Profissional e Tecnológica, Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, Santa Catarina, 2020. Disponível em: https://repositorio.ifsc.edu.br/handle/123456789/1433. Acesso em: 28 abr. 2023.

SANTANA, Guilherme Espinati; MENDONÇA, Maurício Barreto. **Metodologia para avaliação da adesão de boas práticas de proteção de dados com aplicação em estudo de caso**. 2023. 70 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Bacharelado em Sistemas de Informação, Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Rio de Janeiro, 2023. Disponível em: https://www.researchgate.net/profile/Carlos-Pantoja-3/publication/377301167_Metodologia_para_Avaliacao_da_Adesao_de_Boas_Praticas_de_Protecao_de_Dados_Pessoais_com_Aplicacao_em_Estudo_de_Caso/links/659f2dfbc77ed940476ddc30/Metodologia-para-Avaliacao-da-Adesao-de-Boas-Praticas-de-Protecao-de-Dados-Pessoais-com-Aplicacao-em-Estudo-de-Caso.pdf. Acesso em: 17 mar. 2024.

SOUZA, Taciana Rita Santos. **A aplicação da Lei Geral de Proteção de Dados Pessoais nas Instituições Federais de Ensino Superior à luz da abordagem sociotécnica**. 2022. 152 f. Dissertação (Mestrado em Administração) - Programa de Pós-Graduação em Administração, Universidade Federal da Paraíba, João Pessoa, 2022. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/26407?locale=pt_BR. Acesso em: 09 jul 2025.

TENÓRIO FILHO, Luiz; FERREIRA, Pollyana Cassia Gonzaga; MOTA, Francisca Rosaline Leite; SOUZA, Edivanio Duarte de. Os desafios da Implementação da Lei Geral de Proteção de Dados nas Universidades Públicas Federais da Região Nordeste do Brasil. *In*: **XXI Encontro Nacional de Pesquisa em Ciência da Informação – XXI ENANCIB**, Rio de Janeiro, 2021. Disponível em: https://enancib.ancib.org/index.php/enancib/xxienancib/paper/view/456. Acesso em: 09 jul. 2025.

UFRPE. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)**. 2023. Disponível em: https://digital.ufrpe.br/paginas/comite-de-governanca-digital-cgdufrpe/. Acesso em: 09 jul. 2025.

Discente: Igor Bega de Miranda

Orientadora: Dra. Angela Cristina Rocha de Souza

Coorientadora: Dra. Maria Iraê de Souza Corrêa

Universidade Federal Rural de Pernambuco

Julho de 2025

PROFIAP

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA

APÊNDICE B – ROTEIRO DE ENTREVISTA SEMIESTRUTURADO

Convidamos o Sr. para participar como voluntário da pesquisa Proteção de Dados no Setor Público: um estudo em uma universidade federal, que está sob a responsabilidade do pesquisador Igor Bega de Miranda, e-*mail* igor.bega@ufrpe.br, sob a orientação da Prof.ª Dra. Angela Cristina Souza Rocha, *e-mail* angela.souza@ufrpe.br e coorientação da Profª. Dra. Maria Iraê de Souza Corrêa, *e-mail* mariairae.correa@ufrpe.br.

Todas as suas dúvidas podem ser esclarecidas com o responsável por esta pesquisa. Apenas quando todos os esclarecimentos forem dados e a senhor concordar com a realização do estudo, pedimos que rubrique as folhas e assine ao final deste documento, que está em duas vias. Uma via será entregue e a outra ficará com o pesquisador responsável.

Você estará livre para decidir participar ou recusar-se. Caso não aceite participar, não haverá nenhum problema, desistir é um direito seu, bem como será possível retirar o consentimento em qualquer fase da pesquisa, também sem nenhuma penalidade.

INFORMAÇÕES SOBRE A PESQUISA:

➢ Descrição da pesquisa

A pesquisa tem como objetivo investigar como a Lei Geral de Proteção de Dados Pessoais (LGPD) vem sendo aplicada no âmbito da Universidade Federal Rural de Pernambuco (UFRPE).

