



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ISAAC ROZAS RIOS

**TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO
BRASIL: proposta de modelo de maturidade sob a perspectiva dos marcos
legais brasileiros**

JOÃO PESSOA

2024

ISAAC ROZAS RIOS

**TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO
BRASIL: proposta de modelo de maturidade sob a perspectiva dos marcos
legais brasileiros**

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial à obtenção do título de Doutor em Ciência da Informação.

Área de concentração: Ética, Gestão e Políticas de Informação.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

JOÃO PESSOA

2024

Catálogo na publicação
Seção de Catalogação e Classificação

R586t Rios, Isaac Rozas.

Tratamento dos dados pessoais nas universidades
federais do Brasil : proposta de modelo de maturidade
sob a perspectiva dos marcos legais brasileiros / Isaac
Rozas Rios. - João Pessoa, 2024.
533 f. : il.

Orientação: Wagner Junqueira de Araújo.
Tese (Doutorado) - UFPB/CCSA.

1. Lei Geral de Proteção de Dados. 2. Método Delphi.
3. Modelo de maturidade. 4. Segurança da informação. 5.
Dados pessoais - Tratamento. I. Araújo, Wagner
Junqueira de. II. Título.

UFPB/BC

CDU 001.103:342.537.3(043)

ISAAC ROZAS RIOS

**TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO
BRASIL: proposta de modelo de maturidade sob a perspectiva dos marcos
legais brasileiros**

Tese apresentada à Universidade Federal da Paraíba
como parte das exigências do Programa de
Pós-Graduação em Ciência da Informação do Centro de
Ciências Sociais, para obtenção do título de Doutor em
Ciência da Informação.

Área de concentração: Ética, Gestão e Políticas de
Informação.

BANCA EXAMINADORA

Prof. Dr. Wagner Junqueira de Araújo
PPGCI/UFPB (Orientador)

Prof. Dr. Felipe Sá Brasileiro
PPGCI/UFPB (Membro interno)

Prof. Dr. Marckson Roberto Ferreira de Sousa
PPGCI/UFPB (Membro interno)

Prof.^a Dr.^a Marcia Maria De Medeiros Travassos Saeger
PPGCI/UFPB (Membro interno)

Prof.^a Dr.^a Julianne Teixeira e Silva
(Membro externo)

Prof. Dr.^a Ana Carolina Kruta de Araújo Bispo
(Membro externo)

Prof. Dr. Denysson Axel Ribeiro Mota
(Membro externo)

João Pessoa, 18 de dezembro de 2024.



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ATA DE DEFESA DE TESE

Defesa nº 109

Ata da Sessão Pública de Defesa de Tese do(a) Doutorando(a) **ISAAC ROZAS RIOS** como requisito para obtenção do grau de Doutor(a) em Ciência da Informação, Área de Concentração em Informação, Conhecimento e Sociedade e com Linha de pesquisa em Ética, Gestão e Políticas da Informação.

No décimo oitavo dia do mês de dezembro de dois mil e vinte e quatro (18/12/2024), das quatorze horas e trinta minutos às 14:30, na sala virtual do Google Meet, conectaram-se via videoconferência a banca examinadora designada pelo Colegiado do Programa de Pós-Graduação em Ciência da Informação para avaliar o(a) candidato(a) ao Grau de Doutor(a) em Ciência da Informação na Área de Concentração Informação, Conhecimento e Sociedade, o(a) doutorando(a) **ISAAC ROZAS RIOS**. A defesa ocorreu de forma remota, com acesso por meio do link: (<https://meet.google.com/cnj-ogka-eyq>) A banca examinadora foi composta pelos (as) professores(as): Dr. Wagner Junqueira de Araújo – PPGCI/UFPB (Presidente/Orientador), Dr. Fellipe Sá Brasileiro – PPGCI/UFPB (Examinador interno), Dr. Marckson Roberto Ferreira de Sousa – PPGCI/UFPB (Examinador interno), Dra. Ana Carolina Kruta de Araújo Bispo – UFPB (Examinadora externa), Dr. Denysson Axel Ribeiro Mota – UFCA (Examinador externo), Dra. Marcia Maria de Medeiros Travassos Saeger – PPGCI/UFPB (Suplente Interna) e Dra. Julianne Teixeira e Silva – UFPB (Suplente Externa). Dando início aos trabalhos, o(a) Professor(a) Dr(a). Wagner Junqueira de Araújo, Presidente(a) da Banca Examinadora, explicou aos presentes a finalidade da sessão e passou a palavra ao(à) discente para que fizesse oralmente a apresentação do trabalho de tese intitulado: **“TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de modelo de maturidade sob a perspectiva dos marcos legais brasileiros”**. Após a apresentação, o(a) doutorando(a) foi arguido(a) na forma regimental pelos examinadores. Respondidas todas as arguições, o(a) Professor(a) Dr(a). Wagner Junqueira de Araújo, Presidente(a) da Banca Examinadora, acatou todas as observações da banca e procedeu para o julgamento do trabalho, concluindo por atribuir-lhe o conceito:

(X) Aprovado () Insuficiente () Reprovado.

Observações da Banca: A banca considera o trabalho adequado ao que se espera em uma tese de doutorado.
A banca deliberou que devem ser efetuados ajustes sugeridos pelos avaliadores, com atenção especial a seção metodológica.
Incluir um tópico sobre o modelo desenvolvido.
A banca recomenda o trabalho para publicação de partes da tese em artigos e em um livro.

Proclamados os resultados e encerrados os trabalhos, eu, Professor(a) Dr.(a) Wagner Junqueira de Araújo, Presidente da Banca Examinadora, lavrei a presente ata que segue assinada por mim pelos(as) participantes da banca, juntamente com os pareceres de avaliação da tese e da defesa de tese do(a) doutorando(a), devidamente assinados por seus respectivos avaliadores e em formato digital.

João Pessoa, 18 de dezembro de 2024.

Dr. Wagner Junqueira de Araújo
Presidente/ Orientador (a) – PPGCI/UFPB

Dr. Fellipe Sá Brasileiro
Examinador (a) Interno (a) – PPGCI/UFPB

Dr. Marckson Roberto Ferreira de Sousa
Examinador(a) Interno(a) – PPGCI/UFPB

Dra. Ana Carolina Kruta de Araújo Bispo
Examinador (a) Externo (a) – UFPB

Documento assinado digitalmente
 **DENYSSON AXEL RIBEIRO MOTA**
Data: 18/12/2024 17:21:43-0300
Verifique em <https://validar.iti.gov.br>

Dr. Denysson Axel Ribeiro Mota
Examinador (a) Externo (a) – UFCA

Dra. Marcia M^a de Medeiros Travassos Saeger
Suplente Interno(a) –PPGCI/UFPB

Dra. Julianne Teixeira e Silva Suplente
Externo (a) – UFPB

Isaac Rozas Rios
Doutorando(a)

Emitido em 18/12/2024

ATA Nº 1/2024 - PPGCI (11.01.13.37)
(Nº do Documento: 1)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 08/01/2025 15:22)
ANA CAROLINA KRUTA DE ARAUJO BISPO
PROFESSOR DO MAGISTERIO SUPERIOR
1671678

(Assinado digitalmente em 11/01/2025 12:28)
FELLIPE SÁ BRASILEIRO
PROFESSOR DO MAGISTERIO SUPERIOR
1140700

(Assinado digitalmente em 08/01/2025 10:47)
ISAAC ROZAS RIOS
ARQUIVISTA
2352982

(Assinado digitalmente em 10/01/2025 10:33)
JULIANNE TEIXEIRA E SILVA
PROFESSOR DO MAGISTERIO SUPERIOR
1749263

(Assinado digitalmente em 09/01/2025 16:19)
MARCIA MARIA DE MEDEIROS TRAVASSOS
SAEGER
PROFESSOR DO MAGISTERIO SUPERIOR
1853959

(Assinado digitalmente em 08/01/2025 23:02)
MARCKSON ROBERTO FERREIRA DE SOUSA
PROFESSOR DO MAGISTERIO SUPERIOR
1742362

(Assinado digitalmente em 08/01/2025 10:36)
WAGNER JUNQUEIRA DE ARAUJO
PROFESSOR DO MAGISTERIO SUPERIOR
1253974

Para verificar a autenticidade deste documento entre em <https://sipac.ufpb.br/documentos/> informando seu número: **1**,
ano: **2024**, documento (espécie): **ATA**, data de emissão: **08/01/2025** e o código de verificação: **d27a222d64**

AGRADECIMENTOS

Agradeço ao Prof. Dr. Wagner Junqueira de Araújo pela orientação e parceria durante esta jornada. Sua experiência e dedicação foram fundamentais para a realização deste trabalho.

Expresso também minha gratidão aos membros da Banca Examinadora, Prof. Dr. Felipe Sá Brasileiro, Prof. Dr. Marckson Roberto Ferreira de Sousa, Prof.^a Dr.^a Marcia Maria De Medeiros Travassos Saeger, Prof.^a Dr.^a Julianne Teixeira e Silva; Prof. Dr.^a Ana Carolina Kruta de Araújo Bispo e Prof. Dr. Denysson Axel Ribeiro Mota, pelo tempo e contribuições enriquecedoras que possibilitaram o aprimoramento desta pesquisa.

À minha família, pelo apoio, e ao meu filho Samuel, que é minha inspiração diária, minha profunda gratidão por estarem sempre ao meu lado, me incentivando a seguir em frente. Este trabalho também é de vocês.

RESUMO

O avanço tecnológico e os desafios contemporâneos reforçam a importância do tratamento responsável dos dados pessoais, diante dos riscos e impactos associados ao uso inadequado. No âmbito de instituições públicas, como as universidades federais brasileiras, a conformidade normativa enfrenta dificuldades específicas, demandando práticas alinhadas à Lei Geral de Proteção de Dados (LGPD) e outros marcos legais. Este estudo objetivou desenvolver e validar o Modelo de Maturidade para Tratamento de Dados Pessoais (MMTDP), concebido para diagnosticar, planejar e aprimorar práticas. A pesquisa delimitou seu campo às 69 universidades federais brasileiras. Exploratória e descritiva, adotou abordagem qualiquantitativa e foi estruturada com base em estudos de casos múltiplos. A construção do modelo seguiu etapas fundamentadas em literatura especializada, análises normativas e legislações, como a LGPD. A validação foi realizada por meio do método *Delphi*, envolvendo especialistas em proteção de dados pessoais, que contribuíram para ajustes e refinamentos no instrumento de medição. Após a validação, a aplicação prática do MMTDP alcançou 95,65% de participação (66 instituições), permitindo diagnósticos que revelam lacunas e melhorias nas práticas de tratamento de dados pessoais. O modelo, estruturado em cinco dimensões e cinco níveis de maturidade, contempla 25 questões no seu instrumento de medição, promovendo análises comparativas regionais e nacionais, destacando quatro universidades representativas com cenários de níveis de maturidade distintos. A pesquisa percorreu desde a delimitação do campo até a validação empírica, culminando na análise dos resultados. Entre as principais contribuições do modelo, destacam-se sua integração com ferramentas estratégicas e sua capacidade de fomentar avanços contínuos na conformidade normativa e na gestão estratégica de dados pessoais. O MMTDP emerge, portanto, como um instrumento robusto, capaz de apoiar as universidades federais na busca pela excelência, promovendo práticas mais seguras e transparentes na proteção de dados pessoais. Além disso, fortalece a governança e contribui para uma cultura de privacidade e conformidade no setor público, servindo como referência para outras instituições e pesquisas.

Palavras-chave: Lei Geral de Proteção de Dados. Método *Delphi*. Modelo de Maturidade. Segurança da Informação. Tratamento de Dados Pessoais.

ABSTRACT

Technological advancement and contemporary challenges underscore the importance of responsibly handling personal data, given the risks and impacts associated with its improper use. Within public institutions, such as Brazilian federal universities, regulatory compliance faces specific difficulties, requiring practices aligned with the General Data Protection Law (LGPD) and other legal frameworks. This study aimed to develop and validate the Maturity Model for Personal Data Processing (MMTDP), designed to diagnose, plan, and improve practices. The research focused on the 69 federal universities in Brazil. Exploratory and descriptive, it adopted a qualitative-quantitative approach and was structured based on multiple case studies. The model's development followed steps grounded in specialized literature, normative analyses, and legislation, including LGPD. Validation was conducted using the Delphi method, involving experts in personal data protection, who contributed to adjustments and refinements in the measurement instrument. After validation, the practical application of MMTDP achieved 95.65% participation (66 institutions), enabling diagnoses that reveal gaps and improvements in personal data processing practices. The model, structured into five dimensions and five maturity levels, encompasses 25 questions in its measurement instrument, promoting regional and national comparative analyses, highlighting four representative universities with varying maturity levels. The research spanned from field delimitation to empirical validation, culminating in the analysis of results. Among the model's key contributions are its integration with strategic tools and its ability to drive continuous advancements in regulatory compliance and strategic data management. Therefore, MMTDP emerges as a robust instrument, capable of supporting federal universities in their pursuit of excellence, fostering safer and more transparent practices in personal data protection. Additionally, it strengthens governance and contributes to a culture of privacy and compliance in the public sector, serving as a reference for other institutions and research.

Keywords: Delphi Method. General Data Protection Law. Information Security. Maturity Model. Personal Data Processing.

LISTA DE FIGURAS

Figura 1 - Estrutura do trabalho	26
Figura 2 - Fases de desenvolvimento do modelo de maturidade	77
Figura 3 - Fluxograma do método Delphi	102
Figura 4 - Modelo de maturidade para tratamento de dados pessoais	105
Figura 5 - Dimensões do modelo de maturidade para tratamento de dados pessoais	109

LISTA DE QUADROS

Quadro 1 - Marcos históricos sobre privacidade, proteção e tratamento de dados pessoais	37
Quadro 2 - Principais semelhanças entre o GDPR e a LGPD	40
Quadro 3 - Principais divergências entre o GDPR e a LGPD	43
Quadro 4 - Formas de busca utilizada na pesquisa sobre MM	58
Quadro 5 - Modelos de maturidade consagrados na literatura	67
Quadro 6 - As Universidades Federais credenciadas no MEC	87
Quadro 7 - Etapas de aplicação do método Delphi	98
Quadro 8 - Proposta de aplicação do método Delphi nesta pesquisa	102
Quadro 9 - Legislações e Normas que fundamentaram as dimensões	108
Quadro 10 - Síntese das referências legais e normativas utilizada	114
Quadro 11 - LGPD e a predominância da dimensão	116
Quadro 12 - Resolução CONARQ n. 54/2023 e a predominância da dimensão	117
Quadro 13 - Temas definidos para elaboração das questões	119
Quadro 14 - Normas técnicas e jurídicas utilizadas na elaboração das questões	120
Quadro 15 - Critérios de avaliação a partir da segunda rodada	125
Quadro 16 - Respostas positivas da aplicação do método Delphi na primeira rodada	127
Quadro 17 - Questões para a segunda rodada do método Delphi	127
Quadro 18 - Respostas positivas da aplicação do método Delphi na segunda rodada	130
Quadro 19 - Resultado da avaliação e classificação das questões	131
Quadro 20 - Resultado da avaliação e classificação das questões	136
Quadro 21 - Classificação da maturidade	136
Quadro 22 - Ajustes no instrumento de medição do MMTDP	143
Quadro 23 - Questões do instrumento de medição que envolve cada dimensão	146
Quadro 24 - Distribuição das Instituições participantes por classificação	151
Quadro 25 - Classificação da universidades da região norte	154
Quadro 26 - Classificação da universidades da região nordeste	156
Quadro 27 - Classificação da universidades da região centro-oeste	158
Quadro 28 - Classificação da universidades da região sudeste	160
Quadro 29 - Classificação da universidades da região sul	163
Quadro 30 - Respostas do instrumento de medição da UFC	165
Quadro 31 - Pontuação e classificação da UFC	166
Quadro 32 - Respostas do instrumento de medição da UFPB	183
Quadro 33 - Pontuação e classificação da UFPB	184
Quadro 34 - Respostas do instrumento de medição da UFBA	202
Quadro 35 - Pontuação e classificação da UFBA	203
Quadro 36 - Respostas do instrumento de medição da UFRGS	221
Quadro 37 - Respostas do instrumento de medição da UFRGS	222

LISTA DE GRÁFICOS

Gráfico 1 - Classificação do nível de maturidade das universidades por dimensão	152
Gráfico 2 - Classificação do nível de maturidade global das universidades participantes	153
Gráfico 3 - Nível de maturidade das universidades da região norte	155
Gráfico 4 - Nível de maturidade das universidades da região nordeste	157
Gráfico 5 - Nível de maturidade das universidades da região centro-oeste	159
Gráfico 6 - Nível de maturidade das universidades da região sudeste	162
Gráfico 7 - Nível de maturidade das universidades da região sul	164
Gráfico 8 - Níveis de maturidade da Universidade Federal do Ceará	181
Gráfico 9 - Níveis de maturidade da Universidade Federal da Paraíba	200
Gráfico 10 - Níveis de maturidade da Universidade Federal da Bahia	219
Gráfico 11 - Níveis de maturidade da Universidade Federal do Rio Grande do Sul	242
Gráfico 12 - Comparação entre as instituições detalhadas	244

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
APPI	<i>Act on the Protection of Personal Information</i>
BPM	<i>Business Process Management</i>
BPMMM	<i>Business Process Management Maturity Model</i>
BRAPCI	Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação
BSC	<i>Balanced Scorecard</i>
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCPA	<i>Califórnia Consumer Privacy Act</i>
CD	Conselho Diretor
CIM3	<i>Construction Industry Macro Maturity Model</i>
CGLGPD	Comitê Gestor da Lei Geral de Proteção de Dados Pessoais
CMM	<i>Capability Maturity Model</i>
CMMI	<i>Capability Maturity Model Integration</i>
CONARQ	Conselho Nacional de Arquivos
CPF	Certidão de Pessoa Física
DPO	<i>Data Protection Officer</i>
EC	European Community
EIA	<i>Electronic Industries Alliance</i>
EPD	Encarregado de Proteção de Dados
Fala.BR	Plataforma Integrada de Ouvidoria e Acesso à Informação
FURG	Universidade Federal do Rio Grande
GDPR	<i>General Data Protection Regulation</i>
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ICMM	<i>Industrialized Construction Maturity Model</i>
IEC	<i>International Electrotechnical Commission</i>
IN	Instrução Normativa
INSS	Instituto Nacional do Seguro Social
IPD-CMM	Integrated Product Development Capability Maturity Model
ISO	<i>International Organization for Standardisation</i>
KMMM	Knowledge Management Maturity Model

KPMMM	<i>Kerzner Project Management Maturity Model</i>
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
LGPD ^P	<i>Ley General de Protección de Datos Personales</i>
ME	Ministério da Economia
MEC	Ministério da Educação
MM	Modelo de Maturidade
MMGP	Modelo de Maturidade em Gerenciamento de Projetos
MMTDP	Modelo de Maturidade para Tratamento de Dados Pessoais
MPS.BR	Modelo de Processo do Software Brasileiro
NASA	<i>National Aeronautics and Space Administration</i>
NBR	Normas Brasileiras
OPM3	<i>Organizational Project Management Maturity Model</i>
P2MM	<i>PRINCE2 Maturity Model</i>
P3M3	<i>Portfolio, Programme and Project Management Maturity Model</i>
PDCA	Plan, Do, Check and Act
PDPA	Lei de Proteção de Dados Pessoais da Argentina
PPGCI	Programa de Pós-Graduação em Ciência da Informação
(PM)2	<i>Project Management Process Maturity Model</i>
PMI	<i>Project Management Institute</i>
PMMM	<i>Project Management Maturity Model</i>
QMMG	<i>Quality Management Maturity Grid</i>
RG	Regulamento Geral
RGPD	Regulamento Geral sobre a Proteção de Dados
SEI	<i>Software Engineering Institute</i>
SOFTEX	Associação para Promoção da Excelência do Software Brasileiro
SGD	Secretaria de Governo Digital
SNDMM	<i>Sustainable Network Design Maturity Model</i>
SPICE	<i>Standardized Process Improvement for Construction Enterprises</i>
SWOT	<i>Strenghts, Weaknesses, Opportunities e Threats</i>
TC	Tribunal de Contas
TCU	Tribunal de Contas da União
TCLE	Termo de Consentimento Livre e Esclarecido
TRLs	<i>Technology Readiness Levels</i>

UE	União Europeia
UFABC	Universidade Federal do ABC
UFAC	Universidade Federal do Acre
UFAL	Universidade Federal de Alagoas
UFAM	Universidade Federal do Amazonas
UFAPE	Universidade Federal do Agreste de Pernambuco
UFBA	Universidade Federal da Bahia
UFC	Universidade Federal do Ceará
UFCA	Universidade Federal do Cariri
UFCAT	Universidade Federal de Catalão
UFCG	Universidade Federal de Campina Grande
UFCSPA	Universidade Federal de Ciências da Saúde de Porto Alegre
UFDPAR	Universidade Federal do Delta do Parnaíba
UFERSA-RN	Universidade Federal Rural do Semi-Árido
UFES	Universidade Federal do Espírito Santo
UFF	Universidade Federal Fluminense
UFFS	Universidade Federal da Fronteira do Sul
UFG	Universidade Federal de Goiás
UFGD	Universidade Federal da Grande Dourados
UFJ	Universidade Federal de Jataí
UFJF	Universidade Federal de Juiz de Fora
UFLA	Universidade Federal de Lavras
UFMA	Universidade Federal do Maranhão
UFMG	Universidade Federal de Minas Gerais
UFMS	Universidade Federal de Mato Grosso do Sul
UFMT	Universidade Federal de Mato Grosso
UFNT	Universidade Federal do Norte de Tocantins
UFOB	Universidade Federal do Oeste da Bahia
UFOP	Universidade Federal de Ouro Preto
UFOPA	Universidade Federal do Oeste do Pará
UFPA	Universidade Federal do Pará
UFPB	Universidade Federal da Paraíba
UFPE	Universidade Federal de Pernambuco
UFPEL	Universidade Federal de Pelotas

UFPI	Universidade Federal do Piauí
UFPR	Universidade Federal do Paraná
UFR	Universidade Federal de Rondonópolis
UFRA	Universidade Federal Rural da Amazônia
UFRB	Universidade Federal do Recôncavo da Bahia
UFRGS	Universidade Federal do Rio Grande do Sul
UFRJ	Universidade Federal do Rio de Janeiro
UFRN	Universidade Federal do Rio Grande do Norte
UFRPE	Universidade Federal Rural de Pernambuco
UFRR	Universidade Federal de Roraima
UFRRJ	Universidade Federal Rural do Rio de Janeiro
UFS	Universidade Federal de Sergipe
UFSB	Universidade Federal do Sul da Bahia
UFSC	Universidade Federal de Santa Catarina
UFSCAR	Universidade Federal de São Carlos
UFSJ	Universidade Federal de São João del-Rei
UFSM	Universidade Federal de Santa Maria
UFT	Universidade Federal do Tocantins
UFTM	Universidade Federal do Triângulo Mineiro
UFU	Universidade Federal de Uberlândia
UFV	Universidade Federal de Viçosa
UFVJM	Universidade Federal dos Vale do Jequitinhonha e Mucuri
UNB	Universidade de Brasília
UNIFAL-MG	Universidade Federal de Alfenas
UNIFAP	Universidade Federal do Amapá
UNIFEI	Universidade Federal de Itajubá
UNIFESP	Universidade Federal de São Paulo
UNIFESSPA	Universidade Federal do Sul e Sudeste do Pará
UNILA	Universidade Federal da Integração Latino-Americana
UNILAB	Universidade da Integração Internacional da Lusofonia Afro-Brasileira
UNIPAMPA	Universidade Federal do Pampa
UNIR	Universidade Federal de Rondônia
UNIRIO	Universidade Federal do Rio de Janeiro
UNIVASF	Universidade Federal do Vale do São Francisco

SUMÁRIO

1 INTRODUÇÃO	18
1.1 Justificativa	22
1.2 Objetivos	24
1.2.1 Objetivo geral	24
1.2.2 Objetivos específicos	24
1.3 Estrutura do trabalho	24
2 LEGISLAÇÕES SOBRE TRATAMENTO DE DADOS PESSOAIS	27
2.1 Marcos históricos até a década de 80	27
2.2 Marcos históricos após a década de 80 e o Brasil	30
2.3 Regulamento Geral de Proteção de Dados Europeu e a Lei Geral de Proteção de Dados Brasileira	39
2.4 Principais elementos e aspectos da Lei Geral de Proteção de Dados Brasileira para as Organizações Públicas	47
2.4.1 Princípios Fundamentais	47
2.4.2 Tratamento de Dados sensíveis	48
2.4.3 Responsabilidades da Administração Pública	50
2.4.4 Fiscalização e Sanções	51
2.4.5 Outras legislações e normativas que impactam no tratamento dos dados e informações pessoais	53
3 MODELO DE MATURIDADE	57
3.1 Conceito	59
3.2 Breve histórico	62
3.3 Objetivos do modelo de maturidade	68
3.4 Fundamentos de modelo de maturidade	70
3.5.1 Dimensões	70
3.5.2 Níveis de maturidade	71
3.5.3 Natureza dos modelos de maturidade	74
3.5.4 Eficácia e aplicabilidade de um modelo de maturidade	76
3.5 Construção de um modelo de maturidade	77
4 PERCURSO METODOLÓGICO	82
4.1 Caracterização da pesquisa	82
4.2 Delimitação do campo e sujeitos da pesquisa	86
4.3 Universo e amostra da pesquisa	91
4.4 Instrumentos e percursos para coleta e análise dos dados	94
4.5 Método Delphi	95
4.5.1 Características do Método Delphi	95
4.5.2 Vantagens e desvantagens	97
4.5.3 Etapas de aplicação do método	98
4.5.3.1 Escolha dos especialistas	99
4.5.3.2 Rodada Inicial	99
4.5.3.3 Feedback controlado	100
4.5.3.4 Rodadas subsequentes	100
4.5.3.5 Consenso e relatório final	101

4.5.4 Aplicação do método Delphi para os objetivos desta pesquisa	102
4.6 Etapas para o Desenvolvimento e Validação do Modelo de Maturidade	103
5 DESENVOLVIMENTO DO MODELO DE MATURIDADE PARA TRATAMENTO DE DADOS PESSOAIS	105
5.1 Escopo	105
5.2 Design do modelo	106
5.2.1 Níveis de Maturidade	106
5.2.2 Dimensões para o tratamento de dados e informações pessoais	108
5.2.3 Natureza do modelo proposto	112
5.3 Preencher	112
5.3.1 Conteúdo: Fundamentação legal e normativa do instrumento de medição do modelo de maturidade	113
5.3.2 Conteúdo: Correlação entre os artigos das leis e os itens normativos com as dimensões do Modelo proposto	115
5.3.3 Conteúdo: Definição dos temas e assuntos propostos para o instrumento de medição	118
5.3.4 Conteúdo: Correlação dos temas e assuntos propostos em cada questão com as normas legais e técnicas	120
5.3.5 Método de avaliação: Construção e formatação do questionário inicial - Instrumento de Medição	122
5.3.6 Método de avaliação: Aplicação do Método Delphi	123
5.3.6.1 Validação do questionário antes de iniciar a primeira rodada	124
5.3.6.2 Critérios do Delphi para a primeira rodada	124
5.3.6.3 Critérios do Delphi para as rodadas seguintes	125
5.3.6.4 Realização da primeira rodada do método Delphi	125
5.3.6.5 Realização da segunda rodada do método Delphi	129
5.3.6.6 Encerramento do Delphi e consolidação do instrumento de medição	132
5.3.6.7 Refinamento do instrumento	132
5.3.7 Mecanismo de medição do Modelo de Maturidade para Tratamento de Dados Pessoais	133
5.3.7.1 Estrutura do Instrumento de Medição	133
5.3.7.2 Escala de Avaliação	133
5.3.7.3 Ponderação das Questões	134
5.3.7.4 Cálculo da Maturidade nas dimensões	134
5.3.7.5 Classificação no Nível de Maturidade:	136
5.3.7.4 Cálculo da Maturidade Global	137
5.3.7.5. Relatório de análises e resultados	138
5.3.7.6 Validação e Revisão Periódica	139
5.4 Testar e Implementar	139
6 ANÁLISES E RESULTADOS	146
6.1 Tipos de análises do MMTDP	147
6.1.1 Análise Institucional	147
6.1.1.1 Análise por dimensão	147
6.1.1.2 Análise global ou holística	148
6.1.2 Análise Comparativa	149
6.2 Resultados Gerais	151

6.2.1 Panorama no contexto nacional	151
6.2.2 Análise Regional: Região Norte	154
6.2.3 Análise Regional: Região Nordeste	156
6.2.4 Análise Regional: Região Centro-Oeste	158
6.2.5 Análise Regional: Região Sudeste	160
6.2.6 Análise Regional: Região Sul	163
6.3 Resultados Institucionais	165
6.3.1 Universidade Federal do Ceará (UFC)	165
6.3.1.1 Dimensão 1: Governança de Dados e Boas Práticas	167
6.3.1.2 Dimensão 2: Políticas e Processos de Tratamento de Dados	169
6.3.1.3 Dimensão 3: Treinamento e Conscientização	172
6.3.1.4 Dimensão 4: Segurança da Informação e Tecnologia	175
6.3.1.5 Dimensão 5: Acesso à Informação e Transparência	178
6.3.1.6 Análise Global da Instituição	180
6.3.2 Universidade Federal da Paraíba (UFPB)	183
6.3.2.1 Dimensão 1: Governança de Dados e Boas Práticas	185
6.3.2.2 Dimensão 2: Políticas e Processos de Tratamento de Dados	188
6.3.2.3 Dimensão 3: Treinamento e Conscientização	191
6.3.2.4 Dimensão 4: Segurança da Informação e Tecnologia	194
6.3.2.5 Dimensão 5: Acesso à Informação e Transparência	197
6.3.2.6 Análise Global da Instituição	200
6.3.3 Universidade Federal da Bahia (UFBA)	202
6.3.3.2 Dimensão 2: Políticas e Processos de Tratamento de Dados	207
6.3.3.3 Dimensão 3: Treinamento e Conscientização	210
6.3.3.4 Dimensão 4: Segurança da Informação e Tecnologia	212
6.3.3.5 Dimensão 5: Acesso à Informação e Transparência	216
6.3.3.6 Análise Global da Instituição	218
6.3.4 Universidade Federal do Rio Grande do Sul (UFRGS)	221
6.3.4.1 Dimensão 1: Governança de Dados e Boas Práticas	223
6.3.4.2 Dimensão 2: Políticas e Processos de Tratamento de Dados	227
6.3.4.3 Dimensão 3: Treinamento e Conscientização	230
6.3.4.4 Dimensão 4: Segurança da Informação e Tecnologia	234
6.3.4.5 Dimensão 5: Acesso à Informação e Transparência	238
6.3.4.6 Análise Global da Instituição	241
6.3.5 Comparando essas instituições	243
7 CONSIDERAÇÕES FINAIS	247
REFERÊNCIAS	249
APÊNDICE A - Marcos históricos sobre privacidade, proteção e tratamento de dados pessoais	261
APÊNDICE B - Questionário para identificação do encarregado pelo tratamento de dados pessoais nas universidades federais	265
APÊNDICE C - Diretrizes sobre o painel de especialistas	266
APÊNDICE D - Itens normativos envolvidos em cada uma das questões iniciais propostas para cada dimensão do modelo de maturidade	268
APÊNDICE E – As 50 primeiras questões propostas para compor o instrumento de	

medição do Modelo de Maturidade para Tratamento de Dados Pessoais	274
APÊNDICE F – Questionário inicial construído na plataforma questionpro e TCLE	285
APÊNDICE G – Relatório gerado pela plataforma questionpro após a primeira rodada do método delphi	314
APÊNDICE H – Relatório de feedback da primeira rodada do método delphi	368
APÊNDICE I – Questionário da segunda rodada na plataforma questionpro e TCLE	377
APÊNDICE J – Relatório de feedback da segunda rodada do método delphi (relatório final)	396
APÊNDICE K – Relatório gerado pela plataforma questionpro após a segunda rodada do método delphi	407
APÊNDICE L – Instrumento de medição do MMTDP	437
APÊNDICE M – Base de análises e recomendações padronizadas para cada resposta possível do instrumento de medição	450
APÊNDICE N – Relatório gerado pelo questionpro após o teste do modelo de maturidade	494
APÊNDICE O – Instrumento de medição ajustado após o teste piloto	519

1 INTRODUÇÃO

A globalização criou uma rede interconectada entre nações, resultando em um crescimento exponencial de dados que impacta diretamente a economia, os negócios, as políticas públicas e a sociedade em geral. Os avanços tecnológicos possibilitam um compartilhamento amplo e ágil, além da coleta e análise de grandes volumes de dados em tempo real, o que suscita preocupações crescentes quanto à privacidade e à segurança dessas informações. As populações contemporâneas convivem com a necessidade constante de atualização e preparação, pois a sociedade da informação exige uma reflexão sobre a importância dos dados e a urgência de prudência no tratamento dessas informações, especialmente no que tange à proteção de dados pessoais.

As instituições de ensino, em particular, vêm enfrentando um crescimento exponencial no volume de dados em razão das suas atividades de pesquisa, ensino e extensão. Esse aumento requer um tratamento cuidadoso das informações, especialmente para atender às exigências da Lei Geral de Proteção de Dados (LGPD) e de outras regulamentações pertinentes. Nesse contexto, a gestão responsável dos dados é fundamental para garantir a qualidade e a segurança das informações, gerando benefícios significativos para indivíduos e organizações e constituindo um diferencial competitivo. Sua operacionalização exige recursos tecnológicos, cumprimento de legislações e um sistema de gestão eficiente, sendo essencial para promover acessibilidade, transparência, controle, proteção, rastreabilidade e suporte à tomada de decisões.

Atualmente, observa-se um crescente envolvimento da sociedade com as inovações tecnológicas, impulsionado pela nova geração de “nativos digitais”. Crianças e adolescentes ingressam cada vez mais cedo na internet, redes sociais, aplicativos, serviços on-line, jogos eletrônicos e e-commerce. Todos esses meios envolvem dados que frequentemente revelam aspectos íntimos e privados da vida humana. Robredo (2011, p. 31) destaca que, "no contexto dominado pela cultura da Internet, a Ciência da Informação deve se preocupar com o comportamento dos usuários e com os meios que utilizam para satisfazer suas necessidades de informação."

Dessa forma, a maneira como dados e informações são tratados e organizados pode representar grandes riscos para indivíduos, organizações e a sociedade em geral. O crescimento desordenado do volume de dados, que circulam sem as devidas precauções, pode ocasionar sérios problemas, como ocorreu no Equador em setembro de 2019, quando cerca de 17 milhões de cidadãos tiveram seus dados vazados em um ataque hacker ao sistema de informações populacionais (Winder, 2019).

Em 2021, o Brasil também enfrentou episódios de vazamentos massivos de dados pessoais, revelando informações de cerca de 223 milhões de CPFs, quantidade que excede a estimativa da população brasileira, o que levanta suspeitas sobre a inclusão de dados de indivíduos falecidos. Essa exposição envolveu dados como nomes, datas de nascimento, endereços, além de informações sobre escolaridade, benefícios do Instituto Nacional do Seguro Social (INSS), renda, imagens faciais, *scores* de crédito, dados financeiros, declarações de imposto de renda, registros de telefonia e até mesmo informações do *LinkedIn*. A divulgação pública desses dados suscitou preocupações significativas quanto à segurança e à privacidade, sendo que esses vazamentos foram explorados por criminosos com fins lucrativos (G1, 2021). Diante desses cenários, evidencia-se a imprescindibilidade das normas e preceitos legais para o tratamento e proteção de dados pessoais.

No Brasil, diversas legislações abordam questões relacionadas à privacidade e à proteção dos dados. A Constituição Federal de 1988 menciona como inviolável a intimidade, a vida privada, a honra e a imagem da pessoa. O Código de Defesa do Consumidor (Lei n. 8.078/1990) estabelece a proteção do consumidor, bem como normas que sustentam as atividades dos bancos de dados de proteção ao crédito. O Código Civil Brasileiro (Lei n. 10.406/2002) assegura o direito da personalidade como intransmissível e irrenunciável. A Lei do Cadastro Positivo (Lei n. 12.414/2011) regulamenta bancos de dados com informações de adimplemento de pessoas físicas e jurídicas, com o objetivo de criar um histórico de crédito, e estabelece o direito de exclusão desses dados, mediante solicitação do titular. A Lei de Acesso à Informação (LAI), Lei n. 12.527/2011, dispõe, em seu art. 31, que “o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais”. A Lei n. 12.965/2014, também conhecida como Marco Civil da

Internet, define princípios, direitos e deveres do uso da internet no Brasil, reforçando a proteção de dados e os cuidados necessários para seu acesso e uso.

Até 2018, as legislações brasileiras abordavam questões específicas sobre o tratamento de dados pessoais, porém ainda não havia uma lei dedicada exclusivamente ao tema. Paralelamente, nesse mesmo ano, entrou em vigor o Regulamento Geral de Proteção de Dados na Europa, conhecido como GDPR (*General Data Protection Regulation*) ou RGPD (Regulamento Geral sobre a Proteção de Dados), que versa sobre os direitos de privacidade e proteção de dados pessoais na União Europeia (UE) e estabelece requisitos para transferências internacionais de dados.

Esse regulamento tem sido aplicado com rigor por seus reguladores. Em maio de 2023, uma multa recorde de US\$1,3 bilhão foi imposta à empresa Meta por transferir dados pessoais de usuários do *Facebook* na Europa para os servidores nos Estados Unidos. Ziady (2023) destaca que “o regulador da UE disse que o processamento e armazenamento de dados pessoais nos Estados Unidos infringe a lei europeia de privacidade de dados de assinatura, conhecida como Regulamento Geral de Proteção de Dados”. A empresa foi ainda condenada a cessar o processamento de dados pessoais dos usuários europeus em solo estadunidense no prazo de seis meses.

Como o Brasil não possuía uma legislação específica sobre proteção de dados, encontrava-se em desvantagem competitiva. Diante disso, e com a necessidade de acompanhar as mudanças internacionais, foi sancionada, em 14 de agosto de 2018, a Lei n. 13.709, conhecida como Lei Geral de Proteção de Dados, com métricas semelhantes às do GDPR, trazendo no seu art. 1º que esta Lei:

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

Essa legislação entrou em vigor plenamente a partir de 3 de maio de 2021, amparando diretamente a proteção dos dados dos indivíduos, regulamentando os princípios, direitos e obrigações relacionados ao tratamento dos dados e bases de dados pessoais, além de impor graves sanções aos operadores e controladores que descumprirem as disposições legais.

Atualmente, os órgãos públicos, e em especial as universidades federais, empenham-se em aprimorar o uso do conteúdo informacional de seus acervos, com o intuito de elevar a eficiência operacional e assegurar o monitoramento contínuo de suas atividades e processos organizacionais. No entanto, esse esforço ocorre em um cenário de crescente exigência de conformidade com legislações e normas que regulamentam a proteção e o devido tratamento de dados pessoais, especialmente com a implementação da Lei Geral de Proteção de Dados.

Diante desse contexto, formula-se o seguinte problema de pesquisa: **Em que medida as universidades federais brasileiras atendem aos requisitos legais do país para o tratamento e a proteção de dados pessoais?** Esse questionamento é de natureza interdisciplinar, envolvendo conhecimentos da Ciência da Informação, Arquivologia, Tecnologia da Informação, Segurança da Informação e Direito. Engloba aspectos práticos e teóricos dessas áreas, que convergem para assegurar a conformidade legal e a proteção dos dados administrados.

Neste cenário, pressupõe-se que, embora as universidades federais brasileiras busquem continuamente aprimorar seus sistemas, processos e serviços, a implementação das ações necessárias para alcançar conformidade plena com as exigências legais de proteção de dados enfrenta obstáculos específicos, inerentes ao contexto administrativo e organizacional desses órgãos públicos. A burocracia institucional torna o planejamento e a execução das medidas de conformidade mais lentos, dificultando o cumprimento dos prazos estipulados pela LGPD e por outras legislações pertinentes.

Além disso, as mudanças organizacionais necessárias para a adaptação completa à legislação são frequentemente prejudicadas por fatores como resistência à mudança na cultura institucional, necessidade contínua de treinamento e capacitação dos profissionais envolvidos, falta de apoio consistente e incentivo por parte dos gestores e problemas de comunicação interna. Esses fatores dificultam o engajamento das equipes e ampliam o tempo necessário para a implementação efetiva das práticas exigidas pela lei, comprometendo a eficácia das políticas de proteção de dados pessoais.

Assim, o nível de conformidade das universidades federais com a LGPD e demais regulamentações varia entre as instituições. Aquelas que contam com apoio contínuo e orientação clara da alta gestão — refletidos no acompanhamento de atualizações legais, na criação de políticas robustas de governança de dados e no

investimento em recursos humanos e tecnológicos — tendem a apresentar maior aderência às exigências. Em contrapartida, instituições que enfrentam dificuldades em áreas como capacitação de servidores, gestão de mudanças e implementação de controles de segurança e transparência podem ter limitações que comprometem a efetividade de suas práticas de proteção de dados e informações pessoais.

Assim, a conformidade das universidades federais com a LGPD e demais regulamentações depende de um esforço integrado que envolva não apenas a execução de processos técnicos, mas também o compromisso em promover uma cultura de governança de dados pessoais, com políticas que assegurem proteção, rastreabilidade, privacidade, acesso controlado e transparência no tratamento dessas informações.

1.1 Justificativa

A relevância da pesquisa justifica-se pelas demandas do Governo Federal, sobretudo por meio da Lei n. 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais e proteção dos direitos fundamentais de liberdade e privacidade. Essa legislação entrou em vigor plenamente em 3 de agosto de 2021 e inclui um capítulo específico sobre as regras e responsabilidades no tratamento de dados pelo poder público, além de prever sanções administrativas que variam de advertências a multas de até R\$50.000.000,00 (cinquenta milhões de reais) por infração.

A Emenda Constitucional n. 115 de 10 de fevereiro de 2022, também altera a Constituição Federal ao incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e estabelecer a competência privativa da União para legislar sobre essa matéria. Tal mudança demonstra a relevância social da proteção de dados e a importância do tratamento adequado das informações pelas organizações. Castro (2023, p. IX) ressalta “a importância da publicação de estudos especificamente dedicados à proteção de dados no Brasil, especialmente considerando a sua notável evolução nos últimos anos”.

Assim, compreendendo o potencial influenciador das universidades e a importância de sua adequação às legislações vigentes, torna-se necessário avaliar o nível dessas instituições no que concerne ao tratamento de dados pessoais, isto é,

identificar o grau de maturidade com que gerenciam e administram documentos e registros que contêm informações pessoais.

Para que essas intenções se concretizem, é necessário que ocorram mudanças no âmbito dessas instituições. As universidades federais precisam revisar a forma como educam, conduzem pesquisas, interagem com a comunidade externa e, principalmente, como desenvolvem seus próprios processos de gestão e operações (Palaver Garcia, 2021, p. 2).

Em nível pessoal, o interesse pela temática surge de exigências profissionais, uma vez que o pesquisador, servidor federal em uma instituição de ensino, lida diariamente com as solicitações de inovações tecnológicas e adequações técnicas às legislações que impactam os sistemas de gestão institucional. Diante disso, surgiram necessidades de adequação ao processo eletrônico, ao barramento (arquitetura de comunicação entre sistemas de instituições distintas) e, atualmente, às demandas da LGPD e outras legislações sobre a tramitação de dados pessoais.

No âmbito teórico-prático, este estudo oferece uma abordagem contemporânea e relevante, ainda pouco explorada nas organizações públicas brasileiras, considerando a urgência de adequação aos requisitos legais e a carência de capacitação dos profissionais envolvidos. Ademais, propõe-se realizar uma análise de conformidade no uso de legislações complementares, como a LGPD (focada na tramitação e proteção dos dados) e a LAI (que exige transparência e acesso), por meio da elaboração de instrumentos inéditos para coleta de dados e análise de maturidade no tratamento de dados e informações pessoais nas universidades federais.

A relevância da pesquisa para o Programa de Pós-Graduação em Ciência da Informação reside na abordagem de elementos como acesso e uso da informação, curadoria digital, direito à informação e gestão da segurança da informação, componentes essenciais para contextualizar a aplicação e análise do modelo proposto.

Uma consulta realizada em 8 de novembro de 2024 na Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (Brapci) revelou um aumento nas publicações sobre a Lei Geral de Proteção de Dados desde sua promulgação. Foram identificadas 72 (setenta e duas) publicações dedicadas ao tema, com destaque para o ano de 2023, que registrou o maior número de estudos, totalizando 17 publicações. No campo da Ciência da Informação, a LGPD tem sido

predominantemente abordada sob as perspectivas de competência da informação, políticas de privacidade, governança, gestão da informação, gestão da segurança da informação e sistemas de informação. Essa análise ressalta a crescente relevância desse tópico no contexto da Ciência da Informação.

Os resultados desta pesquisa podem contribuir com as instituições de ensino superior, em especial as universidades federais brasileiras, auxiliando-as na identificação de áreas que demandam adequação às exigências legais. Assim, essas instituições poderão conduzir suas atividades e procedimentos administrativos de maneira segura, responsável e eficiente, em conformidade com as regulamentações que regem o tratamento de dados e informações pessoais. Ademais, este estudo pode servir como referência tanto para os profissionais da área quanto para futuras pesquisas sobre o tema.

1.2 Objetivos

1.2.1 Objetivo geral

Desenvolver um modelo de maturidade para o tratamento de dados pessoais nas universidades federais brasileiras, fundamentado na Lei Geral de Proteção de Dados e nos marcos legais correlatos.

1.2.2 Objetivos específicos

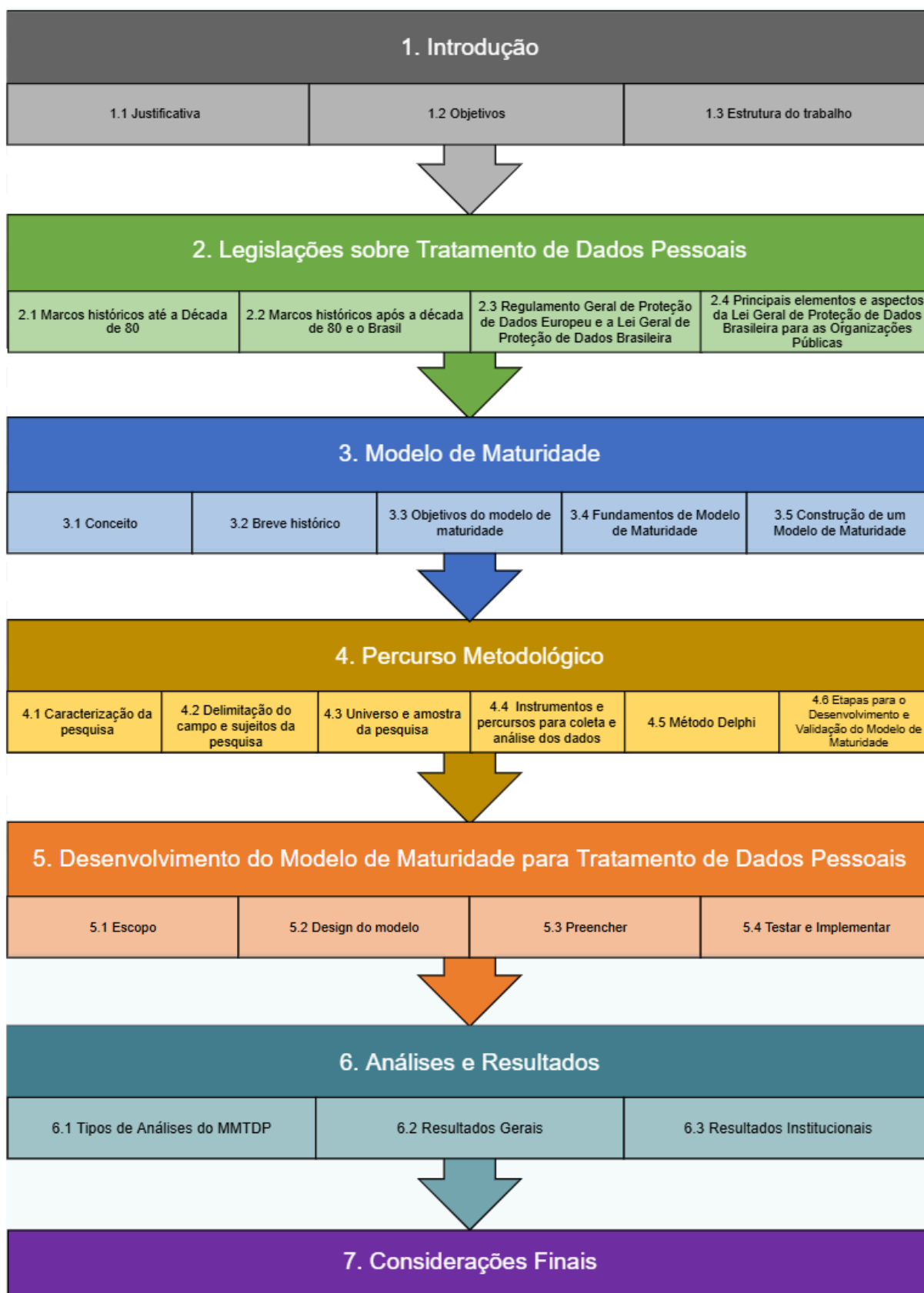
- a) Identificar as legislações e normas brasileiras que impactam o tratamento de dados pessoais.
- b) Analisar os elementos essenciais para a composição do modelo de maturidade aplicável nas universidades federais brasileiras, definindo suas dimensões, níveis de maturidade e inter-relações.
- c) Elaborar o instrumento de medição do modelo de maturidade proposto.
- d) Validar e estruturar o instrumento de medição proposto por meio do método *Delphi*.
- e) Aplicar e testar o modelo de maturidade proposto nas universidades federais do país.