➢ Esclarecimento do período de participação do voluntário na pesquisa, início, término e número de visitas para a pesquisa

O indivíduo que aceitar participar voluntariamente da pesquisa responderá aos questionamentos da entrevista semiestruturada, cuja duração será flexível, tendo em vista que o participante terá o tempo que julgar necessário para responder as indagações.

➢ RISCOS diretos para o voluntário

Consideram-se como eventuais riscos a possibilidade de desconforto com alguma pergunta e de identificação do respondente, bem como o cansaço. Os riscos têm nível de gradação “baixo”. Quanto ao desconforto e possibilidade de identificação, será entregue ao entrevistado um Termo de Consentimento Livre e Esclarecido (TCLE), indicando que as informações obtidas serão utilizadas exclusivamente para o desenvolvimento do estudo, bem como que a coleta de dados não possui fins financeiros, nem serão repassadas a terceiros. As entrevistas serão agendadas em data e horário compatíveis com a agenda dos respondentes, mitigando a possibilidade de cansaço e, após transcrição, não será atribuído o conteúdo diretamente a eles, a fim de diminuir a possibilidade de identificação.

Durante a pesquisa, as informações coletadas serão armazenadas em computador protegido por senha, *firewall* e antivírus. Periodicamente, serão realizadas cópias de seguranças dos dados em

dispositivo USB e disco rígido externo. Esses cuidados serão tomados para contornar os riscos inerentes ao mundo virtual e às limitações dos equipamentos eletrônicos utilizados. Todas as informações desta pesquisa serão confidenciais e divulgadas apenas em eventos ou publicações científicas, não havendo identificação dos voluntários, a não ser entre os responsáveis pelo estudo. Concluído o estudo, o pesquisador armazenará as informações coletadas em dispositivo eletrônico local, HD externo e computador pessoal, apagando todo e qualquer registro que esteja ao seu alcance de qualquer plataforma virtual, ambiente compartilhado ou "nuvem", nos termos da Carta Circular nº 1/2021-CONEP/SECNS/MS. Os dados coletados ficarão armazenados no endereço residencial do pesquisador pelo período mínimo de cinco anos, sendo garantida a divulgação dos resultados aos participantes e à instituição em cujos dados foram coletados, conforme disposições da Resolução n. 510/2016 e da Norma Operacional n. 001/2013, ambas do CNS.

Parte I – Dados demográficos

1) Nome: _____

2) Qual a sua área de formação na graduação? _____

3) Qual seu cargo na instituição? _____

4) Qual sua função na instituição? _____

5) Há quanto tempo trabalha na instituição?

( ) Menos de 1 ano ( ) Entre 1 e 5 anos ( ) Entre 6 e 10 anos ( ) Entre 11 e 20 anos

( ) Acima de 20 anos

6) Há quanto tempo atua como responsável pela implementação da LGPD? _____?

Parte II – Entrevista

a) Encarregado de Proteção de Dados (EPD)

1. Quais são as atividades da sua função relacionadas à proteção de dados pessoais?
2. Você tem conhecimento sobre a Política de Privacidade e Proteção de Dados Pessoais na UFRPE, aprovada na Resolução CONSU/UFRPE 103/2021? Em caso positivo, quais os elementos dessa política que você pode destacar?
3. Além dessa política, há outros instrumentos normatizando e orientando o tratamento de dados pessoais na instituição? Se sim, quais?
4. Quais as ações implementadas na UFRPE relacionadas à proteção de dados? Quando começaram a ser implementadas? Quem são os responsáveis por essas ações?