1.3 Estrutura do trabalho

Este trabalho está estruturado em sete seções, inter-relacionadas e complementares (conforme ilustrado na **Figura 1**). A Seção 1 introduz o tema da pesquisa, incluindo suas justificativas, problematização e objetivos. As Seções 2 e 3 abordam o referencial teórico. Na Seção 2, são discutidos conceitos e marcos legislativos que fundamentam a criação de normativas para o tratamento adequado de dados e informações pessoais. A Seção 3 apresenta abordagens teóricas sobre os conceitos, a importância e as principais características dos modelos de maturidade.

A Seção 4 descreve o percurso metodológico, incluindo a natureza da pesquisa, a delimitação do campo e dos sujeitos, bem como os instrumentos para a coleta e análise de dados, com ênfase no método *Delphi*. Na Seção 5, é detalhado o desenvolvimento do modelo de maturidade para o tratamento de dados pessoais proposto. A Seção 6 traz a descrição da análise dos dados coletados, com ponderações dos resultados da pesquisa. Finalmente, são apresentadas na última Seção, as considerações finais do trabalho.

Figura 1 - Estrutura do trabalho



Fonte: Elaborado pelo autor.

2 LEGISLAÇÕES SOBRE TRATAMENTO DE DADOS PESSOAIS

No mundo digital altamente conectado em que vivemos, os dados pessoais tornaram-se uma das *commodities* mais valiosas. Desde informações básicas, como nomes e endereços, até detalhes mais sensíveis, como preferências pessoais e histórico de navegação na internet, nossos dados são coletados, armazenados e utilizados por empresas e organizações em diversos setores. Nesse contexto, a importância e a relevância dos tratamentos adequados aos dados pessoais tornam-se evidentes. Portanto, o uso adequado dessas informações é essencial para garantir a privacidade, a segurança e a confiança dos indivíduos, além de cumprir com as regulamentações e leis de proteção de dados em vigor.

Os tratamentos adequados aos dados pessoais englobam práticas como coleta transparente e consentida, armazenamento seguro, limitação de acesso, anonimização quando possível e descarte adequado. Priorizar essas medidas permite que as organizações construam relacionamentos sólidos e duradouros com seus clientes, ao mesmo tempo em que demonstram responsabilidade e ética no tratamento das informações que lhes são confiadas.

Com o avanço tecnológico no que diz respeito à coleta, uso e compartilhamento de dados e informações, observa-se um aumento significativo do volume informacional acumulado nas empresas. Isso implica um crescimento proporcional do interesse da sociedade em saber como a privacidade e a proteção desses dados estão sendo gerenciados, o que exige maior atenção aos procedimentos e estratégias adotados pelas organizações para o tratamento desses dados.

2.1 Marcos históricos até a década de 80

No Brasil, o tratamento dos dados pessoais ganhou notoriedade com o advento da Lei Geral de Proteção de Dados, promulgada em agosto de 2018. Isso remete à busca pelo entendimento de sua origem na sociedade e no país. Alguns pesquisadores acreditam que o marco inicial dessa temática no mundo teve início no século XIX, mais precisamente em 1890, com a publicação do artigo *The Right to Privacy* nos Estados Unidos, que traz em sua essência a preocupação e reflexão sobre o direito à privacidade dos indivíduos. Segundo Warren e Brandeis (1890, p.

215, tradução nossa): “O objetivo geral em vista é proteger a privacidade da vida privada e, em qualquer grau e em qualquer conexão...”.

Outro marco mundial importante de reflexão foi a Declaração Universal dos Direitos Humanos, esboçada pelo canadense John Peters Humphrey e elaborada oficialmente pela Organização das Nações Unidas, em 10 de dezembro de 1948, em Paris. Esse documento contribuiu significativamente para a popularização da legislação referente ao direito à privacidade.

A partir da Segunda Guerra Mundial, com o avanço tecnológico e a popularização dos computadores para o processamento de dados, inclusive os pessoais, as discussões sobre a importância e a necessidade de proteção dos dados pessoais no uso das ferramentas tecnológicas cresceram, levando ao surgimento dos primeiros normativos sobre o tema. Segundo Facchini Neto e Demoliner (2018, p. 28):

As primeiras normas visando a tutela de dados pessoais surgiram na década de 1970 e são classificadas pela doutrina como sendo a “primeira geração” de leis de proteção de dados. São elas: a *Hessisches Datenschutzgesetz* (Lei de Proteção de Dados Hessiana), em 1970; a *Data Legen 289* (ou *Datalag*), em 1973, na Suécia; e o *Privacy Act* nos Estados Unidos da América, em 1974.

Para compreender essas leis, é necessário observar os contextos governamentais e organizacionais desse período. As principais nações estavam em processo de reformas sociais e busca do bem-estar social, o que exigia dos governos um sistema robusto e sofisticado de planejamento governamental capaz de lidar com o volume de dados coletados sobre os cidadãos, visando a eficiência no cumprimento das obrigações públicas. Isso explica tanto o entusiasmo em relação às novas tecnologias quanto a preocupação com a burocracia automatizada e desumanizada que estavam sendo produzidas. Portanto, as primeiras normativas de proteção de dados não se concentravam na proteção direta da privacidade individual. Em vez disso, elas se concentravam no processamento de dados na sociedade.

Percebe-se também que essas normas tinham um caráter mais técnico, utilizando termos como dados, banco de dados, registros de dados, etc., em vez de nomenclaturas mais humanizadas como privacidade, informação ou proteção de assuntos privados. A transição da primeira para a segunda geração de normas sobre a proteção de dados aconteceu com o entendimento da necessidade de

considerar a proteção dos dados pessoais, tanto sob o aspecto tecnológico do processamento desses dados quanto na perspectiva da privacidade individual dos cidadãos. Era necessário estabelecer uma maior conexão entre os aspectos técnicos e os direitos individuais, permitindo que os indivíduos tivessem maior poder de decisão sobre quais de seus dados poderiam ser usados e para quais propósitos. A partir desse entendimento, surgiram normativas com abordagens mais humanizadas.

Em 1977, mais precisamente em 27 de janeiro, foi publicada a primeira Lei Federal sobre Proteção de Dados, da República Federativa da Alemanha, denominada *Bundesdatenschutzgesetz*, que entrou em vigor em 1978. Nesse mesmo período, surgiu na França a *Loi relative à l' informatique, aux fichiers et aux libertés*, Lei n. 78-17, de 6 de janeiro de 1978, com ênfase na proteção da privacidade e dos dados pessoais do cidadão, mesma abordagem semelhante à proposta na Lei Austríaca (*Datenschutzgesetz*) de 1978 (France, 1978; Facchini Neto; Demoliner, 2018, p. 28-29). A privacidade informacional começou a aparecer também como direito fundamental nas constituições federais de Portugal (1976), Áustria (1978) e Espanha (1978). Países como Alemanha, França, Áustria, Suécia, Noruega e Dinamarca também se destacaram nessa vanguarda.

Na década de 80, ocorreu o desenvolvimento das tecnologias de telecomunicação e da conexão entre computadores através das redes, possibilitando as transferências de dados de forma rápida, o que consequentemente, dificultou a rastreabilidade das informações e criou novos desafios legais quanto à segurança e à proteção dos dados pessoais. Em 28 de janeiro de 1981, foi lançado o primeiro instrumento de vínculo jurídico com caráter internacional sobre o domínio da proteção de dados. Conhecida por Convenção 108 ou Convenção de Estrasburgo, essa foi a Convenção do Conselho Europeu acerca da proteção das pessoas singulares no que se refere ao tratamento automatizado de dados pessoais.

O marco mais relevante nessa geração foi o parecer do Tribunal Constitucional Alemão, que reconheceu a inconstitucionalidade da Lei de Censo, estabelecendo diretrizes para o tratamento dos dados pessoais na esfera pública. Conforme Colombo (2021, p. 58) “foi no contexto da judicialização da Lei do Censo de 1983 (*Volkszählungsgesetz*), no Tribunal Constitucional Alemão, que foram abertas sólidas *guidelines* acerca do tratamento de dados pessoais pelo Poder Público”. Foi essa famosa decisão censitária da corte alemã que popularizou o termo

autodeterminação informacional. Maldonado e Blum (2021, p. 30) definem autodeterminação informativa como o “direito de controle pessoal sobre o trânsito de dados relativos ao próprio titular”. Ruaro (2020, p. 234) acrescenta que: “a sentença confirmou que os dados pessoais estão constitucionalmente protegidos na Alemanha. Isto significa que os indivíduos têm o poder de decidir quando e até que ponto as informações pessoais podem ser publicadas”.

É nesse contexto que ocorre a transição de geração de normativas de proteção de dados pessoais, caracterizada pela autodeterminação informacional e pela transferência do direito para os próprios cidadãos, que passam a participar de todo o processo de tratamento dos dados, desde sua coleta até o armazenamento, transferência ou compartilhamento. Surgem, a partir disso, muitas adaptações legislativas, como a emenda da lei de proteção de dados Austríaca (1986), a Lei Finlandesa de registro de pessoas (1987), a disposição constitucional na Holanda, garantindo a proteção de dados individuais (1988), e a emenda Geral à Lei Federal Alemã de Proteção de Dados (1990), entre outras.

Porém, esse cenário produziu um novo desafio: a complexidade das pessoas arcarem com o alto custo financeiro e social para executar a autodeterminação informativa. A proteção de dados passou a ser privilégio das minorias; apenas aqueles que tinham disponibilidade econômica e social conseguiam exercer seu direito. Isso abriu espaço para a quarta geração de normas de proteção de dados, que tinham como principal objetivo retificar essa problemática, reequilibrando o poder de negociação. A ideia era fortalecer a posição dos indivíduos em relação às grandes instituições, resultando em novas abordagens legais, como a proibição do processamento de dados pessoais sensíveis em órgãos públicos (aplicada na Noruega, Finlândia, Dinamarca, Bélgica, França e Reino Unido), e as restrições de negociação contratual de direitos básicos de proteção de dados individuais para acesso, correção e exclusão de indivíduos (aplicados na Suíça e Alemanha).

2.2 Marcos históricos após a década de 80 e o Brasil

No contexto brasileiro, é válido destacar que a Constituição Federal promulgada em 5 de outubro de 1988 desempenha um papel pioneiro na moldagem das bases iniciais para a regulação do tratamento de dados pessoais no país. Esse documento fundamental para a legislação nacional contém dispositivos que abordam

questões cruciais relacionadas à privacidade, ao sigilo de informações e à preservação da imagem dos cidadãos. Em particular, declara que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Brasil, 1988, art. 5º, inc. X).

Fica evidenciado o cuidado com a proteção da privacidade dos cidadãos, mas ainda distante do efetivo cuidado com a proteção e o tratamento dos dados pessoais. Em 11 de Setembro de 1990, sucede a Lei n. 8.078 (Código de Defesa do Consumidor), que dispõe sobre a proteção do consumidor e dá outras providências. No seu teor traz o seguinte texto: “O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (Brasil, 1990, art. 43). Nesta legislação é possível observar a proteção ao direito de acesso aos dados pessoais que estão em posse de empresas, criando a possibilidade de acessar seus dados pessoais que estão armazenados nas bases de dados das organizações, trabalhando as regras que sustentam as atividades dos bancos de dados de proteção ao crédito.

De grande relevância para os arquivistas e profissionais da informação, destaca-se também a Lei n. 8.159, de 8 de janeiro de 1991, que no seu artigo 4º, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Brasil, 1991, art. 4º).

Retornando para a conjuntura mundial, em 24 de outubro de 1995, surge a Diretiva 95/46/EC do Parlamento Europeu e do Conselho, tornando-se a principal referência normativa da quarta geração, pois oferecia um código de conduta para a proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados. Nessa diretiva, fica proibido o processamento de dados sensíveis (raça, religião, opiniões políticas, etc.) por órgãos públicos, exceto em casos específicos. E é nessa abordagem que

manifesta-se o desenvolvimento da ideia da estruturação de uma norma geral de proteção de dados, que poderia ser complementada por regulamentações específicas. Isso significaria a disseminação e aceitação da norma em toda a Europa, o que ajudaria principalmente países com os regimes de proteção de dados inadequados.

No Brasil, destaca-se a Lei n. 9.296 de 1996, que regulamenta o inciso XII da Constituição Federal Brasileira:

É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988, art. 5º, inc. XII).

Nesse período, surge a Lei n. 9.507, de 12 de novembro de 1997, que regula o direito de acesso a informações e disciplina o rito processual do habeas data. No cenário internacional, é proclamada a Carta dos Direitos Fundamentais da União Europeia, em 7 de dezembro de 2000, pelo Parlamento Europeu, pela Comissão Europeia e pelo Conselho da União Europeia, que entrega em seu artigo oitavo o seguinte:

Art. 8º. Proteção de dados pessoais: 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente" (União Europeia, 2000, p. 10, tradução nossa).

Na América Latina, a Argentina destaca-se por possuir normas sobre proteção de dados pessoais desde 1994 e por criar, em 4 de outubro de 2000, a *Ley de Protección de los Datos Personales* - Lei de Proteção de Dados Pessoais da Argentina (PDPA), n. 25.326, que contempla a proteção à privacidade de dados pessoais e concede acessos individuais a qualquer informação armazenada em registros ou bancos de dados. O país é considerado pioneiro, seguido pelo Uruguai, na América do Sul, em assegurar a qualificação de adequado pela União Europeia para tratamento e transmissão de dados internacionais.

No Brasil, em 2010, é aprovada a Resolução do Conselho Nacional de Justiça n. 121, que dispõe sobre a divulgação de dados processuais eletrônicos na rede

mundial de computadores, expedição de certidões judiciais e dá outras providências. Essa legislação fortalece o princípio da transparência. Em 2011, duas legislações importantes para o tratamento de dados entraram em vigor: a Lei n. 12.414 - Lei do Cadastro Positivo; e a Lei n. 12.527 - Lei de Acesso à Informação. A primeira disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, tendo ainda a possibilidade de correção do que estiver incorreto.

Já a LAI, 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 n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Essa lei define informação pessoal como “aquela relacionada à pessoa natural identificada ou identificável” (Brasil, 2011, art.4, inc. IV). A Lei de Acesso à Informação também trata do tratamento das informações pessoais, que deve ser realizado de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais.

Em 2012, é sancionada a Lei n. 12.737 (Lei de Crimes Informáticos), também conhecida como a Lei Carolina Dieckmann, decorrente do desrespeito envolvendo a atriz brasileira, que possibilitou criminalizar a invasão de aparelhos eletrônicos com a intenção de obtenção de dados e informações pessoais. Em 2013, surge o Projeto de Lei do Senado n. 330, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Esse Projeto de Lei passará por diversos comentários e alterações, resultando, por fim, na Lei Geral de Proteção de Dados.

Entretanto, a norma predecessora brasileira de maior relevância para o surgimento da LGPD no Brasil é a Lei n. 12.965 (Marco Civil da Internet), de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Dias e Bolesina (2017, p. 6) complementa que o:

Marco Civil da Internet tem atuação mais ampla e dinâmica para a proteção de dados pessoais, em comparação às demais legislações brasileiras, mas ainda assim pouco específica – muito embora tenha se adiantado no assunto em solo brasileiro.

Ela já traz a proteção da privacidade e dos dados pessoais como princípios, além de promover o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos como objetivo do uso da internet no

país. Esta norma é regulamentada pelo Decreto n. 8.771, de 11 de maio de 2016, mesma data do Decreto n. 8.777 que institui a Política de Dados Abertos do Governo Federal.

Paralelamente, na Europa, em 27 de abril de 2016, a Diretiva 95/46/EC é revogada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, sendo implementado em 25 de maio de 2018, o GDPR, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e regulamenta a exportação de dados pessoais para fora da União Europeia e do Espaço Econômico Europeu.

As normas jurídicas europeias acompanharam o dinamismo vivenciado nos países, adequando-se aos desafios proporcionados pelos desenvolvimentos tecnológicos, bem como as transformações sociais e ideológicas de cada período. A proteção de dados migrou da visão funcional decorrente dos processamentos de dados para o contexto humano dos indivíduos, focando na abordagem dos direitos individuais. Posteriormente, na privacidade informacional e na autodeterminação informacional, bem como nos direitos participativos. Com o surgimento da ideia de uma norma geral de proteção de dados, que abrangeria até os países com precariedade legislativa, podendo ser apoiados por normas técnicas que regulamentam especificidades de participação e segurança.

O GDPR serviu de inspiração para diversas legislações sobre a proteção de dados pessoais no mundo: *Ley General de Protección de Datos Personales* (LGPD) no México (2017); *California Consumer Privacy Act* (CCPA) dos Estados Unidos (2018); e, no Brasil, em 13 de maio de 2016, é apresentado o Projeto de Lei Federal n. 5.276/2016, que resultou, posteriormente, na lei de proteção de dados pessoais brasileira.

Assim, em 14 de agosto de 2018, é anunciada a Lei Geral de Proteção de Dados Pessoais do Brasil, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Maldonado e Blum (2021, p. 59) evidenciam que:

Nesse contexto, é demasiadamente positivo a LGPD basear-se no GDPR, pois agora o Brasil pode ser reconhecido mundialmente por ter uma legislação robusta, equivalente à norma da União Europeia,

facilitando explicações de segurança jurídica para empresas internacionais que buscam investir no País, bem como pela possibilidade da análise, pela Comissão Europeia, do livre fluxo de dados com o Brasil, com base em uma decisão de adequação, assim como Argentina e Uruguai, na América Latina, já estão cancelados.

A LGPD passou por um longo processo de criação e implementação, resultando em diversas mudanças. Ela entraria em vigor 18 meses após a sua publicação. No entanto, faz-se oportuno ressaltar que a vigência, em sua plenitude, só veio acontecer a partir do dia três de maio de 2021. A aplicabilidade desta lei apoia diretamente a proteção dos dados dos indivíduos, regulamentando os princípios, direitos e obrigações relacionados ao trâmite dos dados e das bases de dados relacionadas às pessoas, como também imputa graves sanções aos operadores e controladores de dados que não cumprirem as disposições legais.

No oriente, o Japão com a publicação da *Act on the Protection of Personal Information* (APPI), Lei sobre Proteção de informações pessoais Japonesa, torna-se o primeiro país oriental a ser considerado adequado pela União Europeia, em 23 de janeiro de 2019, permitindo transferência de dados pessoais com garantias de proteção desses dados.

A primeira alteração da LGPD ocorreu em 08 de julho de 2019, com a criação da Lei n. 13.853, que traz algumas providências e cria a Autoridade Nacional de Proteção de Dados (ANPD). Em seguida, com o advento da pandemia do coronavírus (Covid-19), surge a segunda mudança na LGPD, com a Lei n. 14.010, de 10 de junho de 2020, que, em seu artigo 20, prorroga o início da vigência dos artigos 52, 53 e 54 da LGPD para agosto de 2021. Esses artigos alterados, referem-se às sanções administrativas e multas por infrações cometidas no âmbito da lei. Em 20 de agosto de 2020, é publicada a Recomendação n. 73 do Conselho Nacional de Justiça, com o intuito de orientar os órgãos do Poder Judiciário brasileiro quanto às ações iniciais para adequação à LGPD; e em 21 de setembro de 2020, a Resolução n. 334 do Conselho Nacional de Justiça institui o Comitê Consultivo de Dados Abertos e Proteção de Dados no âmbito do Poder Judiciário. Outras duas normativas relevantes foram anunciadas em 15 de outubro de 2020, as Portarias n. 212 e n. 213, que instituíram, respectivamente, o Grupo de Trabalho destinado à elaboração de estudos e de propostas voltadas à adequação dos tribunais à Lei Geral de Proteção de Dados e o Comitê Gestor da Lei Geral de

Proteção de Dados Pessoais (CGLGPD) no âmbito do Conselho Nacional de Justiça.

Já na Europa, conforme o artigo 45 do Regulamento (UE) 2016/679, a Comissão Europeia pode avaliar a adequação do nível de proteção de um país fora da União Europeia e decidir se este país está adequado ou não em realizar transferências de dados pessoais com os países membros. Atualmente, os países considerados adequados¹, são Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido e Uruguai. O Reino Unido, ainda abrange as trocas de dados no setor da aplicação da lei, reguladas pelo artigo 36 da Diretiva (UE) 2016/680.

O Brasil vem buscando esse reconhecimento, pois essa adequação proporciona aos países fora da União Europeia um benefício de competitividade, uma vez que terão acesso privilegiado ao mercado único europeu e aos seus canais comerciais. Para consolidar a evolução do Brasil em relação à preocupação com a proteção de dados pessoais, em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional n. 115, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e estabelecer a competência exclusiva da União para legislar sobre proteção e tratamento de dados pessoais.

Nota-se, portanto, que a evolução do tratamento de dados pessoais tornou-se um tema de extrema relevância, tanto em âmbito mundial quanto no Brasil. Maldonado e Blum (2021, p. 13) enfatizam que:

Nesse curto período de pouco mais de três anos, assistimos à evolução da proteção de dados em termos mundiais, de forma recorrente e primordial, proliferando-se eventos, congressos, cursos, workshops, produções acadêmicas e documentários no Brasil e em boa parte do mundo ocidental.

Com o avanço da tecnologia e a crescente interconectividade, surgiram preocupações sobre a proteção da privacidade e a utilização adequada das informações pessoais. O Quadro 1 busca fornecer um panorama resumido dos marcos históricos importantes relacionados à privacidade, à proteção e ao

¹ Os países não pertencentes à União Europeia que são considerados com um nível adequado de proteção de dados, podem ser acessados em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_lt. Acesso em: 24 de outubro de 2022.

tratamento de dados pessoais em nível global e no contexto brasileiro. Esse panorama abrange desde as primeiras iniciativas regulatórias até os mais recentes desenvolvimentos legislativos, refletindo a busca contínua por um equilíbrio entre a inovação tecnológica e a salvaguarda dos direitos individuais.

Quadro 1 - Marcos históricos sobre privacidade, proteção e tratamento de dados pessoais

Ano	Local da publicação	Marco
1890	Estados Unidos	Publicação do artigo " <i>The Right to Privacy</i> ", de <i>Warren e Brandeis</i> , com as primeiras ideias sobre proteger a privacidade dos indivíduos.
1948	França	Declaração Universal dos Direitos Humanos, esboçada por <i>John Peters Humphrey</i> e elaborada oficialmente pela Organização das Nações Unidas.
1970	Alemanha	<i>Hessisches Datenschutzgesetz</i> (Lei de Proteção de Dados Hessiana), foi a primeira Lei de proteção de dados na Alemanha e no Mundo.
1973	Suécia	<i>Data Legen 289</i> (A Lei Sueca), proteção aos dados pessoais processados em registros informatizados tradicionais.
1974	Estados Unidos	<i>Privacy Act</i> (Lei de Privacidade), estabelece um código de práticas para o tratamento de informações pessoais mantidas em sistemas de registros por agências federais.
1977	Alemanha	<i>Bundesdatenschutzgesetz</i> , primeira Lei Federal sobre Proteção de Dados.
1978	França e Áustria	<i>Loi relative à l' informatique, aux fichiers et aux libertés</i> (Lei n. 78-17) na França e a <i>Datenschutzgesetz</i> (Lei Austríaca), ênfase na proteção da privacidade e dos dados pessoais do cidadão.
1983	Alemanha	<i>Volkszählungsurteil</i> (Julgamento do Recenseamento), parecer do Tribunal Constitucional Alemão, tornando constitucional a proteção de dados pessoais na Alemanha.
1986	Áustria	Lei de proteção de dados Austríaca.
1987	Finlândia	Lei Finlandesa de registro de pessoas.
1988	Holanda e Brasil	Disposição Constitucional Holandesa e a publicação da Constituição Federal Brasileira, de 05 de outubro de 1988, podendo ser considerada um marco incipiente no tratamento dos dados pessoais no país, já que cita termos como privacidade, sigilo de dados e imagem.

1990	Alemanha e Brasil	A Emenda Geral à Lei Federal Alemã de Proteção de Dados e a Lei brasileira n. 8.078, que dispõe sobre a proteção do consumidor e dá outras providências.
1991	Brasil	Lei n. 8.159, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.
1995	Luxemburgo	A Diretiva 95/46/EC do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, estabelece um código de conduta para a proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados.
2000	França	A Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, proclamada pelo Parlamento Europeu, pela Comissão Europeia e pelo Conselho da União Europeia.
2011	Brasil	Lei 12.414/2011 - Lei do Cadastro Positivo, disciplina a formação e consulta a bancos de dados, a Lei 12.527/2011 - Lei de Acesso à Informação, trata das informações pessoais que deverá ser realizado de forma transparente e com respeito À intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
2012	Brasil	Lei n. 12.737 - Lei Carolina Dieckmann, possibilitou criminalizar a invasão de aparelhos eletrônicos com a intenção de obtenção de dados e informações pessoais.
2013	Brasil	Projeto de Lei do Senado n. 330, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências
2014	Brasil	Lei n. 12.965 (Marco Civil da Internet), estabelece princípios, garantias, direitos e deveres para o uso da internet no país
2016	França	Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados), de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
2018	Brasil	Lei n. 13.709 (Lei Geral de Proteção de Dados), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
2022	Brasil	Emenda Constitucional n. 115, de 10 de fevereiro de 2022, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixa a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Fonte: elaborado pelo autor.

Esses marcos estão relacionados às necessidades e interesses de organizações e sociedades no que tange à privacidade, proteção e tratamento de dados pessoais, tanto no âmbito global quanto no Brasil. A abrangência temporal inicia-se em 1890, com a publicação do artigo "*The Right to Privacy*" nos Estados Unidos, e se estende até 2022, com a Emenda Constitucional n. 115 promulgada no Brasil. Esses marcos refletem uma evolução histórica e o reconhecimento de que o tratamento de dados não é um processo finalizado, mas sim contínuo. Visa manter um alto nível de proteção individual sob uma coesão internacional, que conduzirá, cada vez mais, uma homogeneidade normativa mundial.

Foi elaborado um cronograma histórico, apresentado como um "timeline", que destaca os marcos sobre privacidade, proteção e tratamento de dados pessoais no mundo e no Brasil. Esse recurso permite acompanhar facilmente os avanços e as mudanças ao longo do tempo, oferecendo uma visão abrangente e visualmente acessível da evolução da proteção de dados pessoais. O "timeline" pode ser consultado em detalhes no **Apêndice A**, onde os marcos relacionados ao Brasil estão destacados em verde, enquanto os do restante do mundo aparecem em azul.

2.3 Regulamento Geral de Proteção de Dados Europeu e a Lei Geral de Proteção de Dados Brasileira

A LGPD brasileira foi inspirada no Regulamento (UE) 2016/679, consequentemente, essa convergência entre as legislações, poderá viabilizar a possibilidade de classificação do país como adequado para assegurar relacionamento e transferências de dados entre as empresas brasileiras e os países membros da União Europeia. As duas normativas compartilham objetivos comuns de proteger a privacidade e os direitos dos indivíduos em relação ao tratamento de seus dados pessoais e visam estabelecer diretrizes claras e consistentes para o uso responsável e seguro das informações pessoais.

Seguindo essas premissas, tanto o Regulamento Geral de Proteção de Dados da União Europeia quanto a Lei Geral de Proteção de Dados do Brasil são marcos legais significativos, embora cada uma tenha sua própria abordagem e especificidades, é importante destacar as principais semelhanças entre essas duas

legislações. Essa análise permite uma compreensão mais clara das bases legais compartilhadas por essas leis de proteção de dados tão relevantes no cenário global. O Quadro 2 oferece uma visão comparativa das principais disposições e princípios comuns entre o GDPR e a LGPD, destacando as convergências e especificidades em termos de escopo, consentimento, direitos dos titulares dos dados, autoridades de supervisão, sanções e penalidades, entre outras.

Quadro 2 - Principais semelhanças entre o GDPR e a LGPD

Aspecto	GDPR		LGPD	
	Artigo	O que diz a lei	Artigo	O que diz a lei
Objetivo	1º	Proteger os direitos e liberdades fundamentais das pessoas físicas em relação ao tratamento de seus dados pessoais.	1º e 3º	Garantir a proteção dos dados pessoais dos cidadãos brasileiros e regulamentar o tratamento dessas informações.
Abrangência e Extraterritorialidade	2º e 3º	Aplica-se a todos os países da União Europeia e a empresas que processam dados pessoais de cidadãos da UE.	1º e 3º	Aplica-se a todas as atividades de tratamento de dados realizadas no território brasileiro ou que tenham como finalidade a oferta de bens ou serviços no Brasil ou o tratamento de dados de pessoas localizadas no país.
Consentimento	6º a 8º	Requer o consentimento explícito e específico do titular dos dados para o tratamento, com informações claras sobre a finalidade.	7º e 8º	Exige o consentimento do titular para o tratamento dos dados, além de informações claras sobre a finalidade e a forma de tratamento.
Crianças e Adolescentes	8º	Definem as condições aplicáveis da lei para crianças e adolescentes	14º	Formaliza as regras para o tratamento de dados pessoais de crianças e adolescentes

Direitos dos Titulares	12º a 23º	Assegura uma série de direitos, como acesso, retificação, exclusão, portabilidade e o direito de ser esquecido.	17º a 22º	Concede aos titulares dos dados uma série de direitos, incluindo acesso, correção, eliminação, portabilidade e revogação do consentimento.
Responsabilidades do Controlador	24º a 27º	Estabelece que o controlador é responsável pelo cumprimento do GDPR e deve implementar medidas de segurança adequadas.	42º a 45º	Define que o controlador é responsável pelo tratamento dos dados pessoais e deve adotar medidas para garantir a segurança dessas informações.
Encarregado de Proteção de Dados	37º a 39º	Recomenda-se a designação de um Encarregado de Proteção de Dados (<i>Data Protection Officer</i> - DPO) para monitorar o tratamento de dados e garantir a conformidade.	23º (III) e 41º	Obriga a nomeação de um Encarregado de Proteção de Dados (EPD) para supervisionar as atividades de tratamento de dados.
Transferências Internacionais	44º a 50º	Permite a transferência de dados para países fora da UE, desde que haja um mecanismo adequado de proteção dos dados.	33º a 36º	Regulamenta as transferências internacionais de dados e exige garantias apropriadas para países sem nível adequado de proteção.
Autoridade de Controle e Supervisão	51º	Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento.	55º	Cria a Autoridade Nacional de Proteção de Dados, órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território brasileiro

Sanções	83º e 84º	Estabelece multas significativas em caso de violação do GDPR, podendo chegar a 20 milhões de euros ou 4% do faturamento anual global da empresa, o que for maior.	52º a 54º	Prevê penalidades em caso de infrações à LGPD, incluindo multas que podem alcançar até 2% do faturamento da empresa, limitadas a R\$50 milhões por infração.

Fonte: Elaborado pelo autor.

O Quadro 2 destaca as principais semelhanças entre o GDPR da União Europeia e a LGPD do Brasil. Ambos os regulamentos visam salvaguardar os direitos fundamentais das pessoas em relação ao processamento de seus dados pessoais, estabelecendo requisitos claros para o consentimento, direitos dos titulares, responsabilidades dos controladores e medidas de segurança. Além disso, ambos regulamentam a atuação de Encarregados de Proteção de Dados e prevêm sanções para infrações.

Uma das especificidades dessas leis, está relacionada a precisão jurídica, enquanto o GDPR, no seu art. 3º prevê a sua aplicação de forma explícita e direta. A Lei brasileira apresenta algumas imprecisões técnicas na sua redação quanto à aplicação territorial e extraterritorial, exigindo que a ANPD delibere sobre a interpretação da Lei e da sua competência, tendo papel crucial de mitigar essas imprecisões (Maldonado; Blum, 2021, p. 60-61).

Apesar de apresentar especificidades diferentes quanto às penalidades impostas em caso de descumprimento, fica evidente que a preocupação com a proteção dos dados pessoais e a promoção de um ambiente digital mais seguro e transparente são objetivos compartilhados por essas duas legislações, contribuindo para a construção de um cenário global mais respeitoso e responsável em relação à privacidade e à gestão de informações pessoais e sensíveis.

No entanto, existem algumas divergências significativas entre o GDPR e a LGPD. Nota-se que as diferenças entre as normativas já iniciam-se na estruturação dos documentos. Enquanto o GDPR contempla 99 (noventa e nove) artigos em 11 (onze) capítulos, a LGPD abarca 65 (sessenta e cinco) artigos em 10 (dez) capítulos. Evidenciando que a LGPD é mais sucinta que o GDPR. Pinheiro (2023, p. 10), destaca outra diferença relevante:

A versão nacional é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê "prazo razoável".

Segue o Quadro 3 com mais alguns pontos divergentes importantes entre as normativas.

Quadro 3 - Principais divergências entre o GDPR e a LGPD

Aspecto	GDPR	LGPD
Base Legal para o Processamento de Dados	Estabelece seis bases legais para o processamento de dados pessoais, incluindo consentimento, cumprimento de contrato e interesse legítimo do controlador ou de terceiros.	A LGPD possui dez bases legais para o tratamento de dados, incluindo consentimento, cumprimento de obrigação legal, proteção da vida ou da integridade física e legítimo interesse.
Dados Sensíveis	Conhecidos como "categorias especiais de dados pessoais". Incluindo informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, saúde, vida sexual ou orientação sexual, bem como dados genéticos e biométricos. Destaca regras mais rígidas para o processamento desses tipos de dados.	São os "dados pessoais sensíveis", e incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de natureza religiosa, filosófica ou política, saúde ou vida sexual, bem como dados genéticos e biométricos. Enfatiza a importância do consentimento específico e informado, garantindo que os titulares dos dados estejam plenamente cientes de como seus dados sensíveis serão utilizados.
Tratamento de dados de menores	A legislação europeia aceita o consentimento de menores com pelo menos 16 anos de idade. Com idade inferior, o consentimento do progenitor, tutor ou responsável legal é obrigatório (Ruaro, 2020, p. 245).	A legislação brasileira exige o consentimento dos pais ou responsáveis para o processamento de dados pessoais de qualquer pessoa menor de 18 anos, conforme definido pelo Estatuto da Criança e do Adolescente (Ruaro, 2020, p. 245).

Políticas de proteção de dados	A legislação europeia exige que os responsáveis pelo tratamento de dados tomem as medidas técnicas e organizativas adequadas para assegurar que o tratamento de dados seja efetuado em conformidade com a lei (Ruaro, 2020, p. 245).	A legislação brasileira, por outro lado, trata da implementação de um programa de governança e proteção de dados como uma faculdade para os controladores de dados (Ruaro, 2020, p. 245).
Relação dos representantes	Empresas fora da UE que processam dados de cidadãos da UE precisam designar um representante da UE. E a indicação de controlador ou processador deve ser constituída por escrito por um representante dos Estados-Membros (Ruaro, 2020, p. 245).	A regulamentação brasileira não possui um requisito equivalente de representante, prevê que a empresa estrangeira seja notificada e intimada de todos os atos processuais na pessoa do agente, representante ou pessoa responsável por sua filial, agência, estabelecimento ou escritório instalado no Brasil (Ruaro, 2020, p. 245).
Não responsabilização dos agentes	A legislação europeia contém apenas os seguintes pontos descritos: (1) se a pessoa natural ou jurídica não se encontrar enredada no tratamento dos dados; (2) se, apesar dos danos, o tratamento for efetuado em conformidade com a lei (Ruaro, 2020, p. 245).	Têm três proposições em que o controlador/operador não é responsabilizado: (1) se a pessoa natural ou jurídica não estiver envolvida no tratamento dos dados; (2) se, apesar dos danos, o tratamento for efetuado de acordo com as disposições legais; (3) se os agentes provarem que o dano foi causado exclusivamente pela pessoa do titular dos dados, ou por terceiros (Ruaro, 2020, p. 245).
Relação ao marketing direto	O regulamento europeu fornece previsões concretas. O titular dos dados tem o direito de se opor, a qualquer momento, ao tratamento dos seus dados pessoais, incluindo a definição de perfis, na medida em que esteja relacionado com o marketing direto (Ruaro, 2020, p. 246).	A legislação brasileira aplica as regras gerais de consentimento, transparência e direito de oposição dos titulares de dados pessoais (Ruaro, 2020, p. 246).

Relação entre o controlador e operador	A legislação europeia prevê que o tratamento de dados efetuado por um operador deve ser regido por um contrato ou outro ato jurídico que vincule o responsável pelo tratamento ao operador (Ruaro, 2020, p. 246).	Enquanto a legislação brasileira exige que o operador processe os dados de acordo com as instruções do controlador, não há necessidade de formalização através de um contrato (Ruaro, 2020, p. 246).
Relatório de Impacto	Na lei europeia está previsto que o controlador deve prover um relatório de impacto à proteção de dados pessoais, quando o tratamento resultar em um elevado risco para o direito e a liberdade das pessoas. O GDPR traz ainda uma detalhada descrição do que deve ser abordado neste relatório (Ruaro, 2020, p. 246).	A lei brasileira não deixou claro em quais situações o controlador será obrigado a realizar um relatório de impacto à proteção de dados pessoais, delegando a uma regulamentação posterior o tratamento desta matéria (Ruaro, 2020, p. 246).
Transferência de dados	A regulamentação europeia alega que a transferência internacional dos dados pode ser realizada independentemente de autorização específica caso a Comissão Europeia reconheça que o país terceiro assegure um nível de proteção adequado. Caso não, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo agente (Ruaro, 2020, p. 246).	A lei brasileira permite a transferência de dados pessoais para países ou órgãos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto. A LGPD estabelece apenas diretrizes genéricas a serem observadas pelas autoridades nacionais (Ruaro, 2020, p. 246).
Fiscalização do cumprimento da lei	A regulamentação europeia estabelece a criação do Comitê Europeu para Proteção de Dados, responsável por assegurar a aplicação coerente do GDPR (Ruaro, 2020, p. 246). Cada Estado-Membro tem uma autoridade de supervisão independente responsável por fazer cumprir a legislação.	A Autoridade Nacional de Proteção de Dados é o órgão responsável pela fiscalização e aplicação da LGPD no Brasil.

Fonte: adaptado de Ruaro (2020, p. 244-247).

Esse quadro destaca algumas divergências entre o GDPR europeu e a LGPD do Brasil. Divergências em relação à quantidade de bases legais para o processamento de dados pessoais; Mostra ainda que as definições de dados sensíveis são similares, porém, a LGPD enfatiza ainda mais a importância do consentimento específico e informado para seu processamento.

Outras diferenças incluem o tratamento de dados de menores, as políticas de proteção de dados, a relação dos representantes, aspectos para não responsabilização dos agentes, a relação com o marketing direto, a relação entre controlador e operador, os relatórios de impacto e a transferência de dados. A fiscalização do cumprimento da lei também apresenta diferenças, com o GDPR instituindo o Comitê Europeu para Proteção de Dados, enquanto a LGPD estabelece a Autoridade Nacional de Proteção de Dados para a supervisão e aplicação das regras no Brasil. Essas divergências ilustram que apesar das similaridades entre as normativas, existem abordagens distintas dos dois regulamentos na proteção e no tratamento de dados pessoais, refletindo as nuances culturais, legais e sociais de cada região.

Para o Brasil, a Lei Geral de Proteção de Dados trouxe um novo panorama para o tratamento e proteção de dados pessoais em diversas esferas da sociedade. No contexto dos órgãos públicos, a LGPD exerce um papel de destaque ao estabelecer diretrizes claras para a coleta, armazenamento, processamento e compartilhamento de dados pessoais e sensíveis. Entre esses órgãos, as Universidades Federais Brasileiras, como pilares de educação, pesquisa e inovação, desempenham um papel crucial na produção no tratamento de dados pessoais de docentes, discentes, técnicos administrativos e demais colaboradores.

Os dados pessoais podem ser definidos como qualquer informação que permita a identificação de uma pessoa física de forma direta ou indireta. Entre os exemplos mais comuns incluem-se nome e sobrenome, endereço residencial, endereço de e-mail (quando contém elementos que possibilitem a identificação do titular, como nome e sobrenome), gênero, data de nascimento, número de documentos cadastrais, como RG, CPF e Carteira de Trabalho, dados de geolocalização provenientes de dispositivos móveis e número de telefone pessoal. Esses elementos exemplificam a ampla abrangência dos dados pessoais e ressaltam a importância de protegê-los, especialmente em conformidade com

legislações vigentes. Neste cenário, é essencial compreender os principais elementos abordados na LGPD sobre como deve ser realizado o tratamento de dados pessoais nas esferas públicas.

2.4 Principais elementos e aspectos da Lei Geral de Proteção de Dados Brasileira para as Organizações Públicas

O advento da Lei Geral de Proteção de Dados no cenário jurídico brasileiro revolucionou a forma como as organizações, incluindo a Administração Pública, abordam o tratamento de dados e informações pessoais. No âmbito governamental, o capítulo IV, da Lei 13.709 de 2018, assume um papel central ao estabelecer diretrizes e normas específicas para o manuseio de dados pessoais pelos órgãos públicos. Esta seção apresenta um exame detalhado das disposições da LGPD relacionadas à Administração Pública, destacando suas obrigações e responsabilidades. Ele explora os princípios fundamentais que orientam o tratamento de dados, o cuidado com dados sensíveis, às medidas de segurança necessárias, bem como a supervisão e sanções associadas à conformidade. Esta seção visa fornecer uma compreensão abrangente das implicações da LGPD na administração governamental e a importância de proteger os direitos de privacidade dos cidadãos enquanto desempenham as funções públicas.

Assim, a Lei Geral de Proteção de Dados brasileira estabelece uma série de elementos e aspectos essenciais que as organizações públicas devem considerar e cumprir ao tratar dados pessoais. Aqui estão alguns dos principais elementos e aspectos da LGPD para as organizações públicas:

2.4.1 Princípios Fundamentais

Os princípios fundamentais da LGPD são essenciais na administração pública, fornecendo um arcabouço sólido para o tratamento de dados e informações pessoais. Esses princípios orientam as organizações a coletar, usar e proteger dados pessoais de maneira ética e legal. Eles estabelecem padrões de transparência, necessidade, segurança e responsabilidade, garantindo que os direitos de privacidade dos cidadãos sejam respeitados em todas as interações com o governo. Neste contexto, compreender e aplicar esses princípios é essencial para

promover a confiança pública e garantir o cumprimento da lei na administração pública. Os princípios fundamentais são:

- **Finalidade e Adequação** - A administração pública deve coletar dados pessoais apenas para finalidades específicas e legítimas relacionadas às suas funções governamentais. Os dados não podem ser usados de maneira incompatível com essas finalidades.
- **Necessidade e Qualidade** - A coleta de dados pela administração pública deve ser estritamente necessária para o desempenho de suas funções. Os dados devem ser precisos, atualizados e relevantes para as atividades governamentais em questão.
- **Transparência e Acesso** - A administração pública deve ser transparente sobre como os dados pessoais são coletados, usados, armazenados, compartilhados e eliminados. Os cidadãos têm o direito de acessar suas informações pessoais mantidas pelo governo e verificar sua exatidão. Isso promove a prestação de contas e a confiança na administração pública.
- **Segurança e Prevenção** - A administração pública é responsável por adotar medidas rigorosas de segurança de dados para proteger as informações pessoais dos cidadãos. Isso inclui a prevenção de acessos não autorizados e a implementação de protocolos de segurança para evitar vazamentos de dados.
- **Responsabilidade e Boa-fé** - A administração pública é responsável por garantir o cumprimento da LGPD em todas as suas atividades de tratamento de dados pessoais. Ela deve agir de boa-fé, garantindo que os cidadãos tenham seus direitos de privacidade respeitados e que as práticas de tratamento de dados estejam em conformidade com a lei.

Esses princípios são especialmente relevantes para a administração pública, já que ela lida com dados e informações pessoais, inclusive sensíveis, devendo agir sempre com responsabilidade e transparência em suas operações relacionadas a dados e informações pessoais.

2.4.2 Tratamento de Dados sensíveis

A LGPD impõe restrições adicionais ao tratamento de dados sensíveis, como informações sobre saúde, religião, orientação sexual e origem racial. O tratamento desses dados requer um nível mais alto de proteção e uma justificativa legítima, como o interesse público.

- Definição de Dados Pessoais Sensíveis - de acordo com a LGPD, dados pessoais sensíveis são:

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018, art. 5º, inc. II).

Esses dados são considerados mais sensíveis devido ao potencial de discriminação e violação da privacidade que podem representar.

- Bases Legais para o Tratamento de Dados Sensíveis - conforme o artigo 11 da LGPD, o tratamento de dados pessoais sensíveis requer consentimento expresso do titular dos dados, exceto quando for indispensável para: cumprir obrigações legais ou regulatórias pelo controlador; executar políticas públicas previstas em leis ou regulamentos; realizar estudos por órgãos de pesquisa (priorizando sempre a anonimização); exercer regularmente direitos, incluindo o exercício de direitos em processos judiciais; proteger a vida ou a integridade física do titular dos dados ou de terceiros; garantir a saúde ou prevenir fraudes e a segurança do titular dos dados.
- Consentimento - O consentimento desempenha um papel central na estrutura da LGPD. Essa importância é evidenciada pelas 35 ocorrências do termo no texto da Lei. Essa análise de relevância não se limita apenas à quantificação do termo, mas também aborda o aspecto qualitativo, identificando um sistema normativo intrinsecamente relacionado ao conceito de consentimento, consolidando-o como elemento central (Bioni, 2021, p. 133).

Obter o consentimento dos titulares de dados sensíveis, no contexto do poder público, pode ser mais desafiador, tornando outras bases legais, como o interesse público, mais relevantes. No entanto, quando o consentimento é necessário, as organizações devem obter uma autorização clara e específica dos titulares dos dados sensíveis. A LGPD é explícita quando diz que:

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei. Parágrafo único. A informação à autoridade nacional de

que trata o caput deste artigo será objeto de regulamentação (Brasil, 2018, art. 27).

- Medidas de Segurança Reforçadas - dados pessoais sensíveis requerem medidas de segurança mais robustas, considerando o risco mais elevado de impacto negativo em caso de violação. A Administração Pública deve implementar salvaguardas técnicas e organizacionais adequadas para proteger esses dados contra acesso não autorizado ou vazamentos.
- Anonimização e Pseudonimização - para mitigar os riscos associados ao tratamento de dados sensíveis, a Administração Pública, baseada no artigo 12 da LGPD, pode adotar técnicas de anonimização ou pseudonimização. Isso envolve a remoção ou substituição de informações pessoais identificáveis para tornar os dados menos identificáveis.
- Fiscalização e Sanções - a LGPD estabelece autoridades de fiscalização que monitoram o cumprimento das obrigações de proteção de dados, incluindo o tratamento de dados pessoais sensíveis. As sanções por não conformidade podem ser particularmente severas quando se trata desses dados.

É essencial que o poder público compreenda os requisitos da LGPD relacionados a dados pessoais sensíveis e adote políticas e práticas rigorosas de proteção de dados para garantir o cumprimento da lei e a preservação dos direitos de privacidade dos cidadãos. Além disso, a sensibilização e a capacitação dos funcionários são fundamentais para garantir que o tratamento de dados sensíveis seja realizado de maneira ética e legal.

2.4.3 Responsabilidades da Administração Pública

De acordo com a Lei Geral de Proteção de Dados, a Administração Pública possui uma série de responsabilidades cruciais no tratamento de dados pessoais. Isso inclui a nomeação de um Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO) para supervisionar a conformidade com a lei, a adoção de medidas de segurança adequadas para proteger os dados pessoais, a transparência na comunicação com os titulares dos dados e a notificação às autoridades e aos titulares em caso de violação de dados. Essas responsabilidades garantem a proteção dos direitos de privacidade dos cidadãos e promovem a confiança nas práticas de tratamento de dados da Administração Pública.

- Nomeação de Encarregado de Proteção de Dados (DPO) - Todos os órgãos públicos devem nomear um Encarregado de Proteção de Dados para supervisionar a conformidade com a LGPD. No capítulo IV da LGPD, que é uma parte específica da Lei para tratamento de dados pelo poder público, diz que “seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais” (Brasil, 2018, art. 23, inc. III). Já a seção II do capítulo VI da LGPD vai complementar esse preceito legal:

O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados (Brasil, 2018, art. 41).

- Transparência e Comunicação - a Administração Pública deve ser transparente sobre suas práticas de tratamento de dados, comunicando de forma clara e acessível aos titulares.
- Medidas de Segurança - A Administração Pública deve implementar medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados e/ou vazamentos.
- Relatórios de Incidentes - em caso de violação de dados, a Administração Pública deve notificar as autoridades e os titulares, conforme exigido pela LGPD (artigo 48).

2.4.4 Fiscalização e Sanções

A Lei Geral de Proteção de Dados estabelece um conjunto de mecanismos de fiscalização e aplicação de sanções específicas para o tratamento de dados pessoais pelo poder público. Essas medidas visam garantir que os órgãos governamentais cumpram rigorosamente as obrigações de proteção de dados

peçoais e promovam a transparência e a responsabilidade no tratamento de informações peçoais dos cidadãos.

- **Autoridade Nacional de Proteção de Dados (ANPD)** - a ANPD é a entidade governamental responsável por fiscalizar o cumprimento da LGPD pelo poder público. Ela possui autoridade para investigar, auditar e aplicar sanções em caso de não conformidade com a lei.
- **Fiscalizações e Auditorias** - a ANPD tem o poder de realizar auditorias e fiscalizações em órgãos públicos para verificar se estão em conformidade com a LGPD. Essas ações podem ocorrer de forma programada, em resposta a denúncias ou incidentes de segurança de dados.
- **Sanções Administrativas** - Assim como para o setor privado, a LGPD prevê sanções administrativas para órgãos públicos que não estejam em conformidade. As sanções incluem advertências, multas, bloqueio de dados peçoais, suspensão parcial ou total do tratamento de dados e a proibição temporária ou definitiva do tratamento de dados peçoais. As multas podem ser substanciais e dependem da gravidade da infração.

Inclusive, a Autoridade Nacional de Proteção de Dados já aplicou a primeira sanção por indícios de infração à Lei Geral de Proteção de Dados Peçoais (LGPD) a uma microempresa de telecomunicações que recebeu advertência e multa total de R\$14,4 mil. A advertência, sem imposição de medidas corretivas, deu-se por falta de indicação do encarregado pelo tratamento de dados peçoais. Já as duas multas — cada uma no valor de R\$7,2 mil — foram aplicadas por descumprimento dos deveres relativos à fiscalização da ANPD e das hipóteses em que é permitido o tratamento de dados peçoais, conforme a lei (Consultor Jurídico, 2023).

- **Obrigaçāo de Notificação de Violações** - Os órgãos públicos sāo obrigados a notificar a ANPD e os titulares dos dados em caso de violaçaō de dados que possam resultar em riscos ou danos para os titulares. A notificaçaō deve ser feita dentro de um prazo estabelecido pela lei.
- **Recursos Judiciais**: Assim como o setor privado, órgãos públicos tēm o direito de contestar as decisōes da ANPD e buscar recursos judiciais em caso de sanções ou determinações da autoridade.
- **Compromisso com a Conformidade** - órgãos públicos sāo incentivados a adotar medidas proativas para garantir a conformidade com a LGPD. Isso inclui a implementaçāo de polítics de proteçaō de dados, a realizaçaō de avaliações de

impacto à proteção de dados, a capacitação dos funcionários e a transparência nas práticas de tratamento de dados pessoais.

Ainda nos termos da Lei, o Artigo 31 permite que a autoridade nacional intervenha quando houver infrações à LGPD por parte desses órgãos públicos, autorizando-a a enviar um informe com medidas apropriadas para encerrar a violação, demonstrando o compromisso de coibir práticas não conformes. E o Artigo 32 confere à autoridade nacional o poder de solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais, além de oferecer sugestões para a adoção de padrões e boas práticas nos tratamentos de dados pessoais realizados pelo setor público. Essas disposições visam a garantir a conformidade com a LGPD e promover a responsabilidade e transparência no tratamento de dados pessoais por parte do Poder Público.

Assim, a LGPD estabelece um quadro jurídico rigoroso para a Administração Pública no que diz respeito ao tratamento de dados pessoais. É essencial que os órgãos governamentais estejam plenamente cientes de suas obrigações e responsabilidades sob esta lei, garantindo a proteção adequada dos direitos de privacidade dos cidadãos enquanto cumprem suas funções públicas. A conformidade com essas disposições é vital para promover a confiança do público e a transparência no governo.

2.4.5 Outras legislações e normativas que impactam no tratamento dos dados e informações pessoais

Além da Lei Geral de Proteção de Dados, o cenário regulatório brasileiro é marcado por diversas outras normativas que exercem influência significativa sobre o tratamento de dados pessoais pelo poder público. Essas legislações abrangem temas que vão desde o acesso à informação até à privacidade e a segurança dos cidadãos, estabelecendo também diretrizes e responsabilidades adicionais para órgãos governamentais. Podemos citar algumas dessas normativas, como:

- A Lei n. 9.507/1997, conhecida como Lei do Habeas Data, concede aos cidadãos o direito de acessar informações armazenadas em entidades públicas, bem como de retificar registros imprecisos. Isso se alinha diretamente com a proteção de dados pessoais, uma vez que permite que os indivíduos controlem e verifiquem a exatidão de suas informações pessoais.

- A Lei n. 9.784/1999, ou Lei Geral do Processo Administrativo, estabelece procedimentos para a Administração Pública, incluindo o tratamento de dados pessoais em processos administrativos. Ela se relaciona com a LGPD ao exigir que os órgãos públicos ajam de maneira transparente e justa em seus procedimentos, protegendo os direitos dos cidadãos em relação ao tratamento de dados pessoais.
- A Lei n. 12.527/2011, conhecida como Lei de Acesso à Informação, promove a transparência governamental ao garantir o acesso do público a informações públicas. Ela está intrinsecamente ligada à LGPD, pois ambas visam a equilibrar o acesso à informação com a proteção dos dados pessoais dos cidadãos. Essa conexão enfatiza a importância de garantir que o acesso às informações públicas não comprometa a privacidade e a segurança dos dados pessoais.
- A Associação Brasileira de Normas Técnicas (ABNT) estabelece diretrizes e boas práticas para a gestão da segurança da informação em organizações, através das seguintes Normas Brasileiras (NBR): ISO/IEC 27701:2019, 27014:2021, 27001:2024, 27002:2022, 27005:2023, 27035:2023 e 29134:2024. Essas normas oferecem um conjunto abrangente de controles de segurança que podem ser implementados para proteger ativos de informação, contribuindo na gestão quanto ao acesso, transparência, proteção, segurança e tratamento dos dados pessoais.
- O Decreto n. 9.637/2018 Institui a Política Nacional de Segurança da Informação, com objetivo de proteger informações sensíveis e estratégicas do governo brasileiro. Ela estabelece princípios, responsabilidades e diretrizes gerais para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, bem como para a gestão de riscos cibernéticos.
- O Decreto n. 10.046/2019 estabelece diretrizes para a governança no compartilhamento de informações no contexto da administração pública federal e cria o Cadastro Base do Cidadão, juntamente com o Comitê Central de Governança de Dados. E o Decreto n. 11.226, de 25 de novembro de 2022 traz alterações e orientações sobre como as organizações públicas devem cumprir as obrigações da LGPD, garantindo a conformidade com os padrões de proteção de dados e a preservação dos direitos de privacidade dos cidadãos.
- A Instrução Normativa (IN) do Gabinete de Segurança Institucional n. 1, datada de 27 de maio de 2020, é um documento oficial que estabelece diretrizes e normas para a segurança da informação e a proteção de dados no âmbito do governo federal brasileiro. Ela visa promover a confidencialidade, integridade e

disponibilidade das informações governamentais, estabelecendo protocolos e procedimentos para lidar com questões relacionadas à segurança cibernética e à gestão de riscos.

- A Instrução Normativa da Secretaria de Governo Digital (SGD) do Ministério da Economia (ME) n. 117/2020 aborda a designação do Encarregado pelo Tratamento de Dados Pessoais nos órgãos e entidades da administração pública federal direta, autárquica e fundacional. O Encarregado é responsável por zelar pela proteção dos dados pessoais, atuar como canal de comunicação com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD), e garantir o cumprimento das normas de proteção de dados no ambiente organizacional público.
- Acórdão n. 1.384/2022 - Plenário do Tribunal de Contas da União (TCU) do dia 15 de junho de 2022 que foi decorrente da publicação do resultado do processo de auditoria TC 039.606/2020-1 realizada em 382 (trezentos e oitenta e duas) organizações públicas federais para avaliar a aderência de suas ações às diretrizes estabelecidas pela Lei Geral de Proteção de Dados - LGPD, autorizada pelo Acórdão 2.909/2020-TCU-Plenário. Esse trabalho buscou avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. A fiscalização foi estruturada a partir de três questões de auditoria: Q1) As organizações se estruturaram para a condução de iniciativas de adequação à LGPD? Q2) As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD? Q3) A ANPD e o CNPD (Conselho Nacional de Proteção de Dados) estão estruturados e em operação conforme estabelecido na LGPD? O trabalho foi conduzido em conformidade com as Normas de Auditoria do TCU.
- Resolução CONARQ n. 54/2023 elaborada para orientar a aplicação da Lei Geral de Proteção de Dados Pessoais em relação aos arquivos permanentes, sejam eles custodiados por entidades públicas ou privadas. Seu propósito é assegurar que os dados pessoais contidos nestes arquivos sejam tratados de acordo com os princípios e diretrizes estabelecidos na LGPD, garantindo assim a privacidade, segurança e integridade dessas informações ao longo do tempo. A resolução define procedimentos e padrões para a gestão documental que estejam em conformidade com a legislação de proteção de dados, contribuindo para uma abordagem

consistente e responsável no tratamento de informações pessoais nos arquivos permanentes.

- Por fim, destacam-se as Resoluções CD/ANPD n. 15, de 24 de abril de 2024, e CD/ANPD n. 18, de 16 de julho de 2024, que aprovam, respectivamente, o Regulamento de Comunicação de Incidente de Segurança e o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

Este contexto normativo complexo exige uma abordagem integrada e estratégica por parte das entidades públicas para assegurar a conformidade e a proteção adequada dos dados pessoais, enquanto cumprem suas obrigações legais e promovem a transparência nas ações governamentais.

3 MODELO DE MATURIDADE

Esta seção compreende uma revisão de escopo sobre Modelo de Maturidade (MM), englobando uma explanação acerca da gênese desses modelos e de suas aplicações e tipologias mais comuns. Destaca-se, nesse âmbito, explicar os propósitos subjacentes e as características inerentes de modelos específicos de destaque. Geralmente, os modelos de maturidade são desenvolvidos por acadêmicos e profissionais da indústria, e sua utilização tem crescido significativamente nos últimos anos. As aplicações desses modelos são amplas e variadas. Elas abrangem diversos domínios, incluindo o desenvolvimento de software, tecnologia da informação, gestão de processos, gestão de projetos, gestão de negócios, gestão da qualidade, gestão do conhecimento, entre outros.

O tratamento dos dados e informações pessoais deve ser realizado e acompanhado de forma apropriada, a fim de assegurar o eficiente desempenho organizacional. Nesse contexto, os modelos de maturidade desempenham um papel fundamental ao diagnosticar o posicionamento da empresa, facultando um suporte valioso no planejamento estratégico de melhorias voltadas ao tratamento desses dados e informações. A aplicação de modelos de maturidade nas organizações cresce gradativamente, aumentando a popularidade dessa ferramenta no âmbito empresarial. Tal tendência, por sua vez, amplifica de modo proporcional o interesse suscitado também na esfera acadêmica. Esta seção empreende uma análise profunda dos conceitos e das características inerentes aos modelos de maturidade, proporcionando, adicionalmente, um resgate dos modelos de maturidade mais amplamente difundidos, assim como dos contextos primordiais nos quais esses modelos encontram sua aplicação preeminente.

Com base nessa premissa, foi realizada uma revisão sistemática das produções publicadas sobre os termos “modelo de maturidade” e/ou “*maturity model*”, no intuito de identificar as aplicabilidades mais utilizadas e suas principais características. Essa pesquisa contribuiu na fundamentação teórica para a construção e desenvolvimento de uma proposta de modelo de maturidade para tratamento de dados pessoais, produto desta tese.

A revisão sistemática foi realizada em cinco bases de dados científicas conveniadas à Plataforma de Periódicos da Coordenação de Aperfeiçoamento de

Pessoal de Nível Superior (CAPES) vinculada ao Ministério da Educação (MEC). O principal método para coleta e análise dos dados foi o *ProKnow-C (Knowledge Development Process – Constructivist)*².

Segundo Ilesbik Valmorbidia *et al.* (2016, p. 12) "o objetivo principal do *Proknow-C* é construir conhecimento sobre um fragmento da literatura científica, inicialmente no pesquisador e, quando da publicação dos resultados da investigação, aos leitores da comunidade científica do tema". Foram selecionados artigos de cinco bases de dados científicas: 1) *Scopus (elsevier)*; 2) *Scielo.ORG*; 3) *ScienceDirect (Elsevier)*; 4) *CINAHL with full text (EBSCOhost)*; e, 5) *Web of Science - Coleção Principal (Clarivate Analytics)*. E as consultas foram realizadas por meio da expressão "modelo de maturidade" OR "*maturity model*". Sendo limitado às publicações, entre os anos de 2012 a 2022. A área de estudo selecionada foram "Negócios, gestão e contabilidade", "Ciências Sociais" e "Ciências da Decisão". Segue, no quadro 4, os "*string* de busca" ou a forma de busca, realizada em cada base de dados científica:

Quadro 4 - Formas de busca utilizada na pesquisa sobre MM

Base Científica	Forma de busca (link ou string de busca)
EBSCOhost	" <i>maturity model</i> " or "modelo de maturidade" Data de publicação: 20120101-20211231
Scielo.ORG	Expressão: " <i>maturity model</i> " or "modelo de maturidade" Filtros aplicados: (Ano de publicação: 2019) (Ano de publicação: 2017) (Ano de publicação: 2020) (Ano de publicação: 2015) (Ano de publicação: 2013) (Ano de publicação: 2014) (Ano de publicação: 2016) (Ano de publicação: 2018) (Ano de publicação: 2012) (Ano de publicação: 2021)
ScienceDirect	" <i>maturity model</i> " ou "modelo de maturidade" Ano : 2012-2022
Scopus	TITLE-ABS-KEY(" <i>maturity model</i> " ou "modelo de maturidade") E (LIMIT-TO (PUBYEAR,2022) OU LIMIT-TO (PUBYEAR,2021) OU LIMIT-TO (PUBYEAR,2020) OU LIMIT-TO (PUBYEAR,2019) OU LIMIT-TO (PUBYEAR,2018) OU LIMIT-TO (PUBYEAR,2017) OU LIMIT-TO (PUBYEAR,2016) OU LIMIT-TO (PUBYEAR,2015) OU LIMIT-TO (PUBYEAR,2014) OU LIMIT-TO (PUBYEAR,2013) OU LIMIT-TO (PUBYEAR,2012)) E (LIMIT-TO (SUBJAREA,"BUSI"))

² *Proknow-C* é um processo descritivo e sequencial em que o conhecimento sobre o tema em análise vai sendo construído mediante as etapas. Definida a visão de mundo adotada, ocorre a seleção de estudos de forma criteriosa, após vem o levantamento quantitativo das produções no que tange às características dos autores, periódicos e publicações do tema, levando a uma reflexão sobre o fragmento da literatura selecionado a partir da filiação teórica adotada na pesquisa, estabelecendo relações entre a produção e a teoria do tema em destaque (Castelli, 2018, p. 62).

	OU LIMIT-TO (SUBJAREA,"SOCI") OU LIMIT-TO (SUBJAREA,"DECI ")) E (LIMIT-TO (DOCTYPE,"ar") OU LIMIT-TO (DOCTYPE,"ch") OU LIMIT-TO (DOCTYPE,"bk")) AND (LIMIT-TO (OA,"all")) E (LIMIT-TO (EXACTKEYWORD,"Modelo de Vencimento") OU LIMIT-TO (EXACTKEYWORD,"Modelos de Vencimento") OU LIMIT-TO (EXACTKEYWORD,"Maturidade"))
<i>Web of Science</i>	https://www.webofscience.com/wos/woscc/summary/6669ea18-c0a1-4d24-b51b-dead28709913-22ee1709/times-cited-descending/1

Fonte: elaborado pelo autor.

As consultas ocorreram no período entre 10 de fevereiro a 13 de fevereiro de 2022 e resultaram na exportação de 294 (duzentos e noventa e quatro) artigos das bases de dados. Com o objetivo de estabelecer uma maior proximidade com as disciplinas pertencentes ao campo das Ciências Sociais Aplicadas, especialmente Ciência da Informação e Administração, foram realizadas leituras individuais dos títulos e resumos dos textos pré-selecionados. Isso resultou na eliminação de 39 (trinta e nove) documentos redundantes e de 150 (cento e cinquenta) documentos que demonstraram distanciamento em relação às áreas de interesse estipuladas. Como resultado, foram selecionados 105 (cento e cinco) documentos.

Posteriormente, 26 (vinte e seis) textos foram excluídos devido à indisponibilidade de acesso integral ao seu conteúdo. Esse processo culminou na seleção de 72 (setenta e dois) documentos, os quais foram submetidos a uma leitura completa e avaliação. Finalmente, para enriquecer o estudo, houve a inclusão de incursões bibliográficas provenientes das obras referenciadas pelos documentos eleitos nesta revisão, bem como pela incorporação de publicações contemporâneas que, conforme critério do autor deste trabalho, foram consideradas essenciais para conferir um alicerce conciso à construção desta seção.

3.1 Conceito

Para compreender o que é o modelo de maturidade, é necessário entender a sua essência. Maturidade implica progredir de algum estado inicial para um estado mais avançado. A noção de evolução está implícita nos estágios de crescimento, sugerindo que o progresso passa por uma série de estados intermediários no caminho para níveis de maturidade mais elevados (Sen; Ramamurthy; Sinha, 2012, p. 338, tradução nossa).

Assis *et al.* (2012, p. 418) ressaltam que a “maturidade pode ser entendida como a extensão em que o processo é explicitamente definido, gerenciado, medido, controlado e eficaz”. A maturidade reflete o quão desenvolvida está uma organização sob uma abordagem específica. Antunes (2001, p. 45) diz que “[...] a maturidade permite a avaliação de qualquer ser, coisa ou sistema, visando determinar as suas características e desempenhos, nomeadamente os seus pontos fortes e fracos em plena atividade”

A maturidade pode ser vista como um processo gradual de aquisição de competências ao longo do tempo, conquistado por meio de planejamento e ações destinadas ao aperfeiçoamento, com o intuito de conduzir a organização à realização de seus objetivos. Em cada modelo de maturidade, será proposta uma forma de avaliar o grau de maturidade das competências da organização, podendo ser comparados com outras organizações.

De uma perspectiva mais prática, Costa e Ramos (2013, p. 236-237) afirmam que a maturidade “pode ser entendida como a utilização de práticas adequadas para cada organização, segundo sua área de atuação, porte, complexidade e recursos disponíveis”. Eles ainda complementam que “as organizações maduras procedem de modo sistemático e as imaturas atingem seus resultados graças aos esforços heróicos de indivíduos usando abordagens que eles criam mais ou menos espontaneamente”. Já Rosemann e De Bruin (2005, p. 1, tradução nossa) dizem que “a maturidade é como uma medida para avaliar as capacidades de uma organização em relação a uma determinada disciplina”. Nesse sentido, Proença e Borbinha (2018, p. 1, tradução nossa) destacam que:

Uma avaliação de maturidade pode ser usada para medir o nível de maturidade atual de um determinado aspecto de uma organização de maneira significativa, permitindo que as partes interessadas identifiquem claramente pontos fortes e áreas de melhoria, e, consequentemente, priorizem o que fazer para atingir níveis de maturidade mais elevados.

Assim, um modelo de maturidade é um roteiro evolucionário para implementar as práticas vitais de um ou mais domínios de um campo organizacional. A fim de promover uma abordagem que possibilite aumentar a capacidade de uma área específica dentro de uma organização, esses modelos são usados como base avaliativa e comparativa em busca de melhorias contínuas.

Um modelo de maturidade pode ser visto como um quadro referencial para a compreensão do desenvolvimento de uma organização ao longo do tempo. Em outras palavras, é uma ferramenta de avaliação que permite que a empresa avalie o seu progresso em relação a um determinado conceito (Hepper, 2017, p. 13).

Hepper (2017, p. 29) explica ainda que “o modelo de maturidade fornece uma visão geral, composta por pequenos elementos e, assim, de forma abrangente, explica como implementar o desenvolvimento de um produto ou de um processo”. Já Prado (2004, p.19), diz que “modelo de maturidade em gestão de projetos é essencialmente um arquétipo de crescimento que estabelece estágios pré-definidos, permitindo auto avaliações e aperfeiçoamentos”.

Os modelos de maturidade foram projetados para avaliar a maturidade (ou seja, competência, capacidade, nível de sofisticação) de um domínio selecionado com base em um conjunto de critérios mais ou menos abrangentes. Eles geralmente usam avaliações ou declarações qualitativas, mas também podem ser apoiados por relatos descritivos adicionais e também por medidas quantitativas. (Kirkwood; Alinaghian; Srai, 2011, p. 16, tradução nossa).

Um modelo de maturidade é aquele que aponta as trilhas já demarcadas, pelas quais as organizações deveriam passar, e os marcos a serem atingidos sequencialmente, a ponto de perseguir resultados mais efetivos e previsíveis na gestão de seus projetos (Costa; Ramos, 2013, p. 237).

Portanto, compreende-se que um modelo de maturidade representa uma abordagem sistemática voltada para a avaliação e o aprimoramento dos processos, projetos, sistemas e capacidades inerentes a uma organização. Seu propósito fundamental reside em contribuir para que a organização alcance um patamar mais elevado de eficiência, eficácia e satisfação de seus clientes. Tais modelos se configuram por meio de uma sucessão de etapas ou níveis claramente definidos, os quais delineiam os distintos graus de maturidade que uma organização pode vir a atingir em relação a um contexto específico.

Os modelos de maturidade podem ser aplicados em diversas áreas, como gestão de projetos, segurança da informação, privacidade de dados e outras áreas de gerenciamento. Eles possibilitam a identificação de pontos fortes e oportunidades de melhoria nos processos, sistemas, produtos e capacidades, orientando a organização na implementação de mudanças que visam melhorar o desempenho,

preparar-se para auditorias, avaliações regulatórias e outras formas de fiscalizações. Conforme ratificado por Costa e Ramos (2003, p. 237):

É possível notar que o modelo de maturidade é um referencial usado para avaliar a capacidade de processos na realização de seus objetivos, localizar oportunidades de melhoria de produtividade e qualidade e de redução de custos, e planejar e monitorar as ações de melhoria contínua dos processos empresariais.

Para um entendimento mais profundo sobre modelos de maturidade é fundamental compreender a origem e suas raízes para adquirir uma perspectiva abrangente e embasada sobre seu propósito e evolução. O estudo da origem de um modelo de maturidade nos permite compreender os desafios e contextos que levaram à sua concepção, bem como as necessidades e demandas específicas que buscava atender. Além disso, ao analisar as raízes de um modelo, podemos identificar as teorias, metodologias e práticas que influenciaram sua construção, fornecendo *insights* sobre suas bases conceituais e referências teóricas. Ao investigar a origem e as raízes de um modelo de maturidade, somos capazes de obter uma visão mais aprofundada de sua aplicabilidade, utilidade e eficácia, permitindo uma análise crítica e embasada em seu uso e adaptação aos contextos atuais.

3.2 Breve histórico

A origem dos modelos de maturidade remonta ao início dos anos 50, quando estudiosos da época se propuseram a discutir ideias e metodologias em torno da compreensão do comportamento das organizações e seus profissionais frente à competitividade emergente.

Um dos precursores da ideia de maturidade como uma evolução de etapas foi Maslow (1954), que desenvolveu uma concepção análoga à teoria de estágios. Essa concepção, posteriormente, seria aplicada nos primeiros modelos de maturidade. Maslow estabeleceu uma hierarquia para as necessidades humanas, na qual determinada necessidade humana só poderia ser alcançada quando as necessidades básicas predecessoras na hierarquia fossem supridas. Isso pode ser comparado a uma espécie de estágios de motivação, representando a evolução das necessidades humanas.

Outra ideia semelhante foi desenvolvida por Donald Kirkpatrick (1959), que estabeleceu uma metodologia de avaliação em quatro níveis (reação, aprendizagem, comportamento e resultados) para medir a eficácia dos programas de treinamento e seus impactos nas organizações.

Já o Simon Kuznets (1965, p. 215, tradução nossa) aplicou um raciocínio similar para avaliar o crescimento econômico, estabelecendo diretrizes adicionais para o desenvolvimento de uma teoria de estágios. Ele afirmou que:

(1) as características de cada estágio devem ser distintas e empiricamente testáveis; e (2) a relação analítica de qualquer estágio com seu predecessor ou sucessor deve ser bem definida - identificando quais processos fazem com que um elemento se mova de um estágio para o próximo.

A maturidade em si tem suas raízes no campo da gestão da tecnologia da informação e, posteriormente, na gestão de projetos, processos e qualidade. *Nolan* (1973) foi o primeiro a idealizar uma teoria de estágios para acompanhar o crescimento do uso de tecnologias da informação nas empresas. Ele sugeriu que o planejamento, a organização e o controle das atividades associadas ao uso dos recursos de computador poderiam ser avaliados com base no grau de satisfação dos usuários. Ele dividiu essa teoria em quatro estágios: 1. Iniciação, relacionado à aquisição de computadores; 2. Contágio, relacionado ao desenvolvimento intenso do sistema; 3. Controle, relacionado ao aumento nos controles de acompanhamento; e 4. Integração, que abordava a orientação usuário/serviço.

As principais características para a formulação da teoria dos estágios são: (1) a identificação dos elementos e (2) a concepção de seu crescimento ao longo do tempo. O conceito de um elemento é que ele é genérico para um campo particular e pode ser especificado por um conjunto de atributos. As teorias de estágio se baseiam na premissa de que os elementos nos sistemas passam por uma série de estágios distintos ao longo de um período de tempo e que esses estágios podem ser descritos (Nolan, 1973, p. 400, tradução nossa).

Para muitos autores, Philip B. Crosby foi o precursor do modelo de maturidade aplicado à gestão. Em 1979, ele lançou o livro intitulado *Quality is Free: The Art of Making Quality Certain*, no qual apresentou uma abordagem diferente para o gerenciamento da qualidade. Sob uma perspectiva métrica quantitativa mensurável, ele desenvolveu catorze etapas que promoveriam, de uma forma

sistemática, o aumento da qualidade em uma organização. Ele também criou uma ferramenta organizacional chamada *Quality Management Maturity Grid* (QMMG), que ajudaria os gestores a identificar o estado atual da gestão da qualidade em suas organizações. Essa ferramenta inclui cinco estágios de evolução (incerteza, despertar, iluminação, sabedoria e certeza). Com base no posicionamento da empresa, seria possível elaborar um plano de ação mais consistente para melhorar a qualidade. A QMMG é considerada o antecessor do *Capability Maturity Model* (CMM).

Em 1988, Watts S. Humphrey lançou o livro intitulado *Characterizing the Software Process: A Maturity Framework*, introduzindo o conceito de *Capability Maturity Model* (CMM). Isso representou um marco significativo no campo da engenharia de software e na gestão de processos. A gênese dessa ferramenta foi concebida com o propósito intrínseco de realizar uma avaliação objetiva da aptidão dos processos inerentes aos prestadores de serviços governamentais, no âmbito da implementação de projetos de software subcontratados.

Posteriormente, na década de 90, o Instituto de Engenharia de Software (SEI - *Software Engineering Institute*) da Universidade Carnegie Mellon desenvolveu uma ferramenta focada no processo de desenvolvimento de software, chamada *Capability Maturity Model* (CMM). Em 1991, Mark C. Paulk liderou a iniciativa de desenvolver uma representação abrangente do CMM, que incluía áreas de processo e práticas definidas. Essa visão ambiciosa se concretizou com a conclusão da Versão 1.1 em janeiro de 1993, representando um ponto de referência importante na evolução do CMM. Em 1995, Mark C. Paulk, junto com seus colegas Charles V. Weber, Bill Curtis e Mary Beth Chrissis, publicou o CMM como um livro, tornando-o amplamente disponível e influente no campo de desenvolvimento de software e gerenciamento de processos.

Assim, o CCM tornou-se um modelo de gestão que contribui não só para o diagnóstico e avaliação da maturidade de processos relacionados ao desenvolvimentos de *softwares*, mas também a outros contextos. Este modelo é representado por cinco níveis de maturidade: inicial, repetível, definido, gerenciado com métricas e otimizado.

Desde 1991, CMMs foram desenvolvidos para uma miríade de disciplinas. Alguns dos mais notáveis incluem modelos para engenharia de sistemas, engenharia de software, aquisição de software, gerenciamento e desenvolvimento de força de trabalho e desenvolvimento integrado de produtos e processos (Software Engineering Institute, 2002, p. i, tradução nossa).

Os níveis de maturidade do CMM abrangem características específicas para cada estágio. A etapa inicial apresenta um processo informal, imprevisível e sem controle. O estágio seguinte, chamado de repetível, é representado por um processo disciplinado, mais realista e baseado no histórico. No estágio definido, os processos são consistentes e padronizados. No estágio Gerenciado, o processo é previsível e controlado quantitativamente. Por fim, no estágio otimização, o processo está consolidado e é aperfeiçoado continuamente.

Com o surgimento do modelo de maturidade de capacidade da Universidade Carnegie Mellon, ocorreu a popularização dos modelos de maturidade. Diversas outras organizações profissionais e acadêmicas começaram a estudar, adequar e criar novos modelos de maturidade para atender às suas necessidades específicas, o que diversificou bastante a aplicabilidade desses modelos. De acordo com Costa e Ramos (2013, p. 237) “os modelos de maturidade em gestão de projetos surgem a partir da década de 1990, com o propósito de medir e melhorar a habilidade da organização na execução de seus processos de gerenciamento de projetos”.

Surge a partir desses contextos modelos que ganharam certa relevância, como: *Project Management Maturity Model* (PMMM); *Kerzner Project Management Maturity Model* (KPMMM); Modelo de Maturidade em Gerenciamento de Projetos (MMGP), todos derivados do CMM e caracterizados por apresentarem cinco níveis de maturidade também.

Semelhante ao CMM, o Modelo de Maturidade do BPM foi projetado para ser uma ferramenta de autoavaliação e avaliação de terceiros. A autoavaliação é feita na forma de um questionário. As questões são quantitativas e baseadas em uma escala de cinco pontos. A escala corresponde às descrições genéricas dos requisitos do estágio. Consequentemente, as respostas podem ser relacionadas a um estágio de maturidade (Rosemann; De Bruin, 2005, p. 7, tradução nossa). Esse modelo é conhecido popularmente como *Business Process Management Maturity Model* (BPMMM).

Neste período, destaca-se o projeto *Capability Maturity Model Integration* (CMMI)³, com o intuito de resolver o problema do uso de vários CMMs ao mesmo tempo. A missão era concatenar três modelos consagrados: (1) Modelo de Maturidade de Capacidade para Software v2.0 rascunho C, (2) Padrão Interino da *Electronic Industries Alliance* (EIA/IS) 731 e (3) Modelo de Maturidade de Capacidade de Desenvolvimento de Produto Integrado - *Integrated Product Development Capability Maturity Model* (IPD-CMM) v0.98, padronizando em uma única estrutura de melhoria para ser usado em organizações que buscam melhoria de processo em toda a empresa (Software Engineering Institute, 2002, p. ii, tradução nossa).

O objetivo do CMM *Integration* é fornecer orientação para melhorar os processos de sua organização e sua capacidade de gerenciar o desenvolvimento, aquisição e manutenção de produtos ou serviços. Ajudando a organização a avaliar sua maturidade organizacional ou capacidade de área de processo, estabelecer prioridades para melhoria e implementá-las. Assim, um modelo CMMI ajuda a definir objetivos e prioridades de melhoria de processos, aprimora processos e fornece orientação para garantir processos estáveis, capazes e maduros. Servindo como um guia para a melhoria dos processos organizacionais (Software Engineering Institute, 2002, p. 1, tradução nossa). De acordo com Sen, Ramamurthy e Sinha (2012, p. 338, tradução nossa):

Modelos de maturidade como *Capability Maturity Model* (CMM) , *Capability Maturity Model Integration* (CMMI) e ISO 9001 desempenham um papel extremamente importante em ajudar as empresas de software a alcançar níveis mais elevados de maturidade, em seu processo de desenvolvimento e produto de qualidade.

Nota-se que, com o passar dos anos, diversos modelos de maturidade foram propostos para diferentes contextos. O Quadro 5 visa lançar luz sobre um conjunto seletivo de modelos de maturidade que têm contribuído significativamente para a otimização de práticas e processos em diferentes áreas, desde o desenvolvimento de software até a gestão de projetos, passando pela melhoria de processos, gestão do conhecimento e outros domínios cruciais da administração. Esses modelos representam marcos importantes na trajetória da gestão e na promoção da excelência organizacional.

³ O projeto CMMI envolveu diversas pessoas de diferentes organizações em todo o mundo.

Quadro 5 - Modelos de maturidade consagrados na literatura

Ano(s)	Modelo	Desenvolvedor
1987-1997	CMM (<i>Capability Maturity Model</i>)	SEI (<i>Software Engineering Institute</i>)
1993-2018	CMMI (<i>Capability Maturity Model Integration</i>)	SEI (<i>Software Engineering Institute</i>)
1998-2003	OPM3 (<i>Organizational Project Management Maturity Model</i>)	PMI (<i>Project Management Institute</i>)
1998	Berkeley (PM)2 Model (<i>Project Management Process Maturity Model</i>)	Berkeley
1999	KPMMM (<i>Kerzner Project Management Maturity Model</i>)	Harold Kerzner
2000	SPICE (<i>Standardized Process Improvement for Construction Enterprises</i>)	Sarshar et al.
2002	PMMM (<i>Project Management Maturity Model</i>)	PM Solutions
2002	KMMM (<i>Knowledge Management Maturity Model</i>) Siemens	Ehms e Langen
Setorial (2002) Corporativo (2004)	MMGP (Modelo de Maturidade em Gerenciamento de Projetos)	Darci Prado
2003	MPS.BR (Modelo de Processo do Software Brasileiro)	SOFTEX (Associação para Promoção da Excelência do Software Brasileiro)
2005-2006	BPM (BPM Maturity Model)	Rosemann e de Bruin
2006-2008	P3M3 (<i>Portfolio, Programme and Project Management Maturity Model</i>)	OGC (<i>Office of Government Commerce</i>)
2008-2011	SNDMM (<i>Sustainable Network Design Maturity Model</i>)	Kirkwood, Alinaghian e Srai
2009	P2MM (<i>PRINCE2 Maturity Model</i>)	OGC (<i>Office of Government Commerce</i>)
2012	CIM3 (<i>Construction Industry Macro Maturity Model</i>)	Willis e Rankin
2020	ICMM (<i>Industrialized Construction Maturity Model</i>)	Wang et al.

Fonte: elaborado pelo autor.

Cada modelo de maturidade apresentado possui uma origem claramente estabelecida, com autoria ou equipe de desenvolvimento identificáveis, além de um período definido de concepção e evolução. É possível aprofundar-se em qualquer

um desses modelos por meio das informações disponibilizadas, que podem ser facilmente acessadas em mecanismos de busca ou em bases de dados científicas.

As fontes de consulta, além de fornecerem informações detalhadas, atuam como guias que permitem uma análise mais profunda da aplicabilidade, pertinência e características distintivas de cada modelo. Esses modelos, por sua vez, refletem uma busca constante por eficácia, excelência e inovação nos respectivos domínios de atuação. Ao explorar essas estruturas, torna-se viável compreender as melhores práticas, metodologias e estratégias que têm impulsionado o progresso contínuo das organizações.

3.3 Objetivos do modelo de maturidade

Em geral, os modelos de maturidade são ferramentas valiosas que auxiliam as organizações a atingirem seus objetivos e melhorarem continuamente sua eficiência e eficácia. Gibson e Nolan (1974, p. 87, tradução nossa) afirmam que, por meio dos MM, “a administração pode ser capaz de antecipar os problemas e resolvê-los antes que eles comecem”. Segundo Leal (2008, p. 33):

Modelos de maturidade são mecanismos capazes de quantificar numericamente a maturidade. Estes modelos auxiliam a elaboração de processos, indicam melhores práticas e fazem com que as organizações se desenvolvam de forma constante.

Toda a empresa pode comparar e avaliar instituições, identificando aquelas mais maduras para utilizá-las como referências internas e exemplos de orientações, ao mesmo tempo em que direciona seu foco em organizações menos maduras, apoiando sistematicamente seu aprimoramento (Rosemann; De Bruin, 2005, p. 7, tradução nossa). Um Modelo de Maturidade de processo é um diferencial que pode ser empregado para avaliar a capacidade da organização realizar seus processos de acordo com seus objetivos, identificar pontos de melhoria de produtividade, qualidade e redução de custos, e também auxilia no planejamento e monitoramento dos processos (Assis *et al.*, 2012).

Assim, um modelo de maturidade deve encontrar o equilíbrio adequado entre complexidade e simplificação. Um modelo mais simples normalmente é mais fácil de

compreender e é mais aceito pelos usuários, enquanto um modelo complexo tende a retratar a realidade de forma mais precisa. No contexto dos modelos de maturidade, os modelos simples fornecem uma única perspectiva de maturidade, ao passo que os modelos mais complexos oferecem *insights* em vários estágios de maturidade (Rosemann; De Bruin, 2005, p. 4-5, tradução nossa).

O objetivo primordial dos modelos de maturidade é definir os estágios de maturação. Um modelo de maturidade atende a um propósito descritivo quando pode ser aplicado para avaliar o estado atual de uma organização. Ele desempenha um propósito prescritivo ao identificar níveis futuros desejáveis de maturidade e fornecer orientações sobre como implementar medidas de melhoria correspondentes. Além disso, um modelo de maturidade cumpre um propósito comparativo ao permitir *benchmarking* interno e externo (Röglinger; Pöppelbuß; Becker, 2012, p. 330, tradução nossa).

Normalmente, as empresas buscam avaliar a maturidade das suas capacidades para aumentar eficiência, reduzir despesas, elevar a satisfação dos clientes, aumentar a receita e obter vantagem competitiva. Humphrey (1988, p. 74, tradução nossa) observou que “ao posicionar sua organização em uma estrutura de maturidade, os profissionais de *software* e a gerência podem identificar áreas em que as ações de melhoria provavelmente terão maior impacto”.

Dessa forma, a maturação, ou o processo de amadurecimento, é compreendido como um avanço organizacional. Entre os objetivos de um modelo de maturidade, podem ser incluídos:

- Fornecer uma estrutura para avaliar a eficiência e eficácia de uma organização em uma área específica.
- Identificar pontos fortes e fracos da organização em diversos aspectos.
- Oferecer diretrizes para aprimorar os processos e práticas organizacionais.
- Alcançar alto desempenho e competitividade no mercado.
- Promover a melhoria contínua e o desenvolvimento da organização.
- Proporcionar uma base de comparação com outras organizações no mesmo setor.
- Auxiliar na identificação das tecnologias e ferramentas mais adequadas para dar suporte aos processos da organização.
- Estimular a colaboração e a comunicação entre equipes e departamentos da organização.

Em resumo, os modelos de maturidade desempenham um papel multifacetado e abrangente nas organizações, visando diversos objetivos essenciais. Eles fornecem uma estrutura para avaliar e aprimorar a eficiência, eficácia e capacidade de entrega de uma organização em uma área específica, identificando pontos fortes e áreas de melhoria. Além disso, essas ferramentas promovem o alto desempenho e a competitividade no mercado, impulsionando a busca pela excelência contínua e o desenvolvimento organizacional. Também desempenham um papel fundamental na seleção das tecnologias e ferramentas adequadas para sustentar os processos organizacionais e na promoção da colaboração e comunicação entre equipes e departamentos. Em suma, os modelos de maturidade constituem recursos valiosos para as organizações que buscam aprimorar sua capacidade e competitividade em um ambiente empresarial em constante evolução.

3.4 Fundamentos de modelo de maturidade

O modelo de maturidade pode ser compreendido como uma ferramenta de avaliação e acompanhamento de uma ou mais competências de uma organização. Essa ferramenta é composta por níveis de maturidade que permitem posicionar a empresa dentro de um contexto específico e vislumbrar maneiras de buscar o aprimoramento nessa competência (dimensão) avaliada. Os fundamentos de um modelo de maturidade incluem as dimensões e os níveis de maturidade, também conhecido como etapas ou estágios de maturidade. Esses dois fundamentos estão interligados.

3.5.1 Dimensões

A dimensão é um campo específico de interesse que deve ser avaliado no modelo de maturidade a ser desenvolvido. As dimensões proporcionam uma abordagem estruturada e um caminho para a melhoria contínua da organização. Essas dimensões irão variar de acordo com o interesse específico do modelo de maturidade construído. Por sua vez, os níveis de maturidade mensuram o grau de maturidade da organização no contexto avaliado, refletindo o desempenho atual da empresa e a sua relação com as melhores práticas.

Conforme destacado por Batenburg, Neppelenbroek e Shahim (2014, p. 47, tradução nossa), um “modelo de maturidade é construído definindo seus dois pilares

básicos, as dimensões de maturidade e os níveis de maturidade”. Soares *et al.* (2019, p. 49), reforçam que “os modelos de maturidade geralmente podem ser caracterizados por seus níveis, dimensões, respondentes e propósito”.

Para compreender um modelo de maturidade, é necessário reconhecer e entender suas dimensões, bem como os requisitos e características que descrevem cada nível de maturidade no modelo. Conforme destacado por Batenburg, Neppelenbroek e Shahim (2014, p. 46, tradução nossa), “dimensões são áreas para estruturar o campo de interesse, às vezes chamadas de áreas-chave. Uma dimensão pode ser especificada por atividades, características comuns e medidas para cada nível de maturidade”.

As dimensões de um modelo de maturidade variam de acordo com a área de aplicação. No entanto, algumas dimensões são comuns a diversos modelos de maturidade, como, por exemplo, processo, pessoas, tecnologia e cultura. Tomando os exemplos citados, a dimensão “processo” permite avaliar a maturidade da organização em relação a procedimentos, métodos ou segmentos específicos, verificando sua eficiência e eficácia. A dimensão “pessoas” avalia a maturidade dos indivíduos envolvidos, considerando suas habilidades e conhecimentos necessários. A dimensão “tecnologia” avalia a utilização de tecnologias apropriadas e eficazes para dar suporte às demandas inerentes a uma determinada capacidade. Por fim, a dimensão “cultura” analisa se a cultura organizacional é propícia ao sucesso e a melhoria contínua. Dessa forma, essas dimensões, quando consideradas em conjunto, contribuem para a formação do posicionamento e da imagem da organização em uma área ou capacidade específica.

A quantidade de dimensões em um modelo de maturidade pode variar de acordo com os objetivos e necessidades da organização. O número de dimensões será determinado pelos objetivos específicos que o modelo busca alcançar e pelos aspectos da organização que precisam ser avaliados.

3.5.2 Níveis de maturidade

A identificação da maturidade em relação ao objeto de análise é realizada por meio da atribuição de níveis de maturidade. Os níveis de maturidade e sua relação com as estratégias competitivas desempenham um papel crucial no processo de planejamento estratégico, assim como na implementação das estratégias (Hepper, 2017, p. 13).

Os níveis de maturidade desempenham um papel fundamental na construção de um modelo de maturidade eficaz, uma vez que posicionam a organização em uma escala de avaliação da maturidade. Conforme salientado por Fogaça (2021, p. 45), “o nível de maturidade retrata o posicionamento da organização perante níveis estabelecidos, constituídos de um conjunto de pré-requisitos que garantam a melhoria no desempenho global da organização”.

A atribuição dos níveis de maturidade a um modelo é o processo de determinar o caminho de evolução que a organização deve percorrer para atingir a eficiência na gestão de uma determinada dimensão avaliada. Batenburg, Neppelenbroek e Shahim (2014, p. 48, tradução nossa) explicam que:

Existem duas abordagens para determinar os níveis de maturidade: uma abordagem de nível fixo, usando uma quantidade fixa de níveis de maturidade para cada dimensão representando um caminho de maturação; e, uma abordagem de área de foco, usando um número variável de níveis de maturidade para cada dimensão suportando diferenças na granularidade.

Os níveis de maturidade podem ser revistos durante uma reavaliação de um modelo proposto, flexionando-se para atender novas demandas ou melhorar a relação direta com uma determinada dimensão, a fim de aprimorar a qualidade de aplicação do modelo.

A quantidade de níveis em um modelo de maturidade varia de acordo com o modelo específico e as necessidades da organização. Alguns modelos de maturidade podem ter apenas três ou quatro níveis, enquanto outros podem ter vários níveis. Existem exemplos na literatura de modelos com apenas três níveis (comum) e alguns com até nove (raros, como os *Technology Readiness Levels* (TRLs)⁴) (Kirkwood; Alinaghian; Srai, 2011, p. 19, tradução nossa).

O número de níveis é determinado pelos objetivos específicos do modelo e pelos aspectos da organização a serem avaliados. Os níveis geralmente descrevem diferentes estágios de maturidade em relação a uma determinada dimensão ou área. SOFTEX (2021, p. 7) destaca que o nível de maturidade “caracteriza o estágio de maturidade de uma organização/unidade organizacional com relação a seus processos”. Por exemplo, em um modelo de maturidade para processos, os níveis podem descrever estágios como: inicial, definido, melhorado e otimizado, com o

⁴ Foi desenvolvido pela NASA em 1974 e formalizado em 1989. Inicialmente, incluía sete níveis, mas na década de 1990 a NASA adotou a escala de nove níveis que ganharia ampla aceitação.

propósito de ajudar as organizações a identificar sua posição em relação a cada nível e fornecer recomendações para alcançar um nível mais elevado de maturidade.

O estágio mais baixo representa um estado inicial, caracterizado, por exemplo, por uma organização com poucas capacidades na área em questão. Em contraste, o estágio mais alto representa a plena maturidade. Avançar no caminho de evolução entre esses dois extremos implica em uma progressão contínua em termos de capacidades organizacionais ou desempenho do processo (Becker; Knackstedt; Pöppelbuß, 2009, p. 213, tradução nossa).

Portanto, os níveis de maturidade em um modelo representam estágios progressivos de desenvolvimento da organização em uma determinada área e/ou capacidade. SOFTEX (2021, p. 16) ressalta que “à medida que a organização evolui nos níveis de maturidade, evolui o nível de capacidade com que deve executar os processos”. Os níveis de maturidade representam uma escalada de maturidade, desde a falta de interesse da organização até a excelência da organização sobre o assunto avaliado. Essa avaliação permite que as organizações identifiquem áreas de melhoria e possam buscar alto desempenho e competitividade.

A medição do nível de maturidade em gestão de projetos, por exemplo, proporciona à organização uma compreensão de suas forças e fraquezas nos processos e auxilia na estruturação de planos de ação para melhorar a gestão de seus projetos. Outro benefício é a possibilidade de comparação de seu nível de maturidade em relação às melhores práticas de organizações similares (Costa; Ramos, 2013, p. 242).

Em resumo, um modelo de maturidade é caracterizado por níveis de maturidade, cada um deles definido por requisitos que a organização deve cumprir. Geralmente, esses níveis seguem uma sequência ordenada, permitindo que a organização progrida de um nível para outro à medida que atende a requisitos pré-definidos. Normalmente, a organização flutua de um nível para o outro. Mas, se a organização mantiver o foco na melhoria contínua, seu objetivo será atingir e manter-se no mais alto nível de maturidade do modelo.

A evolução nos níveis de maturidade é um processo natural, mas requer o comprometimento da alta administração na área em questão. Como confirmado por Hepper (2017, p. 29), “assim que uma organização atinge plenamente o nível atual, está apta a evoluir para o próximo nível”.