5. Há reuniões periódicas entre o EPD e a equipe responsável pela governança de dados, vinculada à Secretaria de Tecnologias Digitais (STD), para avaliar a aplicação dessa política no âmbito da UFRPE?
6. Em seu Plano de Desenvolvimento Institucional (PDI), a UFRPE estabeleceu como meta adequar 75% dos serviços da instituição à LGPD até o final do ano de 2024. Na sua opinião, essa meta será alcançada? Quais os fatores que vêm influenciando o alcance dessa meta estratégica?
7. Há alguma unidade organizacional que realize o acompanhamento e o monitoramento, de forma regular, para assegurar o *compliance* dos serviços prestados pela UFRPE com a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD)?
8. Na instituição existe programa de *compliance* em proteção de dados pessoais? Em caso positivo, como é o funcionamento?
9. Há algum instrumento normativo institucional que discipline incidentes de exposição e vazamento de dados pessoais na instituição? Se sim, qual é esse instrumento e qual é a sua abrangência? Em caso negativo, quais os óbices para que esse instrumento normativo seja criado?
10. Como a instituição gerencia incidentes de segurança envolvendo dados pessoais?
11. No âmbito da UFRPE, o EPD é consultado pela comunidade acadêmica sobre o compartilhamento e/ou incidentes de dados pessoais? Em caso positivo, qual o assunto que mais suscita orientações?
12. Qual é o principal tipo de incidente identificado? Você poderia citar algum caso específico e como foi tratado?
13. Já houve algum episódio de incidente/vazamento de dados pessoais pelo qual a UFRPE respondeu legalmente?
14. A instituição oferece capacitação e programas de conscientização sobre a proteção de dados pessoais de forma sistemática? Se sim, quem participa dessa capacitação?
15. Na sua opinião, quais ações devem ser adotadas para fortalecer a cultura de proteção de dados pessoais na UFRPE?
16. Na sua opinião, no âmbito geral, quais os desafios da instituição para implementação das práticas de proteção de dados pessoais? Dentre esses, no âmbito de sua atuação, qual deles você ressalta?

b) Diretor da Secretaria de Tecnologias Digitais

1. Quais são as atividades da sua função relacionadas à proteção de dados pessoais?
2. Você tem conhecimento sobre a Política de Privacidade e Proteção de Dados Pessoais na UFRPE, aprovada na Resolução CONSU/UFRPE 103/2021? Em caso positivo, quais os elementos dessa política que você pode destacar?
3. Além dessa política, há outros instrumentos normatizado e orientando o tratamento de dados pessoais na instituição? Se sim, quais?
4. Quais as ações implementadas na UFRPE relacionadas à proteção de dados? Quando começaram a ser implementadas? Quem são os responsáveis por essas ações?
5. Há reuniões periódicas entre a equipe da Secretaria de Tecnologias Digitais (STD) com o EPD para avaliar a aplicação dessa política no âmbito da UFRPE?
6. Quais ferramentas/sistemas/tecnologias são utilizadas para proteger dados pessoais na instituição?
7. Há ambiente de custódia (virtual) desses dados, sem acesso à internet, que garantam proteção e integridade dos dados?
8. Você considera que, atualmente, a Universidade consegue assegurar um ambiente de segurança adequado? Em caso negativo, qual o principal fator que compromete esse ambiente virtual?
9. Em seu Plano de Desenvolvimento Institucional (PDI), a UFRPE estabeleceu como meta adequar 75% dos serviços da instituição à LGPD até o final do ano de 2024. Na sua opinião, essa meta será alcançada? Quais os fatores que vêm influenciando o alcance dessa meta estratégica?
10. Há alguma unidade organizacional que realize o acompanhamento e o monitoramento, de forma regular, para assegurar o compliance dos serviços prestados pela UFRPE com a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD)?
11. Na instituição existe programa de compliance em proteção de dados pessoais? Em caso positivo, como é o funcionamento?
12. Há algum instrumento normativo institucional que discipline incidentes de exposição e vazamento de dados pessoais na instituição? Se sim, qual é esse instrumento e qual é a sua abrangência? Em caso negativo, quais os óbices para que esse instrumento normativo seja criado?
13. Como a instituição gerencia incidentes de segurança envolvendo dados pessoais?

14. Qual é o principal tipo de incidente identificado? Você poderia citar algum caso específico e como foi tratado?
15. Já houve algum episódio de incidente/vazamento de da dos pessoais pelo qual a UFRPE respondeu legalmente?
16. A instituição oferece capacitação e programas de conscientização sobre a proteção de dados pessoais de forma sistemática? Se sim, quem participa dessa capacitação?
17. Na sua opinião, quais ações devem ser adotadas para fortalecer a cultura de proteção de dados pessoais na UFRPE?
18. Na sua opinião, no âmbito geral, quais os desafios da instituição para implementação das praticas de proteção de dados pessoais? Dentre esses, no âmbito de sua atuação, qual deles você ressalta?