3.5.3 Natureza dos modelos de maturidade

Quanto à natureza de um modelo de maturidade, esta pode ser descritiva, prescritiva e/ou comparativa. Um modelo descritivo deve propor critérios de mensuração para cada nível de maturidade, enquanto um modelo prescritivo abrange os elementos do modelo descritivo e, também oferece medidas de melhoria, sugerindo ações de melhores práticas. Conforme explicado por Röglinger, Pöppelbuß e Becker (2012, p. 332, tradução nossa):

Modelos de maturidade destinados a um propósito descritivo de uso precisam fornecer critérios de avaliação intersubjetivamente verificáveis para cada estágio e nível de granularidade. Modelos de maturidade seguindo um propósito prescritivo precisam incluir medidas de melhoria no sentido de boas ou melhores práticas para cada estágio e – se disponível – nível de granularidade.

A natureza descritiva de um modelo de maturidade refere-se à sua capacidade de descrever o desempenho atual de uma organização em uma determinada área. Isso é alcançado por meio da avaliação dos processos e práticas da organização em relação aos padrões estabelecidos pelo modelo, permitindo à organização identificar seus pontos fortes e fracos e obter uma compreensão clara de sua situação atual. Por outro lado, a natureza prescritiva de um modelo de maturidade refere-se à sua capacidade de fornecer diretrizes e recomendações para a melhoria dos processos e práticas da organização. O modelo pode identificar áreas específicas que precisam de aprimoramento e oferecer soluções práticas para melhorar o desempenho da organização. A natureza prescritiva do modelo auxilia a organização a atingir seus objetivos e a melhorar continuamente.

Röglinger, Pöppelbuß e Becker (2012, p. 333, tradução nossa) reforçam que “os modelos de maturidade prescritivos devem incluir um cálculo de decisão”. Batenburg, Neppelenbroek e Shahim (2014, p. 46, tradução nossa) complementam que “um modelo de maturidade prescritivo fornece informações mais detalhadas e, portanto, é desejável usá-lo como entrada para o modelo de maturidade a ser desenvolvido”.

Portanto, os modelos de maturidade que se destinam a fins prescritivos devem pelo menos fornecer um catálogo de medidas genéricas de melhoria e diretrizes básicas de seleção que pode ser adaptadas às necessidades individuais da organização e a configurações específicas (Röglinger; Pöppelbuß; Becker, 2012,

p. 341, tradução nossa). No que diz respeito ao propósito prescritivo de uso, as organizações devem ser especialmente cautelosas.

Além da natureza do modelo de maturidade poder ser descritiva e/ou prescritiva, De Bruin *et al.* (2005, p. 2, tradução nossa) acrescentaram a possibilidade de um modelo de maturidade ser de natureza comparativa:

Um modelo comparativo permite a comparação entre indústrias ou regiões. Um modelo desse tipo seria capaz de comparar práticas semelhantes entre organizações para fazer benchmarking da maturidade em indústrias distintas. Um modelo comparativo reconheceria que níveis semelhantes de maturidade em diferentes indústrias podem não se traduzir em níveis semelhantes de valor empresarial.

Esse tipo de modelo é desenvolvido, principalmente, com o objetivo de identificar semelhanças e diferenças entre as entidades em estudo, muitas vezes para fins de *benchmarking*, aprendizado, avaliação relativa de desempenho ou para entender como diferentes práticas ou abordagens se comparam em contextos diversos.

Embora se possam considerar as naturezas dos modelos como distintas, na realidade, elas representam estágios evolutivos no ciclo de vida de um modelo. Inicialmente, um modelo adota uma abordagem descritiva, aprofundando a compreensão da situação atual no domínio em questão. À medida que a compreensão sólida da situação atual se desenvolve, o modelo progride em direção a uma abordagem prescritiva, tornando possível implementar melhorias substanciais e repetíveis. Posteriormente, um modelo pode evoluir para ter uma natureza comparativa, aplicando-se a uma variedade de organizações para adquirir dados suficientes que permitam uma comparação válida (De Bruin *et al.*, 2005, p. 2, tradução nossa).

Nota-se que um modelo de maturidade ideal deve ter elementos descritivos, prescritivos e, se possível, comparativos. Isso significa que, por um lado, deve descrever as características e capacidades necessárias para alcançar um determinado nível de maturidade e, por outro, deve prescrever ações a serem tomadas para melhorar a maturidade, proporcionando uma compreensão abrangente da situação atual da organização e oferecendo diretrizes para a melhoria. Um modelo mais completo abrangeria a natureza comparativa, permitindo

comparações e avaliações entre diferentes entidades, como organizações, sistemas, processos ou qualquer outro objeto de análise.

3.5.4 Eficácia e aplicabilidade de um modelo de maturidade

A eficácia dos modelos de maturidade é sustentada por um conjunto fundamental de características. Essas características essenciais são os pilares que permitem que esses modelos cumpram seu propósito e auxiliem as organizações na busca por aprimoramento e excelência em áreas específicas. Dentre essas características cruciais, destacam-se:

- Clareza na definição de padrões: que possibilita a avaliação e melhoria do desempenho organizacional por meio de padrões bem definidos.
- A escalabilidade: que permite o progresso contínuo, ajustando-se às necessidades e ao crescimento da organização.
- Objetividade ancorada em critérios transparentes: que assegura a imparcialidade na avaliação, com critérios transparentes e claros.
- Adaptabilidade às necessidades específicas: que atende às demandas particulares de cada organização.
- Flexibilidade para lidar com mudanças: que capacita a organização a enfrentar e se adaptar às mudanças no ambiente.
- Capacidade de fornecer orientações práticas: que oferece diretrizes e recomendações concretas para a melhoria contínua.

Essas são apenas algumas das características de um modelo de maturidade eficaz. Cada modelo pode apresentar suas próprias características específicas, adaptadas às necessidades da organização e à área em questão.

No que diz respeito à aplicabilidade, é notável a ampla gama de possibilidades de atuação, mas os modelos mais comuns incluem:

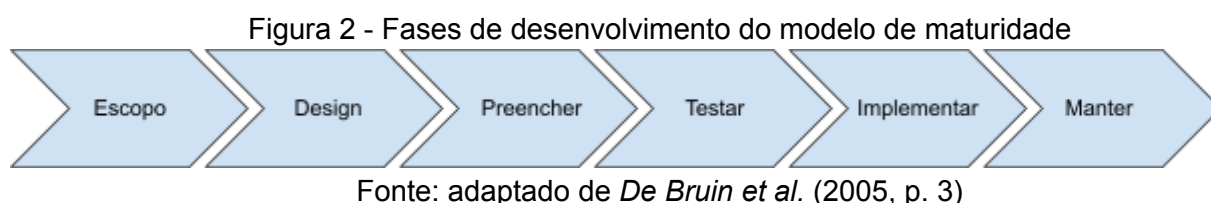
- Modelos de maturidade de processos: que avaliam e aprimoram a eficiência e eficácia dos processos empresariais.
- Modelos de maturidade de tecnologia da informação: que focam no desempenho e eficiência dos sistemas de tecnologia da informação de uma organização.
- Modelos de maturidade de segurança da informação: que se concentram na avaliação e melhoria da segurança da informação em uma organização.

- Modelos de maturidade de gerenciamento de projetos: que visam aprimorar a eficiência e eficácia dos processos de gerenciamento de projetos em uma organização.

Estas são apenas algumas das possibilidades de uso dos modelos de maturidade disponíveis. No entanto, é importante ressaltar que outros modelos podem ser personalizados para atender às necessidades específicas de uma organização.

3.5 Construção de um modelo de maturidade

Com base na leitura dos diversos modelos de maturidade existentes na literatura, percebe-se que a elaboração de um modelo de maturidade é um processo complexo que envolve várias etapas. De Bruin *et al.* (2005, p. 3, tradução nossa) relatam que a estrutura de desenvolvimento de um modelo de maturidade deve seguir a estrutura genérica da Figura 2.



As principais etapas para a elaboração de um modelo de maturidade (Software Engineering Institute, 2002; De Bruin *et al.*, 2005; Van Steenbergem *et al.*, 2010) são:

1. **Escopo:** A primeira etapa é definir claramente o propósito do modelo e o escopo da avaliação. Isso envolve identificar as áreas específicas que serão avaliadas e os objetivos que se desejam alcançar com a construção do modelo. De Bruin *et al.* (2005, p. 3, tradução nossa) ressaltam que “a combinação de decisões de escopo influenciará todas as fases restantes no framework genérico proposto para o desenvolvimento do modelo” e essas escolhas distinguem o modelo a ser construído dos outros existentes e determinam suas especificidades e aplicabilidade.
2. **Design:** Esta etapa, também chamada de projeto, envolve a arquitetura do modelo e está relacionada à revisão bibliográfica das áreas definidas no escopo, o

público a ser atingido, a definição dos níveis de maturidade, bem como a identificação dos indicadores e critérios de avaliação. Todos os MM devem definir os níveis de maturidade que irão constituir seu arquétipo, bem como seus componentes estruturais. Além de seus elementos estruturais essenciais, alguns modelos de maturidade podem fornecer definições adicionais sobre construtos do cenário em que são aplicados.

- **Revisão Bibliográfica:** É importante realizar uma revisão da literatura existente na área de interesse para entender as melhores práticas, os padrões e os conceitos relevantes a serem considerados. Isso ajudará a embasar o modelo em conhecimentos sólidos.
- **Definir Níveis de Maturidade:** O modelo deve definir os níveis de maturidade que serão usados para avaliar o desempenho da organização. Cada nível representa um grau crescente de maturidade e deve ser claramente definido em termos de características e práticas.
- **Identificar Indicadores e Critérios:** Para cada nível de maturidade, é necessário identificar os indicadores e critérios que serão usados para avaliar o desempenho da organização. Esses indicadores devem ser objetivos, mensuráveis e relevantes para a área em questão.

Quanto ao projeto do modelo a ser construído, De Bruin *et al.* (2005, p.4, tradução nossa) destacam que “o design do modelo precisa, portanto, encontrar um equilíbrio adequado entre uma realidade muitas vezes complexa e a simplicidade do modelo”.

3. **Preencher:** Após a consolidação do escopo e do design do modelo, é o momento de determinar o conteúdo do modelo. Nesta etapa, é desenvolvido o Método de Avaliação que deve ser com base nos indicadores e critérios identificados. O método de avaliação pode ser feito por meio de questionários, entrevistas ou conjunto de diretrizes que permitam avaliar o desempenho da organização em relação aos níveis de maturidade definidos. A confirmação dos componentes selecionados a partir de múltiplas fontes de evidência aprimora a abrangência dos resultados do modelo de maturidade final. A escolha do método de avaliação deve sempre levar em conta o objetivo e características do modelo a ser proposto. De Bruin *et al.* (2005, p. 6) ratifica quando dizem que:

É improvável que uma revisão da literatura (por mais abrangente que seja) identifique informações suficientes para preencher essa camada de detalhes. Recomenda-se que sejam considerados métodos de pesquisa exploratória, como a técnica *Delphi*, a técnica do Grupo Nominal, entrevistas de estudo de caso e grupos focais. A seleção da técnica ou técnicas mais apropriadas dependerá das partes interessadas envolvidas no desenvolvimento do modelo e dos recursos disponíveis para a equipe de desenvolvimento.

O importante ao preencher o modelo é selecionar a combinação de métodos mais apropriados para o desenvolvimento do modelo no contexto das decisões de escopo anteriores e dos resultados desejados. Embora os procedimentos empregados para preencher o modelo possam variar conforme o contexto, a incorporação de abordagens complementares concorre para a concepção de um modelo robustamente estruturado e apto a ser submetido a testes subsequentes.

Quanto à elaboração das questões para compor o método de avaliação, são as dimensões do domínio que oferecem uma sólida orientação. Outra alternativa é utilizar questões previamente formuladas e empregadas em outras capacidades. A incorporação de escalas *Likert*⁵ (ou equivalentes) pode aprimorar a confiabilidade e consistência das respostas, possibilitando uma fácil correlação dos resultados com os estágios de maturidade. É importante equilibrar a quantidade de perguntas e garantir que elas sejam validadas, assegurando que meçam efetivamente o que se pretende avaliar (De Bruin *et al.*, 2005, p. 7, tradução nossa).

4. Testar: Antes de implementar o modelo, é importante que ele seja validado por meio de testes pilotos. Isso envolve a aplicação do modelo em um conjunto limitado de organizações para verificar sua eficácia e fazer ajustes conforme necessário. Ao selecionar um instrumento para conduzir uma avaliação, é necessário considerar a generalização do modelo, juntamente com os recursos disponíveis para a realização das avaliações. A validação de um modelo é representada pela validação da aparência e do conteúdo. Nesta perspectiva, De Bruin *et al.* (2005, p. 8, tradução nossa) explicam que:

⁵ É uma escala de medição desenvolvida em 1932 por Rensis Likert, sendo comumente usada em questionários e muito popular em pesquisas de opinião. Permitindo que as pessoas expressem o quanto concordam com uma afirmação.

A seleção de métodos complementares para o preenchimento do modelo ajuda a alcançar a validade da aparência, enquanto a validade de conteúdo é avaliada pela representação abrangente do domínio, considerando a revisão da literatura e a amplitude do domínio abordado.

Além da avaliação da construção e integridade do modelo, torna-se relevante assegurar que os instrumentos e métodos de avaliação estejam verificados se estão realmente aptos a mensurar aquilo que se deseja investigar, bem como a sua confiabilidade, com vistas a garantir que os resultados obtidos sejam precisos e consistentes. Batenburg, Neppelenbroek e Shahim (2014, p. 50, tradução nossa) ratificam que “após o preenchimento do questionário, o modelo de maturidade deve ser apresentado aos entrevistados para que os mesmos comentem e identifiquem falhas ou incertezas no modelo de maturidade proposto”.

Assim, a validação do modelo de maturidade é resultado da análise da proposta do modelo e da sua aplicação por parte dos entrevistados selecionados, os quais são detentores de *expertise* nas áreas correspondentes aos objetivos primordiais do modelo proposto.

5. Implementar: após a criação e teste do modelo de maturidade, é crucial disponibilizá-lo para uso e verificar sua aplicabilidade em um contexto mais amplo. Isso envolve duas etapas essenciais: promover uma aceitação mais ampla e aprimorar a padronização do modelo.

6. Manter: O objetivo final de um modelo de maturidade é promover a melhoria contínua. Portanto, é importante incentivar e apoiar as organizações no processo de aprimoramento do modelo. Essas são as principais questões envolvidas na elaboração de um modelo de maturidade. De Bruin *et al.* (2005, p. 9, tradução nossa) enfatizam que “a relevância contínua de um modelo só será garantida através da manutenção ao longo do tempo”. É um processo que requer pesquisa, planejamento e desenvolvimento cuidadosos, avaliações e implementações, e um compromisso com a melhoria contínua.

Outra forma de aperfeiçoar o modelo é aplicar diferentes formas de coleta de informações. Podendo conduzir estudos de caso ou grupos focais, incentivando sempre mais a interação crítica dos participantes, isso pode levar a novas perspectivas e crenças em relação ao modelo de maturidade e ao questionário de

avaliação proposto. Além disso, o modelo de maturidade pode ser usado como uma ferramenta de autoavaliação.

A construção de um modelo de maturidade é um processo meticuloso que envolve a definição de etapas específicas, desde a delimitação do escopo até a implementação e manutenção contínua. Cada fase contribui para a criação de um instrumento sólido, capaz de diagnosticar, planejar e aperfeiçoar as práticas organizacionais avaliadas. Na seção seguinte, abordam-se os aspectos metodológicos adotados para a construção desta tese, incluindo a caracterização da pesquisa, a delimitação do campo e dos sujeitos, o universo e a amostra, a seleção dos instrumentos de coleta e análise, e as etapas para o desenvolvimento e validação do modelo de maturidade, além das estratégias empregadas para assegurar a validade e a confiabilidade dos resultados obtidos.

4 PERCURSO METODOLÓGICO

O percurso metodológico consiste na trajetória da investigação, abarcando os métodos, procedimentos e diretrizes adotados com o propósito de alcançar um objetivo previamente estabelecido. Nesse contexto, a presente seção delineia a rota que o pesquisador empreendeu neste estudo, em concordância com os objetivos previamente estipulados. Com o intuito de aprofundar a compreensão, são a seguir apresentados a caracterização do estudo e a proposição dos instrumentos e procedimentos para a coleta e análise dos dados. O percurso metodológico assume papel fundamental na construção de um estudo sólido e na obtenção de resultados confiáveis, possibilitando ao pesquisador documentar e justificar as etapas seguidas na investigação do problema de pesquisa.

4.1 Caracterização da pesquisa

Para realizar uma caracterização apropriada da pesquisa, é essencial compreender o significado do termo "pesquisa" em seu contexto científico. De forma resumida, de acordo com Silva e Menezes (2001, p. 19), a pesquisa é definida como o ato de “procurar respostas para indagações propostas”. Adicionalmente, Minayo, Deslandes e Gomes (2016, p. 16) contribuem para essa compreensão, destacando a pesquisa como:

A atividade básica da ciência na sua indagação e construção da realidade. É a pesquisa que alimenta a atividade de ensino e a atualiza frente à realidade do mundo. Portanto, embora seja uma prática teórica, a pesquisa vincula pensamento e ação. Ou seja, nada pode ser intelectualmente um problema se não tiver sido, em primeiro lugar, um problema da vida prática. As questões da investigação estão, portanto, relacionadas a interesses e circunstâncias socialmente condicionadas. São frutos de determinada inserção na vida real, nele encontrando suas razões e seus objetivos.

Nesse sentido, uma pesquisa é iniciada quando um questionamento é formulado, delineando um problema a ser investigado e estabelecendo o propósito do estudo. O objetivo principal desta pesquisa é desenvolver um modelo de maturidade para o tratamento de dados e informações pessoais nas Universidades Federais do Brasil, à luz da Lei Geral de Proteção de Dados e de outros marcos

legais e normativos técnicos relevantes. Metodologicamente, trata-se de uma pesquisa científica inserida nas ciências sociais aplicadas, de natureza exploratória-descritiva com estudo de casos múltiplos e abordagem quali-quantitativa. Além disso, a pesquisa assume um caráter propositivo, ao desenvolver uma nova ferramenta de gestão - o modelo de maturidade para tratamento de dados pessoais - a ser validada através do método *Delphi* e conforme os princípios da LGPD e outros marcos legais correlatos.

Enquadra-se como um estudo de casos múltiplos, uma vez que, após a construção e validação do modelo, o modelo foi aplicado em 66 universidades, oferecendo diferentes cenários de análise. Essa abordagem permitiu uma compreensão abrangente da eficácia do modelo proposto, bem como a avaliação comparativa dos níveis de maturidade nas competências das instituições estudadas. Conforme Gil (2008, p. 56-57) salienta, o “estudo de caso é caracterizado pelo estudo profundo e exaustivo de um ou de poucos objetos, de maneira a permitir o seu conhecimento amplo e detalhado [...]”. Além disso, Severino (2007, p. 121) descreve que o estudo de caso “se concentra no estudo de um caso particular, considerado representativo de um conjunto de casos análogos, por ele significativamente representativo”.

Considerando que, de forma surpreendente, 66 instituições preencheram o instrumento de medição deste modelo, o que representa aproximadamente 95,65% das universidades convidadas, um resultado que contraria as expectativas de Lakatos e Marconi (2003, p. 201), que afirmam que “em média, os questionários expedidos pelo pesquisador alcançam 25% de devolução”. Tendo em vista o tempo necessário para analisar detalhadamente os resultados de cada instituição, tornou-se indispensável limitar o escopo desta etapa da pesquisa, a fim de garantir sua conclusão dentro do prazo estipulado.

Apesar de análises abrangentes terem sido realizadas com todas as instituições participantes, a análise institucional aprofundada foi focada em quatro delas: UFC, UFPB, UFBA e UFRGS. A seleção baseou-se em dois critérios principais: a ordem de envio das respostas e os níveis de maturidade global distintos identificados no MMTDP. A UFC foi escolhida por ser a primeira a responder, apresentando nível de maturidade emergente, enquanto a UFPB destacou-se como a primeira entre as instituições classificadas com nível intermediário. A UFBA e a UFRGS foram selecionadas por serem, respectivamente, as primeiras a atingir os

níveis de maturidade avançado e exemplar. Como nenhuma instituição obteve classificação no nível de maturidade global inicial, esse perfil não foi incluído nas análises aprofundadas. Essa abordagem possibilitou a representação de diferentes cenários, ampliando a compreensão dos resultados e assegurando diversidade de perspectivas.

Esta pesquisa adota uma abordagem exploratória-descritiva, com o objetivo de investigar e descrever como as Universidades Federais do Brasil estão se preparando para atender às obrigações legais relacionadas ao tratamento de dados e informações pessoais. Inicialmente, foram discutidos e analisados elementos que contribuíram para a formulação de um modelo de maturidade, proposto como ferramenta de gestão para avaliar e monitorar o cumprimento dessas obrigações. O modelo é detalhado, com suas dimensões de análise e níveis de maturidade claramente definidos.

No que tange à natureza exploratória da pesquisa, parte-se da premissa de que uma investigação científica, por meio de revisão bibliográfica, visa familiarizar-se com um tema, fenômeno ou problema específico. Esse tipo de pesquisa permite compreender melhor a complexidade do problema e identificar possíveis indicadores-chave para avaliar a conformidade legal. Como observado por Andrade (2010, p. 112), “a pesquisa exploratória, na maioria dos casos, constitui um trabalho preliminar ou preparatório para outro tipo de pesquisa”.

Por outro lado, a pesquisa descritiva tem como objetivo analisar e descrever a situação atual das Universidades Federais em relação à aplicação da Lei Geral de Proteção de Dados e demais legislações brasileiras relacionadas sobre o tratamento de dados e informações pessoais. Gil (2008, p. 28) destaca que a pesquisa descritiva:

Têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados.

Por fim, a natureza desta pesquisa é classificada como exploratória e descritiva, pois combina elementos de exploração e descrição de um fenômeno ou tema específico. Lakatos e Marconi (2003, p. 188) definem que estudos exploratório-descritivos como:

Estudos exploratórios que têm por objetivo descrever completamente determinado fenômeno, como, por exemplo, o estudo de um caso para o qual são realizadas análises empíricas e teóricas. Podem ser encontradas tanto descrições quantitativas e/ou qualitativas quanto acumulação de informações detalhadas como as obtidas por intermédio da observação participante. Dá-se precedência ao caráter representativo sistemático e, em consequência, os procedimentos de amostragem são flexíveis;

Já com relação à abordagem metodológica, esta pesquisa adota uma perspectiva quali-quantitativa, integrando abordagens qualitativas e quantitativas. A vertente qualitativa concentra-se em fenômenos específicos das instituições investigadas, levando em consideração o contexto das obrigações legais e seu cumprimento nas universidades. Essa abordagem abrange aspectos subjetivos, interpretações e análise de dados, principalmente, não numéricos. Michel (2009, p. 36-37) afirma que:

A pesquisa qualitativa considera que há uma relação dinâmica, particular, contextual e temporal entre o pesquisador e o objeto de estudo. Por isso, carece de uma interpretação dos fenômenos à luz do contexto, do tempo, dos fatos. O ambiente da vida real é a fonte direta para a obtenção dos dados, e a capacidade do pesquisador de interpretar essa realidade, com isenção e lógica, baseando-se em teoria existente, é fundamental para dar significado às respostas.

Complementando essa visão, Gerhardt e Silveira (2009, p. 32) acrescentam que a pesquisa qualitativa lida “com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais”. Dessa forma, ela permite uma compreensão mais profunda dos fenômenos sociais e humanos, destacando-se pela capacidade de revelar aspectos complexos da realidade que os métodos quantitativos não abordam adequadamente.

Nesse contexto, destacam-se métodos como a análise comparativa, a análise de conteúdo e a análise de tendências, que podem ser aplicados em conjunto com o método *Delphi*. A análise de conteúdo permite explorar os significados subjacentes nas respostas dos participantes, identificando aspectos mais profundos das opiniões. A análise comparativa, por sua vez, ajuda a identificar semelhanças e diferenças nas respostas. Além disso, a análise de tendências possibilita a identificação de padrões ou mudanças nas respostas ao longo das rodadas do *Delphi*, ajudando a captar a evolução das opiniões ou comportamentos dos participantes. Esses métodos complementam o *Delphi*, que, por sua natureza

iterativa, favorece o refinamento contínuo das respostas e contribui para o consenso entre os especialistas.

Paralelamente, esta pesquisa incorpora elementos quantitativos, como estatísticas resultantes da análise dos dados coletados por meio de questionários e a utilização da Escala Likert. Conforme Pereira (2018, p. 67) observa, “muitas vezes os métodos qualitativos podem se transformar em quantitativos por meio do emprego de questões fechadas, por exemplo, pelo emprego da Escala Likert.”

A pesquisa quantitativa, por sua vez, concentra-se em fatos e exige que as variáveis sejam rigorosamente definidas, com mensuração pré-estabelecida pelo próprio método. Essa abordagem geralmente envolve uma análise mediada por critérios matemáticos e utiliza dados numéricos para investigar fenômenos, permitindo realizar análises estatísticas que visam identificar padrões e estabelecer relações entre variáveis. A coleta de dados é frequentemente realizada por meio de questionários estruturados, experimentos ou levantamentos, com a análise assistida por ferramentas estatísticas. Pereira (2018, p. 69) ressalta que:

Nos métodos quantitativos, faz-se a coleta de dados quantitativos ou numéricos por meio do uso de medições de grandezas e obtém-se por meio da metrologia, números com suas respectivas unidades. Estes métodos geram conjuntos ou massas de dados que podem ser analisados por meio de técnicas matemáticas como é o caso das porcentagens, estatísticas e probabilidades, métodos numéricos, métodos analíticos e geração de equações e/ou fórmulas matemáticas aplicáveis a algum processo.

Uma das principais vantagens da pesquisa quantitativa é sua objetividade, que proporciona resultados precisos e verificáveis. Essa abordagem é especialmente valiosa para testar hipóteses e validar teorias, utilizando amostras representativas e procedimentos bem estabelecidos. No entanto, a pesquisa quantitativa pode ser limitada na compreensão de aspectos subjetivos ou complexos da realidade, frequentemente exigindo a complementação com métodos qualitativos.

Dessa forma, os métodos qualitativos e quantitativos são considerados complementares, e sua combinação configura uma pesquisa quali-quantitativa, possibilitando uma compreensão mais abrangente dos fenômenos investigados.

4.2 Delimitação do campo e sujeitos da pesquisa

A definição do campo de pesquisa é essencial para delimitar o espaço geográfico e institucional onde o fenômeno de interesse ocorre. Neste estudo, o campo de pesquisa abrange as Universidades Federais do Brasil, que são classificadas pela Lei Geral de Proteção de Dados como agentes de tratamento de dados pessoais, especificamente como “controladores”, conforme estipulado no art. 5, inciso VI da LGPD: “Controlador: pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relacionadas ao tratamento de dados pessoais” (Brasil, 2018).

A escolha das universidades como foco da pesquisa baseia-se no papel fundamental dessas instituições na produção, disseminação e aplicação do conhecimento em diversas áreas. Elas atuam como centros catalisadores de inovação, contribuindo para o avanço científico, tecnológico, social e cultural. Como ressalta Teixeira (2005, p. 18):

Se não considerarmos a produção do conhecimento como uma das finalidades da universidade, estaremos na contramão do futuro. Há que se conectar universidade e conhecimento, pois a primeira deve ter papel de produzir um saber contextualizado e social.

Conforme o artigo 52 da Lei de Diretrizes e Bases da Educação, as universidades são definidas como “instituições pluridisciplinares de formação dos quadros profissionais de nível superior, de pesquisa, de extensão e de domínio e cultivo do saber humano” (Brasil, 1996). Atualmente, o Brasil conta com 69 Universidades Federais credenciadas junto ao Ministério da Educação, conforme consulta realizada em 10 de janeiro de 2023 no portal oficial do MEC: <https://emec.mec.gov.br/>. A seguir, apresenta-se o Quadro 6 com as universidades que integram o conjunto das instituições credenciadas.

Quadro 6 - As Universidades Federais credenciadas no MEC

Instituição	Sigla	Município	UF
Universidade da Integração Internacional da Lusofonia Afro-Brasileira	UNILAB	Redenção	CE
Universidade de Brasília	UNB	Brasília	DF
Universidade Federal da Bahia	UFBA	Salvador	BA
Universidade Federal da Fronteira Sul	UFFS	Chapecó	SC
Universidade Federal da Grande Dourados	UFGD	Dourados	MS
Universidade Federal da Integração Latino-Americana	UNILA	Foz do Iguaçu	PR
Universidade Federal da Paraíba	UFPB	João Pessoa	PB

Instituição	Sigla	Município	UF
Universidade Federal de Alagoas	UFAL	Maceió	AL
Universidade Federal de Alfenas	UNIFAL-MG	Alfenas	MG
Universidade Federal de Campina Grande	UFCG	Campina Grande	PB
Universidade Federal de Catalão	UFCAT	Catalão	GO
Universidade Federal de Ciências da Saúde de Porto Alegre	UFCSPA	Porto Alegre	RS
Universidade Federal de Goiás	UFG	Goiânia	GO
Universidade Federal de Itajubá	UNIFEI	Itajubá	MG
Universidade Federal de Jataí	UFJ	Jataí	GO
Universidade Federal de Juiz de Fora	UFJF	Juiz de Fora	MG
Universidade Federal de Lavras	UFLA	Lavras	MG
Universidade Federal de Mato Grosso	UFMT	Cuiabá	MT
Universidade Federal de Mato Grosso do Sul	UFMS	Campo Grande	MS
Universidade Federal de Minas Gerais	UFMG	Belo Horizonte	MG
Universidade Federal de Ouro Preto	UFOP	Ouro Preto	MG
Universidade Federal de Pelotas	UFPEL	Pelotas	RS
Universidade Federal de Pernambuco	UFPE	Recife	PE
Universidade Federal de Rondônia	UNIR	Porto Velho	RO
Universidade Federal de Rondonópolis	UFR	Rondonópolis	MT
Universidade Federal de Roraima	UFRR	Boa Vista	RR
Universidade Federal de Santa Catarina	UFSC	Florianópolis	SC
Universidade Federal de Santa Maria	UFSM	Santa Maria	RS
Universidade Federal de São Carlos	UFSCAR	São Carlos	SP
Universidade Federal de São João Del Rei	UFSJ	São João del Rei	MG
Universidade Federal de São Paulo	UNIFESP	São Paulo	SP
Universidade Federal de Sergipe	UFS	São Cristóvão	SE
Universidade Federal de Uberlândia	UFU	Uberlândia	MG
Universidade Federal de Viçosa	UFV	Viçosa	MG
Universidade Federal do ABC	UFABC	Santo André	SP
Universidade Federal do Acre	UFAC	Rio Branco	AC
Universidade Federal do Agreste de Pernambuco	UFAPE	Garanhuns	PE
Universidade Federal do Amapá	UNIFAP	Macapá	AP
Universidade Federal do Amazonas	UFAM	Manaus	AM
Universidade Federal do Cariri	UFCA	Juazeiro do Norte	CE
Universidade Federal do Ceará	UFC	Fortaleza	CE
Universidade Federal do Delta do Parnaíba	UFDPAR	Parnaíba	PI
Universidade Federal do Espírito Santo	UFES	Vitória	ES
Universidade Federal do Estado do Rio de Janeiro	UNIRIO	Rio de Janeiro	RJ

Instituição	Sigla	Município	UF
Universidade Federal do Maranhão	UFMA	São Luís	MA
Universidade Federal do Norte do Tocantins	UFNT	Araguaína	TO
Universidade Federal do Oeste da Bahia	UFOB	Barreiras	BA
Universidade Federal do Oeste do Pará	UFOPA	Santarém	PA
Universidade Federal do Pampa	UNIPAMPA	Bagé	RS
Universidade Federal do Pará	UFPA	Belém	PA
Universidade Federal do Paraná	UFPR	Curitiba	PR
Universidade Federal do Piauí	UFPI	Teresina	PI
Universidade Federal do Recôncavo da Bahia	UFRB	Cruz das Almas	BA
Universidade Federal do Rio De Janeiro	UFRJ	Rio de Janeiro	RJ
Universidade Federal do Rio Grande	FURG	Rio Grande	RS
Universidade Federal do Rio Grande do Norte	UFRN	Natal	RN
Universidade Federal do Rio Grande do Sul	UFRGS	Porto Alegre	RS
Universidade Federal do Sul da Bahia	UFSB	Itabuna	BA
Universidade Federal do Sul e Sudeste do Pará	UNIFESSPA	Marabá	PA
Universidade Federal do Tocantins	UFT	Palmas	TO
Universidade Federal do Triângulo Mineiro	UFTM	Uberaba	MG
Universidade Federal do Vale do São Francisco	UNIVASF	Petrolina	PE
Universidade Federal dos Vales do Jequitinhonha e Mucuri	UFVJM	Diamantina	MG
Universidade Federal Fluminense	UFF	Niterói	RJ
Universidade Federal Rural da Amazônia	UFRA	Belém	PA
Universidade Federal Rural de Pernambuco	UFRPE	Recife	PE
Universidade Federal Rural do Rio de Janeiro	UFRRJ	Seropédica	RJ
Universidade Federal Rural do Semi-Árido	UFERSA	Mossoró	RN
Universidade Tecnológica Federal do Paraná	UTFPR	Curitiba	PR

Fonte: MEC.

Essas informações permitem a identificação imediata de cada uma das instituições, sua sigla, suas localizações geográficas e respectivos estados. Esses dados constituem a base primordial para as etapas da coleta de dados realizada nesta pesquisa.

Nesse contexto, as universidades federais do Brasil exercem um papel crucial na gestão responsável de dados e informações pessoais, garantindo a conformidade com a Lei Geral de Proteção de Dados e demais normativas aplicáveis. A nomeação de um Encarregado de Proteção de Dados (EPD), também referido como Data Protection Officer (DPO), conforme previsto nos artigos da LGPD, é um requisito fundamental. Esse profissional atua diretamente na instituição, promovendo a

implementação de políticas e práticas adequadas para o tratamento dos dados e informações pessoais.

O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados (Brasil, 2018, art. 41).

Esse profissional é responsável por garantir o cumprimento das normas de proteção de dados pela instituição, atuando como intermediário entre a organização, os titulares dos dados e a autoridade reguladora. Suas funções incluem orientar sobre boas práticas, monitorar a conformidade com a legislação vigente, além de receber e processar reclamações e comunicações dos titulares. O Encarregado de Proteção de Dados também interage diretamente com a Autoridade Nacional de Proteção de Dados (ANPD), recebendo suas comunicações e orientando os funcionários sobre os procedimentos adequados no tratamento de dados pessoais. Para exercer essas funções de forma eficaz, o EPD deve atuar com independência e imparcialidade, assegurando a integridade dos processos de conformidade e a confiança de todos os envolvidos.

Portanto, considera-se fundamental que a instituição designe para a função um profissional com amplo conhecimento e expertise em tratamento e proteção de dados e informações pessoais, a fim de assegurar uma atuação eficaz no cumprimento das normas e na implementação de boas práticas. No contexto desta pesquisa, os encarregados pelo tratamento de dados das universidades federais do Brasil constituem os sujeitos centrais do estudo, sendo fundamentais para o desenvolvimento do modelo de maturidade, uma vez que atuam diretamente na aplicação do método *Delphi* como especialistas.

A participação desses profissionais foi fundamental para identificar as temáticas e os componentes estruturais que compõem o instrumento de medição do

modelo de maturidade proposto. Ademais, as universidades, enquanto organizações, tiveram um papel crucial tanto na validação da ferramenta quanto na avaliação da eficácia das capacidades previstas no referido modelo.

Com o objetivo inicial de verificar se as instituições já haviam designado seus encarregados de proteção de dados, foi elaborada uma solicitação de informação (**Apêndice B**) para cada universidade federal listada no Quadro 6, com a finalidade de obter os dados de contato desses profissionais. Essa solicitação foi fundamentada na Lei Geral de Proteção de Dados e na Lei de Acesso à Informação, sendo enviada por meio da plataforma Fala.BR (Plataforma Integrada de Ouvidoria e Acesso à Informação).

Entre os dias 4 e 5 de abril de 2023, as solicitações de informação foram enviadas às universidades federais do Brasil. Naquele momento, duas instituições – a Universidade Federal de Rondonópolis e a Universidade Federal do Norte do Tocantins – não estavam listadas no Fala.BR e, portanto, não receberam a solicitação. Das 67 universidades contatadas, todas responderam, resultando em um índice de resposta de 100%. No entanto, cinco delas ainda não haviam designado um encarregado para o tratamento de dados pessoais: a Universidade Federal da Grande Dourados, a Universidade Federal de Jataí, a Universidade Federal do Amazonas, a Universidade Federal de Viçosa e a Universidade Federal do ABC.

É importante destacar que, ao longo da pesquisa, essa realidade passou por algumas mudanças. Instituições que inicialmente não haviam designado um encarregado de proteção de dados passaram a fazê-lo, enquanto outras, que já haviam designado um profissional, enfrentaram a saída ou substituição desse encarregado. O acompanhamento constante dos responsáveis designados foi mantido ao longo do desenvolvimento do modelo de maturidade. O diálogo ativo com os participantes da pesquisa, promovido pela plataforma Fala.BR, facilitou a aplicação dos questionários, fundamentais para a construção e validação do instrumento de medição por meio do método *Delphi*.

4.3 Universo e amostra da pesquisa

Em contextos acadêmicos e científicos, é imperativo delimitar o universo e selecionar criteriosamente a amostra de pesquisa, uma vez que esses parâmetros influenciam diretamente na validade e aplicabilidade dos resultados obtidos. O

universo refere-se ao conjunto de todos os elementos ou unidades sujeitos à investigação em um determinado contexto, abarcando todas as possibilidades, frequentemente caracterizadas por sua vastidão e inacessibilidade.

Segundo Lakatos e Marconi (2003, p. 223), a delimitação do universo “consiste em explicitar que pessoas ou coisas, fenômenos etc. serão pesquisados, enumerando suas características comuns, como, por exemplo, sexo, faixa etária, organização a que pertencem, comunidade onde vivem etc”. Já a amostra corresponde a uma seleção representativa desses elementos, destinada a uma análise detalhada. Conforme Lakatos e Marconi (2003, p. 163):

Após a escolha do assunto, o pesquisador pode decidir ou pelo estudo de todo o universo da pesquisa ou apenas sobre uma amostra. Neste caso, será aquele conjunto de informações que lhe possibilitará a escolha da amostra, que deve ser representativa ou significativa. Nem sempre há possibilidade de pesquisar todos os indivíduos do grupo ou da comunidade que se deseja estudar, devido à escassez de recursos ou à premência do tempo. Nesse caso, utiliza-se o método da amostragem, que consiste em obter um juízo sobre o total (universo), mediante a compilação e exame de apenas uma parte, a amostra, selecionada por procedimentos científicos.

Neste estudo, o universo é composto pelas 69 (sessenta e nove) universidades federais brasileiras e seus respectivos encarregados de tratamento de dados. A amostra, por sua vez, deve ser uma seleção criteriosa desse universo, de forma a refletir representativamente a totalidade. Patton (2001, p. 244, tradução nossa) ressalta que:

Não existem regras para o tamanho da amostra na pesquisa qualitativa. O tamanho da amostra depende do que você deseja saber, do propósito da pesquisa, do que está em jogo, do que será útil, do que terá credibilidade e do que pode ser feito com o tempo e os recursos disponíveis.

Para um entendimento mais técnico do dimensionamento amostral, considerando "N" como o número total de elementos do universo ou população (representado pela variável "X"), tal que $X_N = X_1; X_2; X_3; \dots; X_N$, e "n" como o número de elementos da amostra (representado pela variável minúscula "x"), tal que $x_n = x_1; x_2; x_3; \dots; x_n$ onde $x_n < X_N$ e $n < N$, destacam-se as duas principais categorias no processo de amostragem: a amostragem não probabilística e a amostragem probabilística (Lakatos; Marconi, 2003, p. 223).

Neste estudo, a amostragem foi não probabilística e determinada pela técnica de amostragem intencional, também conhecida como amostragem por tipicidade. De acordo com Gil (2008, p. 94), a amostragem por tipicidade “constitui um tipo de amostragem não probabilística e consiste em selecionar um subgrupo da população que, com base nas informações disponíveis, possa ser considerado representativo de toda a população”.

É importante destacar que, em amostragens intencionais ou por tipicidade, a relevância não está estritamente na quantidade de participantes, mas na qualidade das informações obtidas. Nesse sentido, Fontanella, Ricas e Turato (2008, p. 20) enfatizam que “o que há de mais significativo nas amostras intencionais não se encontra na quantidade de seus sujeitos, mas na maneira como se concebe a sua representatividade e na qualidade das informações obtidas deles”. Isso reforça a importância de uma seleção criteriosa dos participantes, levando em consideração características que conferem autenticidade à amostra, tornando-a verdadeiramente representativa do fenômeno em estudo.

Portanto, a constituição da amostra neste estudo foi guiada pela premissa de que os encarregados designados pelas instituições possuem ampla competência e especialização no tratamento de dados e informações pessoais. Acredita-se que esses profissionais desempenham um papel central tanto na construção quanto na validação do instrumento de medição do modelo de maturidade proposto. A representatividade amostral está diretamente relacionada ao número de respondentes que preencheram os questionários aplicados.

Para garantir a efetividade desta pesquisa, foi fundamental considerar a dinâmica do método *Delphi* na constituição da amostra. Embora o número ideal de participantes possa variar, dentro deste contexto, recomenda-se a formação de um grupo mínimo de 10 especialistas. Grupos menores que esse podem comprometer a obtenção de um consenso robusto, enquanto grupos excessivamente grandes podem gerar dificuldades na gestão e análise dos dados. Essa abordagem equilibrada assegura a inclusão de diversas perspectivas, contribuindo para a eficácia do processo (Marques; Freitas, 2018, p. 396).

A amostragem intencional adotada neste estudo assegura a representatividade por meio da inclusão dos encarregados pelo tratamento de dados nas universidades federais, com base em critérios que priorizam a qualidade das informações fornecidas. No contexto do método *Delphi*, essa representatividade não

se baseia exclusivamente no número de participantes, mas, sobretudo, na competência dos selecionados, a qual é essencial para a construção e validação do instrumento de medição do modelo proposto. O método *Delphi* caracteriza-se pela utilização de grupos reduzidos, porém altamente qualificados, o que torna a amostragem intencional uma escolha adequada.

4.4 Instrumentos e percursos para coleta e análise dos dados

Os instrumentos utilizados em uma investigação científica são fundamentais para garantir a coleta, medição, registro e análise de dados, sempre em consonância com o objeto de estudo. Conforme afirmam Laville e Dionne (1999, p. 337), as técnicas de pesquisa são definidas como o "procedimento empregado para recolher dados de pesquisa ou para analisá-los". A escolha apropriada dos instrumentos de coleta e análise de dados exige uma avaliação criteriosa das características do tema de estudo, seus objetivos, o problema de pesquisa e a revisão bibliográfica existente (Michel, 2009, p. 64). O instrumento de coleta de dados, como questionários, formulários de observação ou listas de tópicos para entrevistas, deve ser projetado com o objetivo de registrar informações de maneira eficiente e precisa (Mattar; Oliveira; Motta, 2014, p. 163). Em particular, no caso dos questionários, Andrade (2010, p. 134) enfatiza que:

Para elaborar as perguntas de um questionário é indispensável levar em conta que o informante não poderá contar com explicações adicionais do pesquisador. Por este motivo, as perguntas devem ser muito claras e objetivas. A preferência deve recair sobre o emprego de perguntas fechadas, ou seja, as que pedem respostas curtas e previsíveis. Perguntas fechadas são aquelas que indicam três ou quatro opções de resposta ou se limitam à resposta afirmativa ou negativa, e já trazem espaços destinados à marcação da escolha.

Além das perguntas fechadas, existem os questionários mistos, que combinam questões fechadas e abertas, permitindo um equilíbrio entre a facilidade de análise e a profundidade das respostas. O desenvolvimento de instrumentos como questionários é uma etapa essencial para garantir a coleta eficiente de dados.

Neste estudo, foram empregadas de maneira complementar a pesquisa bibliográfica, a pesquisa documental e a aplicação de questionários. A pesquisa bibliográfica desempenhou um papel crucial ao fornecer a base teórica necessária

para a construção da tese, orientando a revisão dos conceitos e das abordagens existentes. A pesquisa documental, por sua vez, consistiu na análise de manuais, regulamentos, normas e legislações pertinentes, sendo essencial para o desenvolvimento do modelo de maturidade proposto, uma vez que ofereceu o embasamento necessário para a definição das dimensões e critérios de avaliação. Já os questionários, foram de suma importância ao longo de todo o processo de pesquisa, viabilizando a coleta e análise das informações relevantes. Vale ressaltar que o questionário utilizado como instrumento de medição do modelo de maturidade passou por um processo rigoroso de avaliação, validação e refinamento por meio do método *Delphi*, o que garantiu sua robustez e confiabilidade.

4.5 Método *Delphi*

O método *Delphi* é amplamente utilizado em pesquisas qualitativas, composto por uma série de rodadas de questionários e *feedback* de especialistas em um determinado campo de estudo. Desenvolvido em 1953 por Norman Dalkey, da RAND Corporation, e Olaf Helmer, do Instituto para o Futuro, o método *Delphi* foi inicialmente aplicado para obter um consenso confiável entre especialistas em defesa militar sobre a questão de um possível ataque com bomba atômica. A técnica envolvia revisões sucessivas das opiniões dos especialistas, resultando em um consenso convergente (Boberg; Morris-Khoo, 1992, p. 27, tradução nossa).

Essa metodologia é amplamente empregada para lidar com questões complexas e incertas, como previsões de cenários futuros ou processos decisórios. Dias (2007, p. 27) destaca que:

Delphi é uma técnica qualitativa, de previsão de tendências, que tem sido utilizada com êxito tanto por empresas públicas como por organizações privadas que têm despertado para a necessidade de ampliar seu horizonte de planejamento. Algumas destas empresas atuam em setores estratégicos e têm feito uso do método a fim de subsidiar tomada de decisões mais seguras.

4.5.1 Características do Método *Delphi*

A essência do método *Delphi* reside em sua abordagem intuitiva e interativa, na qual um grupo de especialistas participa de múltiplas rodadas para responder a questões específicas. Conforme explicado por Daychoum (2016, p. 404):

O princípio do método é intuitivo e interativo. Implica a constituição de um grupo de especialistas em determinada área de conhecimento, que respondem a uma série de questões. O método se apoia em reunir as opiniões desses peritos que trabalham individualmente e frequentemente nem estão presentes fisicamente no mesmo local. As iterações do método são denominadas “*rounds*” (rodadas).

O método *Delphi* apresenta três características fundamentais. Primeiramente, o **anonimato** entre os participantes é essencial para minimizar a influência mútua, uma vez que os especialistas não interagem diretamente entre si durante o processo. Em segundo lugar, a **interação controlada por *feedback*** ocorre em rodadas, onde, após cada etapa, um resumo das respostas anteriores é fornecido aos participantes, com o intuito de reduzir distorções e manter o foco nos objetivos do estudo. Por fim, a **utilização de respostas estatísticas** do grupo permite mitigar a pressão por conformidade, resultando em uma previsão que reflete predominantemente a opinião da maioria, embora perspectivas minoritárias também possam ser consideradas. Em resumo, o método *Delphi* caracteriza-se pelo anonimato, pela interação com *feedback* controlado e pelo uso de respostas estatísticas grupais, promovendo uma abordagem rigorosa e objetiva para a tomada de decisões ou previsões (Daychoum, 2016, p. 404).

A escolha do método *Delphi* para o desenvolvimento deste modelo foi motivada pela sua natureza interativa, envolvendo especialistas em tratamento de dados e informações pessoais. Tal característica o torna especialmente apropriado para lidar com questões complexas e para preencher lacunas de evidências empíricas. Nesse contexto, De Bruin *et al.* (2005, p. 6, tradução nossa) afirmam:

Embora o tempo decorrido e os recursos envolvidos no uso da técnica *Delphi* tenham sido significativos, esse método foi considerado o mais apropriado para o modelo de maturidade BPM por várias razões, incluindo: (1) proporcionou a oportunidade de acessar um amplo grupo de especialistas globais do domínio; (2) atendeu às restrições orçamentárias e de recursos existentes; e (3) permitiu a identificação de questões contemporâneas. A técnica *Delphi* envolve a identificação e seleção de um painel de especialistas dos quais se busca informações sobre um tópico específico por meio da conclusão iterativa de várias pesquisas. Os estudos *Delphi* são considerados benéficos quando: (1) lidam com questões complexas; (2) buscam combinar pontos de vista para melhorar a tomada de decisões; (3) contribuem para um estado de conhecimento incompleto; e (4) onde há falta de evidência empírica. O desenvolvimento de um modelo de maturidade em um domínio complexo envolve todos esses quatro pontos.

4.5.2 Vantagens e desvantagens

O método *Delphi* é amplamente utilizado em várias áreas, como energia, transporte, telecomunicações, biotecnologia, economia, marketing e novas tecnologias, especialmente por organizações que necessitam ampliar seu horizonte de planejamento (Dias, 2007, p. 27). Essa técnica qualitativa permite capturar uma ampla gama de variáveis inter-relacionadas, promovendo o pensamento independente e a construção de soluções coletivas. As principais vantagens do método *Delphi* incluem:

- Anonimato: Previne conflitos de opiniões e evita o domínio de personalidades, incentivando respostas mais sinceras e imparciais.
- Diversidade geográfica: Facilita a participação de especialistas de diferentes regiões, enriquecendo a análise com múltiplas perspectivas.
- Flexibilidade e custo-efetivo: Permite a participação remota, reduzindo custos de logística em comparação a reuniões presenciais.
- Revisão de respostas: Oferece a possibilidade de especialistas revisarem suas opiniões com base no feedback coletivo, promovendo um consenso mais preciso.
- Controle sistemático: Garante objetividade e refinamento contínuo dos resultados ao longo das rodadas, aprimorando a qualidade final das respostas.

O método *Delphi* apresenta algumas desvantagens que merecem consideração. A natureza iterativa do processo, que envolve múltiplas rodadas de perguntas e revisões, pode torná-lo demorado, atrasando a obtenção de resultados

e potencialmente desengajando os participantes. Embora a interação remota e anônima favoreça a sinceridade das respostas, ela pode limitar a exploração abrangente do conhecimento dos especialistas. Adicionalmente, a interferência dos pesquisadores (facilitadores), mesmo que mínima, pode introduzir viés nas respostas, enquanto a diversidade entre os participantes, embora enriquecedora, pode dificultar a comunicação e a análise eficazes. A complexidade e a quantidade de dados gerados aumentam a demanda por processamento, e a qualidade dos questionários é fundamental, uma vez que perguntas mal elaboradas podem comprometer a validade dos resultados.

Para minimizar as desvantagens do método *Delphi*, diversas estratégias podem ser adotadas. Primeiramente, um planejamento cuidadoso das rodadas de perguntas pode reduzir o tempo necessário para o processo; definir prazos claros e concisos para as respostas acelera a obtenção de resultados. Para garantir uma exploração abrangente do conhecimento dos especialistas, recomenda-se utilizar ferramentas interativas que facilitem a comunicação, mesmo em um ambiente remoto. Além disso, a elaboração de questionários de alta qualidade, com perguntas claras e objetivas, pode mitigar a introdução de viés e aumentar a validade dos resultados. Para maximizar a eficácia, é essencial selecionar cuidadosamente os especialistas, priorizando aqueles com experiência relevante e reconhecimento na área analisada. Por fim, é importante monitorar o engajamento dos participantes e, quando necessário, implementar estratégias de incentivo que mantenham o interesse e a participação ativa ao longo de todo o processo.

4.5.3 Etapas de aplicação do método

A aplicação do método *Delphi* segue um processo estruturado e interativo. A seguir, o Quadro 7 descreve de forma concisa as etapas principais da aplicação do método *Delphi*:

Quadro 7 - Etapas de aplicação do método *Delphi*

Etapas	Descrição
Escolha dos especialistas	Os especialistas são escolhidos com base em seu conhecimento sobre o tema ou assunto abordado.
Rodada Inicial	O facilitador envia as questões iniciais com as instruções, e os especialistas analisam e dão suas opiniões.
Feedback Controlado	O facilitador recebe as respostas, resume e consolida e envia o feedback para os especialistas.

Rodadas Subsequentes	O processo se repete até que um consenso ou critério seja alcançado.
Consenso e Relatório Final	Análise das respostas e elaboração do relatório final.

Fonte: elaborado pelo autor.

4.5.3.1 Escolha dos especialistas

A seleção dos especialistas é crucial para o sucesso do método *Delphi*. Devem ser considerados aspectos como o conhecimento técnico, a experiência, a relevância e reconhecimento dos especialistas em relação ao tema. O número ideal de participantes pode variar, mas é recomendado um grupo mínimo de 10 especialistas. Grupos menores podem dificultar a obtenção de um consenso robusto, enquanto grupos muito grandes podem tornar a gestão e análise dos dados excessivamente complexas (Marques; Freitas, 2018, p. 396). Neste estudo, o processo foi iniciado com 69 especialistas, os encarregados de proteção de dados das universidades federais do Brasil, esperando-se uma redução gradual no número de participantes ao longo das rodadas. Esse fenômeno é comum, conforme Marques e Freitas (2018, p. 396):

É importante sinalizar que, normalmente, no máximo metade das pessoas responde ao primeiro contato e é comum alguns participantes desistirem no meio do processo, levando o tamanho do painel a diminuir de rodada para rodada. Assim, é aconselhável começar com um grupo de especialistas de tamanho confortavelmente superior ao mínimo que se quer atingir.

4.5.3.2 Rodada Inicial

O processo *Delphi* normalmente inicia com a elaboração de um questionário inicial, que pode conter questões abertas, fechadas ou mistas. A escolha por questões mistas ou fechadas é comum, pois facilita a análise das respostas. Embora o questionário seja a ferramenta mais utilizada, outros formatos, como entrevistas ou grupos focais, também podem ser empregados. No entanto, o questionário é frequentemente preferido para garantir o anonimato dos participantes e simplificar a análise dos dados.

A elaboração das perguntas deve ser feita com cuidado, priorizando clareza e objetividade, para garantir que os especialistas compreendam plenamente o que está sendo solicitado. Além disso, é fundamental equilibrar a quantidade de questões, evitando tanto a superficialidade quanto a exaustão dos participantes.

Desde a primeira rodada, é recomendável que o método *Delphi* seja claramente explicado aos especialistas, incluindo instruções detalhadas sobre o preenchimento do questionário, assegurando o anonimato dos participantes, e informando sobre as datas limite para o retorno das respostas (Boberg; Morris-Khoo, 1992, p. 31, tradução nossa). Nesse momento, os especialistas avaliam as questões propostas e podem sugerir novos tópicos que considerem relevantes para a investigação.

4.5.3.3 Feedback controlado

O feedback entre as rodadas do método *Delphi* é um elemento crucial no processo. A análise detalhada das respostas dos especialistas em cada rodada anterior permite que os pesquisadores elaborem os questionários subsequentes de forma mais estruturada. Essa análise combina métodos qualitativos, especialmente nas fases iniciais, com técnicas quantitativas, como estatísticas descritivas e testes que identificam relações entre as respostas. Os resultados estatísticos do grupo, uma vez que as respostas são tratadas de forma coletiva, são complementados por trechos anônimos representativos de opiniões consensuais ou divergentes. Esses trechos contribuem para a construção de uma visão ampla sobre os pontos de concordância e discordância, permitindo que os especialistas reflitam sobre suas próprias posições.

Esse processo de retroalimentação é essencial para que os participantes possam avaliar as perspectivas coletivas, funcionando como uma forma de comunicação indireta entre os especialistas, mediada pelos pesquisadores. A síntese dos resultados, incluindo justificativas para o agrupamento de temas, além da apresentação de tendências e divergências, é fundamental para o progresso do estudo e para o refinamento das questões ao longo do processo.

4.5.3.4 Rodadas subsequentes

Nas rodadas subsequentes, os questionários tornam-se mais estruturados, concentrando-se na classificação de itens em escalas de importância. Esse formato facilita a quantificação do consenso entre os especialistas e permite identificar os temas mais relevantes para o estudo. Conforme o processo avança, os questionários tendem a ser predominantemente fechados, baseando-se nas respostas e comentários colhidos nas rodadas anteriores. A escolha cuidadosa do

formato e do conteúdo dos questionários é fundamental para o sucesso do método *Delphi*, pois influencia diretamente a qualidade dos dados coletados e a eficiência na obtenção dos resultados esperados.

Segundo Kayo e Securato (1997, p. 53), o método *Delphi* geralmente envolve entre duas e quatro rodadas:

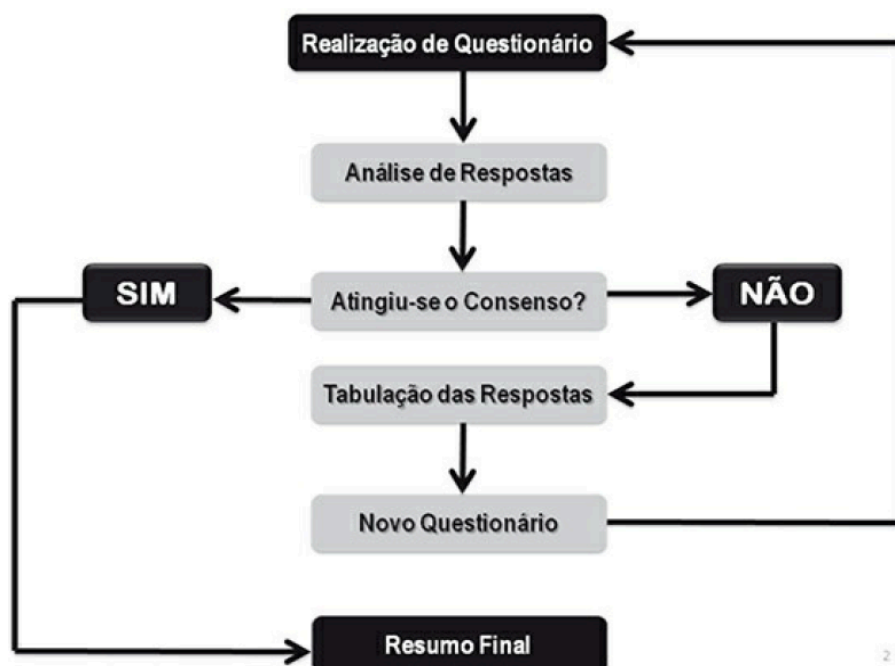
A grande maioria das pesquisas produzem, no máximo, quatro rodadas. Entretanto, nada impede que se faça um número menor, desde que os objetivos tenham sido atingidos. Por outro lado, um número maior não é aconselhável em virtude de restrições de tempo e pelo fato de não existirem mudanças de opinião significativas nas rodadas posteriores, conforme atestam experiências já realizadas.

Portanto, recomenda-se que o processo de consulta aos especialistas seja realizado em pelo menos duas ou três rodadas. Esse número é suficiente para refinar as opiniões e alcançar um consenso de maneira eficaz. Entretanto, deve-se evitar exceder quatro rodadas, uma vez que isso pode comprometer o engajamento dos participantes. A repetição prolongada tende a gerar cansaço e desmotivação, afetando tanto a qualidade das respostas quanto à eficácia no alcance dos objetivos do estudo.

4.5.3.5 Consenso e relatório final

O processo do método *Delphi* é concluído quando os níveis ou critérios de estabilidade e consenso desejados são atingidos. Não há critérios rígidos para determinar esses parâmetros; em geral, o consenso é alcançado quando há baixa divergência nas respostas, enquanto a estabilidade se refere à ausência de novas contribuições e a pequenas alterações nas respostas entre as rodadas.

Os facilitadores têm a responsabilidade de decidir se uma nova rodada é necessária ou se o processo pode ser encerrado. Ao final, um relatório é produzido, destacando as áreas de concordância e divergência entre os especialistas. Neste estudo, o relatório final fornecerá as questões selecionadas para compor o instrumento de medição do modelo de maturidade, além de oferecer insights sobre o grau de concordância e as áreas de dissenso, contribuindo para o desenvolvimento das melhores métricas para avaliar a maturidade das universidades federais no tratamento e proteção de dados e informações pessoais. A seguir, apresenta-se um fluxograma das etapas para melhor visualização do fluxo de aplicação do método *Delphi*.

Figura 3 - Fluxograma do método *Delphi*

Fonte: Daychoum (2016, p. 405).

4.5.4 Aplicação do método *Delphi* para os objetivos desta pesquisa

Nesta pesquisa, o método *Delphi* foi utilizado com o objetivo de identificar e selecionar as questões mais relevantes para compor o instrumento de medição do modelo de maturidade no tratamento de dados pessoais. Para isso, foi elaborado um documento (**Apêndice C**) que detalha a execução do método, incluindo um cronograma com prazos para cada fase do processo de aplicação. Os encarregados pelo tratamento de dados das universidades, que são os sujeitos desta pesquisa, participaram como especialistas no processo. Definiu-se previamente uma proposta de aplicação do método:

Quadro 8 - Proposta de aplicação do método *Delphi* nesta pesquisa

Etapa	Equipe de desenvolvedores/Facilitadores	Painel de especialistas
1	Os pesquisadores apresentam e enviam a estrutura inicial do instrumento de medição, que contém as questões elaboradas com base no referencial teórico, visando obter a primeira rodada de apreciação dos especialistas.	Os especialistas avaliam as questões propostas quanto à sua significância e relevância para a dimensão em que foram enquadradas, tendo a liberdade de sugerir novas questões que considerem pertinentes ao modelo.

2	Consolidam-se as respostas e sugestões dos especialistas, resultando em uma nova rodada que integra as sugestões mais bem avaliadas da rodada anterior, juntamente com o feedback coletivo e anônimo. Os temas de baixa relevância são excluídos, conforme sugerido por Daychoum (2016, p. 404).	Recebem o feedback das avaliações da rodada anterior e reavaliam a nova proposta, classificando as questões conforme sua relevância.
3	Consolidam-se as respostas dos especialistas e elabora-se o feedback coletivo. Avalia-se a necessidade de uma nova rodada para ajustes de consenso ou, caso os objetivos e critérios tenham sido alcançados, encerra-se o processo e elabora-se o relatório final.	Se houver uma nova rodada para ajuste de consenso, os especialistas reavaliam a nova proposta. Caso contrário, recebem o feedback do relatório final.

Fonte: elaborado pelo autor.

O objetivo final deste processo foi assegurar a contribuição de especialistas com conhecimento aprofundado no tema, visando alcançar um consenso quanto às questões mais relevantes para elaboração do instrumento de medição do modelo de maturidade no tratamento de dados pessoais. O detalhamento das etapas e dos critérios empregados na aplicação do método *Delphi* nesta pesquisa está descrito na **seção 5.3.6**. O relatório final apresenta os temas selecionados e oferece *insights* sobre o grau de concordância e as áreas de divergência entre os especialistas, contribuindo para o desenvolvimento de métricas robustas e adequadas à avaliação da maturidade de universidades federais no tratamento e proteção de dados pessoais.

4.6 Etapas para o Desenvolvimento e Validação do Modelo de Maturidade

O desenvolvimento do modelo de maturidade proposto seguiu uma estrutura composta por etapas interdependentes, fundamentadas nas contribuições de De Bruin et al. (2005), Software Engineering Institute (2002) e Van Steenberg et al. (2010), conforme detalhado na **seção 3.5** deste trabalho. O primeiro passo consistiu na definição do escopo e dos objetivos do modelo, estabelecendo as áreas específicas a serem avaliadas e os resultados desejados. Em seguida, a fase de design envolveu a criação da arquitetura do modelo, que incluiu uma revisão

bibliográfica das áreas de interesse, além da definição dos níveis de maturidade, das dimensões a serem avaliadas e dos critérios de avaliação.

Durante a fase de preenchimento, a escolha do questionário como método de avaliação foi essencial, sendo complementada pela técnica *Delphi* no processo de validação, avaliação e refinamento do instrumento de medição. Este processo de validação contemplou tanto a aparência quanto o conteúdo do modelo, sendo conduzido por especialistas encarregados da proteção de dados das universidades, os quais asseguraram a representatividade e a confiabilidade dos elementos propostos. Após a validação, o modelo foi testado e implementado nas universidades federais brasileiras. Por meio de testes pilotos, foi possível realizar ajustes no instrumento com base nos resultados obtidos, garantindo a adequação do modelo à realidade das instituições.

O desenvolvimento detalhado do modelo de maturidade proposto é descrito na **seção 5**, na qual a combinação de diferentes técnicas e métodos de pesquisa, como o *Delphi*, contribuiu significativamente para superar os desafios e limitações inerentes a cada abordagem. Essa integração assegurou que os dados construídos e coletados fossem apropriados para avaliar as capacidades organizacionais, conforme destacado no modelo a ser aplicado nas universidades federais brasileiras.

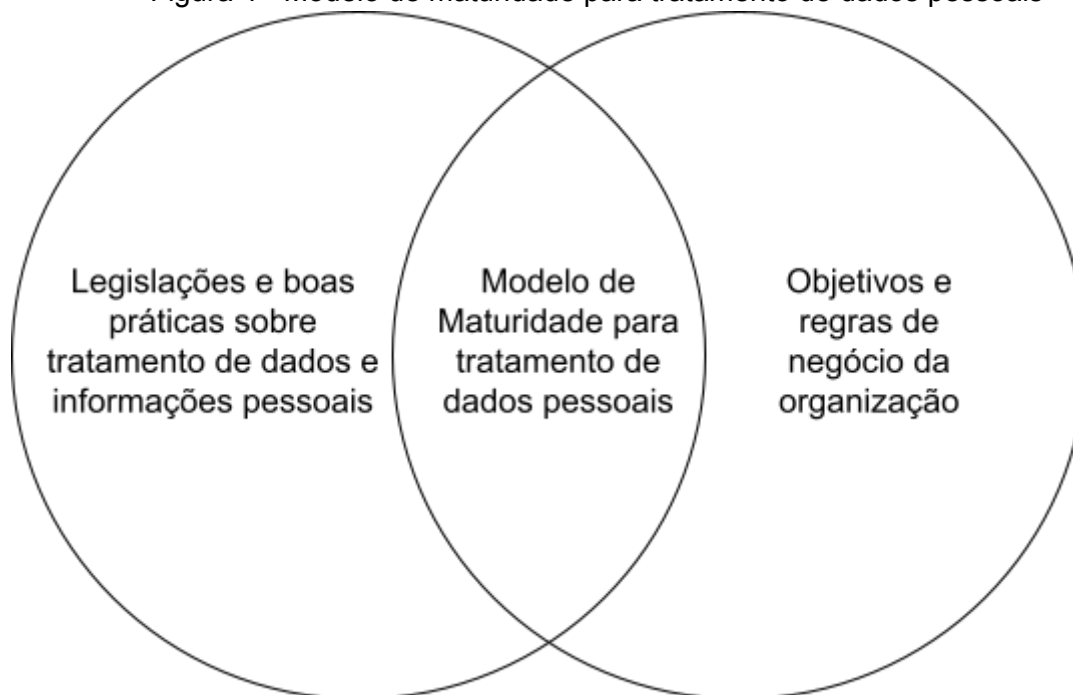
5 DESENVOLVIMENTO DO MODELO DE MATURIDADE PARA TRATAMENTO DE DADOS PESSOAIS

No contexto atual, no qual a proteção de dados pessoais e a transparência no tratamento dessas informações se tornaram imperativos legais e éticos, as empresas enfrentam o desafio de assegurar conformidade com leis como a LGPD (Lei Geral de Proteção de Dados), a LAI (Lei de Acesso à Informação) e demais legislações e normativos que impactam no tratamento de dados e informações pessoais. Com o propósito de auxiliar as organizações nesse processo de adequação e melhoria contínua, foi desenvolvido o Modelo de Maturidade para o Tratamento de Dados Pessoais (MMTDP), seguindo as fases propostas por Software Engineering Institute (2002); De Bruin *et al.*, (2005); e Van Steenbergem *et al.* (2010), detalhado na **seção 3.5** deste trabalho.

5.1 Escopo

O modelo de maturidade proposto representa a intersecção entre as legislações, normativas e boas práticas relacionadas ao tratamento e proteção de dados e informações pessoais e os objetivos e regras de negócio das organizações.

Figura 4 - Modelo de maturidade para tratamento de dados pessoais



Fonte: elaborado pelo autor.

O objetivo de um modelo de maturidade é ser aplicado como uma ferramenta de referência utilizada para avaliar o grau de desenvolvimento e eficiência dos processos de uma organização. Permite identificar o alinhamento desses processos com normas e as melhores práticas, permitindo identificar pontos de melhoria. Além disso, um modelo de maturidade auxilia no planejamento e a monitorar ações de melhoria contínua, garantindo que os processos organizacionais sejam aprimorados de forma consistente em direção aos objetivos estabelecidos.

Neste projeto o modelo proposto tem o foco de capacitar as organizações na evolução contínua de seus processos de gestão de dados e informações pessoais, assegurando que tais dados sejam tratados de maneira ética, legal e segura. Ao alcançar níveis mais elevados de maturidade, as organizações não apenas cumprem as leis aplicáveis, mas também se destacam como líderes na proteção da privacidade e na garantia do acesso transparente às informações pessoais. Isso fortalece a confiança dos clientes e partes interessadas, ao mesmo tempo em que reduz riscos legais e reputacionais, posicionando as organizações para um futuro de sucesso sustentável em um ambiente cada vez mais regulamentado e focado na privacidade.

5.2 Design do modelo

O processo de identificação dos componentes que envolvem a arquitetura do modelo foi conduzido por meio de uma revisão da literatura, abrangendo diferentes modelos de maturidade e legislações, normativas e boas práticas relacionadas ao tratamento e proteção de dados e informações pessoais. Essa abordagem possibilitou a criação de um conjunto inicial de elementos apresentados a seguir.

5.2.1 Níveis de Maturidade

Este modelo foi pensado para ser composto por cinco níveis de maturidade, proporcionando uma estrutura abrangente para avaliar e aprimorar a maneira como as organizações lidam com dados e informações pessoais. Cada nível de maturidade representa uma fase distinta no caminho em direção à conformidade sólida e, por fim, à liderança na proteção, privacidade, transparência e acesso a esses dados. Abaixo estão apresentados os níveis de maturidade do modelo proposto:

1. Nível inicial: A organização não possui processos formais para o tratamento e proteção de dados e informações pessoais, com práticas desestruturadas que não estão em conformidade com as normas e legislações aplicáveis.
2. Nível emergente: A organização começa a adotar políticas e processos básicos para o tratamento e proteção de dados pessoais, embora a conformidade com a legislação ainda seja inconsistente e os processos não estejam totalmente implementados.
3. Nível intermediário: A organização implementou políticas e processos que atendem minimamente às legislações, mas ainda precisa aprimorar a eficiência e a eficácia na gestão de dados pessoais.
4. Nível avançado: A organização demonstra conformidade sólida com as legislações e possui medidas eficazes e eficientes de tratamento e proteção de dados pessoais, mas ainda necessita de práticas de monitoramento contínuo da conformidade.
5. Nível exemplar: A organização atende aos requisitos legais, mantém um monitoramento constante da conformidade por meio de indicadores e relatórios, e se destaca como referência em proteção e gestão de dados pessoais.

Esses níveis de maturidade representam uma progressão gradual que a organização pode percorrer. A jornada começa no nível inicial, onde não há processos formais e há desacordo com as leis de proteção de dados pessoais. Ela culmina no nível exemplar, em que a organização não apenas cumpre rigorosamente as normativas, mas também se torna uma referência na gestão de dados pessoais. Entre esses extremos, encontramos o nível emergente, caracterizado pelo início da adoção de políticas; o nível intermediário, onde as políticas estão implementadas, mas requerem aprimoramentos; e o nível avançado, marcado por uma sólida conformidade legal, embora ainda necessite de monitoramento contínuo.

Essa progressão representa um compromisso crescente com a proteção e o tratamento dos dados e informações pessoais, assim como a conformidade com as leis aplicáveis, à medida que a organização amadurece em suas políticas e práticas de gestão nas dimensões avaliadas.

5.2.2 Dimensões para o tratamento de dados e informações pessoais

As dimensões destinadas ao tratamento de dados e informações pessoais representam os pilares fundamentais de um modelo de maturidade concebido com o propósito de auxiliar as organizações na gestão responsável e eficaz dos dados e informações pessoais que estão sob sua custódia. Cada dimensão desse modelo desempenha um papel crucial na jornada em direção à conformidade legal, e excelência na proteção, transparência, privacidade e acesso a esses dados.

Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de uma programa mais consistente de *compliance* digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura (Pinheiro, 2023, p. 79).

Desde o estabelecimento de uma governança de dados sólida até a garantia da conscientização dos colaboradores e a implementação de medidas de segurança, essas dimensões oferecem o arcabouço necessário para enfrentar os desafios cada vez mais complexos e críticos relacionados ao tratamento de dados pessoais.

A definição das dimensões foi fundamentada em uma análise detalhada da pesquisa bibliográfica e documental, incorporando tanto autores quanto legislações relevantes, assegurando assim um embasamento teórico e normativo sólido. A partir desse levantamento, foram identificadas e organizadas as áreas mais críticas e relevantes para a construção deste modelo. O processo de refinamento, que resultou na seleção das cinco dimensões, teve como objetivo tornar o modelo mais simplificado e foi orientado pela visão dos pesquisadores, no intuito de facilitar sua aplicação e compreensão no contexto específico para o qual foi desenvolvido. As legislações e normas que embasam as questões abordadas nas dimensões estão detalhadas a seguir.

Quadro 9 - Legislações e Normas que fundamentaram as dimensões

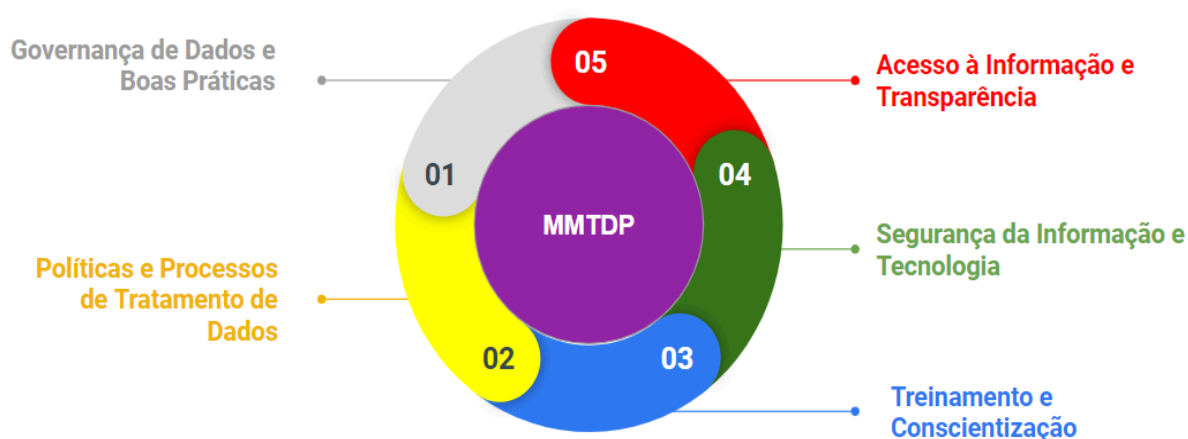
Dimensão	Legislações e Normas
Governança de Dados e Boas Práticas	LGPD (Lei n. 13.709/2018); ABNT NBR ISO/IEC 27701:2019; ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 38500:2018; ABNT NBR ISO/IEC 27014:2021; Decreto n. 9.637/2018; Decreto n. 10.046/2019; Resolução CONARQ n. 54/2023; Lei n. 13.853/2019; IN SGD/ME nº 117/2020

Políticas e Processos de Tratamento de Dados	LGPD (Lei n. 13.709/2018); ABNT NBR ISO/IEC 27701:2019; ABNT NBR ISO/IEC 27002:2022; Resolução CONARQ n. 54/2023; Decreto n. 9.637/2018; Lei de Arquivos (Lei n. 8.159/1991); Lei n. 10.741/2003; ABNT NBR ISO/IEC 29134:2024; Lei n. 7.232/1984
Treinamento e Conscientização	LGPD (Lei n. 13.709/2018); ABNT NBR ISO/IEC 27701:2019; ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023; ABNT NBR ISO/IEC 27035:2023; Resolução CONARQ n. 54/2023; Decreto n. 9.637/2018; Decreto-Lei nº 2.848/1940 (Código Civil); Lei n. 7.232/1984
Segurança da Informação e Tecnologia	LGPD (Lei n. 13.709/2018); ABNT NBR ISO/IEC 27001; ABNT NBR ISO/IEC 27002:2022; Resolução CONARQ n. 54/2023; Decreto n. 9.637/2018; Lei n. 7.232/1984; Instrução Normativa GSI/PR n. 1/2020
Acesso à Informação e Transparência	LGPD (Lei n. 13.709/2018); ABNT NBR ISO/IEC 27701:2019; ABNT NBR ISO/IEC 27002:2022; Resolução CONARQ n. 54/2023; Lei de Acesso à Informação (Lei n. 12.527/2011); Decreto n. 9.637/2018; IN SGD/ME n. 117/2020; Lei n. 7.232/1984; Lei de Arquivos (Lei n. 8.159/1991); Constituição Federal de 1988; Decreto n. 7.724/2012;

Fonte: elaborado pelo autor.

Para proporcionar uma compreensão mais clara da construção do MMTDP e suas inter-relações, optou-se pelo uso de cores para representação visual de cada dimensão.

Figura 5 - Dimensões do modelo de maturidade para tratamento de dados pessoais



Fonte: elaborado pelo autor.

- Dimensão 1: Governança de Dados e Boas Práticas (cor cinza)

Esta dimensão foca em aspectos estratégicos da governança de dados e proteção de informações pessoais. Avalia como a organização estabelece sua estrutura de governança para garantir o cumprimento de normas e legislações, além de promover práticas responsáveis no tratamento de dados. Inclui a nomeação formal de um Encarregado de Proteção de Dados (DPO), a criação de comitês, a implementação de programas estratégicos e a definição clara das responsabilidades institucionais e individuais. Uma governança sólida assegura que a instituição esteja preparada para lidar com os desafios e riscos relacionados à privacidade e proteção de dados pessoais.

- Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela)

Esta dimensão avalia os aspectos técnicos e operacionais relacionados ao tratamento de dados pessoais, com foco na existência, implementação e eficácia de procedimentos e processos. Analisam-se os aspectos do ciclo de vida dos dados, desde a coleta até o armazenamento, uso, compartilhamento e descarte - além da capacidade de identificar, avaliar e mitigar riscos. A gestão do consentimento, a proteção de dados sensíveis e de dados de crianças e adolescentes, e o atendimento aos direitos dos titulares são monitorados continuamente. O objetivo é garantir que o tratamento dos dados seja ético, legal e seguro, por meio de práticas bem definidas e processos documentados.

- Dimensão 3: Treinamento e Conscientização (cor azul)

Esta dimensão avalia o nível de treinamento e conscientização dos colaboradores e partes interessadas em relação ao tratamento e proteção de dados e informações pessoais. Foca na implementação de programas estruturados e contínuos que garantam que todos na organização compreendam as implicações legais, éticas e normativas envolvidas. O treinamento adequado é essencial para assegurar que os colaboradores sigam as políticas e procedimentos estabelecidos, estejam preparados para lidar com os riscos e incidentes, e atuem de forma proativa. A eficácia dos programas é monitorada continuamente, promovendo uma cultura organizacional de proteção de dados e privacidade, crucial para mitigar riscos e garantir o cumprimento das legislações aplicáveis.

- Dimensão 4: Segurança da Informação e Tecnologia (cor verde)

Esta dimensão avalia as medidas de segurança implementadas para proteger dados e informações pessoais, com foco na infraestrutura de Tecnologia da Informação (TI) da organização. A avaliação inclui medidas preventivas, como a prevenção de violações de dados, o uso de criptografia, autenticação forte, e outras práticas tecnológicas avançadas. O objetivo central é assegurar a confidencialidade, integridade e disponibilidade dos dados, princípios essenciais de segurança. Além disso, a dimensão examina a conformidade com normas e regulamentações de segurança da informação, avaliando a eficácia das proteções implementadas em sistemas e redes da organização. A segurança da informação é considerada não apenas uma exigência legal, mas também um pilar fundamental para garantir a confiança e proteger a reputação da organização junto ao público.

- Dimensão 5: Acesso à Informação e Transparência (cor vermelha)

Esta dimensão avalia a disponibilidade e transparência das informações fornecidas ao público, assegurando a conformidade com as normas de acesso à informação. Isso inclui a demonstração clara de transparência nas práticas de tratamento e proteção de dados pessoais, garantindo que as partes interessadas tenham acesso adequado às informações sobre como seus dados são gerenciados. Além disso, a dimensão analisa a capacidade da organização de gerar relatórios precisos para garantir conformidade com regulamentações de privacidade e acesso à informação. Também avalia a eficácia na comunicação com partes afetadas, autoridades regulatórias e demais interessados sobre incidentes de segurança. Isso inclui registros detalhados de como esses incidentes foram tratados e as lições aprendidas, reforçando a confiança e aprimorando continuamente as práticas organizacionais.

À medida que as organizações se deparam com uma crescente conscientização sobre a importância da proteção de dados pessoais e a necessidade de conformidade com as normativas vigentes, essas dimensões tornam-se fundamentais para a construção de uma estrutura organizacional sólida. Ao adotar uma abordagem centrada no titular de dados, especialmente no tratamento de informações sensíveis, as organizações garantem o cumprimento dos requisitos legais e éticos, ao mesmo tempo em que constroem a confiança do público. Conforme avançam nos níveis de maturidade, não apenas cumprem as leis, mas também estabelecem um padrão exemplar de responsabilidade, privacidade, transparência e segurança no tratamento de dados, fortalecendo sua reputação e mitigando riscos. A avaliação consistente e eficaz dessas dimensões é, portanto, essencial para o sucesso a longo prazo em um ambiente de dados cada vez mais regulamentado e orientado pela privacidade.

5.2.3 Natureza do modelo proposto

O modelo de maturidade em proposição adota predominantemente uma natureza prescritiva, delineando diretrizes rigorosamente definidas e requisitos fundacionais para a gestão de dados pessoais no âmbito das Universidades Federais. Este modelo é sustentado por um sólido alicerce jurídico que incorpora a Lei Geral de Proteção de Dados, a Lei de Acesso à Informação e outras normativas legislativas pertinentes, estabelecendo um robusto arcabouço regulatório destinado a assegurar a conformidade institucional com as exigências normativas relacionadas ao tratamento de dados e informações pessoais. Simultaneamente, à medida que sua implementação progressiva se consolida e as atividades das instituições se aprimoram, vislumbra-se a possibilidade de que o modelo venha a adquirir uma natureza comparativa. Esse desenvolvimento potencial facultaria às universidades federais não apenas cumprir as obrigações legais, mas também capacitar-se para realizar análises comparativas, confrontando suas práticas com padrões de excelência.

5.3 Preencher

Com base no delineamento do escopo e do design do modelo, avançou-se para a definição do **conteúdo e do método de avaliação**. Dada a natureza, os níveis de maturidade e as dimensões previamente estabelecidas, concluiu-se que o

questionário seria o instrumento de medição (método de avaliação) mais adequado para o modelo. Nessa fase, tornou-se essencial adotar uma estratégia que garantisse rigor e eficácia ao instrumento na avaliação das capacidades organizacionais voltadas ao tratamento e à proteção de dados e informações pessoais nas universidades federais brasileiras.

Para assegurar tal robustez, seguiram-se alguns processos e critérios específicos. O primeiro passo consistiu na análise e definição dos conteúdos que deveriam estruturar o instrumento de medição do modelo. Para isso, foi realizado um estudo minucioso das normas, legislações e regulamentos relacionados ao tratamento e à proteção de dados e informações pessoais. Com base nessa análise, foram identificados os temas relevantes. A partir desses temas, elaboraram-se um questionário com perguntas iniciais, que posteriormente seriam submetidas a um processo de avaliação, classificação, refinamento e consolidação, pelos especialistas, culminando na seleção das questões que comporiam o método de avaliação do modelo de maturidade proposto.

O procedimento para avaliação, seleção e refinamento das questões que comporiam o instrumento de medição do modelo de maturidade, foi o método *Delphi*. Esse método permitiu, por meio dos critérios pré-estabelecidos e da participação direta dos especialistas (encarregados de proteção de dados), identificar quais itens melhor representam cada dimensão do modelo. Para uma compreensão detalhada sobre o método *Delphi*, é possível consultar a **seção 4.5** deste trabalho.

5.3.1 Conteúdo: Fundamentação legal e normativa do instrumento de medição do modelo de maturidade

Para a construção do instrumento de medição do modelo proposto, foi fundamental realizar uma análise aprofundada das principais normas e legislações que regem o tratamento e a proteção de dados pessoais. Dentre os marcos legais essenciais, destaca-se a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), que estabelece os pilares da proteção de dados no Brasil. Complementando esse arcabouço, as normas técnicas ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27002:2022 oferecem diretrizes e boas práticas para a gestão da privacidade e da segurança da informação, respectivamente. Adicionalmente, a Resolução CONARQ n. 54/2023 fornece orientações específicas para a aplicação da

LGPD no contexto dos arquivos permanentes. Além dessas, diversas legislações, normas complementares e instruções normativas foram cuidadosamente consideradas para assegurar uma abordagem abrangente e consistente na formulação do questionário. A seguir, apresenta-se uma síntese das principais legislações e normas utilizadas.

Quadro 10 - Síntese das referências legais e normativas utilizada

Categoria	Legislação/Norma	Descrição
Legislação Principal	Lei n. 13.709/2018 (LGPD)	Estabelece diretrizes gerais para a proteção de dados pessoais no Brasil.
Legislação Arquivística	Resolução CONARQ n. 54/2023	Estabelece diretrizes para a aplicação da LGPD em arquivos permanentes.
	Lei n. 8.159/1991 (Lei de Arquivos)	Estabelece a política de arquivos públicos e privados no Brasil.
Legislações Complementares	Decreto n. 10.046/2019	Estabelece o compartilhamento de dados no setor público.
	Decreto n. 9.637/2018	Regula a Política Nacional de Segurança da Informação.
	Decreto n. 7.724/2012	Regulamenta a Lei de Acesso à Informação.
	Lei n. 12.527/2011 (Lei de Acesso à Informação)	Regula o acesso a informações públicas e a transparência na administração pública.
	Lei n. 10.741/2003 (Estatuto do Idoso)	Protege os dados e direitos de idosos.
	Lei n. 7.232/1984 (Política Nacional de Informática)	Regula o uso da informática no Brasil, com implicações para a proteção de dados.
	Decreto-Lei n. 2.848/1940 (Código Civil)	Regula aspectos civis, incluindo questões de privacidade.
Normas Técnicas Principais	ABNT NBR ISO/IEC 27002:2022	Fornecer boas práticas para a gestão da segurança da informação.
	ABNT NBR ISO/IEC 27701:2019	Oferece diretrizes para a gestão da privacidade de dados pessoais.
Normas Técnicas Complementares	ABNT NBR ISO/IEC 27005:2023	Diretrizes para a gestão de riscos de segurança da informação.
	ABNT NBR ISO/IEC 27035:2023	Diretrizes para o gerenciamento de incidentes de segurança da informação.
	ABNT NBR ISO/IEC 29134:2024	Diretrizes para avaliação de impacto de privacidade.

	ABNT NBR ISO/IEC 27014:2021	Diretrizes para a governança da segurança da informação.
	ABNT NBR ISO/IEC 38500:2018	Governança corporativa de tecnologia da informação
Instruções Normativas	Instrução Normativa GSI/PR n. 1/2020	Regras de segurança cibernética para órgãos públicos.
	Instrução Normativa SGD/ME n. 117/2020	Regulamenta a implementação de processos digitais no governo federal, com impacto na proteção de dados.

Fonte: elaborado pelo autor.

A leitura minuciosa das legislações e normas apresentadas no quadro foi crucial, pois forneceu a fundamentação legal e técnica necessária para assegurar a conformidade com os requisitos estabelecidos. Esses marcos regulatórios e normativos ofereceram diretrizes essenciais para a formulação de temas que garantem um tratamento seguro e transparente de dados e informações pessoais, em estrita conformidade com a legislação vigente. Ademais, a compreensão aprofundada dessas referências foi vital para o desenvolvimento do instrumento de medição proposto, o qual visa avaliar, de maneira precisa, o nível de maturidade organizacional no âmbito da proteção de dados, promovendo, assim, boas práticas e mitigando riscos.

5.3.2 Conteúdo: Correlação entre os artigos das leis e os itens normativos com as dimensões do Modelo proposto

A Lei Geral de Proteção de Dados representa a norma central no Brasil para a proteção de dados pessoais. Para facilitar a análise desta legislação, foi elaborado um quadro que sintetiza os principais objetivos de cada artigo, delineando as áreas e os tópicos abordados e associando-os às dimensões predominantes do instrumento de medição. Para proporcionar uma compreensão mais clara, adotou-se uma codificação por cores, a qual permite uma visualização eficaz da influência das dimensões do Modelo de Maturidade em Tratamento de Dados Pessoais. As cores utilizadas são as mesmas que estão predefinidas na Figura 6 desta pesquisa.

O Quadro 11, construído com base na LGPD, apresenta os artigos da legislação de forma organizada, com a representação das cores das dimensões predominantes associadas a cada item normativo. Essa metodologia não apenas

facilita a visualização, mas também evidencia como cada artigo se relaciona com as dimensões propostas no MMTDP.

Quadro 11 - LGPD e a predominância da dimensão

Artigos da LGPD	Dimensão predominante
Arts. 1 a 6 - Fundamentos, aplicação da Lei, definições e princípios	1
Art. 7 - Hipóteses legais	1
Art. 8 - Consentimento	2
Art. 9 - Direitos do titular	2
Art. 10 - Legítimo interesse	2
Art. 11 - Dados sensíveis	2
Art. 12 - Anonimização	2
Art. 13 - Dados de saúde pública, estudos e pesquisas	2
Art. 14 - Crianças e adolescentes	2
Art. 15 e 16 - Término de tratamento	2
Arts. 17 a 22 - Direitos do titular	2
Art. 23 - Princípio do interesse público (finalidade)	1
Art. 24 - Regras para empresas públicas e sociedades de economia mista	1
Art 25 - Dados em formatos interoperável	4
Arts. 26 e 27 - Compartilhamento de dados pelo Poder Público	2
Art. 28 - Vetado	Não se aplica
Arts. 29 e 32 - Autoridade Nacional (poderes e responsabilidades)	Não se aplica
Arts. 33 a 36 - Transferência internacional de dados	2
Art. 37 - Registros de operações de tratamento de dados pessoais	5
Art. 38 - Relatório de impactos quando solicitado	5
Art. 39 - Agentes de tratamento (como deve proceder o operador de dados)	3
Art. 40 - Padrões de interoperabilidade/portabilidade/acesso	5
Art. 41 - Indicação do Encarregado (DPO)	1
Arts. 42 a 45 - Responsabilidade dos agentes de tratamento	3
Arts. 46 e 47 - Segurança e sigilo dos dados	4
Art. 48 - Gestão de incidentes e monitoramento	5
Art. 49 - Sistemas	4
Arts. 50 e 51 - Boas práticas e Governança	1
Arts. 52 a 54 - Sanções administrativas	3
Art. 55 - Vetado	Não se aplica
Arts. 55 (A-M) - Autoridade Nacional de Proteção de Dados (ANPD)	Não se aplica
Arts. 56 a 58 - Vetados	Não se aplica
Arts. 58 (A e B) - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	Não se aplica
Art. 59 - Vetado	Não se aplica
Art. 60 - Alterações na Lei 12.965/2014 (dados na internet)	Não se aplica
Art. 61 - Regras para empresas estrangeiras	Não se aplica
Art. 62 - Acesso a dados tratados pela União	Não se aplica

Art. 63 - Banco de dados	4
Art. 64 - Importância das demais leis sobre o tema	2
Art. 65 - Quando entra em vigor a Lei	1

Fonte: adaptado da LGPD.

Essa abordagem analítica foi igualmente aplicada na Resolução CONARQ n. 54/2023, que regulamenta a aplicação da LGPD aos arquivos permanentes. É pertinente destacar que a identificação de uma única dimensão para cada artigo **não indica exclusividade**, mas sim um maior impacto naquela dimensão específica. Os artigos que não foram especificados por cores referem-se àqueles vetados ou que não possuem aplicabilidade nas Universidades Federais, que constituem o foco desta pesquisa. O Quadro 12 refere-se à Resolução CONARQ n. 54/2023, que trata da aplicação da LGPD aos arquivos permanentes.

Quadro 12 - Resolução CONARQ n. 54/2023 e a predominância da dimensão

Artigos do Conarq n. 54/2023	Dimensão predominante
Art. 1 - Finalidade e aplicação	1
Art. 2 - Tratamento de dados pessoais em Arquivos Permanentes	1
Art. 3 - Conceitos	1
Art. 4 - Diretrizes para o tratamento de dados pessoais em AP	2
Art. 5 - Dados pessoais em AP	2
Art. 6 - Dados pessoais de pessoas falecidas	2
Art. 7 - Vedação de eliminação de AP	2
Art. 8 - Revogação de consentimento	2
Art. 9 - Anonimização ou pseudominimização sem comprometer autenticidade e integridade do documento	2
Art. 10 - Direito de informação para os titulares de dados pessoais	2
Art. 11 - Requerimento do titular de dados	2
Art. 12 - Solicitação de retificação de dados pessoais	2
Art. 13 - Política de privacidade de dados pessoais	1
Art. 14 - Política de segurança de dados pessoais tratados	4
Art. 15 - Divulgação de violação de dados, destruição ou alteração	5
Art. 16 - Contratos	2
Art. 17 - Recolhimento deve ser formalizado se constar dados pessoais	5
Art. 18 - Requisitos para descrever arquivos com dados pessoais	5
Art. 19 - Revisão dos instrumentos de pesquisa de acervos com dados pessoais	5
Art. 20 - Registro de restrição de acesso, risco ou dano potencial no instrumento de pesquisa	5
Art. 21 - Acesso	5
Art. 22 - Terceiros interessados em acesso devem aceitar condições de uso	5
Art. 23 - Regras de acesso aos documentos de AP com dados pessoais	5

Art. 24 - Arquivos privados (promover acesso)	5
Art. 25 - Arquivos privados (disponibilização)	5
Art. 26 - Dúvidas entrar em contato com o CONARQ	1
Art. 27 - Vigor	Não se aplica

Fonte: adaptado do Conarq n.54/2023.

É imprescindível enfatizar que a dinâmica de identificação de predominância desempenhou um papel fundamental na correlação entre as normativas e as dimensões propostas. Em relação às demais normas e legislações, a abordagem adotada foi mais pontual, com foco no conteúdo dos itens ou artigos, destacando as seções relevantes, o que tornou dispensável a elaboração de um quadro. Com a análise das legislações relativas ao tratamento e à proteção de dados pessoais concluída, chegava-se ao momento de desenvolver o questionário que serviria como instrumento de medição do modelo de maturidade proposto.

5.3.3 Conteúdo: Definição dos temas e assuntos propostos para o instrumento de medição

O segundo passo no desenvolvimento do questionário consistiu em identificar, nas normas técnicas e jurídicas, os principais temas ou tópicos relevantes para as organizações públicas no que diz respeito ao tratamento e à proteção de dados e informações pessoais. O objetivo foi compreender o que precisa ser feito e como, para que essas instituições possam monitorar, implementar e gerir processos de forma eficaz, alinhando-se aos objetivos das dimensões propostas.

A partir da análise das normativas e dos objetivos de cada dimensão, foram definidos temas que garantem uma cobertura abrangente e significativa dos assuntos pertinentes ao tratamento e à proteção de dados pessoais nas instituições. Esses temas foram essenciais para orientar a formulação das questões que compõem o instrumento de medição, assegurando que cada dimensão fosse representada de maneira coerente e completa. O resultado desse trabalho está detalhado no Quadro 13, que apresenta os temas abordados em cada questão, de acordo com a dimensão correspondente.