c) Coordenador de Governança Digital

1. Quais são as atividades da sua função relacionadas à proteção de dados pessoais?
2. Você tem conhecimento sobre a Política de Privacidade e Proteção de Dados Pessoais na UFRPE, aprovada na Resolução CONSU/UFRPE 103/2021? Em caso positivo, quais os elementos dessa política que você pode destacar?
3. Além dessa política, há outros instrumentos normatizado e orientando o tratamento de dados pessoais na instituição? Se sim, quais?
4. Quais as ações implementadas na UFRPE relacionadas à proteção de dados? Quando começaram a ser implementadas? Quem são os responsáveis por essas ações?
5. Há reuniões periódicas entre a equipe da Secretaria de Tecnologias Digitais (STD) com o EPD para avaliar a aplicação dessa política no âmbito da UFRPE?
6. Quais ferramentas/sistemas/tecnologias são utilizadas para proteger dados pessoais na instituição?
7. Há ambiente de custódia (virtual) desses dados, sem acesso à internet, que garantam proteção e integridade dos dados?
8. Você considera que, atualmente, a Universidade consegue assegurar um ambiente de segurança adequado? Em caso negativo, qual o principal fator que compromete esse ambiente virtual?
9. Em seu Plano de Desenvolvimento Institucional (PDI), a UFRPE estabeleceu como meta adequar 75% dos serviços da instituição à LGPD até o final do ano de 2024. Na

sua opinião, essa meta será alcançada? Quais os fatores que vêm influenciando o alcance dessa meta estratégica?

10. Há alguma unidade organizacional que realize o acompanhamento e o monitoramento, de forma regular, para assegurar o compliance dos serviços prestados pela UFRPE com a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD)?
11. Na instituição existe programa de compliance em proteção de dados pessoais? Em caso positivo, como é o funcionamento?
12. Há algum instrumento normativo institucional que discipline incidentes de exposição e vazamento de dados pessoais na instituição? Se sim, qual é esse instrumento e qual é a sua abrangência? Em caso negativo, quais os óbices para que esse instrumento normativo seja criado?
13. Como a instituição gerencia incidentes de segurança envolvendo dados pessoais?
14. Qual é o principal tipo de incidente identificado? Você poderia citar algum caso específico e como foi tratado?
15. Já houve algum episódio de incidente/vazamento de da dos pessoais pelo qual a UFRPE respondeu legalmente?
16. A instituição oferece capacitação e programas de conscientização sobre a proteção de dados pessoais de forma sistemática? Se sim, quem participa dessa capacitação?
17. Na sua opinião, quais ações devem ser adotadas para fortalecer a cultura de proteção de dados pessoais na UFRPE?
18. Na sua opinião, no âmbito geral, quais os desafios da instituição para implementação das práticas de proteção de dados pessoais? Dentre esses, no âmbito de sua atuação, qual deles você ressalta?

ANEXO – *FRAMEWORK* DE PROTEÇÃO DE DADOS

Para cada questão, responda: Sim (S), Não (N), Parcialmente (P), Não Aplicável (NA)

Seção	ID	Questão	Resposta
1. Segurança para Privacidade	1.1	A equipe de trabalho ou organização possui inventário de ativos sistêmicos centralizado e atualizado?	
	1.2	Os sistemas em que são armazenados dados pessoais possuem *backup*?	
	1.3	A organização ou equipe de trabalho conta com normativos de segurança da informação publicados e comunicados?	
	1.4	Os ativos sistêmicos da organização contam com recursos que controlem o acesso físico e lógico?	
	1.5	Os dados pessoais processados nos ativos sistêmicos da organização são criptografados em trânsito e em repouso?	
	1.6	A organização ou equipe de trabalho conta com plano de continuidade de negócios e recuperação de desastres?	
	1.7	Os *data centers* físicos gerenciados pela organização possuem infraestrutura de segurança nos termos da ISO 27001?	
	1.8	Regras de gestão de acessos aos sistemas de acordo com a necessidade e adequação de cada colaborador (controle de acessos e segregação de funções)?	
	1.9	É mantida trilha de auditoria de acesso, edição, cópia ou deleção de dados em todos os ativos da empresa que possuem dados pessoais?	
	1.10	São aplicadas regras de anonimização, pseudonimização e/ou mascaramento aos dados pessoais?	
	1.11	A organização ou equipe de trabalho possui Comitê de Segurança da Informação?	
	1.12	A companhia estabeleceu regras para a utilização de dispositivos eletrônicos corporativos ou pessoais?	
	1.13	A organização ou equipe de trabalho conta com medidas de controle de segurança para acesso a rede da empresa?	
	1.14	A organização utiliza plataformas colaborativas seguras para fins de comunicações profissionais?	
2. Estrutura de Privacidade	2.1	Há uma estrutura organizacional de governança para Privacidade?	
	2.2	Um Programa de Privacidade foi estabelecido?	
	2.3	Há uma Matriz de Riscos de Privacidade ou alguma identificação dos possíveis riscos?	
	2.4	Foi nomeado um DPO (Encarregado pelo Tratamento de Dados)?	