Quadro 13 - Temas definidos para elaboração das questões

Questões	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5
1	Programa ou Plano de Governança	Identificação das Categorias de Dados Pessoais e dos Titulares de Dados Pessoais	Programa ou Plano de Capacitação	Política de Segurança da Informação (POSIC)	Transparência
2	Encarregado de Proteção de Dados	Identificação dos Agentes (operadores) de Tratamento de Dados Pessoais	Conscientização dos Agentes de Tratamento de Dados sobre seus Papéis e Responsabilidades	Provisionamento de Usuários	Política de Classificação da Informação
3	Comitê Interno para Tratamento de Dados e Informações Pessoais	Controlador Conjunto	Treinamento e Capacitação dos Colaboradores (Terceirizados e Parceiros)	Criptografia	Publicização do Encarregado de Proteção de Dados
4	Identificação de Outras Legislações, Normas ou Regulamentos	Identificação dos Processos e Atividades Operacionais Relacionadas aos Dados Pessoais	Capacitação Quanto aos Riscos Associados ao Tratamento Inadequado de Dados Pessoais	Gestão de Backup e Trilhas de Auditoria	Publicização da Política de Privacidade
5	<i>Legitimate Interests Assessment</i> (LIA)	Análise de Impacto de Privacidade ou PIA (Privacy Impact Assessment)	Capacitação Quanto às Possíveis Sanções Administrativas Aplicadas pela ANPD	Inteligência de Ameaças e Gestão de Vulnerabilidades	Procedimentos de Comunicação à ANPD e ao Titular de Dados em Caso de Ocorrência de Incidentes de Segurança
6	Política de Privacidade	Ajuste dos contratos e Convênios	Capacitação Quanto aos Procedimentos Adequados para a Gestão de Incidentes	Controle de Acesso e Autenticação Segura	Relatório de Impacto de Proteção de Dados Pessoais (RIPD) ou <i>Data Protect Impact Assessment</i> (DPIA)
7	Identificação de Compartilhamento e Transferência de Dados Pessoais	Compartilhamento e Transferência Internacional de dados e Informações Pessoais com Terceiros	Treinamentos Específicos para o Tratamento de Dados Pessoais Sensíveis, Bem como Dados de Crianças e Adolescentes	Gestão de Incidentes de Segurança da Informação	Divulgação dos Incidentes Decorrentes de Perdas, Destruição, Falsificação, Acesso não Autorizado e Liberação Não Autorizada
8	Gestão de Ativos, Mapeando de fluxos (Personal Data Flow Map) e Inventário de Dados Pessoais	Direitos dos Titulares de Dados Pessoais	Avaliação Periódicas e Monitoramento dos Resultados dos Treinamentos e Capacitações	Monitoramento e Controle de Eventos Associados à Violação e Vazamento de Dados Pessoais	Mecanismos para Incentivo de Relatos de Incidentes e Falhas de Segurança da Informação

9	Revisão e Atualização Regular das Políticas e Procedimentos Institucionalizados	Gestão de Consentimento dos Titulares de Dados Pessoais	Promoções Regulares de Eventos, Treinamentos, Campanhas e/ou Capacitações	Privacy by Design e Privacy by Default para os Sistemas Institucionais	Programa ou Plano de Comunicação
10	Compliance Digital, Monitoramento de Indicadores ou Auditorias Específicas	Mascaramento, Pseudonimização ou Anonimização de Dados e Informações Pessoais	Disponibilização de Recursos Específicos para Fomentar Capacitações e Treinamentos	Risk Assessment (Avaliação de Risco), Garantindo Confidencialidade, Integridade e Disponibilidade dos Dados Pessoais	Procedimentos Documentados e Disponibilizados

Fonte: elaborado pelo autor.

Dessa forma, sintetiza a associação entre cada dimensão e as temáticas abordadas nas questões correspondentes, facilitando a identificação do objetivo central de cada questão do instrumento.

5.3.4 Conteúdo: Correlação dos temas e assuntos propostos em cada questão com as normas legais e técnicas

Após a definição dos temas a serem abordados em cada questão, foi necessário realizar a identificação precisa dos itens normativos e artigos legais que subsidiariam o desenvolvimento dessas questões. Esse processo de correlação cuidadosa entre temas e normativas garante a validade jurídica do questionário, assegurando que cada questão proposta esteja fundamentada em uma base normativa sólida.

Como exemplo, o Quadro 14 ilustra a associação entre as questões da Dimensão 1 (Governança de Dados e Boas Práticas) e os respectivos itens normativos e artigos jurídicos utilizados na sua elaboração.

Quadro 14 - Normas técnicas e jurídicas utilizadas na elaboração das questões

	Dimensão 1: Governança de Dados e Boas Práticas									
Normas/Questões	1	2	3	4	5	6	7	8	9	10

Lei n. 13.709/2018	art. 50 e art. 52, § 1º, inciso IX	art. 5º, inciso VIII, art. 23, inciso III e art. 41	art. 50	art. 7º, inciso II, art. 11, inciso II, alínea "a", art. 23, art. 26, inciso IV, art. 34, inciso I e art. 50	art. 6º, inciso I, art. 7º, art. 10, art. 15, art. 16, capítulo IV (arts. 23-32), art. 37 e art. 50	art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II	art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50	art. 50	art. 23, inciso I, art. 32, art. 50 e art. 51	art. 50, inciso I, alínea "h"
ABNT NBR ISO/IEC 27701:2019		item 6.3.1.1	item 6.3.1.1	itens 5.2.1 e 7.2.2	itens 7.2, 7.3, 7.4.1 e 8.2	itens 7.3, 7.4 e 8.3	itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5	itens 6.5.1, 6.5.3, 7.2.8 e 8.2.6	itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2	itens 5.7, 6.9.4, 6.9.7 e 6.15 e 8.2.6
ABNT NBR ISO/IEC 27002:2022				item 5.31		itens 5.34 e 6.6	item 5.14	itens 5.9, 5.10, 5.11 e 8.1.1	itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8	itens 5.22, 5.35, 5.36, 6.7, 8.15, 8.16 e 8.34
Resolução CONARQ n. 54/2023				art. 2º, parágrafo único	art. 2º, parágrafo único, arts. 4º-12 e art. 18	art. 4º, art. 13 e art. 20	art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V		art. 1º e art. 19	
Decreto n. 9.637/2018	X		art. 15							
Decreto n. 10.046/2019	X		X							
ABNT NBR ISO/IEC 27014:2021	X									
Lei n. 13.853/2019		x								
IN SGD/ME n. 117/2020		art. 1º								

Fonte: elaborado pelo autor.

Assim, estabelece a correlação direta entre as questões e os respectivos artigos legais e normativos que fundamentam a construção das questões para a Dimensão 1. Para acessar as demais normas e artigos jurídicos que embasam as questões das outras dimensões, consulte o **Apêndice D** deste trabalho. Essa metodologia assegura a coerência entre os aspectos jurídicos e normativos aplicados e a formulação das questões, garantindo a relevância e a precisão do instrumento de medição desenvolvido para avaliar a maturidade da organização nas dimensões propostas pelo modelo.

5.3.5 Método de avaliação: Construção e formatação do questionário inicial - Instrumento de Medição

Com os temas previamente definidos, deu-se início à construção do questionário. Para cada uma das cinco dimensões, foram estabelecidas 10 perguntas, representando os 10 temas principais de cada dimensão, totalizando 50 questões. Além disso, foi incluída uma pergunta aberta, permitindo que os especialistas sugerissem novas questões que considerassem relevantes e não haviam sido contempladas.

Cada questão foi estruturada da seguinte maneira: primeiro, o número identificador dentro de sua respectiva dimensão; seguido pelo enunciado da pergunta e pelos dispositivos normativos que a embasam, correlacionando a questão com as normas legais aplicáveis e destacando sua relevância jurídica. Após a apresentação dos dispositivos normativos, as alternativas de resposta foram disponibilizadas, permitindo aos respondentes avaliar as questões em uma escala de relevância. A seguir, um exemplo dessa estrutura:

Dimensão 1: Governança de Dados e Boas Práticas (cor cinza)

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (**art. 50 e art. 52, § 1º, inciso IX, da Lei n. 13.709/2018; Decreto n. 9.637/2018 e Decreto n. 10.046/2019 e ABNT NBR ISO/IEC 27014:2021**)

() 1

() 2

() 3

() 4

() 5

Todas as questões construídas estão disponíveis no **Apêndice E** deste trabalho. A modalidade escolhida para a aplicação do questionário foi on-line e a plataforma de desenvolvimento foi o QuestionPro.

O QuestionPro é uma plataforma de pesquisa online utilizada por empresas de todos os tamanhos, instituições acadêmicas e pesquisadores individuais. Ela possibilita a criação de diversos tipos de pesquisas e oferece um plano gratuito com recursos básicos, além de diversas opções pagas que proporcionam funcionalidades adicionais conforme as necessidades específicas dos usuários (Nascimento, 2019, p. 23).

Essa ferramenta é gratuita para usuários com o máximo de 10 pesquisas, sendo que as pesquisas não podem ultrapassar 200 respostas. A plataforma dispõe de versões pagas que abrangem mais configurações e possibilidades. Mesmo a ferramenta na versão gratuita disponibiliza diversas configurações para elaboração e análise do questionário, entre elas estão: mais de 25 tipos de perguntas diferentes, personalização de cores e interface, exportação de dados da pesquisa em formatos .xls e .csv, ramificação por lógica de respostas, dashboard de relatórios compartilhável, entre outras. Caso queira verificar como o questionário ficou após ser implementado no QuestionPro, basta acessar o **Apêndice F** deste trabalho. Esse questionário foi utilizado como instrumento preliminar para a primeira rodada do método *Delphi*, que é o método de avaliação utilizado no modelo de maturidade proposto.

5.3.6 Método de avaliação: Aplicação do Método *Delphi*

O método *Delphi* foi aplicado para reunir e sintetizar as opiniões de especialistas sobre a relevância das questões que compõem o instrumento de medição do modelo de maturidade para o tratamento de dados pessoais nas universidades federais brasileiras. Esse processo ocorreu em rodadas de avaliação, nas quais as contribuições dos especialistas foram analisadas e utilizadas para aprimorar o instrumento. Com o conteúdo e o questionário inicial construído, foram estabelecidos os critérios técnicos para cada rodada, começando pela avaliação inicial da relevância de cada questão em suas respectivas dimensões.

O objetivo da primeira rodada do método foi apresentar aos especialistas o questionário inicial, para que eles pudessem avaliar e selecionar as questões mais relevantes para cada dimensão, além de possibilitar sugestões de novas questões

que ainda não haviam sido contempladas. Nas rodadas seguintes, o objetivo foi refinar e classificar as questões que fariam parte do instrumento de medição do modelo proposto. Assim, os especialistas poderiam contribuir diretamente para a escolha das questões finais que seriam incluídas no instrumento de medição, bem como determinar o peso relativo de cada questão para a avaliação da capacidade organizacional nas dimensões estabelecidas para o modelo.

5.3.6.1 Validação do questionário antes de iniciar a primeira rodada

Antes do início da primeira rodada do método *Delphi*, foram realizadas algumas etapas importantes. Primeiramente, houve uma validação técnico-redacional do questionário, na qual dois especialistas em proteção de dados verificaram se as perguntas formuladas mantinham clareza e precisão técnica. Em seguida, foi realizada uma revisão linguística por um especialista em Língua Portuguesa, com o objetivo de assegurar a correção gramatical, a clareza textual e a correta adequação às normas vigentes. Por fim, foi feita uma análise funcional da ferramenta. Nesse contexto, vinte indivíduos selecionados aleatoriamente responderam ao questionário, avaliando todos os procedimentos de interação e o funcionamento da plataforma online onde o questionário está hospedado.

5.3.6.2 Critérios do *Delphi* para a primeira rodada

Na primeira rodada do método *Delphi*, os especialistas foram convidados a avaliar a relevância de cada questão em relação à dimensão correspondente, utilizando uma escala de Likert de 1 a 5, a qual indicava diferentes níveis de importância, conforme descrito a seguir:

- 1: Irrelevante para a dimensão;
- 2: Pouca relevância para a dimensão;
- 3: Relevante para a dimensão;
- 4: Muita relevância para a dimensão;
- 5: Total relevância para a dimensão.

O critério adotado para a seleção das questões foi a média aritmética simples das respostas. As cinco questões com as maiores médias em cada dimensão avançariam para a rodada seguinte. No entanto, em caso de empate na quinta posição, todas as questões empatadas seriam mantidas, garantindo que nenhuma questão com potencial relevância fosse descartada prematuramente. Além das

avaliações quantitativas, as sugestões qualitativas fornecidas pelos especialistas seriam analisadas e, quando pertinentes, incorporadas na próxima rodada, visando o aperfeiçoamento contínuo do questionário.

Outro aspecto crucial dessa etapa foi o rigor na seleção dos participantes. Especialistas que não aceitassem formalmente o Termo de Consentimento Livre e Esclarecido (TCLE) ou que apresentassem respostas incompletas seriam automaticamente excluídos, assegurando a integridade e a confiabilidade dos dados coletados.

5.3.6.3 Critérios do *Delphi* para as rodadas seguintes

A partir da segunda rodada, a avaliação das questões foi aprimorada com base nos valores de média aritmética simples, mediana e moda das respostas dos especialistas, os quais receberam *feedback* anônimo dos resultados da rodada anterior. Esse retorno permitiu uma análise mais robusta e fundamentada dos itens, favorecendo uma convergência gradual nas respostas.

Quadro 15 - Critérios de avaliação a partir da segunda rodada

Critério de Avaliação	Média	Mediana	Moda	Peso no Modelo
Alta Relevância	Superior a 4,5	Superior a 4,5	Igual a 5	Peso 5
Média Relevância	Entre 4 e 4,5	Entre 4 e 4,5	4 ou 5	Peso 3
Baixa Relevância	Inferior a 4	Inferior a 4	Inferior a 4	-

Fonte: elaborado pelo autor.

O processo de avaliação seria repetido em rodadas subsequentes até que, no mínimo, 25 questões fossem classificadas como de alta ou média relevância. As questões classificadas como de baixa relevância deveriam ser eliminadas, assegurando que o questionário final incluísse apenas itens de relevância significativa. As questões de alta relevância receberam um peso 5 no modelo, influenciando de forma mais decisiva o cálculo da maturidade organizacional, enquanto as de média relevância foram atribuídas peso 3. Com base nos resultados consolidados pelo método *Delphi*, ajustes no modelo de maturidade seriam implementados, garantindo sua representatividade e qualidade final.

5.3.6.4 Realização da primeira rodada do método *Delphi*

Após a submissão e aprovação da pesquisa pelo Comitê de Ética do Centro de Ciências da Saúde da UFPB, sob o número de protocolo 78884624.3.0000.5188,

em 18 de abril de 2024, iniciou-se a aplicação do método *Delphi*. O estudo abrangeu as 69 universidades federais brasileiras, que foram contactadas por meio da plataforma Fala.BR. Por essa plataforma, foi disponibilizado um *link* que direcionava tanto para o questionário quanto para o Termo de Consentimento Livre e Esclarecido (TCLE), ambos hospedados na QuestionPro.

O objetivo era engajar os encarregados de proteção de dados das instituições para que participassem como especialistas do método *Delphi*, sendo responsáveis pela seleção das questões que comporiam o instrumento de medição de um modelo de maturidade no tratamento de dados pessoais. O prazo para resposta foi estabelecido até 8 de maio de 2024, condicionado à formalização do consentimento dos encarregados em participar da pesquisa.

Das 69 universidades abordadas, 26 encarregados completaram o questionário na QuestionPro e submeteram suas respostas formalmente via Fala.BR, dentro do prazo estipulado. A Universidade Federal da Fronteira Sul (UFFS) contribuiu com duas respostas, pois possui dois encarregados distintos: um responsável pelos dados pessoais de servidores e outro pelos dados acadêmicos; ambos decidiram participar da pesquisa. Além disso, 21 instituições, embora sem resposta direta pelo Fala.BR, forneceram os contatos dos encarregados, permitindo o envio da solicitação por e-mail, ao considerar a demanda como subjetiva e discricionária e optando por não mantê-la via Fala.BR. Duas outras instituições solicitaram o questionário em formato PDF, e após recebê-lo, também decidiram fornecer o contato do encarregado para que o questionário fosse encaminhado diretamente. Entre os dias 23 e 25 de abril de 2024, 23 encarregados foram contatados por e-mail, contudo, apenas um respondeu ao questionário, o que reflete a baixa eficácia desse método de contato.

Seis instituições informaram que encaminharam o questionário ao encarregado de proteção de dados e, por se tratar de uma decisão discricionária, encerraram a demanda no Fala.BR. Dentre essas, dois encarregados participaram posteriormente, respondendo ao questionário. Outras sete instituições recusaram formalmente a solicitação, justificando-se com motivos como ausência de encarregado designado, greves de servidores ou recente nomeação de encarregado que se julgou despreparado para contribuir com a pesquisa. Adicionalmente, oito instituições solicitaram a extensão do prazo até 20 de maio de 2024. Dentre essas, seis responderam ao questionário, uma informou que o questionário havia sido

encaminhado ao encarregado, mas sem resposta, e a outra recusou a participação em razão de fortes chuvas no Rio Grande do Sul, que redirecionaram o encarregado a outras demandas. O Quadro 16 sintetiza as respostas positivas obtidas na primeira rodada do método *Delphi*:

Quadro 16 - Respostas positivas da aplicação do método *Delphi* na primeira rodada

Respostas Positivas	Quantidade
Formalmente via Fala.BR e dentro do prazo	26
Após encaminhamento pela instituição (via e-mail)	02
Envio direto aos e-mails fornecidos dos encarregados (fora do Fala.BR)	01
Formalmente via Fala.BR após prorrogação do prazo	06
Total	35

Fonte: elaborado pelo autor.

Apesar de 34 instituições terem participado (aproximadamente 49,27% das universidades abordadas), o total de respostas foi 35, considerando a situação específica da UFFS. O uso da plataforma Fala.BR se mostrou o meio mais eficiente para coleta de respostas, com sua política de resposta em até 20 dias e possibilidade de prorrogação única de 10 dias mediante justificativa. A aplicação do questionário na QuestionPro foi finalizada em 31 de maio de 2024.

Na plataforma QuestionPro, registraram-se 138 visualizações e 49 respostas, das quais 35 foram completas e 14 desistências. As desistências ocorreram por ausência de preenchimento do TCLE (três casos) e abandono do questionário sem resposta completa (11 casos). As respostas incompletas foram excluídas da análise. O relatório completo desta primeira rodada, gerado pela QuestionPro, encontra-se no **Apêndice G** deste trabalho.

Além do relatório da QuestionPro, foi produzido um documento com o *feedback* da primeira rodada do método *Delphi*. Esse relatório analisa a avaliação dos especialistas quanto à relevância das questões conforme os critérios determinados no item **5.3.6.2**, evidenciando um consenso em algumas questões e divergências em outras, o que orientou a exclusão de questões com baixa média aritmética nas dimensões. Sugestões adicionais também foram avaliadas e incorporadas quando pertinentes. As questões selecionadas para a segunda rodada foram as seguintes:

Quadro 17 - Questões para a segunda rodada do método Delphi

Questão	Questão	Média	Temas

na 1ª rodada	na 2ª rodada		
D1Q1	D1Q1	4,34	Programa ou Plano de Governança
D1Q2	D1Q2	4,6	Designação do Encarregado de Proteção de Dados
D1Q3	D1Q3	4,43	Comitê Interno para Tratamento de Dados e Informações Pessoais
D1Q6	D1Q4	4,23	Política de Privacidade, atualizado com a sugestão dos especialistas
D1Q7	D1Q5	4,14	Identificação de Compartilhamento e Transferência de Dados Pessoais
-	D1Q6	Sem nota	Princípio da segregação das funções, sugestão dos especialistas
D2Q1	D2Q1	4,14	Identificação das Categorias de Dados Pessoais e dos Titulares de Dados Pessoais
D2Q2	D2Q2	4,26	Identificação dos Agentes (operadores) de Tratamento de Dados Pessoais
D2Q4	D2Q3	4,11	Identificação dos Processos e Atividades Operacionais Relacionadas aos Dados Pessoais
D2Q8	D2Q4	4,14	Direitos dos Titulares de Dados Pessoais
D2Q10	D2Q5	4,14	Mascaramento, Pseudonimização ou Anonimização de Dados e Informações Pessoais
D3Q1	D3Q1	4,14	Programa ou Plano de Capacitação
D3Q2	D3Q2	4,17	Conscientização dos Agentes de Tratamento de Dados sobre seus Papéis e Responsabilidades
D3Q3	D3Q3	3,89	Treinamento e Capacitação dos Colaboradores (Terceirizados e Parceiros)
D3Q4	D3Q4	3,94	Capacitação Quanto aos Riscos Associados ao Tratamento Inadequado de Dados Pessoais
D3Q6	D3Q5	3,8	Capacitação Quanto aos Procedimentos Adequados para a Gestão de Incidentes
D4Q1	D4Q1	4,34	Política de Segurança da Informação, atualizado com a sugestão dos especialistas
D4Q3	D4Q2	4,23	Criptografia
D4Q4	D4Q3	4,2	Gestão de Backup e Trilhas de Auditoria
D4Q5	D4Q4	4,2	Inteligência de Ameaças e Gestão de Vulnerabilidades
D4Q6	D4Q5	4,49	Controle de Acesso e Autenticação Segura
D4Q8	D4Q6	4,23	Monitoramento e Controle de Eventos Associados à Violação e Vazamento de Dados Pessoais
D5Q1	D5Q1	4,29	Transparência
D5Q2	D5Q2	3,91	Política de Classificação da Informação
D5Q3	D5Q3	4,57	Publicização do Encarregado de Proteção de Dados
D5Q4	D5Q4	4,06	Publicização da Política de Privacidade
D5Q5	D5Q5	3,97	Procedimentos de Comunicação à ANPD e ao Titular de

			Dados em Caso de Ocorrência de Incidentes de Segurança
D5Q9	D5Q6	3,91	Programa ou Plano de Comunicação

Fonte: elaborado pelo autor.

Esse relatório completo pode ser consultado no **Apêndice H** deste estudo. O *feedback* orientou ajustes no questionário, marcando o início da segunda rodada, com foco em construir um modelo de maturidade alinhado às melhores práticas e legislações para o tratamento e proteção de dados pessoais nas universidades federais.

5.3.6.5 Realização da segunda rodada do método *Delphi*

Em 19 de junho de 2024, foi iniciada a segunda rodada do método *Delphi*, com o questionário enviado aos 35 encarregados das universidades federais brasileiras que participaram da primeira rodada. O mecanismo de contato foi novamente por meio da plataforma Fala.BR. O convite foi acompanhado de um relatório consolidado dos *feedbacks* anônimo dos resultados da rodada inicial. Conforme as diretrizes da plataforma, as instituições tiveram um prazo de 20 dias para enviar as respostas sobre a relevância das questões em cada dimensão, com o objetivo de refinar e consolidar o instrumento de acordo com os critérios estabelecidos no item **5.3.6.3** deste estudo. Dessa forma, o prazo final para envio foi fixado em 9 de julho de 2024.

No que diz respeito às respostas, 22 encarregados de proteção de dados completaram o questionário dentro do prazo estipulado. Quatro instituições forneceram o contato direto dos encarregados para o encaminhamento via e-mail, fora da plataforma Fala.BR, considerando que a colaboração nesta pesquisa era um ato discricionário. Esses encarregados foram contatados por e-mail em 3 de julho de 2024, e dois deles responderam o questionário.

Além disso, três instituições informaram que o questionário fora encaminhado ao encarregado de proteção de dados, mas, por ser um ato discricionário, o envio da demanda tornava-se finalizada a demanda na plataforma Fala.BR. Um desses encarregados respondeu logo após o término do prazo, e os outros dois foram contatados, novamente, por e-mail, em 3 de julho de 2024, dos quais um completou o questionário posteriormente.

Duas instituições recusaram formalmente o convite pela plataforma Fala.BR. Uma delas justificou a negativa com a exoneração do encarregado e a vacância da função; a outra indicou que o encarregado optou por não responder, desistindo

formalmente de participar. Por fim, quatro instituições solicitaram prorrogação do prazo na plataforma, estendendo-o até 19 de julho de 2024. Dois encarregados responderam dentro do prazo prorrogado, totalizando, ao final, 28 respostas positivas.

Quadro 18 - Respostas positivas da aplicação do método *Delphi* na segunda rodada

Respostas Positivas	Quantidade
Formalmente via Fala.BR e dentro do prazo	22
Após encaminhamento pela instituição (via e-mail)	02
Envio direto aos e-mails fornecidos dos encarregados (fora do Fala.BR)	02
Formalmente via Fala.BR após prorrogação do prazo	02
Total	28

Fonte: elaborado pelo autor.

Ao final, 28 respostas completas foram recebidas, correspondendo a aproximadamente 82% das instituições contatadas. O questionário, elaborado e disponibilizado na plataforma QuestionPro, foi encerrado em 20 de julho de 2024, com 109 visualizações e 32 respostas totais, das quais 28 completas e 4 desistências. As desistências ocorreram por ausência de preenchimento do Termo de Consentimento Livre e Esclarecido (TCLE) ou abandono do questionário sem completá-lo. Conforme previsto, respostas incompletas foram excluídas da análise.

Nesta segunda rodada, o questionário apresentou exclusivamente questões fechadas, como recomendado pela metodologia *Delphi* e conforme os critérios previamente definidos, uma vez que a oportunidade de sugerir novas questões já fora dada a todos os participantes na primeira rodada. O relatório de *feedback* da primeira rodada (**Apêndice H**) registrou as 28 questões que avançaram nesta fase, e o questionário para segunda rodada, produzido no QuestionPro, está disponível no **Apêndice I** deste estudo. Essas questões incluíram as cinco mais bem avaliadas de cada dimensão, questões adicionais propostas e as que apresentaram médias aritméticas iguais à quinta colocada, conforme os critérios estabelecidos.

A seleção e classificação das questões mais relevantes nesta rodada consideraram os valores de média aritmética, moda e mediana, de acordo com o item **5.3.6.3**. A relevância das questões foi classificada como baixa, média ou alta,

de acordo com esses indicadores. O resultado final das 28 questões está apresentado a seguir:

Quadro 19 - Resultado da avaliação e classificação das questões

Dimensão/Questão	Média	Moda	Mediana	DP	Classificação	Peso
D1Q2	4,79	5	5	0,50	Alta	5
D4Q1	4,61	5	5	0,63	Alta	5
D5Q3	4,54	5	5	0,79	Alta	5
D1Q3	4,54	5	5	0,69	Alta	5
D1Q4	4,50	5	5	0,75	Alta	5
D4Q5	4,43	5	5	0,74	Média	3
D4Q6	4,39	5	5	0,79	Média	3
D5Q4	4,32	5	5	0,82	Média	3
D4Q2	4,32	5	5	0,86	Média	3
D2Q5	4,32	5	5	0,98	Média	3
D2Q3	4,32	5	5	0,98	Média	3
D2Q1	4,32	5	5	1,02	Média	3
D4Q3	4,32	5	4,5	0,77	Média	3
D2Q2	4,29	5	5	0,94	Média	3
D5Q1	4,25	5	5	1,14	Média	3
D1Q6	4,25	5	5	1,08	Média	3
D3Q2	4,25	5	4,5	0,89	Média	3
D1Q1	4,21	5	5	1,07	Média	3
D4Q4	4,21	5	4	0,88	Média	3
D5Q2	4,18	5	4,5	0,98	Média	3
D2Q4	4,14	5	4,5	0,97	Média	3
D3Q1	4,14	5	4	1,04	Média	3
D3Q4	4,04	5	4	1,10	Média	3
D3Q3	4,04	5	4	1,07	Média	3
D1Q5	4,04	5	4	1,10	Média	3
D5Q5	3,96	5	4	1,07	Baixa	1
D3Q5	3,96	5	4	1,04	Baixa	1
D5Q6	3,89	5	4	1,07	Baixa	1

Fonte: elaborado pelo autor

O relatório completo de *feedback* da segunda rodada encontra-se no **Apêndice J**, enquanto o relatório produzido automaticamente pela QuestionPro desta rodada está disponível no **Apêndice K**. As rodadas do método *Delphi* foram planejadas com o objetivo de refinar o instrumento até que fossem alcançadas 25

questões classificadas com relevância alta ou média, sendo que as de alta relevância receberam peso 5 no cálculo da maturidade, conferindo-lhes maior impacto no modelo proposto. Como nesta rodada consolidaram-se as 25 questões de relevância desejada, o relatório da segunda rodada foi considerado o documento final do método *Delphi* (**Apêndice J**). Assim, o instrumento de medição tornou-se apto para aplicação, estabelecendo uma base sólida para a avaliação da maturidade das instituições no tratamento e proteção de dados pessoais, além de oferecer subsídios para o aprimoramento contínuo das práticas institucionais nessa área.

5.3.6.6 Encerramento do *Delphi* e consolidação do instrumento de medição

A partir dos resultados obtidos na segunda rodada, foram realizados ajustes essenciais para garantir a representatividade e a qualidade do instrumento de medição do modelo, conforme os critérios preestabelecidos para a aplicação do método *Delphi*. Segundo a teoria do método, o processo é finalizado quando as rodadas de feedback e refinamento atingem um ponto de consenso satisfatório entre os especialistas, assegurando que as respostas refletem com precisão os objetivos de análise. Nesse sentido, a segunda rodada foi considerada a etapa final do processo, visto que todos os objetivos e critérios previamente definidos foram plenamente alcançados, consolidando os pontos de alta e média relevância no instrumento de medição.

Com a conclusão dessa etapa, o instrumento foi devidamente refinado e consolidado, tornando-se plenamente apto para avaliar a maturidade das organizações no tratamento e proteção de dados pessoais. A aplicação criteriosa do método *Delphi* proporcionou valiosos insights, que não apenas orientaram o aprimoramento contínuo das práticas institucionais de governança de dados, mas também estabeleceram uma base sólida para futuras iniciativas no campo do tratamento e proteção de dados pessoais. O instrumento final do MMTDP encontra-se disponível para consulta no **Apêndice L** deste trabalho.

5.3.6.7 Refinamento do instrumento

As rodadas do método *Delphi* desempenharam um papel crucial não apenas na avaliação da relevância das questões, mas também na incorporação das sugestões dos especialistas, permitindo ajustes significativos que contribuíram para o refinamento contínuo do instrumento de medição. Essa dinâmica favoreceu a

consolidação do modelo, ao mesmo tempo em que proporcionou *insights* valiosos para o aprimoramento das práticas relacionadas ao tratamento e à proteção de dados pessoais nas universidades federais brasileiras.

5.3.7 Mecanismo de medição do Modelo de Maturidade para Tratamento de Dados Pessoais

O mecanismo de medição em um modelo de maturidade é uma ferramenta essencial para quantificar o nível de desenvolvimento de uma organização em relação a critérios predefinidos. No âmbito do MMTDP, este mecanismo utiliza um questionário estruturado para avaliar a conformidade com requisitos legais, normativos e melhores práticas no tratamento de dados pessoais nas universidades federais brasileiras. Essa abordagem fornece uma visão clara do estágio de maturidade da organização, facilitando a identificação de áreas bem administradas e daquelas que requerem aprimoramento e monitoramento.

5.3.7.1 Estrutura do Instrumento de Medição

O instrumento de medição é um questionário que abrange cinco dimensões:

- Governança de Dados e Boas Práticas (cor cinza)
- Políticas e Processos de Tratamento de Dados (cor amarela)
- Treinamento e Conscientização (cor azul)
- Segurança da Informação e Tecnologia (cor verde)
- Acesso à Informação e Transparência (cor vermelha)

Os níveis de maturidade variam de ausência de implementação até práticas exemplares e monitoradas, categorizados em:

1. Nível Inicial
2. Nível Emergente
3. Nível Intermediário
4. Nível Avançado
5. Nível Exemplar

5.3.7.2 Escala de Avaliação

A escala de avaliação identifica pontos fortes e áreas para melhorias, proporcionando uma compreensão abrangente do estágio atual da organização.

Cada item do questionário é avaliado utilizando uma escala Likert de 1 a 5. De forma geral, as respostas podem ser interpretadas assim:

1. **Não implementado:** ausência total da prática ou política; a organização desconhece sua importância.
2. **Implementação inicial:** implementação parcial, informal e inconsistente; a prática não é sistemática.
3. **Implementado parcialmente:** implementação estruturada, abrangendo as áreas principais, mas ainda com lacunas.
4. **Implementado de forma eficaz, mas não monitorado:** implementação consistente e abrangente, mas sem monitoramento contínuo.
5. **Implementado com excelência:** implementação rigorosa e contínua, com monitoramento e revisões regulares.

Contudo, essa interpretação será adaptada para refletir de maneira mais clara e precisa a temática abordada em cada questão do questionário. Essa personalização garante que a escala seja alinhada às particularidades do assunto avaliado, facilitando a análise e a compreensão do nível de implementação das práticas ou políticas investigadas.

5.3.7.3 Ponderação das Questões

As questões são ponderadas conforme sua relevância, usando os critérios estabelecidos no método *Delphi*. Questões de alta relevância têm um peso maior, enquanto as de média relevância têm peso menor. Neste modelo, não foram incluídas questões classificadas como de baixa relevância. A distribuição de pesos ficou a seguinte:

- **Alta Relevância:** Peso 5.0
- **Média Relevância:** Peso 3.0

5.3.7.4 Cálculo da Maturidade nas dimensões

O cálculo do nível de maturidade da organização em cada dimensão é realizado através dos seguintes passos:

- **Pontuação Bruta:** soma das pontuações das questões respondidas na dimensão, considerando a ponderação de cada questão.
- **Pontuação Máxima Possível:** soma máxima possível para a dimensão.

- **Pontuação Normalizada:** convertida para uma escala de 0 a 100 pela fórmula:

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

Exemplo: Se a pontuação bruta é 80 e a pontuação máxima é 100, a pontuação normalizada será 80.

Para calcular as maturidades das dimensões no modelo proposto, é fundamental determinar a pontuação máxima possível de cada dimensão, levando em conta as ponderações definidas para cada questão. A seguir, é apresentado o cálculo da pontuação máxima para cada dimensão:

Pontuação Máxima para a Dimensão 1 - Governança de Dados e Boas Práticas (cor cinza) - Esta dimensão contém três perguntas de alta relevância e três perguntas de média relevância, representando a seguinte equação:

$Q1*3 + Q2*5 + Q3*5 + Q4*5 + Q5*3 + Q6*3$. Para calcular a pontuação máxima, consideramos a maior nota possível em todas as questões, resultando em: $(5*3) + (5*5) + (5*5) + (5*5) + (5*3) + (5*3) = 15 + 25 + 25 + 25 + 15 + 15 = 120$ pontos.

Pontuação Máxima para a Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela) - Esta dimensão não possui perguntas de alta relevância, mas contém cinco perguntas de média relevância, o que representa a seguinte equação: $Q7*3 + Q8*3 + Q9*3 + Q10*3 + Q11*3$. Assim, a pontuação máxima será: $(5*3) + (5*3) + (5*3) + (5*3) + (5*3) = 15 + 15 + 15 + 15 + 15 = 75$ pontos.

Pontuação Máxima para a Dimensão 3: Treinamento e Conscientização (cor azul) - Esta dimensão não possui perguntas de alta relevância, mas contém quatro perguntas de média relevância, representadas pela equação: $Q12*3 + Q13*3 + Q14*3 + Q15*3$. A pontuação máxima será: $(5*3) + (5*3) + (5*3) + (5*3) = 15 + 15 + 15 + 15 = 60$ pontos.

Pontuação Máxima para a Dimensão 4: Segurança da Informação e Tecnologia (cor verde) - Esta dimensão contém uma pergunta de alta relevância e cinco perguntas de média relevância, representando a seguinte equação: $Q16*5 + Q17*3 + Q18*3 + Q19*3 + Q20*3 + Q21*3$. A pontuação máxima será: $(5*5) + (5*3) + (5*3) + (5*3) + (5*3) + (5*3) = 25 + 15 + 15 + 15 + 15 + 15 = 100$ pontos.

Pontuação Máxima para a Dimensão 5: Acesso à Informação e Transparência (cor vermelha) - Esta dimensão contém uma pergunta de alta relevância e três perguntas de média relevância, representando a seguinte equação: $Q22*3 + Q23*3 + Q24*5 + Q25*3$. A pontuação máxima será: $(5*3) + (5*3) + (5*5) + (5*3) = 15 + 15 + 25 + 15 = 70$ pontos.

Para facilitar o cálculo das maturidades foi criado um quadro para facilitar a visualização da pontuação máxima de cada dimensão do MMTDP.

Quadro 20 - Resultado da avaliação e classificação das questões

Dimensão	Pontuação máxima
Dimensão 1	120 pontos
Dimensão 2	75 pontos
Dimensão 3	60 pontos
Dimensão 4	100 pontos
Dimensão 5	70 pontos

Fonte: elaborado pelo autor.

5.3.7.5 Classificação no Nível de Maturidade:

A pontuação normalizada é então comparada com os intervalos predefinidos para determinar o nível de maturidade.

Quadro 21 - Classificação da maturidade

Intervalo de Pontuação	Nível de Maturidade
00 - 25	Inicial
26 - 45	Emergente
46 - 70	Intermediário

71 - 90	Avançado
91 - 100	Exemplar

Fonte: elaborado pelo autor.

Para melhor compreensão, vamos ilustrar um exemplo do cálculo da maturidade em uma organização na Dimensão 1. Suponha que a Organização A respondeu às questões da dimensão 1 da escala de avaliação da seguinte forma: Q1 = 2, Q2 = 5, Q3 = 5, Q4 = 1, Q5 = 2 e Q6 = 4. A pontuação bruta é obtida multiplicando a resposta pelo peso de cada questão, conforme segue: $(2 \times 3) + (5 \times 5) + (5 \times 5) + (1 \times 5) + (2 \times 3) + (4 \times 3) = 6 + 25 + 25 + 5 + 6 + 12 = 79$ pontos.

A pontuação máxima possível na Dimensão 1 é 120 pontos. Para calcular a pontuação normalizada, aplicamos a fórmula:

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

Substituindo os valores, temos:

$$\text{Pontuação Normalizada} = \left(\frac{79}{120} \right) \times 100$$

$$\text{Pontuação Normalizada} \approx 65,83$$

Assim, a pontuação normalizada da Organização A na Dimensão 1 é aproximadamente 65,83.

A pontuação normalizada da Organização A, que resultou em aproximadamente 65,83, é então comparada com os intervalos predefinidos para a determinação do nível de maturidade. Como a pontuação da Organização A se encontra entre 46 e 70, podemos classificar sua maturidade na dimensão 1 como Intermediário. Essa avaliação indica que a organização demonstra um nível considerável de maturidade nas práticas relacionadas a essa dimensão específica.

5.3.7.4 Cálculo da Maturidade Global

A maturidade global da organização é a média aritmética das pontuações normalizadas de todas as dimensões.

$$\text{Pontuação Global} = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

PND = Pontuação normalizada da Dimensão

Para melhor compreensão, vamos ilustrar um exemplo do cálculo da maturidade global em uma organização. Suponha que a Organização A teve as seguintes pontuações normalizadas em suas dimensões: D1 = 65,83; D2 = 36; D3 = 30; D4 = 62 e D5 = 65,71.

Como são 5 dimensões neste modelo. Para calcular a pontuação Global, aplicamos a fórmula:

$$\text{Pontuação Global} = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

Substituindo os valores, temos:

$$\text{Pontuação Global} = \left(\frac{65,83 + 36 + 30 + 62 + 65,71}{5} \right)$$

$$\text{Pontuação Global} \approx 54,59$$

Assim, a pontuação global da Organização A é de aproximadamente 54,59.

A pontuação global da Organização A, que resultou em aproximadamente 54,59, é então comparada com os intervalos predefinidos para a determinação do nível de maturidade. Como a pontuação da Organização A se encontra entre 46 e 70, podemos classificar o nível de maturidade global como Intermediário.

O nível “Intermediário” indica que a organização possui uma base para o tratamento de dados, mas ainda precisa aprimorar práticas para alcançar níveis mais elevados de maturidade. No detalhamento das dimensões, a organização mostra progresso significativo em Governança e Segurança da Informação, enquanto em Políticas, Treinamento e Conscientização, há áreas que necessitam de desenvolvimento para garantir conformidade mais ampla e eficaz.

5.3.7.5. Relatório de análises e resultados

O processo de avaliação pode culminar em um relatório detalhado que inclua diversas análises, entre as quais destacam-se:

- Pontuação normalizada em cada dimensão, acompanhada do respectivo nível de maturidade.
- Pontuação global da organização, com o correspondente nível de maturidade.
- Recomendações de melhoria para cada dimensão, com ênfase nas práticas que precisam ser aprimoradas para que a organização avance para níveis mais elevados de maturidade.
- Comparativo regional, apresentando pontuações e classificações por estado, região ou país, incluindo um benchmarking adequado para cada contexto.
- Comparativo temporal (quando aplicável), demonstrando a evolução da organização ao longo de diferentes ciclos de avaliação.
- Outras análises que possibilitem uma compreensão mais aprofundada dos resultados.

5.3.7.6 Validação e Revisão Periódica

A eficácia do instrumento de medição deve ser avaliada e aprimorada regularmente, especialmente em resposta a mudanças legais, novas demandas e necessidades identificadas, de modo a garantir que o modelo permaneça alinhado aos resultados obtidos. Revisões periódicas são fundamentais para assegurar que o modelo reflita as melhores práticas e acompanhe as mudanças regulatórias no tratamento de dados pessoais.

Esse mecanismo de medição proporciona uma forma estruturada e objetiva de avaliar a maturidade das organizações no tratamento de dados pessoais, promovendo o alinhamento com exigências legais, além de expectativas éticas e boas práticas.

5.4 Testar e Implementar

Em 9 de setembro de 2024, todas as 69 universidades federais brasileiras foram formalmente contatadas via plataforma Fala.BR com uma solicitação referente à aplicação do teste piloto do Modelo de Maturidade para Tratamento de Dados Pessoais. O prazo para resposta foi estabelecido até o dia 30 de setembro de 2024, com uma possível extensão permitida até 10 de outubro de 2024. Durante esse período as respostas das instituições foram divididas da seguinte forma:

No prazo: 47 universidades responderam ao questionário dentro do prazo inicial determinado. Dentre estas, quatro instituições recusaram-se a participar. Em

resposta, esclarecemos a importância para a instituição e informamos que qualquer profissional com conhecimento abrangente sobre a instituição ou uma equipe com esse conhecimento holístico estaria apta a preencher o questionário de forma representativa. Após esta intervenção, duas das quatro instituições reconsideraram e resolveram participar; as outras duas mantiveram a negativa. Portanto, ao final do período estipulado, 45 instituições responderam o questionário e 2 recusaram formalmente.

Prorrogação do Prazo: Um total de 22 universidades solicitou prorrogação do prazo, alegando necessidade de mais tempo para concluir o questionário. Assim, duas instituições recusaram-se a participar durante esse período, e as demais responderam até o dia 10 de outubro de 2024. Em resposta às duas negativas, recorremos e esclarecemos a importância para a instituição e informamos que qualquer profissional com conhecimento abrangente sobre a instituição ou uma equipe com esse conhecimento holístico estaria apta a preencher o questionário de forma representativa. A UFAL, uma dessas duas instituições, chegou a abrir um processo interno no intuito de tratar desta solicitação, mas não conseguiu finalizar a resposta até o prazo e nem quis enviar a posteriori. Já a UFRRJ, por exemplo, finalizou em 24 de outubro de 2024, mesmo fora do prazo limite (10 de outubro de 2024) ainda foi incluída sua análise nesse trabalho.

Assim, 66 instituições participaram da pesquisa, representando cerca de 95,65% das universidades convidadas. O instrumento de medição do MMTDP foi elaborado e disponibilizado por meio da plataforma QuestionPro, com conclusão oficial em 10 de outubro de 2024. Contudo, a resposta adicional da UFRRJ foi excepcionalmente aceita fora do prazo estabelecido.

Entre as respostas recebidas, cinco instituições preencheram o questionário de maneira incompleta, o que impediu uma análise integral de algumas dimensões, impossibilitando, assim, a classificação da maturidade dessas dimensões e, consequentemente, a análise global dessas instituições. As instituições com essas limitações de análise foram: a FURG, que não respondeu às questões da Dimensão 4; a UFDPAR, que deixou em branco uma questão da Dimensão 2 e outra da Dimensão 4; a UFJF, que não respondeu a uma questão da Dimensão 4; a UFNT, que omitiu uma da Dimensão 4; e a UFRJ, que respondeu apenas duas das cinco questões da Dimensão 4. Essas omissões restringiram a análise global dessas

instituições, limitando-a às análises apenas das dimensões completamente respondidas.

Para as demais instituições que preencheram integralmente o instrumento, foi realizada a análise do instrumento de medição do MMTDP, permitindo a classificação de maturidade de cada dimensão e a elaboração de uma análise global de cada instituição. As classificações obtidas, assim como as comparações entre os resultados, podem ser observadas na **Seção 6**.

Além da análise e do cálculo da maturidade, realizados de acordo com as diretrizes dos itens **5.3.7.4** a **5.3.7.6** deste trabalho, foi conduzida uma análise qualitativa das capacidades institucionais de algumas das instituições, fundamentada nas respostas ao instrumento de medição. Para facilitar essa análise, desenvolveu-se uma base de dados destinada a aprimorar a compreensão, identificação e descrição dos posicionamentos institucionais a partir das respostas fornecidas no instrumento de medição do MMTDP. Essa base estabelece um padrão de análises e recomendações para cada resposta possível, funcionando como suporte para a composição da análise final de cada dimensão e, posteriormente, para a análise global das instituições.

Essa base estabelece um padrão de análises e recomendações para cada resposta possível, servindo como suporte para a composição da análise final de cada dimensão e, posteriormente, da análise holística das instituições. A seguir, são apresentadas, a título de exemplo, as análises e recomendações padronizadas para cada resposta da primeira questão do instrumento.

Questão 1: A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei n. 13.709/2018; Decreto n. 9.637/2018 e Decreto n. 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

Resposta 1:

"Não, a organização ainda não elaborou um programa, plano de governança ou documento com esse direcionamento."

Análise: A ausência de um programa de governança para dados pessoais representa uma lacuna crítica em termos de conformidade, expondo a organização a riscos regulatórios e operacionais significativos. Sem um documento que defina responsabilidades, políticas e processos para o tratamento de dados, a organização não possui mecanismos adequados para assegurar que suas práticas estejam alinhadas às normativas relevantes, como a LGPD (Lei n. 13.709/2018) e o Decreto n. 10.046/2019.

Recomendação para avanço ao Nível 2: Recomenda-se iniciar o desenvolvimento de um

programa de governança que identifique os principais riscos e requisitos legais da organização. Esse programa deve ser construído em parceria com a alta administração e o DPO, com um plano de ação de curto prazo que contemple a criação de políticas iniciais e procedimentos de conformidade.

Resposta 2:

"Sim, a organização está em fase inicial de elaboração do programa, plano de governança ou documento equivalente com esse direcionamento."

Análise: A fase inicial de elaboração demonstra um progresso, mas a falta de um programa estruturado limita a efetividade das práticas de governança. Embora a intenção de conformidade esteja presente, a ausência de um planejamento concreto dificulta a implementação eficaz das políticas e procedimentos, como exigido pela LGPD (Lei n. 13.709/2018) e pela ABNT NBR ISO/IEC 27014:2021.

Recomendação para avanço ao Nível 3: É necessário desenvolver um cronograma claro para a conclusão do programa, especificando os responsáveis e as áreas prioritárias. A organização também deve assegurar que o programa aborda as normas e boas práticas principais, sendo disseminado entre líderes e setores-chave para garantir adesão.

Resposta 3:

"Sim, a organização já elaborou um programa, plano de governança ou documento equivalente com esse direcionamento, mas este ainda não foi totalmente implementado."

Análise: A elaboração do programa representa um avanço significativo. Entretanto, a implementação parcial reduz a eficácia e compromete a credibilidade do compromisso com a proteção de dados. A organização possui uma base sólida que necessita de formalização e internalização para garantir alinhamento total com as normativas, em especial a LGPD e o Decreto n. 10.046/2019.

Recomendação para avanço ao Nível 4: Para evoluir, a organização deve estabelecer um plano de implementação com etapas e prazos definidos. Recomenda-se que o processo seja monitorado por um comitê de governança de dados, responsável por avaliar o progresso e assegurar que as práticas e políticas estabelecidas sejam seguidas.

Resposta 4:

"Sim, a organização elaborou e implementou o programa, plano de governança ou documento equivalente com esse direcionamento, mas este documento não é monitorado regularmente."

Análise: A implementação do programa demonstra comprometimento com a conformidade, mas a ausência de monitoramento contínuo compromete a atualização e sustentabilidade das práticas de proteção de dados. A conformidade regular com a LGPD e a ABNT NBR ISO/IEC 27701:2019 exige monitoramento para garantir eficácia e adaptação a novas exigências.

Recomendação para avanço ao Nível 5: A organização deve implementar mecanismos de monitoramento contínuos, como auditorias e revisões de compliance, para assegurar a atualização do programa conforme as legislações e normas aplicáveis. Isso garantirá a adequação contínua às regulamentações e reduzirá riscos.

Resposta 5:

"Sim, a organização elaborou e implementou completamente o programa, plano de governança ou documento equivalente com esse direcionamento, e está monitorando regularmente para garantir a conformidade contínua com as regulamentações sobre tratamento e proteção de dados pessoais."

Análise: Esse nível representa uma maturidade elevada e alinhamento completo com as melhores práticas e requisitos normativos, como exigido pela LGPD e pelas normas ISO/IEC 27701:2019 e 27014:2021. A implementação integral e o monitoramento contínuo garantem que o programa de governança é adaptável a mudanças legais e tecnológicas, promovendo uma proteção eficaz dos dados pessoais.

Recomendação para manutenção: Para manter esse nível de maturidade, a organização deve investir em atualizações regulares do programa, considerando as mudanças legislativas e os avanços tecnológicos. Revisões e treinamentos periódicos também são essenciais para manter o comprometimento dos colaboradores e a eficácia do programa.

As demais análises e recomendações padronizadas podem ser consultadas no **Apêndice M** deste trabalho. Essas diretrizes foram desenvolvidas considerando que as universidades federais compartilham missões e visões institucionais similares, além de estarem sujeitas às mesmas legislações e normas. Embora se reconheça a existência de particularidades em cada instituição, a padronização dessas orientações proporciona um ponto de partida estruturado para a análise de cada contexto específico, assegurando uniformidade no tratamento de questões essenciais e recorrentes. Dessa forma, essa base funciona apenas como um suporte, permitindo adaptações que atendam às necessidades e características próprias de cada universidade.

A aplicação prática do modelo permitiu identificar fragilidades que resultaram em oportunidades de aprimoramento. Por exemplo, foram detectadas interdependências entre questões específicas do instrumento que deveriam ter sido previamente reconhecidas para ajustes nas opções de resposta. Observou-se que as questões 6 e 24 dependem diretamente da questão 2, enquanto a questão 25 está vinculada à questão 4. Para sanar essas lacunas, sugere-se incluir a opção "não aplicável" para questões dependentes, sem prejudicar a coerência ou o significado original das respostas. Tais modificações visam aumentar a precisão da avaliação, garantindo que as respostas reflitam com fidelidade a realidade institucional.

Quadro 22 - Ajustes no instrumento de medição do MMTDP

Questão	Resposta	Onde se lê	Leia-se
6	1	"Não, a organização não segue o princípio da segregação das funções, e o Encarregado de Proteção de Dados (EPD) acumula funções que claramente geram conflitos de interesse."	"Não, a organização não segue o princípio da segregação de funções, e o Encarregado de Proteção de Dados (EPD), caso designado, acumula funções que claramente geram conflitos de interesse. Caso a organização não tenha designado o EPD, essa alternativa será considerada 'não aplicável' e equiparada à alternativa de resposta 'não implementado', visto que descumpre um requisito legal."

24	1	"Não, a organização não publiciza a designação do encarregado de proteção de dados nem suas informações de contato."	"Não, a organização não publiciza a designação do Encarregado de Proteção de Dados (EPD) nem suas informações de contato. Caso não exista a designação do EPD, essa questão, embora classificada como 'não aplicável', será tratada como equivalente a 'não implementado', indicando o descumprimento do artigo 41, § 1º da LGPD."
25	1	"Não, a organização não publiciza sua Política de Privacidade."	"Não, a organização não publiciza sua Política de Privacidade. Caso a organização não tenha formalizado ou elaborado uma Política de Privacidade, essa alternativa será considerada 'não aplicável', sendo tratada como equivalente à alternativa 'não implementada', indicando a ausência dessa prática fundamental."

Fonte: elaborado pelo autor.

Dado o caráter mandatário das obrigações, conclui-se que respostas classificadas como "não aplicável" devem ser tratadas como equivalentes à resposta "1" (não implementado). Essa abordagem evidencia a ausência de práticas ou políticas associadas e o desconhecimento sobre a relevância do tema, reforçando a gravidade do descumprimento de itens legalmente obrigatórios.

Outra fragilidade identificada foi a existência de inconsistências em algumas respostas, divergentes da realidade institucional. Por ser funcionário de uma das instituições avaliadas, o pesquisador conseguiu reconhecer tais discrepâncias. Entretanto, é imprescindível que os respondentes compreendam que o propósito central do modelo é promover a melhoria contínua da instituição, eliminando inconsistências e identificando oportunidades de aprimoramento.

Diante do surpreendente número de 66 instituições que preencheram o instrumento de medição deste modelo, representando aproximadamente 95,65% das universidades convidadas, um resultado que supera as expectativas. Considerando o tempo necessário para analisar detalhadamente os resultados qualitativos de cada instituição, foi necessário limitar o escopo desta etapa da pesquisa, a fim de garantir sua conclusão dentro do prazo estipulado.

Dessa forma, foram selecionadas quatro instituições com classificações globais distintas, com o objetivo de representar diferentes cenários, conforme os níveis variados de maturidade identificados no MMTDP. Na **Seção 6**, apresentam-se os resultados gerais obtidos, juntamente com a análise detalhada dessas quatro

instituições, bem como as inferências extraídas desse processo, explorando cada uma delas de forma aprofundada.

6 ANÁLISES E RESULTADOS

O Modelo de Maturidade para Tratamento de Dados Pessoais é uma ferramenta que oferece uma avaliação abrangente e detalhada das capacidades institucionais relacionadas ao tratamento de dados pessoais. Com abordagens adaptáveis, o modelo permite tanto análises segmentadas quanto uma visão holística da conformidade e da eficácia das políticas e processos institucionais nessa área. Dessa forma, ele facilita a identificação de oportunidades de melhoria e o planejamento de ações específicas, promovendo uma evolução contínua e o alcance de níveis cada vez mais elevados de maturidade, assegurando boas práticas e a proteção efetiva dos dados pessoais sob gestão institucional.

A aplicação desse modelo em uma universidade federal, por exemplo, possibilita uma avaliação completa do estágio de desenvolvimento institucional na implementação de políticas e práticas adequadas para o tratamento de dados pessoais, em conformidade com as legislações e normas vigentes. O instrumento de medição do modelo é composto por 25 questões, distribuídas em cinco dimensões, conforme detalhado a seguir.

Quadro 23 - Questões do instrumento de medição que envolve cada dimensão

Dimensão	Questões do Instrumento
Dimensão 1: Governança de Dados e Boas Práticas	Questões 1-6
Dimensão 2: Políticas e Processos de Tratamento de Dados	Questões 7-11
Dimensão 3: Treinamento e Conscientização	Questões 12-15
Dimensão 4: Segurança da Informação e Tecnologia	Questões 16-21
Dimensão 5: Acesso à Informação e Transparência	Questões 22-25

Fonte: elaborado pelo autor.

Estruturado em cinco dimensões-chave, o MMTDP oferece diversas possibilidades analíticas, permitindo a avaliação da maturidade de cada dimensão tanto de forma individual quanto integrada. Além disso, possibilita análises comparativas em contextos nacional e regional, contribuindo para a identificação do posicionamento da instituição nesse cenário e para a detecção de oportunidades de melhoria. Dessa maneira, o modelo favorece o ajuste de planejamentos institucionais, promovendo o avanço contínuo no tratamento de dados pessoais.

6.1 Tipos de análises do MMTDP

O processo de análise do Modelo de Maturidade para Tratamento de Dados Pessoais oferece diversas abordagens que permitem à instituição avaliar, de maneira abrangente e detalhada, suas capacidades no tratamento de dados pessoais. Essas análises estão organizadas em duas categorias principais: a análise institucional, que se concentra nos aspectos internos da organização, podendo ser realizada de forma segmentada, com foco em dimensões específicas, ou de maneira global; e a análise comparativa, que fornece uma perspectiva externa ao posicionar a instituição em relação a outras organizações.

Cada tipo de análise desempenha um papel essencial no direcionamento de ações estratégicas e no aprimoramento contínuo, evidenciando áreas de excelência e identificando lacunas a serem superadas para alcançar elevados padrões de maturidade e conformidade. A seguir, detalham-se os principais aspectos dessas análises.

6.1.1 Análise Institucional

A análise institucional do nível de maturidade no tratamento de dados pessoais pode ser realizada de duas maneiras: por dimensão, em que cada aspecto específico da gestão é avaliado de forma segmentada, ou de forma global, adotando uma perspectiva holística que considera o desempenho geral da instituição. Essas abordagens são complementares, proporcionando *insights* distintos e valiosos para subsidiar decisões estratégicas.

Enquanto a análise por dimensão possibilita a identificação de pontos fortes e fragilidades em áreas específicas, a análise global fornece uma visão panorâmica, essencial para compreender o alinhamento geral da instituição com padrões de excelência e conformidade legal. A seguir, são apresentados os detalhes dessas abordagens.

6.1.1.1 Análise por dimensão

A análise institucional por dimensão permite uma avaliação minuciosa da instituição em cada um dos aspectos que compõem o tratamento de dados pessoais. No modelo proposto, as dimensões avaliadas incluem: Governança de Dados e Boas Práticas, Políticas e Processos de Tratamento de Dados, Treinamento

e Conscientização, Segurança da Informação e Tecnologia e Acesso à Informação e Transparência.

Essa abordagem segmentada viabiliza a análise de cada dimensão com base em critérios e indicadores específicos, que atribuem uma pontuação refletindo o nível de maturidade alcançado em cada área. Dessa forma, a instituição pode identificar, com precisão, suas fortalezas e fragilidades, direcionando esforços de maneira eficiente. A análise por dimensão apresenta diversas vantagens:

- **Identificação de Pontos de Atenção:** Dimensões com pontuações baixas ou que apresentam maior impacto na segurança e conformidade devem ser priorizadas para a alocação de recursos e esforços.
- **Planejamento Direcionado:** A instituição pode desenvolver planos de ação específicos, como revisar políticas, fortalecer a segurança tecnológica ou investir em treinamentos especializados.
- **Monitoramento Evolutivo:** A avaliação contínua por dimensão facilita o acompanhamento do progresso, possibilitando ajustes constantes nos planos de ação e assegurando a conformidade com as exigências normativas.

Além disso, essa abordagem permite comparações ao longo do tempo, evidenciando avanços ou áreas que demandam maior atenção. A segmentação proporciona também a possibilidade de analisar os resultados em contextos específicos, contribuindo para a tomada de decisões mais fundamentadas e alinhadas às necessidades institucionais.

6.1.1.2 Análise global ou holística

A análise global ou holística adota uma perspectiva abrangente ao avaliar o desempenho integrado de todas as dimensões do tratamento de dados pessoais. Essa abordagem proporciona uma visão consolidada da maturidade institucional, permitindo identificar o nível geral de conformidade com boas práticas e legislações aplicáveis. Entre os principais benefícios desta análise, destacam-se:

- **Visão Estratégica:** Ao oferecer um panorama completo, a análise global auxilia a alta gestão na definição de prioridades e na alocação eficiente de recursos.
- **Acompanhamento de Progresso:** Essa abordagem possibilita monitorar a evolução institucional ao longo do tempo, avaliando o impacto das ações implementadas e identificando novas oportunidades de melhoria.

- Tomada de Decisões Informada: Com base na pontuação consolidada, a instituição pode planejar ações estratégicas, como investimentos em infraestrutura de segurança, programas de capacitação ou revisão de políticas.

A análise global desempenha um papel essencial para assegurar que os esforços realizados em dimensões específicas contribuam para o progresso institucional como um todo. Além disso, oferece um diagnóstico aprofundado que embasa o planejamento de médio e longo prazo.

Essa visão integrada permite o monitoramento contínuo do impacto das ações realizadas, orientando decisões como a priorização de recursos, fortalecimento da infraestrutura tecnológica e a capacitação de equipes. Dessa forma, promove-se um avanço sustentável e alinhado aos objetivos institucionais, garantindo o alcance de elevados padrões de excelência no tratamento de dados pessoais.

6.1.2 Análise Comparativa

A análise comparativa é uma abordagem estratégica que possibilita à instituição avaliar seu nível de maturidade no tratamento de dados pessoais em relação a outras organizações, seja em âmbito regional ou nacional. Complementando as análises institucionais internas, essa perspectiva externa oferece um diagnóstico mais amplo e fundamentado, permitindo identificar o posicionamento da instituição no setor e explorar oportunidades para alcançar níveis mais elevados de maturidade.

Os benefícios dessa abordagem são diversos e contribuem significativamente para o planejamento e a implementação de ações de melhoria. Entre eles, destacam-se:

- Identificação de Boas Práticas: Comparar-se com outras instituições possibilita a identificação de estratégias bem-sucedidas aplicadas em contextos semelhantes. Essas práticas podem ser adaptadas e implementadas, promovendo melhorias consistentes sem a necessidade de começar do zero. Além disso, incentiva-se o benchmarking, que estimula um processo contínuo de aprendizado e aprimoramento, elevando o desempenho institucional.

- Diagnóstico de Gaps de Maturidade: A análise comparativa evidencia discrepâncias entre o nível de maturidade da instituição e o de seus pares, destacando áreas com desempenho abaixo da média do setor. Esse diagnóstico direciona ações corretivas prioritárias, alinhando a instituição aos padrões estabelecidos e fortalecendo sua competitividade e conformidade normativa.
- Estímulo à Melhoria Contínua: O posicionamento frente a outras organizações atua como um motivador para a evolução constante. A análise comparativa estabelece metas desafiadoras, incentivando a instituição a superar suas limitações e buscar níveis mais altos de excelência, promovendo uma cultura organizacional de melhoria contínua.
- Base para Decisões de Investimento: A identificação de lacunas específicas em relação a outras instituições fornece uma base sólida para decisões estratégicas de investimento. Com dados precisos, os recursos podem ser direcionados de forma eficiente para fortalecer áreas críticas, impactando positivamente a maturidade institucional e a conformidade com padrões de segurança e governança.

A flexibilidade da análise comparativa permite sua aplicação em diferentes contextos, ajustando-se às necessidades e objetivos institucionais. Seja em âmbito regional ou nacional, ela pode focar em dimensões específicas ou abarcar todas, dependendo das metas organizacionais.

No contexto regional, a análise facilita o compartilhamento de experiências e a adoção de práticas validadas por instituições próximas. A proximidade geográfica favorece colaborações estratégicas, como visitas técnicas e parcerias para implementação de soluções, promovendo o fortalecimento mútuo e o desenvolvimento do setor. Também contribui para avaliar a competitividade regional, fortalecendo *insights* para a adaptação de práticas ao contexto local.

Em escala nacional, essa abordagem amplia o alcance, permitindo à instituição avaliar seu alinhamento com normas e políticas federais. É essencial para assegurar a conformidade com legislações e diretrizes nacionais, além de identificar oportunidades de inovação e adoção de práticas avançadas. A análise nacional também possibilita o reconhecimento de tendências emergentes e o alinhamento com os mais altos padrões de excelência, promovendo competitividade e credibilidade no cenário nacional.

Ao complementar a visão interna da instituição, a análise comparativa fornece um diagnóstico abrangente e fundamentado em parâmetros externos de referência. Essa abordagem não apenas facilita a identificação de áreas prioritárias para aprimoramento, mas também orienta a busca por *benchmarking* e promove avanços consistentes e alinhados às melhores práticas do setor, fortalecendo a maturidade institucional no tratamento de dados pessoais.

6.2 Resultados Gerais

Os dados apresentados foram obtidos por meio da aplicação do Modelo de Maturidade para o Tratamento de Dados Pessoais, evidenciando a participação de 66 universidades federais do Brasil nesta pesquisa. Contudo, algumas dessas instituições não responderam integralmente às questões do instrumento de medição, o que comprometeu a realização de análises pontuais. Em particular, cinco instituições deixaram de fornecer respostas em determinadas questões, inviabilizando a avaliação das dimensões correspondentes e comprometendo, consequentemente, a análise global dessas universidades. A ausência de dados completos limita a interpretação do nível de maturidade dessas instituições no tratamento de dados pessoais. A plataforma QuestionPro gerou um relatório com inferências gerais sobre as instituições participantes, o qual pode ser consultado no **Apêndice N** deste trabalho.

6.2.1 Panorama no contexto nacional

O Quadro 24 sintetiza a quantidade de instituições participantes classificadas em cada nível de maturidade, considerando as dimensões avaliadas. Oferecendo uma visão abrangente do cenário nacional, permitindo identificar o estágio de maturidade das universidades participantes no tratamento de dados pessoais, contribuindo para uma compreensão mais precisa de suas práticas e desafios.

Quadro 24 - Distribuição das Instituições participantes por classificação

Classificação	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global
Inicial	4	6	19	2	5	0
Emergente	15	25	24	10	9	22
Intermediário	23	24	12	24	30	22
Avançado	20	5	8	15	17	14
Exemplar	4	5	3	10	5	3

Não Avaliado	0	1	0	5	0	5

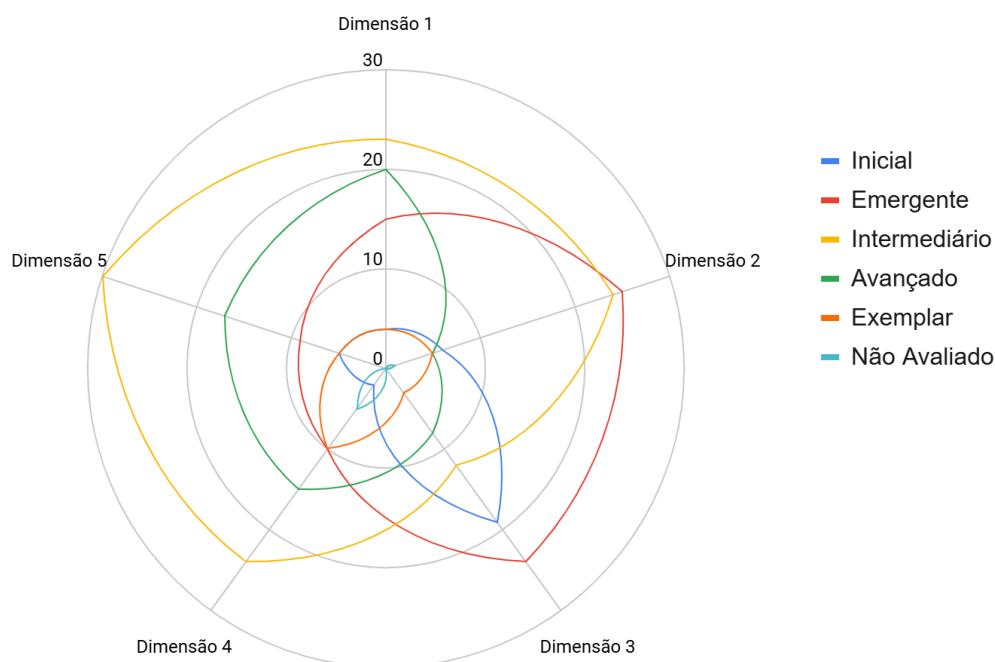
Fonte: elaborado pelo autor.

A análise da distribuição das universidades brasileiras revela que a maioria das instituições alcançou o nível “Intermediário” nas Dimensões 1, 4 e 5, com 23, 24 e 30 universidades, respectivamente. Em contrapartida, as dimensões 2 e 3 apresentaram predominância de instituições no nível “Emergente”, com 25 e 24 universidades, respectivamente.

Na avaliação global, observa-se uma distribuição equilibrada entre os níveis “Emergente” e “Intermediário”, ambos com 22 instituições. Esses dados evidenciam que muitas universidades se encontram em estágios intermediários na implementação de práticas de proteção de dados pessoais, apresentando avanços mais consistentes em algumas dimensões específicas.

Outro aspecto relevante é o número de instituições não avaliadas. Na Dimensão 4, cinco instituições não puderam ser analisadas devido ao preenchimento incompleto do instrumento, impossibilitando o cálculo da maturidade. Situação semelhante foi registrada na Dimensão 2, onde uma instituição permaneceu não avaliada. Essas omissões também impactaram a análise global, resultando em cinco instituições classificadas como "não avaliadas" no nível geral.

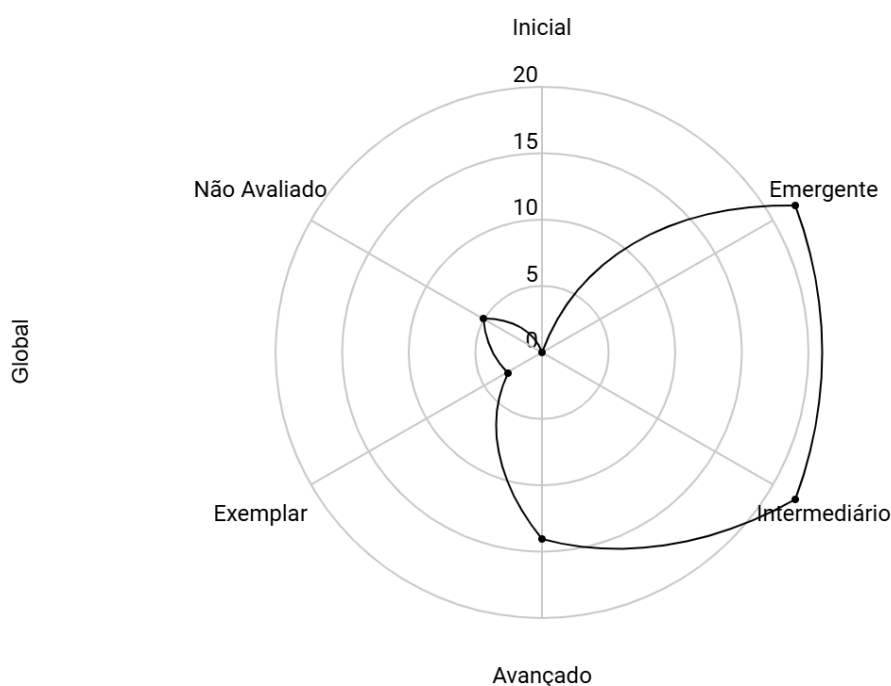
Gráfico 1 - Classificação do nível de maturidade das universidades por dimensão



Fonte: elaborado pelo autor.

O Gráfico 1 complementa a análise ao apresentar de forma visual a distribuição das instituições em cada classificação por dimensão, facilitando comparações e destacando tendências. Essa representação gráfica oferece maior clareza na identificação das áreas de predominância dos diferentes níveis de maturidade.

Gráfico 2 - Classificação do nível de maturidade global das universidades participantes



Fonte: elaborado pelo autor.

A análise global, ilustrada no Gráfico 2, confirma que a maioria das universidades participantes está concentrada nos níveis “Emergente” e “Intermediário”, indicando um progresso parcial, mas ainda insuficiente, na implementação de práticas consistentes e sistemáticas de governança e proteção de dados pessoais. Nenhuma instituição foi classificada no nível “Inicial” na avaliação global, e apenas um número limitado alcançou o nível “Exemplar”, demonstrando excelência nas práticas de tratamento de dados.

As instituições classificadas como “não avaliadas” refletem a ausência de preenchimento de alguns itens do instrumento de medição, etapa fundamental para se obter uma visão precisa e completa do cenário institucional dessas universidades. Esses resultados destacam a necessidade de direcionar esforços e ações

estratégias para o fortalecimento das práticas de tratamento de dados pessoais em âmbito nacional, contribuindo para elevar o nível geral de maturidade.

6.2.2 Análise Regional: Região Norte

Uma abordagem complementar para a análise do nível de maturidade no tratamento de dados pessoais foi examinar a situação das universidades em cada região do país. O Quadro 25 apresenta as classificações por dimensão das universidades localizadas na Região Norte, proporcionando uma visão detalhada do panorama nessa área geográfica.

Quadro 25 - Classificação da universidades da região norte

Universidade	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global	Estado
UFAC	Inicial	Inicial	Inicial	Emergente	Emergente	Emergente	Acre
UFAM	Avançado	Intermediário	Intermediário	Intermediário	Intermediário	Intermediário	Amazonas
UFNT	Inicial	Emergente	Emergente	Não Avaliado	Inicial	Não Avaliado	Tocantins
UFOPA	Emergente	Emergente	Emergente	Emergente	Emergente	Emergente	Pará
UFPA	Avançado	Intermediário	Intermediário	Avançado	Avançado	Avançado	Pará
UFRA	Emergente	Emergente	Inicial	Intermediário	Intermediário	Emergente	Pará
UFRR	Intermediário	Intermediário	Emergente	Intermediário	Intermediário	Intermediário	Roraima
UFT	Emergente	Inicial	Inicial	Intermediário	Emergente	Emergente	Tocantins
UNIFAP	Intermediário	Emergente	Emergente	Emergente	Emergente	Emergente	Amapá
UNIFESSPA	Intermediário	Intermediário	Intermediário	Intermediário	Intermediário	Intermediário	Pará
UNIR	Emergente	Emergente	Inicial	Intermediário	Emergente	Emergente	Rondônia

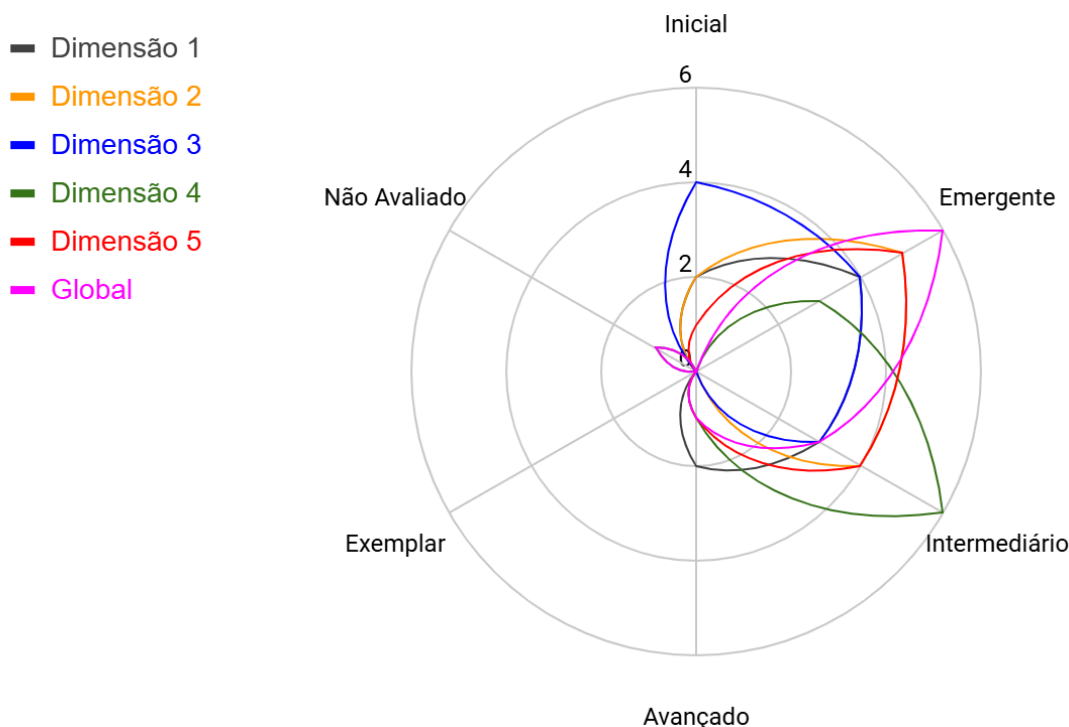
Fonte: elaborado pelo autor.

Os dados apresentados revelam uma significativa heterogeneidade nos níveis de maturidade das universidades da Região Norte. Enquanto algumas instituições, como a UFPA, alcançaram o nível “Avançado” em diversas dimensões, outras, como a UFAC e a UFNT, permanecem predominantemente nos níveis “Inicial” ou “Emergente”, evidenciando a necessidade de esforços mais direcionados para impulsionar melhorias.

A análise global mostra que apenas a UFPA obteve o nível “Avançado”, enquanto a maioria das universidades permanece nos níveis “Emergente” ou “Intermediário”. Essa disparidade reflete o desenvolvimento desigual das práticas de tratamento de dados pessoais, com avanços isolados em algumas instituições e desafios persistentes em outras.

Essa avaliação é essencial para identificar as particularidades de cada estado, permitindo que intervenções e políticas públicas sejam planejadas de forma mais eficaz, considerando as especificidades locais. Além disso, instituições classificadas nos níveis inferiores requerem maior suporte para alcançar níveis mais elevados de maturidade.

Gráfico 3 - Nível de maturidade das universidades da região norte



Fonte: elaborado pelo autor.

O Gráfico 3 complementa as informações ao ilustrar a distribuição das classificações das universidades da Região Norte. A visualização destaca a predominância das classificações “Emergente” e “Intermediário” na maioria das dimensões, enquanto os níveis “Inicial” e “Avançado” aparecem de forma menos expressiva. A ausência de classificações “Exemplares” evidencia a necessidade de melhorias substanciais nas práticas relacionadas ao tratamento de dados pessoais.

Essa perspectiva gráfica facilita a identificação de padrões regionais, indicando onde os esforços devem ser concentrados para promover avanços consistentes. Dimensões como Governança de Dados e Boas Práticas e Segurança da Informação e Tecnologia apresentam maior variabilidade, refletindo os desafios específicos enfrentados por cada instituição.

Ao integrar os dados, obtém-se uma visão abrangente do cenário regional, permitindo orientar estratégias que elevem a maturidade das universidades e promovam maior conformidade com boas práticas e legislações aplicáveis ao tratamento de dados pessoais.

6.2.3 Análise Regional: Região Nordeste

A análise do nível de maturidade no tratamento de dados pessoais entre as universidades da Região Nordeste revela um panorama diversificado. O Quadro 26 apresenta as classificações obtidas em cada dimensão avaliada, oferecendo uma visão detalhada das práticas adotadas pelas instituições dessa região.

Quadro 26 - Classificação da universidades da região nordeste

Universidade	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global	Estado
UFAPE	Inicial	Inicial	Inicial	Emergente	Inicial	Emergente	Pernambuco
UFBA	Avançado	Exemplar	Avançado	Intermediário	Exemplar	Avançado	Bahia
UFC	Intermediário	Inicial	Inicial	Emergente	Emergente	Emergente	Ceará
UFCA	Avançado	Intermediário	Avançado	Exemplar	Intermediário	Avançado	Ceará
UFCG	Intermediário	Emergente	Emergente	Intermediário	Intermediário	Intermediário	Paraíba
UFDPAR	Intermediário	Não Avaliado	Emergente	Não Avaliado	Intermediário	Não Avaliado	Piauí
UFERSA-RN	Avançado	Avançado	Intermediário	Intermediário	Avançado	Avançado	Rio Grande do Norte
UFMA	Emergente	Emergente	Emergente	Avançado	Intermediário	Emergente	Maranhão
UFOB	Intermediário	Emergente	Emergente	Avançado	Intermediário	Intermediário	Bahia
UFPB	Intermediário	Avançado	Intermediário	Avançado	Avançado	Intermediário	Paraíba
UFPE	Intermediário	Emergente	Emergente	Exemplar	Intermediário	Intermediário	Pernambuco
UFPI	Intermediário	Intermediário	Inicial	Intermediário	Avançado	Intermediário	Piauí
UFRB	Intermediário	Intermediário	Emergente	Avançado	Intermediário	Intermediário	Bahia
UFRN	Intermediário	Intermediário	Emergente	Avançado	Intermediário	Intermediário	Rio Grande do Norte
UFRPE	Avançado	Intermediário	Intermediário	Exemplar	Avançado	Avançado	Pernambuco
UFS	Avançado	Intermediário	Exemplar	Exemplar	Avançado	Avançado	Sergipe
UFSB	Emergente	Emergente	Inicial	Intermediário	Intermediário	Emergente	Bahia
UNILAB	Emergente	Emergente	Inicial	Emergente	Intermediário	Emergente	Ceará
UNIVASF	Emergente	Emergente	Inicial	Emergente	Emergente	Emergente	Pernambuco

Fonte: elaborado pelo autor.

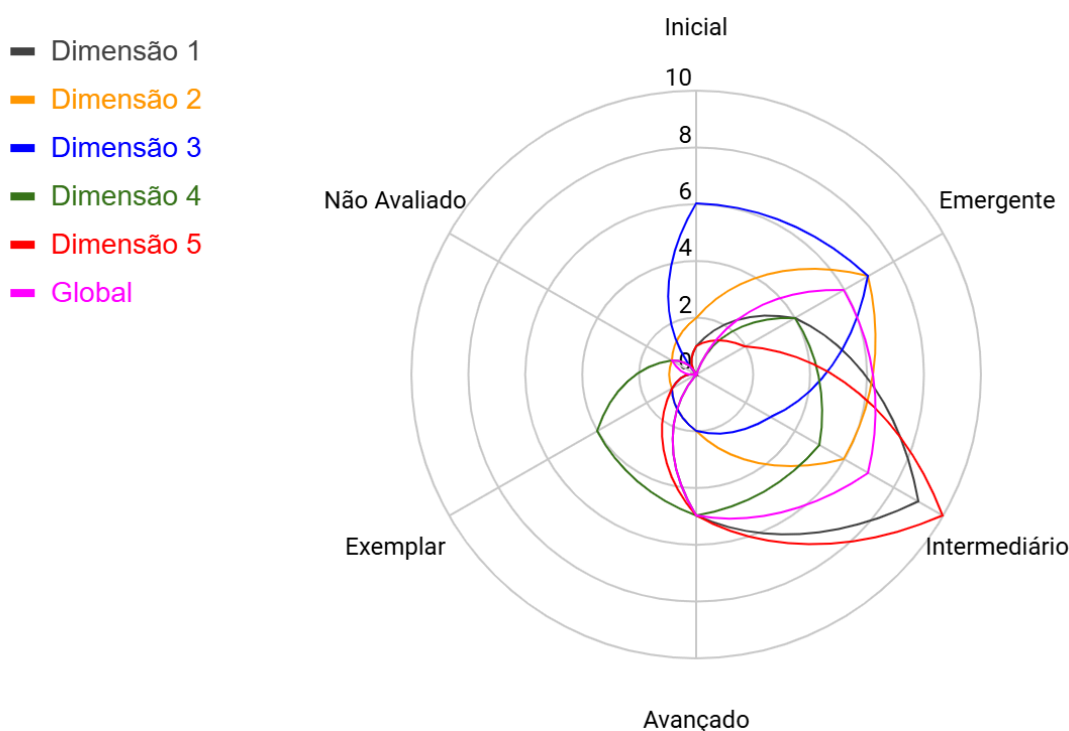
Os dados mostram uma significativa diversidade nos níveis de maturidade das universidades da Região Nordeste. Instituições como a UFBA, a UFRPE e a

UFS destacam-se com classificações elevadas, alcançando níveis “Avançado” ou “Exemplar” em várias dimensões, refletindo práticas consolidadas e maduras no tratamento de dados pessoais. Em contraste, instituições como a UFAPE e a UFC permanecem majoritariamente nos níveis “Inicial” e “Emergente”, evidenciando a necessidade de suporte adicional para o desenvolvimento de suas práticas.

A análise global confirma que a maioria das universidades está concentrada nos níveis “Emergente” e “Intermediário”, enquanto apenas algumas conseguiram avançar para níveis superiores. Além disso, destaca-se a lacuna deixada por instituições como a UFDPAR, que não completaram todas as questões do instrumento de medição, inviabilizando o cálculo de sua maturidade global. Essa ausência de dados compromete uma avaliação mais abrangente e ressalta a necessidade de estratégias para incentivar maior engajamento no preenchimento completo do instrumento.

Esses resultados reforçam a importância de estratégias regionais que atendam às especificidades das universidades nordestinas, promovendo avanços consistentes e sustentáveis.

Gráfico 4 - Nível de maturidade das universidades da região nordeste



Fonte: elaborado pelo autor.

O Gráfico 4 complementa as informações ao ilustrar visualmente a distribuição das classificações das universidades na Região Nordeste. Observa-se

que os níveis “Emergente” e “Intermediário” predominam na maioria das dimensões, enquanto os níveis “Inicial”, “Avançado” e “Exemplar” aparecem de forma menos expressiva. Essa distribuição reflete uma realidade heterogênea, onde algumas universidades avançaram significativamente, enquanto outras enfrentam desafios estruturais e processuais.

A ausência de classificações “Exemplar” em várias dimensões e a predominância de níveis intermediários apontam para a necessidade de ações direcionadas para fortalecer práticas como Governança de Dados e Boas Práticas e Segurança da Informação, que apresentam maior variabilidade entre as instituições.

Ao integrar as análises, é possível identificar padrões regionais e áreas prioritárias para intervenções. Essas informações são essenciais para orientar políticas públicas e esforços institucionais que busquem elevar a maturidade das universidades nordestinas, promovendo maior alinhamento com boas práticas e legislações aplicáveis ao tratamento de dados pessoais.

6.2.4 Análise Regional: Região Centro-Oeste

A análise do nível de maturidade no tratamento de dados pessoais entre as universidades da Região Centro-Oeste revela uma diversidade de classificações. O Quadro 27 apresenta os resultados por dimensão, proporcionando uma visão detalhada do panorama regional.

Quadro 27 - Classificação da universidades da região centro-oeste

Universidade	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global	Estado
UFCAT	Intermediário	Emergente	Emergente	Intermediário	Emergente	Emergente	Goiás
UFG	Intermediário	Inicial	Inicial	Emergente	Inicial	Emergente	Goiás
UFGD	Avançado	Intermediário	Intermediário	Avançado	Avançado	Intermediário	Mato Grosso do Sul
UFJ	Emergente	Emergente	Emergente	Emergente	Intermediário	Emergente	Goiás
UFMS	Exemplar	Exemplar	Exemplar	Exemplar	Avançado	Exemplar	Mato Grosso do Sul
UFMT	Avançado	Intermediário	Avançado	Intermediário	Avançado	Avançado	Mato Grosso
UFR	Intermediário	Emergente	Inicial	Inicial	Intermediário	Emergente	Mato Grosso
UNB	Avançado	Intermediário	Emergente	Avançado	Exemplar	Intermediário	Brasília

Fonte: elaborado pelo autor.

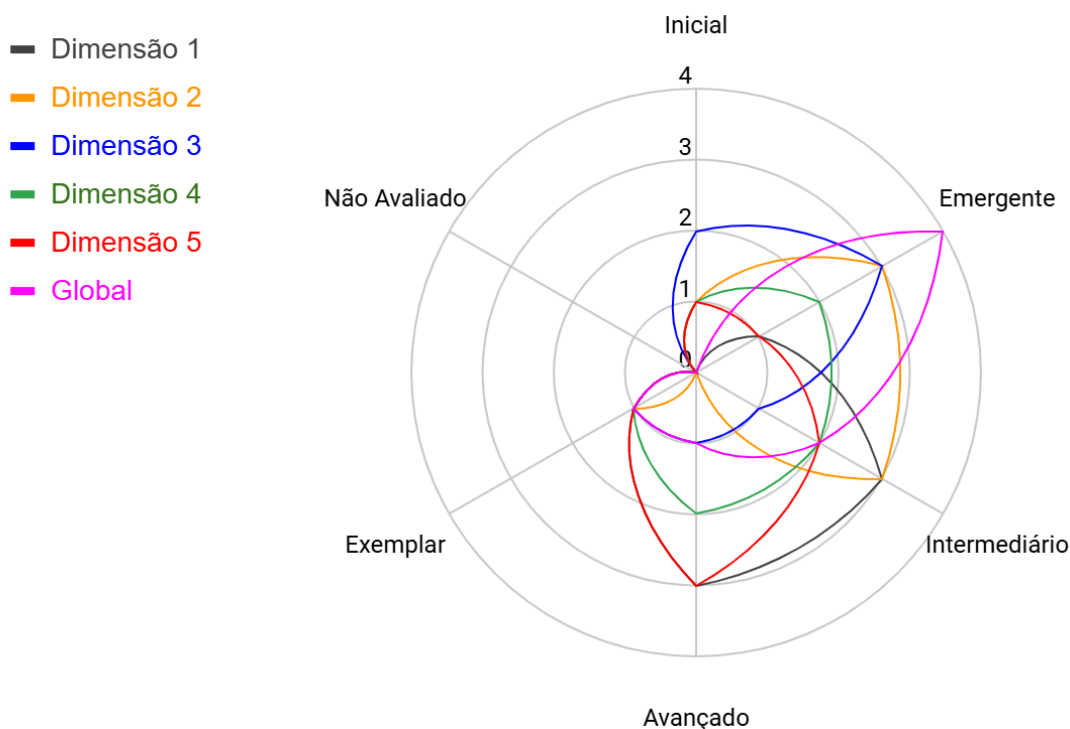
Os resultados evidenciam uma ampla variação nos níveis de maturidade das universidades da Região Centro-Oeste. Instituições como a UFMS e a UNB

destacaram-se ao alcançar classificações “Exemplar” e “Avançado” em diversas dimensões, refletindo práticas bem consolidadas e consistentes no tratamento de dados pessoais. Esses resultados indicam um compromisso elevado com a governança de dados, a segurança da informação e a transparência.

Por outro lado, universidades como a UFG e a UFR, enfrentam desafios significativos, predominando nos níveis “Inicial” e “Emergente”. Esses níveis indicam práticas ainda incipientes ou inconsistentes, demandando esforços direcionados para o avanço em maturidade. Dimensões como Políticas e Processos de Tratamento de Dados e Treinamento e Conscientização mostram-se mais vulneráveis, especialmente entre instituições com classificações mais baixas.

De forma geral, a classificação global das universidades da região varia entre os níveis “Emergente”, “Intermediário”, “Avançado” e “Exemplar”, refletindo a heterogeneidade do desenvolvimento institucional. Essa diversidade aponta para a necessidade de estratégias específicas que atendam às particularidades de cada instituição, fortalecendo aquelas com classificações mais baixas e consolidando as boas práticas já implementadas pelas universidades mais avançadas.

Gráfico 5 - Nível de maturidade das universidades da região centro-oeste



Fonte: elaborado pelo autor.

O Gráfico 5 complementa as informações apresentadas ao ilustrar visualmente a distribuição das classificações das universidades da Região

Centro-Oeste. Observa-se que as classificações “Emergente” e “Intermediário” predominam em várias dimensões, enquanto os níveis “Inicial” e “Exemplar” são menos recorrentes, refletindo uma concentração em estágios intermediários de maturidade.

As instituições mais avançadas, como a UFMS e a UNB, representam referências importantes na região, enquanto as classificações mais baixas reforçam a necessidade de intervenções para promover maior equilíbrio no desenvolvimento institucional. Dimensões como Segurança da Informação e Tecnologia e Governança de Dados e Boas Práticas destacam-se pela maior variabilidade, indicando áreas prioritárias para ações de melhoria.

A análise evidencia tanto avanços significativos em algumas instituições quanto desafios persistentes em outras. O cenário regional aponta para a necessidade de políticas públicas e estratégias institucionais direcionadas para elevar os níveis de maturidade, com foco especial nas instituições que apresentam classificações inferiores. Ao mesmo tempo, é essencial consolidar as práticas avançadas das universidades que já se encontram em níveis superiores, garantindo a manutenção de um padrão elevado e promovendo o compartilhamento de boas práticas.

6.2.5 Análise Regional: Região Sudeste

A Região Sudeste, reconhecida por seu alto nível de desenvolvimento educacional e tecnológico, apresenta um panorama diversificado em relação à maturidade no tratamento de dados pessoais. O Quadro 28 detalha as classificações das universidades por dimensão, oferecendo uma visão abrangente sobre as práticas implementadas nesta região.

Quadro 28 - Classificação da universidades da região sudeste

Universidade	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global	Estado
UFSJ	Intermediário	Emergente	Emergente	Intermediário	Intermediário	Intermediário	Minas Gerais
UFABC	Inicial	Emergente	Inicial	Intermediário	Inicial	Emergente	São Paulo
UFES	Avançado	Intermediário	Avançado	Exemplar	Avançado	Avançado	Espírito Santo
UFF	Avançado	Avançado	Intermediário	Avançado	Intermediário	Avançado	Rio de Janeiro
UFJF	Intermediário	Intermediário	Emergente	Não Avaliado	Intermediário	Não Avaliado	Minas Gerais
UFLA	Avançado	Avançado	Intermediário	Avançado	Avançado	Avançado	Minas Gerais
UFOP	Intermediário	Inicial	Inicial	Inicial	Inicial	Emergente	Minas Gerais

UFRJ	Intermediário	Intermediário	Emergente	Não Avaliado	Intermediário	Não Avaliado	Rio de Janeiro
UFRRJ	Avançado	Intermediário	Avançado	Exemplar	Avançado	Avançado	Rio de Janeiro
UFSCAR	Emergente	Emergente	Inicial	Intermediário	Intermediário	Emergente	São Paulo
UFTM	Avançado	Intermediário	Intermediário	Avançado	Avançado	Intermediário	Minas Gerais
UFU	Exemplar	Exemplar	Avançado	Exemplar	Exemplar	Exemplar	Minas Gerais
UFV	Avançado	Intermediário	Intermediário	Avançado	Avançado	Avançado	Minas Gerais
UFVJM	Emergente	Emergente	Emergente	Intermediário	Emergente	Emergente	Minas Gerais
UNIFAL-MG	Intermediário	Emergente	Inicial	Intermediário	Intermediário	Intermediário	Minas Gerais
UNIFEI	Exemplar	Avançado	Avançado	Exemplar	Avançado	Avançado	Minas Gerais
UNIFESP	Avançado	Intermediário	Emergente	Intermediário	Intermediário	Intermediário	São Paulo
UNIPAMPA	Emergente	Emergente	Inicial	Intermediário	Intermediário	Emergente	São Paulo
UNIRIO	Intermediário	Emergente	Emergente	Intermediário	Intermediário	Intermediário	Rio de Janeiro

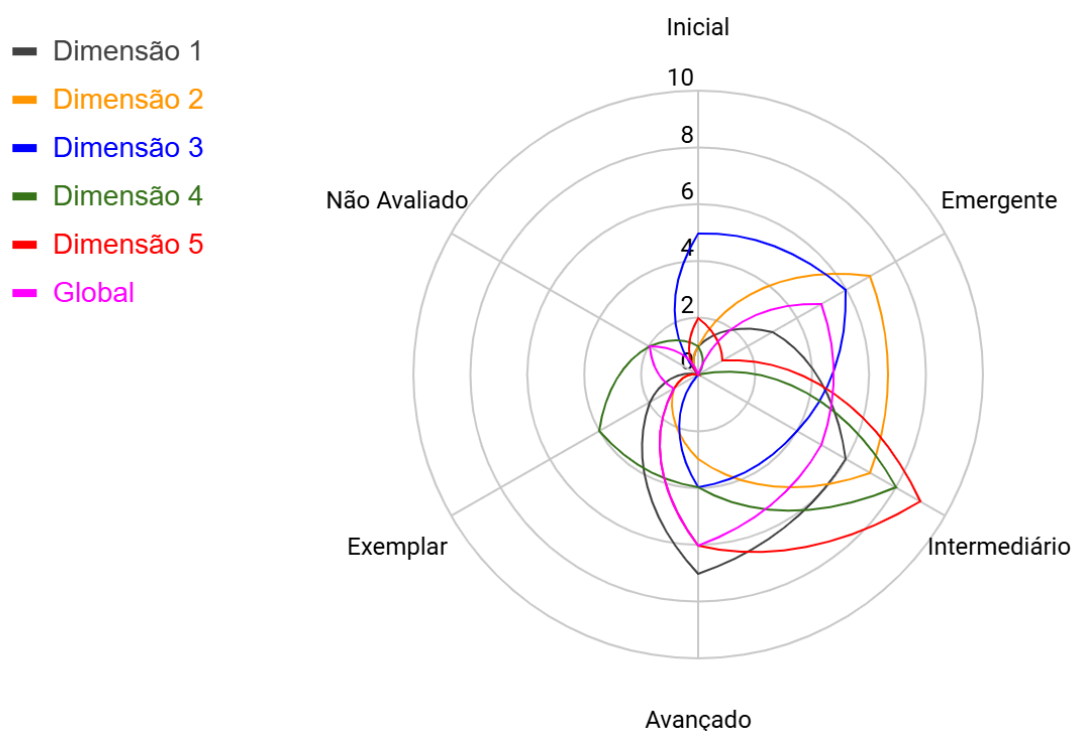
Fonte: elaborado pelo autor.

Os dados apresentados refletem um cenário de ampla variabilidade no nível de maturidade das universidades da Região Sudeste. Instituições, como a UFU e a UNIFEI, destacaram-se ao alcançar o nível “Exemplar” em diversas dimensões, demonstrando práticas consolidadas em governança de dados pessoais, segurança da informação e transparência.

Por outro lado, instituições como a UFABC e a UFOP apresentaram classificações predominantemente nos níveis “Inicial” e “Emergente”, evidenciando desafios significativos na implementação de práticas robustas de tratamento de dados pessoais. Esses resultados indicam a necessidade de suporte direcionado, com foco especial em dimensões como Políticas e Processos de Tratamento de Dados e Treinamento e Conscientização.

A classificação global das universidades varia amplamente, desde “Emergente” a “Exemplar”, refletindo uma disparidade no desenvolvimento institucional. Essa diversidade exige estratégias específicas para atender às instituições menos maduras, ao mesmo tempo em que se busca consolidar as práticas avançadas das universidades mais desenvolvidas.

Gráfico 6 - Nível de maturidade das universidades da região sudeste



Fonte: elaborado pelo autor.