Seção	ID	Questão	Resposta
	2.5	A organização conta com equipe/comitê de Privacidade?	
	2.6	A equipe de trabalho é constantemente conscientizada acerca da proteção de dados e privacidade?	
	2.7	Há algum canal para contato e interação entre titular e encarregado?	
	2.8	Foram estabelecidas Políticas, Normas e Procedimentos de Privacidade?	
	2.9	A organização ou equipe já possui Política de Privacidade (interna e externa) publicadas e comunicadas?	
	2.10	A organização ou equipe estabeleceu matriz RACI para distribuição dos papéis e responsabilidades em Privacidade?	
3. Inventário de Dados Pessoais	3.1	Todos os dados pessoais tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	
	3.2	Todos os dados sensíveis tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	
	3.3	Todos os dados pessoais de menores de idade tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	
	3.4	Todos os dados pessoais de estrangeiros tratados foram identificados e classificados ou pelo menos há mecanismos para fazê-los?	
	3.5	O inventário de dados pessoais já foi estabelecido?	
	3.6	A Equipe conta com mecanismos, já implementados, para o gerenciamento do ciclo de vida dos dados pessoais?	
	3.7	Existe regra de temporalidade definida para a retenção de dados pessoais, incluindo a retenção embasada em legislações específicas?	
4. Legitimidade no Tratamento	4.1	Foram atribuídas bases legais a todas as operações de tratamento de forma adequada?	
	4.2	A organização possui meios de garantir que os dados pessoais são tratados de acordo com finalidades adequadas?	
	4.3	A organização dispõe de meios para garantir que apenas dados pessoais necessários são tratados?	
	4.4	A organização possui meios para comprovar a coleta do consentimento para o tratamento de dados que necessitem de tal base legal?	
	4.5	A organização coleta o consentimento dos responsáveis para o tratamento de dados de crianças?	
	4.6	A organização possui critérios para avaliar o Legítimo Interesse da Organização (LIA - Avaliação de Legítimo Interesse)?	
	4.7	A organização possui meios de assegurar que o titular tenha livre acesso a seus dados pessoais?	

Seção	ID	Questão	Resposta
	4.8	A organização possui entendimento acerca da sua atuação como Operadora e/ou Controladora de dados?	
5. Atendimento a Requisições	5.1	A organização de trabalho possui mecanismo para realizar o atendimento a requisições de titulares de dados?	
	5.2	A organização já realizou atendimento á requisições de titulares de dados?	
	5.3	A organização já eliminou dados pessoais a pedido do titular?	
	5.4	A organização possui meios para registrar e evidenciar que o atendimento às requisições de direitos dos titulares dos dados pessoais foi realizado?	
	5.5	A organização de trabalho já elaborou um modelo de Relatório de Impacto à Proteção de Dados (RIPD)?	
	5.6	A organização já realizou um Relatório de Impacto à Proteção de Dados?	
	5.7	A organização possui meios de identificar, registrar e tratar violações de privacidade?	
	5.8	A organização de trabalho possui mecanismos para informar ao titular e a ANPD acerca de violações a privacidade?	
6. Conformidade de Terceiros	6.1	A equipe elaborou cláusulas de Privacidade e atualizou contratos padrões?	
	6.2	A equipe aditou contratos existentes com cláusulas de Privacidade?	