O Gráfico 6 complementa as informações ao ilustrar visualmente a distribuição das classificações das universidades da Região Sudeste. Observa-se que os níveis “Emergente” e “Intermediário” predominam em várias dimensões, enquanto os níveis “Inicial” e “Exemplar” aparecem com menor frequência. A presença de instituições com classificações mais baixas destaca a necessidade de iniciativas que promovam maior uniformidade no desenvolvimento institucional.

As instituições com classificação superior, como a UFU e a UNIFEI, podem servir como referências regionais, compartilhando boas práticas e modelos bem-sucedidos com outras universidades. Dimensões como Governança de Dados e Boas Práticas e Segurança da Informação apresentam maior variabilidade, indicando áreas prioritárias para intervenções.

A análise evidencia tanto avanços notáveis em algumas universidades quanto desafios persistentes em outras. O cenário regional aponta a necessidade de políticas públicas que incentivem o compartilhamento de boas práticas e fortaleçam áreas vulneráveis. Ao mesmo tempo, é fundamental consolidar os avanços obtidos pelas instituições que já alcançaram níveis elevados de maturidade, assegurando a manutenção de padrões de excelência e contribuindo para o desenvolvimento geral da região.

6.2.6 Análise Regional: Região Sul

A Região Sul apresentou resultados significativos em relação à maturidade no tratamento de dados pessoais. O Quadro 29 detalha as classificações das universidades por dimensão, oferecendo uma visão abrangente sobre o desempenho das instituições da região.

Quadro 29 - Classificação da universidades da região sul

Universidade	Dimensão 1	Dimensão 2	Dimensão 3	Dimensão 4	Dimensão 5	Global	Estado
UFCSPA	Avançado	Intermediário	Emergente	Intermediário	Avançado	Intermediário	Rio Grande do Sul
UFFS	Intermediário	Intermediário	Intermediário	Intermediário	Intermediário	Intermediário	Santa Catarina
UFPEL	Intermediário	Emergente	Emergente	Avançado	Intermediário	Intermediário	Rio Grande do Sul
UFRGS	Exemplar	Exemplar	Exemplar	Exemplar	Exemplar	Exemplar	Rio Grande do Sul
UFSC	Emergente	Emergente	Inicial	Emergente	Intermediário	Emergente	Santa Catarina
UFSJ	Avançado	Intermediário	Emergente	Não Avaliado	Avançado	Não Avaliado	Rio Grande do Sul
UFSM	Avançado	Exemplar	Avançado	Avançado	Exemplar	Avançado	Rio Grande do Sul
UNILA	Emergente	Emergente	Inicial	Avançado	Intermediário	Intermediário	Paraná
UTFPR	Emergente	Intermediário	Emergente	Intermediário	Intermediário	Intermediário	Paraná

Fonte: elaborado pelo autor.

Os dados apresentados destacam a UFRGS, que atingiu o nível “Exemplar” em todas as dimensões e na classificação global. Esse desempenho reflete práticas de governança de dados extremamente consolidadas, com políticas bem definidas, processos rigorosos e monitoramento contínuo, posicionando a universidade como uma referência regional e nacional no tratamento de dados pessoais.

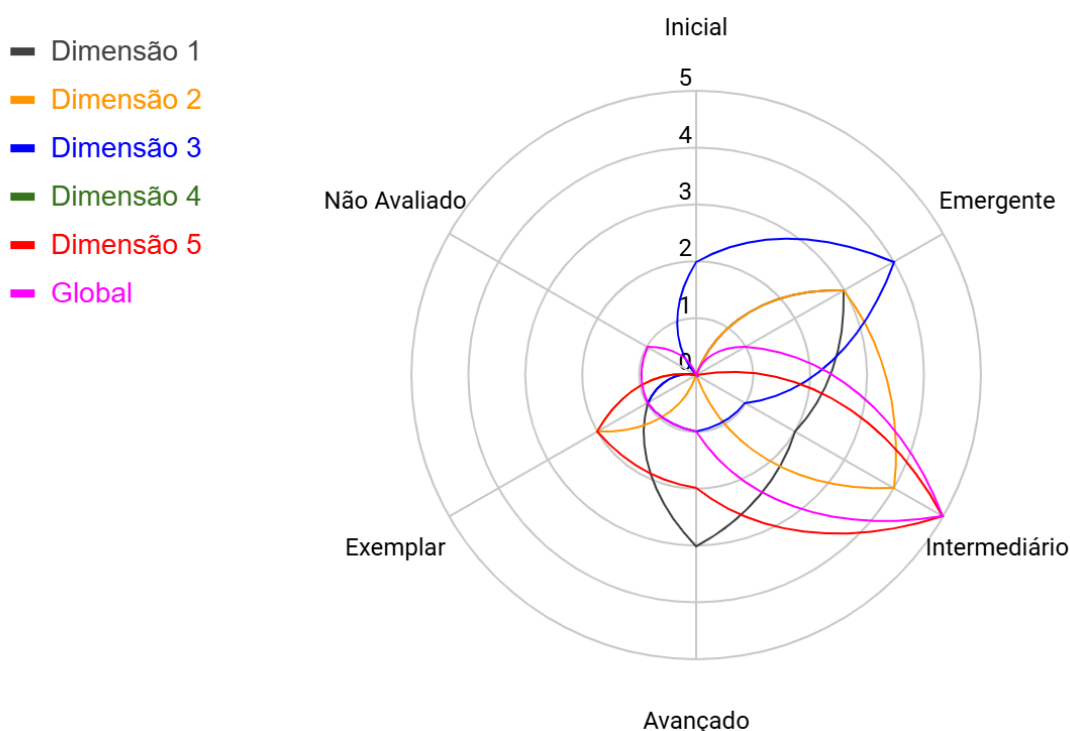
A UFSM também obteve destaque, com classificações predominantemente nos níveis “Avançado” e “Exemplar”, demonstrando práticas maduras e bem estruturadas. Esses resultados reforçam a posição da Região Sul como um polo de excelência no tema.

Por outro lado, instituições como a UFSC e a UTFPR enfrentam desafios, apresentando classificações predominantemente nos níveis “Emergente” ou “Inicial” em várias dimensões. Essas instituições necessitam de investimentos em infraestrutura, formalização de políticas e capacitação de equipes para alcançar

níveis mais elevados de maturidade. Dimensões como Treinamento e Conscientização e Governança de Dados são áreas prioritárias para melhoria.

De forma geral, a análise revela variabilidade nos níveis de maturidade, com a maioria das universidades concentradas nos níveis “Intermediário” e “Emergente” na classificação global. Esse cenário aponta para a necessidade de iniciativas que promovam maior equilíbrio no desenvolvimento institucional, além de consolidar as boas práticas já existentes.

Gráfico 7 - Nível de maturidade das universidades da região sul



Fonte: elaborado pelo autor.

O Gráfico 7 complementa os dados ao ilustrar visualmente a distribuição das classificações das universidades da Região Sul. Embora algumas instituições, como a UFRGS, tenham alcançado o nível “Exemplar”, a maioria das classificações encontra-se nos níveis “Intermediário” e “Emergente”, refletindo a diversidade nos estágios de maturidade.

A ausência de classificação “Exemplar” em algumas dimensões de instituições como a UFSC e a UTFPR reforça a necessidade de ações direcionadas ao aprimoramento de práticas específicas. A disseminação das boas práticas observadas nas instituições mais avançadas, como a UFRGS e a UFSM, pode ser uma estratégia eficaz para promover melhorias nas universidades com níveis mais baixos de maturidade.

A análise das universidades da Região Sul evidencia um cenário promissor, com algumas instituições se destacando por práticas altamente maduras e consolidadas. No entanto, os desafios enfrentados por outras universidades mostram a importância de políticas públicas e estratégias regionais voltadas para o fortalecimento das áreas mais vulneráveis.

A promoção de colaborações entre instituições da região, aliada a adoção de boas práticas das universidades mais avançadas, pode contribuir significativamente para o aumento da maturidade no tratamento de dados pessoais. Consolidar os avanços já obtidos e reduzir as disparidades internas são passos fundamentais para assegurar o desenvolvimento contínuo e sustentável na Região Sul.

6.3 Resultados Institucionais

Os resultados institucionais foram desenvolvidos com base nas respostas fornecidas pelas instituições no instrumento de medição, seguindo a metodologia de cálculo de maturidade e classificação descrita no item 5.3.7 deste trabalho. Esse processo contou com o suporte de uma base de dados padronizada, cujas análises e considerações detalhadas estão disponíveis no **Apêndice M**. A seguir, são apresentadas as realidades de quatro instituições que representam diferentes cenários de maturidade, ilustrando na prática como as capacidades institucionais podem ser avaliadas e aprimoradas por meio do Modelo de Maturidade para Tratamento de Dados Pessoais desenvolvido neste estudo.

6.3.1 Universidade Federal do Ceará (UFC)

Fundada em 1954, a Universidade Federal do Ceará (UFC) possui campi nas cidades de Fortaleza, Sobral, Quixadá, Russas e Crateús. A instituição mantém um site dedicado à Lei Geral de Proteção de Dados, oferecendo informações detalhadas sobre o tema, disponível em: <https://lgpd.ufc.br/pt/>. No que tange à análise de maturidade, a UFC respondeu ao instrumento de medição no dia 10 de setembro de 2024, conforme as respostas registradas.

Quadro 30 - Respostas do instrumento de medição da UFC

Questões	Respostas da UFC
Questão 1	3
Questão 2	4
Questão 3	2

Questão 4	2
Questão 5	1
Questão 6	2
Questão 7	1
Questão 8	1
Questão 9	1
Questão 10	1
Questão 11	2
Questão 12	2
Questão 13	1
Questão 14	1
Questão 15	1
Questão 16	3
Questão 17	2
Questão 18	1
Questão 19	1
Questão 20	2
Questão 21	2
Questão 22	2
Questão 23	1
Questão 24	2
Questão 25	1

Fonte: elaborado pelo autor.

As respostas fornecidas pela UFC foram utilizadas para o cálculo de maturidade, seguindo a metodologia descrita no item **5.3.7** deste trabalho e fundamentando-se nos dados padronizados disponíveis no **Apêndice M**. O Quadro 31 sintetiza a classificação da UFC em cada uma das dimensões avaliadas e apresenta o resultado da maturidade global da instituição.

Quadro 31 - Pontuação e classificação da UFC

Dimensão	Pontuação	Nível de Maturidade
Dimensão 1	48,33	Intermediário
Dimensão 2	24,00	Inicial
Dimensão 3	25,00	Inicial
Dimensão 4	39,00	Emergente
Dimensão 5	31,43	Emergente
Global	33,55	Emergente

Fonte: elaborado pelo autor.

Esses resultados destacam os principais pontos de melhoria para que a UFC eleve seus níveis de maturidade. O detalhamento da análise dessas classificações pode ser observado a seguir.

6.3.1.1 Dimensão 1: Governança de Dados e Boas Práticas

A seguir, apresenta-se o detalhamento do cálculo de pontuação da dimensão 1 para a UFC, que abrange as questões 1 a 6 do instrumento de medição. A pontuação máxima possível para esta dimensão é de 120 pontos. A UFC obteve uma pontuação bruta calculada conforme a fórmula: $Q1*3 + Q2*5 + Q3*5 + Q4*5 + Q5*3 + Q6*3$, resultando em 58 pontos.

Aplicando a equação da pontuação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{58}{120} \right) \times 100 = 48,33 \text{ pontos}$$

Esse valor posiciona a UFC na categoria "Intermediário", conforme os critérios e intervalos estabelecidos no MMTDP.

Análise

A maturidade institucional da UFC em relação à dimensão 1 apresenta avanços em algumas áreas, mas também revela lacunas importantes que necessitam de atenção. A análise evidencia aspectos estruturais e operacionais que impactam diretamente a conformidade da universidade com as normativas vigentes, como a LGPD e padrões internacionais, como a ISO/IEC 27701:2019.

A implementação parcial de um programa de governança de dados demonstra uma base promissora. Contudo, a ausência de formalização completa e de internalização das práticas limita sua eficácia, comprometendo o alinhamento integral às normativas e dificultando a aplicação consistente de medidas de proteção de dados. O reconhecimento formal de um Encarregado de Proteção de Dados (DPO) representa um avanço relevante. No entanto, a falta de integração com áreas estratégicas, como Tecnologia da Informação, Jurídico e Recursos Humanos, restringe a abrangência e eficácia de suas ações, limitando o cumprimento dos princípios de governança.

A criação de um comitê voltado ao tratamento de dados é um indicativo inicial de comprometimento institucional. Entretanto, a ausência de atividades regulares e

de definições claras sobre as responsabilidades desse comitê compromete seu impacto prático. De forma similar, a elaboração de uma Política de Privacidade reflete um compromisso com a transparência no tratamento de dados. No entanto, enquanto essa política não for finalizada e implementada, não gerará as garantias necessárias aos titulares, perpetuando um ambiente de insegurança.

A ausência de identificação formal dos fluxos de compartilhamento e transferência de dados configura uma vulnerabilidade significativa, comprometendo a transparência com os titulares e expondo a instituição a possíveis sanções administrativas por descumprimento de normas legais. Por fim, o reconhecimento da necessidade de segregação de funções no âmbito do DPO é positivo. Contudo, a acumulação de atribuições pelo Encarregado de Proteção de Dados compromete sua independência e imparcialidade, restringindo sua capacidade de supervisão eficiente.

Recomendações

Para promover a evolução da maturidade institucional da UFC no tratamento de dados pessoais, sugere-se a implementação das seguintes ações organizadas por tópicos:

- **Governança de Dados e Políticas Institucionais:**
 - Formalizar e implementar o programa de governança de dados, com etapas e prazos claramente definidos.
 - Criar um comitê responsável por monitorar a implementação e garantir o alinhamento às normativas vigentes.
 - Concluir a elaboração da Política de Privacidade, assegurando que contemple todo o ciclo de vida dos dados, desde a coleta até o descarte.
 - Promover campanhas institucionais para conscientizar colaboradores sobre a Política de Privacidade e sua importância.
- **Encarregado de Proteção de Dados:**
 - Integrar o DPO às áreas estratégicas, como Tecnologia da Informação, Jurídico e Recursos Humanos, promovendo uma abordagem multidisciplinar.

- Estabelecer reuniões regulares entre o DPO e as demais áreas para discutir e solucionar questões de proteção de dados.
 - Avaliar e redistribuir funções acumuladas pelo DPO, assegurando sua independência e neutralidade.
 - Oferecer treinamentos contínuos ao DPO, mantendo-o atualizado sobre mudanças legislativas e práticas de mercado.
- Comitês e Estruturas de Supervisão:
 - Definir com clareza as responsabilidades e os objetivos estratégicos do comitê de proteção de dados.
 - Instituir um calendário de reuniões periódicas e registrar decisões e ações em atas documentadas.
 - Estabelecer indicadores de desempenho para monitorar a eficácia do comitê e o impacto de suas ações na governança de dados.
- Mapeamento e Compartilhamento dos Dados:
 - Realizar um mapeamento detalhado dos fluxos de compartilhamento e transferência de dados, identificando os terceiros envolvidos.
 - Documentar esses fluxos de forma clara, assegurando a conformidade com os princípios da LGPD.
 - Desenvolver mecanismos de comunicação para informar os titulares sobre o compartilhamento de seus dados, promovendo maior transparência.
 - Implementar controles e auditorias periódicas para verificar o cumprimento das políticas de compartilhamento e transferência.

6.3.1.2 Dimensão 2: Políticas e Processos de Tratamento de Dados

A seguir, detalha-se o cálculo da pontuação da Dimensão 2 para a Universidade Federal do Ceará, que abrange as questões 7 a 11 do instrumento de medição. A pontuação máxima para esta dimensão é de 75 pontos. A UFC obteve uma pontuação bruta, calculada conforme a fórmula: $Q7*3 + Q8*3 + Q9*3 + Q10*3 + Q11*3$, resultando em 18 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{18}{75} \right) \times 100 = 24 \text{ pontos}$$

Esse resultado posiciona a UFC na categoria "Inicial", indicando que a instituição está em uma etapa inicial de desenvolvimento nesta área.

Análise

A maturidade institucional da UFC em relação à dimensão 2 apresenta lacunas significativas que comprometem a governança e a conformidade no tratamento de dados pessoais. Essas fragilidades manifestam-se na ausência de mapeamento de dados, identificação de agentes responsáveis e processos formais para assegurar os direitos dos titulares, além da aplicação inconsistente de técnicas de proteção a dados sensíveis. A análise evidencia riscos operacionais e legais que precisam ser tratados como prioridade.

A inexistência de um mapeamento que identifique as categorias de dados pessoais e os respectivos titulares limita a compreensão sobre a amplitude dos dados tratados pela instituição. Essa falta de visibilidade prejudica a gestão segura e dificulta a implementação de controles efetivos e políticas adequadas para garantir a conformidade com a legislação. Outro ponto crítico é a ausência de identificação dos agentes responsáveis pelo tratamento de dados, como controladores e operadores, o que compromete a atribuição de responsabilidades e fragiliza a governança de dados, expondo a riscos de não conformidade e violações de segurança.

Adicionalmente, a ausência de mapeamento dos processos que tratam dados pessoais representa uma vulnerabilidade grave. Sem o entendimento claro de quais atividades envolvem dados pessoais, a instituição enfrenta dificuldades para estruturar controles de proteção e assegurar o cumprimento das exigências legais, como o princípio da finalidade previsto pela LGPD. A inexistência de mecanismos formais para garantir os direitos dos titulares, como acesso, retificação e exclusão de dados, é um dos desafios mais graves identificados. Essa lacuna compromete a confiança dos titulares e expõe a instituição a riscos de penalidades administrativas e danos reputacionais.

Por fim, embora a UFC reconheça a importância de proteger dados sensíveis, a aplicação inconsistente de técnicas, como anonimização e mascaramento, demonstra fragilidades operacionais que comprometem a segurança das

informações. Essa inconsistência aumenta os riscos associados ao tratamento inadequado de dados sensíveis e revela a necessidade de aprimoramento das práticas institucionais.

Recomendações

Para promover a evolução da maturidade institucional nesta dimensão, sugere-se a implementação das seguintes ações organizadas por tópicos:

- **Elaboração de Políticas Institucionais:**
 - Desenvolver políticas abrangentes que cobrem todas as etapas do ciclo de vida dos dados pessoais, desde a coleta até o descarte.
 - Garantir que essas políticas sejam amplamente divulgadas e aplicadas de maneira uniforme em todas as áreas da instituição.
- **Criação de Processos de Atendimento aos Titulares:**
 - Implementar canais formais que permitam o atendimento eficiente às solicitações dos titulares de dados.
 - Estabelecer fluxos de trabalho padronizados para assegurar respostas rápidas e completas às demandas, com registros detalhados para auditorias futuras.
- **Mapeamento de Processos Operacionais:**
 - Realizar um levantamento detalhado das atividades que envolvem dados pessoais, identificando áreas críticas e estabelecendo controles apropriados.
 - Documentar esses processos para facilitar a supervisão e a auditoria contínua.
- **Padronização de Técnicas de Proteção:**
 - Tornar obrigatória a aplicação de técnicas de proteção, como mascaramento e pseudonimização, em todas as áreas que tratam dados sensíveis.
 - Estabelecer diretrizes claras para garantir a consistência e a eficácia dessas práticas.
- **Monitoramento Contínuo:**
 - Instituir um sistema de auditorias periódicas para verificar a conformidade com as políticas institucionais e identificar pontos de melhoria.

- Utilizar indicadores de desempenho para avaliar a eficácia das ações implementadas.
- Capacitação Específica:
 - Promover treinamentos regulares voltados aos responsáveis pela implementação e manutenção dos processos de tratamento de dados.
 - Garantir que a equipe compreenda plenamente as normativas aplicáveis e adote as melhores práticas de governança e segurança de dados.

6.3.1.3 Dimensão 3: Treinamento e Conscientização

A seguir, detalha-se o cálculo da pontuação da Dimensão 3, abrangendo as questões 12 a 15 do instrumento de medição. A pontuação máxima para esta dimensão é de 60 pontos. A UFC obteve uma pontuação bruta, calculada conforme a fórmula: $Q12*3 + Q13*3 + Q14*3 + Q15*3$, totalizando 15 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{15}{60} \right) \times 100 = 25 \text{ pontos}$$

Este resultado posiciona a UFC na categoria "Inicial" na Dimensão 3, conforme os intervalos definidos no MMTDP.

Análise

A maturidade institucional da UFC em relação à dimensão 3 apresenta fragilidades expressivas no que concerne à capacitação, conscientização e treinamento de colaboradores e parceiros envolvidos no tratamento de dados pessoais. A análise evidencia um cenário em que a ausência de práticas estruturadas e contínuas compromete a segurança, a conformidade regulatória e a eficiência no manejo de dados sensíveis.

Embora a instituição tenha realizado capacitações pontuais, a abordagem limitada mostrou-se insuficiente para preparar colaboradores de maneira abrangente e consistente, conforme as exigências do art. 50 da LGPD e das normas da ABNT NBR ISO/IEC 27002:2022. Capacitações esporádicas não são adequadas para abordar os desafios e responsabilidades do tratamento de dados pessoais,

enfraquecendo a capacidade da instituição de mitigar riscos e responder a incidentes de forma eficiente.

Adicionalmente, a inexistência de um programa formal de conscientização direcionado aos agentes de tratamento de dados pessoais constitui uma lacuna importante. Essa deficiência dificulta a compreensão das obrigações legais pelos colaboradores, aumentando os riscos de violações e desrespeito aos direitos dos titulares. A ausência de iniciativas voltadas à conscientização compromete o desenvolvimento de uma cultura institucional voltada à proteção de dados.

A análise identificou também que a falta de treinamentos específicos para colaboradores e parceiros diretamente envolvidos no tratamento de dados eleva os riscos operacionais e regulatórios. Sem orientações claras e práticas, as equipes podem adotar procedimentos inadequados ou negligentes, prejudicando a conformidade com a LGPD e os requisitos das normas internacionais.

Por fim, a ausência de conscientização formal sobre os riscos associados ao tratamento inadequado de dados representa uma vulnerabilidade crítica. Colaboradores que desconhecem as potenciais consequências de violações ou manipulação inadequada de dados estão mais suscetíveis a cometer erros, expondo a instituição a penalidades regulatórias e danos reputacionais. Além disso, essa ausência impede a adoção de práticas preventivas eficazes, conforme recomendam os arts. 42-45 da LGPD e os padrões da ABNT NBR ISO/IEC 27701:2019.

Recomendações

Para promover a evolução da maturidade institucional da UFC na dimensão 3, sugere-se a implementação das seguintes ações:

- **Capacitação Contínua:**
 - Estabelecer um programa regular de capacitação voltado a todos os colaboradores, com foco nos aspectos práticos e teóricos do tratamento de dados pessoais.
 - Garantir que os treinamentos abranjam todo o ciclo de vida dos dados, incluindo coleta, armazenamento, compartilhamento e descarte.
 - Incorporar estudos de caso e simulações práticas para preparar os colaboradores para situações reais.
- **Conscientização dos Agentes de Tratamento:**

- Desenvolver um programa abrangente de conscientização para todos os agentes de tratamento de dados, destacando suas responsabilidades legais e operacionais.
- Utilizar canais internos de comunicação, como newsletters e eventos, para disseminar boas práticas de proteção de dados.
- Criar materiais educativos acessíveis, como guias e vídeos, para facilitar a compreensão das normas e diretrizes.
- **Treinamento Específico para Colaboradores e Parceiros:**
 - Implementar treinamentos específicos para colaboradores e parceiros que lidam diretamente com dados pessoais, abordando técnicas de segurança e proteção.
 - Oferecer capacitações práticas sobre o uso de ferramentas de anonimização, pseudonimização e mascaramento de dados.
 - Monitorar e avaliar regularmente a eficácia dos treinamentos, ajustando o programa para garantir melhorias contínuas.
- **Gestão de Riscos e Conscientização sobre Violações:**
 - Instituir um programa de conscientização para informar os colaboradores sobre os riscos associados ao tratamento inadequado de dados pessoais.
 - Realizar palestras e workshops para destacar as consequências legais, financeiras e reputacionais de violações de dados.
 - Criar um sistema de notificação interna para identificar e tratar rapidamente possíveis falhas ou vulnerabilidades no tratamento de dados.
- **Monitoramento e Auditoria:**
 - Estabelecer auditorias periódicas para avaliar a eficácia dos programas de capacitação e conscientização.
 - Utilizar indicadores de desempenho para monitorar o progresso na implementação das políticas de treinamento e proteção de dados.

- Adaptar os programas de treinamento com base nos resultados das auditorias, garantindo alinhamento às melhores práticas e às exigências normativas.

6.3.1.4 Dimensão 4: Segurança da Informação e Tecnologia

A seguir, apresenta-se o cálculo da pontuação da Dimensão 4, abrangendo as questões 16 a 21 do instrumento de medição. A pontuação máxima é de 100 pontos. A UFC obteve uma pontuação bruta, calculada pela fórmula: $Q16*5 + Q17*3 + Q18*3 + Q19*3 + Q20*3 + Q21*3$, totalizando 39 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{39}{100} \right) \times 100 = 39 \text{ pontos.}$$

Este resultado posiciona a UFC na categoria "emergente", indicando progressos, mas com áreas a serem aprimoradas.

Análise

A análise da dimensão 4 evidencia uma combinação de avanços pontuais e lacunas críticas na gestão da segurança da informação e no uso de tecnologias. Apesar de iniciativas relevantes, como a elaboração de uma Política de Segurança da Informação e o reconhecimento da importância de controles de segurança, a implementação parcial e a falta de mecanismos padronizados comprometem a eficácia das medidas adotadas.

A existência de uma Política de Segurança da Informação representa um avanço significativo. No entanto, sua implementação parcial ou a ausência de adoção formal limita a aplicação consistente das diretrizes, aumentando a vulnerabilidade em algumas áreas. É essencial que essa política seja aplicada de maneira uniforme em toda a organização. Embora a instituição reconheça a relevância da criptografia, a aplicação limitada e inconsistente dessa técnica fragiliza a proteção de dados pessoais, expondo a organização a riscos evitáveis e contrariando as orientações da LGPD e normas como a ABNT NBR ISO/IEC 27701:2019.

A ausência de sistemas de backup e trilhas de auditoria constitui um problema crítico. Sem esses mecanismos, a organização não consegue garantir a

integridade e o ciclo de vida dos dados pessoais, deixando-se vulnerável a perdas de informações em caso de incidentes e comprometendo sua conformidade com normas de segurança. Além disso, a inexistência de processos de coleta e análise de informações sobre vulnerabilidades e ameaças impede a identificação proativa de riscos e a adoção de medidas preventivas, expondo a organização a falhas de segurança evitáveis.

A implementação parcial de controles de acesso e autenticação segura também representa uma vulnerabilidade significativa. A falta de práticas padronizadas em todas as áreas que lidam com dados pessoais dificulta a proteção desses dados, contrariando o art. 50 da LGPD, que exige medidas adequadas de segurança. Embora a organização reconheça a importância do monitoramento, a inexistência de mecanismos formais para controle e resposta a incidentes de violação de dados reduz sua capacidade de reação rápida e eficaz, comprometendo a conformidade com o art. 48 da LGPD.

Recomendações

Para promover a evolução da maturidade institucional da UFC na dimensão 4, sugere-se a adoção das seguintes ações organizadas por tópicos estratégicos

- **Política de Segurança da Informação:**
 - Implementar a Política de Segurança da Informação de maneira abrangente em toda a organização.
 - Estabelecer prazos e etapas claras para garantir a aplicação consistente das diretrizes.
 - Promover treinamentos regulares para conscientizar os colaboradores sobre a importância e a aplicação da política.
- **Proteção de Dados por Criptografia:**
 - Padronizar a aplicação da criptografia para assegurar proteção uniforme em todas as áreas que tratam de dados pessoais.
 - Implementar processos formais de gestão, monitoramento e auditoria do uso da criptografia.
 - Capacitar as equipes para utilizar ferramentas de criptografia de maneira eficaz e consistente.

- Backup e Trilhas de Auditoria:
 - Implementar sistemas de backup e trilhas de auditoria, priorizando inicialmente as áreas críticas.
 - Expandir gradualmente a cobertura desses sistemas para toda a organização.
 - Estabelecer rotinas regulares de verificação para assegurar a confiabilidade dos backups e auditorias.
- Coleta e Análise de Vulnerabilidades:
 - Criar um processo básico de coleta e análise de vulnerabilidades nas áreas de maior risco.
 - Elaborar relatórios periódicos para identificar ameaças e embasar ações de mitigação.
 - Desenvolver um plano de ação para tratar vulnerabilidades identificadas, promovendo maior resiliência.
- Controle de Acesso e Autenticação Segura:
 - Expandir e padronizar os controles de acesso em todas as áreas que tratam de dados pessoais.
 - Implementar práticas de autenticação segura, como a autenticação multifator, para reforçar a proteção.
 - Alinhar os controles aos requisitos da LGPD e aos padrões internacionais de segurança.
- Monitoramento e Resposta a Incidentes:
 - Formalizar o monitoramento de eventos de segurança e expandir os controles para cobrir todas as áreas críticas.
 - Criar um plano de resposta a incidentes, com responsáveis designados e processos documentados.
 - Realizar simulações regulares para preparar as equipes para lidar com incidentes reais.

6.3.1.5 Dimensão 5: Acesso à Informação e Transparência

A seguir, detalha-se o cálculo da pontuação da Dimensão 5 para a Universidade Federal do Ceará, abrangendo as questões 22 a 25 do instrumento de medição. Com uma pontuação máxima de 70 pontos nesta dimensão, a UFC alcançou uma pontuação bruta calculada pela fórmula: $Q22*3 + Q23*3 + Q24*5 + Q25*3$, totalizando 18 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{18}{70} \right) \times 100 = 31,43 \text{ pontos}$$

Este resultado posiciona a UFC na categoria "emergente" nesta dimensão, de acordo com os critérios do MMTDP.

Análise

A análise da dimensão 5 evidencia avanços iniciais, mas também fragilidades significativas na transparência e acessibilidade das informações relacionadas ao tratamento de dados pessoais pela UFC. Embora a instituição demonstre esforços, como a designação de um Encarregado de Proteção de Dados (DPO) e o reconhecimento da importância da transparência, as limitações na comunicação e acessibilidade comprometem a consolidação de uma governança eficaz sobre dados pessoais.

A organização reconhece a relevância da transparência. Contudo, a disponibilização restrita ou pouco acessível das informações relacionadas ao tratamento de dados pessoais reduz a clareza para os titulares, dificultando a compreensão de seus direitos. Essa limitação infringe o art. 23 da LGPD e o Decreto n. 7.724/2012, que estabelecem a clareza e acessibilidade como princípios fundamentais para a disseminação de informações públicas.

A ausência de uma Política de Classificação da Informação foi identificada como uma lacuna crítica. Tal política é indispensável para categorizar e proteger adequadamente dados sensíveis, bem como dados de crianças e adolescentes, conforme os arts. 14 e 46 da LGPD. Sem essa estrutura, a organização enfrenta dificuldades para garantir que os dados mais críticos recebam o tratamento apropriado.

Embora a designação do DPO esteja publicizada, as informações de contato disponibilizadas são limitadas ou de difícil acesso. Essa situação dificulta a comunicação direta com os titulares e compromete a conformidade com os princípios de transparência e acessibilidade previstos na LGPD e na norma ABNT NBR ISO/IEC 27701:2019.

Por fim, a falta de publicização da Política de Privacidade constitui uma falha significativa. Essa ausência prejudica a compreensão, pelos titulares, sobre como seus dados pessoais são tratados, violando o princípio de transparência previsto no art. 6º, inciso VI, da LGPD. Além de comprometer a confiança na instituição, essa falha impede o alinhamento com os requisitos normativos.

Essas fragilidades evidenciam a necessidade de aprimorar a acessibilidade e a clareza das informações fornecidas, bem como de desenvolver políticas e práticas que assegurem uma gestão mais transparente e eficiente dos dados pessoais tratados pela instituição.

Recomendações

Para fortalecer a maturidade na dimensão 5, propõem-se as seguintes ações organizadas por tópicos estratégicos:

- **Transparência e Clareza na Comunicação:**
 - Ampliar a acessibilidade das informações sobre o tratamento de dados pessoais em canais institucionais, como o site oficial da UFC.
 - Disponibilizar as informações em linguagem clara e acessível, garantindo que todos os interessados compreendam os procedimentos adotados pela organização.
 - Criar um painel de transparência que centralize informações sobre o tratamento de dados pessoais.
- **Política de Classificação da Informação:**
 - Desenvolver e implementar uma Política de Classificação da Informação que diferencie dados pessoais, dados sensíveis e dados de crianças e adolescentes.
 - Capacitar as equipes responsáveis para compreenderem e aplicarem corretamente as diretrizes da política.
 - Integrar a política ao sistema de governança de dados da instituição, alinhando-a às normas ABNT NBR ISO/IEC 27701:2019 e à LGPD.

- **Acessibilidade do Encarregado de Proteção de Dados:**
 - Tornar as informações de contato do DPO mais visíveis e acessíveis em plataformas públicas, como o site institucional.
 - Garantir múltiplos canais de contato, como e-mail, telefone e formulários on-line, para facilitar a comunicação com os titulares de dados.
 - Atualizar regularmente as informações de contato do DPO, assegurando sua precisão e disponibilidade.
- **Publicização da Política de Privacidade:**
 - Desenvolver e publicar a Política de Privacidade em formatos acessíveis e linguagem clara.
 - Disponibilizar a política em locais estratégicos, como o site institucional e espaços físicos, para facilitar o acesso dos titulares.
 - Realizar atualizações regulares na Política de Privacidade, incorporando mudanças legislativas e avanços tecnológicos.
- **Monitoramento e Auditoria**
 - Implementar auditorias periódicas para avaliar a aplicação das políticas e a eficácia das ações implementadas.
 - Definir indicadores de desempenho para medir o nível de acessibilidade e compreensão das informações pelos titulares.
 - Elaborar relatórios de conformidade para identificar áreas de melhoria contínua e propor ações corretivas.

6.3.1.6 Análise Global da Instituição

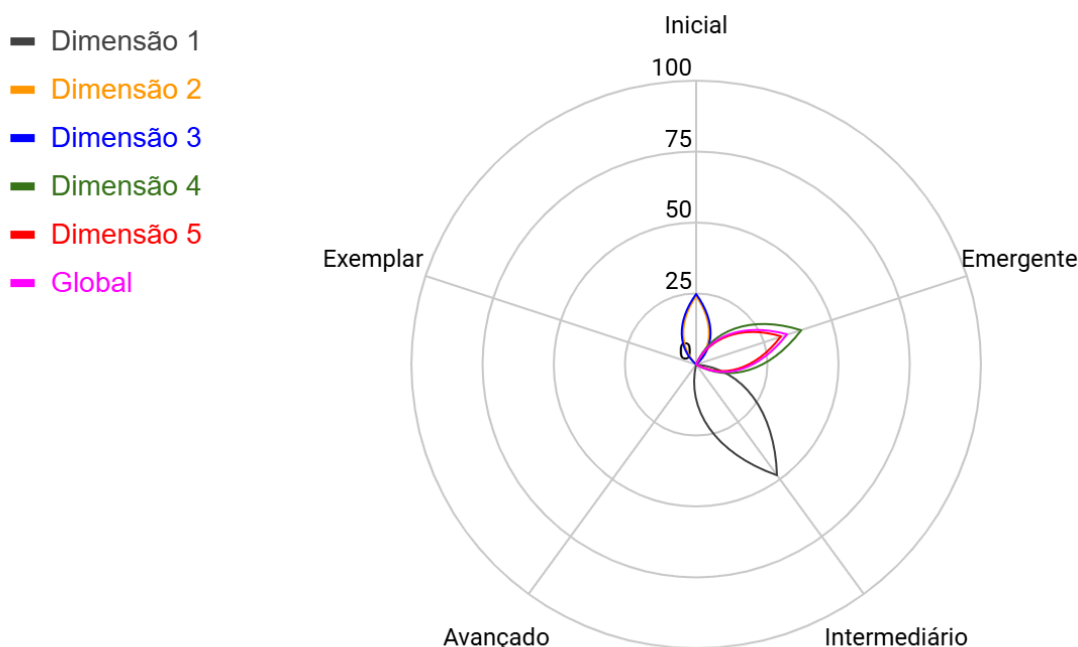
A análise global dos resultados da Universidade Federal do Ceará (UFC) revelou que a instituição encontra-se no estágio de maturidade “**Emergente**” no que tange ao tratamento de dados pessoais. Esse diagnóstico foi obtido por meio do cálculo de maturidade descrito no item **5.3.7.4**, de acordo com a fórmula:

$$Pontuação\ Global = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

Os resultados indicaram as seguintes pontuações: PND1 = 48,33 pontos, PND2 = 24 pontos, PND3 = 25 pontos, PND4 = 39 pontos e PND5 = 31,43 pontos. A pontuação global calculada foi de 33,55 pontos, refletindo iniciativas iniciais, mas ainda insuficientemente estruturadas para atender plenamente às exigências legais

e às boas práticas de proteção de dados. O Gráfico 8, ilustra as capacidades organizacionais avaliadas pela universidade:

Gráfico 8 - Níveis de maturidade da Universidade Federal do Ceará



Fonte: elaborado pelo autor.

O Gráfico 8 destaca que a dimensão "Governança de Dados e Boas Práticas" apresentou o melhor desempenho, atingindo o nível intermediário. Esse resultado reflete avanços na proteção de dados pessoais, como a criação de políticas de segurança e a designação de responsáveis por sua implementação. Contudo, essas ações ainda carecem de formalização e integração sistêmica, o que limita sua eficácia e impede a instituição de alcançar níveis mais elevados de maturidade.

Entre os desafios identificados estão a necessidade de estabelecer estruturas formais de governança e de definir claramente responsabilidades institucionais e individuais. Além disso, a criação de mecanismos robustos de monitoramento e resposta a incidentes, bem como a ampliação da capacitação dos colaboradores, são medidas fundamentais para superar as fragilidades existentes. Persistem lacunas na transparência dos processos e na adoção de tecnologias que garantam a confidencialidade, integridade e disponibilidade dos dados.

Apesar dessas limitações, a análise evidencia um início promissor de conscientização sobre a importância da proteção de dados pessoais. Iniciativas

pontuais, se ampliadas e formalizadas, podem servir como base para a construção de uma estrutura sólida e eficiente.

Para que a UFC evolua em sua maturidade institucional e atenda às exigências legais, é recomendável a adoção de medidas estratégicas em diferentes frentes. Inicialmente, é imprescindível fortalecer a governança, formalizando políticas de segurança que sejam acessíveis, abrangentes e que definam de maneira clara os papéis e responsabilidades de todos os agentes envolvidos. Adicionalmente, a criação de comitês e instâncias de governança dedicadas ao acompanhamento contínuo das ações relacionadas à proteção de dados contribuirá para consolidar uma estrutura eficiente e alinhada às melhores práticas.

No âmbito da capacitação e conscientização, torna-se indispensável implementar programas regulares de treinamento voltados para todos os envolvidos no tratamento de dados pessoais. Esses programas devem promover uma cultura organizacional que valorize a privacidade e a proteção de informações sensíveis. Além disso, campanhas educativas são essenciais para reforçar a importância do cumprimento das políticas internas e da legislação vigente, criando um ambiente de engajamento e responsabilidade compartilhada.

Em relação à segurança da informação e tecnologia, é fundamental adotar medidas técnicas avançadas, como criptografia padronizada, autenticação robusta e controles rigorosos de acesso. Investimentos em sistemas de monitoramento contínuo, voltados à detecção e prevenção de vulnerabilidades, também são recomendados, assim como a criação de planos formais de resposta a incidentes, garantindo ações rápidas e eficazes diante de falhas de segurança.

No que tange à transparência e comunicação, é essencial aprimorar os mecanismos que assegurem aos titulares um acesso claro e fácil às informações sobre o uso de seus dados pessoais. Paralelamente, é necessário aperfeiçoar os processos de comunicação com autoridades regulatórias e outras partes interessadas, garantindo a apresentação tempestiva de relatórios sobre incidentes e planos de mitigação de riscos.

Por fim, no campo da gestão de riscos e conformidade, a UFC deve realizar avaliações regulares dos riscos associados ao tratamento de dados, implementando medidas preventivas e corretivas para mitigar eventuais falhas. A conformidade contínua com as normativas legais e técnicas aplicáveis requer processos bem

documentados e auditáveis, assegurando a sustentabilidade e a eficiência das práticas institucionais relacionadas à proteção de dados pessoais.

A posição atual da UFC no nível “Emergente” reflete o início de uma jornada em direção a um sistema mais confiável e eficaz para a proteção de dados pessoais. O reconhecimento das lacunas existentes e a disposição para superá-las evidenciam o potencial da instituição para evoluir sua maturidade institucional, desde que as ações recomendadas sejam implementadas com prioridade e compromisso. Com uma abordagem estratégica e integrada, a UFC poderá não apenas alcançar maior conformidade legal, mas também consolidar-se como referência em responsabilidade e ética no tratamento de dados pessoais. Esse avanço fortalecerá a confiança na instituição e contribuirá para a consolidação de sua reputação em um cenário regulatório e tecnológico cada vez mais exigente.

6.3.2 Universidade Federal da Paraíba (UFPB)

Fundada em 1955, a Universidade Federal da Paraíba (UFPB) possui campi nas cidades de João Pessoa, Areia, Bananeiras e Litoral Norte (Mamanguape e Rio Tinto). Ao longo de sua trajetória, a UFPB passou por transformações institucionais que fortaleceram sua presença regional e ampliaram suas áreas de atuação acadêmica e de pesquisa.

A UFPB possui um portal específico para a Lei Geral de Proteção de Dados, onde divulga informações e orientações sobre assuntos relacionados, em: <https://www.ufpb.br/acessoainformacao/contents/menu/acesso-a-informacao/privacidade-e-protecao-de-dados-pessoais>. Em relação ao instrumento de medição de maturidade, a UFPB submeteu suas respostas em 27 de setembro de 2024, conforme detalhado.

Quadro 32 - Respostas do instrumento de medição da UFPB

Questões	Respostas da UFPB
Questão 1	3
Questão 2	4
Questão 3	2
Questão 4	2
Questão 5	1
Questão 6	2
Questão 7	1

Questões	Respostas da UFPB
Questão 8	1
Questão 9	1
Questão 10	1
Questão 11	2
Questão 12	2
Questão 13	1
Questão 14	1
Questão 15	1
Questão 16	3
Questão 17	2
Questão 18	1
Questão 19	1
Questão 20	2
Questão 21	2
Questão 22	2
Questão 23	1
Questão 24	2
Questão 25	1

Fonte: elaborado pelo autor.

As respostas fornecidas pela UFPB foram utilizadas para o cálculo de maturidade, seguindo a metodologia detalhada no item **5.3.7** deste trabalho e fundamentando-se nos dados padronizados disponíveis no **Apêndice M**. O Quadro 33 sintetiza a classificação da UFPB em cada dimensão avaliada, além do resultado da maturidade global da instituição.

Quadro 33 - Pontuação e classificação da UFPB

Dimensão	Pontuação	Nível de Maturidade
Dimensão 1	56,67	Intermediário
Dimensão 2	72,00	Avançado
Dimensão 3	65,00	Intermediário
Dimensão 4	82,00	Avançado
Dimensão 5	74,29	Avançado
Global	69,99	Intermediário

Fonte: elaborado pelo autor.

Esses resultados evidenciam os principais pontos de melhoria para que a UFPB eleve seus níveis de maturidade. O detalhamento da análise e recomendações pode ser observado a seguir.

6.3.2.1 Dimensão 1: Governança de Dados e Boas Práticas

A seguir, apresenta-se o cálculo de pontuação da Dimensão 1 para a Universidade Federal da Paraíba, que abrange as questões 1 a 6 do instrumento de medição. A pontuação máxima possível para esta dimensão é de 120 pontos. A UFPB obteve uma pontuação bruta calculada conforme a fórmula: $Q1*3 + Q2*5 + Q3*5 + Q4*5 + Q5*3 + Q6*3$, resultando em 68 pontos.

Aplicando equação da pontuação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{68}{120} \right) \times 100 = 56,67 \text{ pontos}$$

Esse valor, enquadrado nos intervalos predefinidos para a classificação de maturidade, posiciona a universidade na categoria "Intermediário" nesta dimensão.

Análise

A análise da dimensão 1 evidencia o estágio inicial de maturidade institucional da Universidade Federal da Paraíba em relação à governança de dados pessoais e às boas práticas. Embora a instituição tenha realizado avanços iniciais, como a designação do Encarregado de Proteção de Dados (DPO) e a elaboração de uma Política de Privacidade, as ações ainda carecem de integração sistêmica, formalização e implementação plena.

O programa de governança de dados encontra-se em fase de elaboração, demonstrando intenção de alinhamento às normas vigentes, como a LGPD e a ABNT NBR ISO/IEC 27014:2021. Contudo, a ausência de um planejamento estruturado compromete a aplicabilidade prática das diretrizes propostas, dificultando a consolidação de práticas organizacionais eficazes e alinhadas às exigências legais.

A designação formal do DPO representa um avanço significativo no fortalecimento da governança. No entanto, a falta de integração com áreas estratégicas, como Tecnologia da Informação, Jurídico e Recursos Humanos, limita sua eficácia e impede a adoção de uma abordagem multidisciplinar robusta. De

forma semelhante, o comitê de governança, embora em estágio avançado, carece de articulação mais eficaz com outras áreas institucionais para maximizar sua atuação estratégica.

A Política de Privacidade, apesar de elaborada, necessita de aprimoramentos e de alinhamento contínuo às demandas normativas e às expectativas dos titulares de dados. Paralelamente, o mapeamento informal e incompleto dos processos de compartilhamento e transferência de dados compromete a transparência e o controle, expondo a instituição a riscos regulatórios e operacionais.

Por fim, a implementação parcial do princípio da segregação de funções, com a acumulação de responsabilidades pelo DPO, configura uma vulnerabilidade relevante. A ausência de independência plena compromete a neutralidade necessária para a supervisão das atividades relacionadas à proteção de dados, contrariando os princípios de governança previstos na legislação e nas normas técnicas.

Recomendações

Para aprimorar a maturidade institucional da UFPB na dimensão 1, recomenda-se a adoção das seguintes ações estratégicas:

- Programa de Governança:
 - Formalizar o programa de governança de dados com etapas detalhadas, cronograma de implementação e definição clara dos responsáveis.
 - Garantir o alinhamento do programa às exigências da LGPD e normas internacionais, como a ABNT NBR ISO/IEC 27014:2021.
 - Promover a disseminação do programa entre líderes e colaboradores, incentivando a adesão às diretrizes estabelecidas.
- Atuação do DPO:
 - Fortalecer a integração do DPO com áreas estratégicas por meio de reuniões regulares e maior alinhamento de objetivos institucionais.
 - Elaborar um manual que define claramente as responsabilidades do DPO, assegurando sua independência e imparcialidade.
 - Oferecer treinamentos contínuos ao DPO para mantê-lo atualizado em relação às mudanças legislativas e às melhores práticas de mercado.

- Comitê de Governança:
 - Estabelecer responsabilidades claras para o comitê, criando um plano de trabalho com objetivos estratégicos e indicadores de desempenho.
 - Instituir reuniões periódicas com registros formais das decisões tomadas, assegurando transparência e rastreabilidade das ações.
 - Ampliar a integração do comitê com outras áreas institucionais para garantir a aplicação uniforme das políticas discutidas.
- Política de Privacidade:
 - Concluir e implementar a Política de Privacidade, cobrindo todas as etapas do ciclo de vida dos dados pessoais, desde a coleta até o descarte.
 - Divulgar a política de forma acessível e compreensível para todos os titulares de dados.
 - Realizar treinamentos para capacitar os colaboradores sobre os procedimentos estabelecidos pela política.
- Compartilhamento e Transferência de Dados:
 - Formalizar e concluir o mapeamento dos fluxos de compartilhamento e transferência de dados, identificando as partes envolvidas e os dados compartilhados.
 - Desenvolver mecanismos de comunicação claros para informar os titulares sobre o compartilhamento de seus dados.
 - Implementar controles e auditorias regulares para verificar a conformidade com as normas relacionadas ao compartilhamento de dados.
- Segregação de Funções:
 - Reavaliar as atribuições do DPO, distribuindo responsabilidades que possam comprometer sua neutralidade.
 - Estabelecer políticas formais que garantam a segregação de funções, minimizando riscos de conflitos de interesse.

- Realizar auditorias periódicas para avaliar a independência e a eficácia do DPO na supervisão das atividades relacionadas à proteção de dados.

6.3.2.2 Dimensão 2: Políticas e Processos de Tratamento de Dados

A seguir, apresenta-se o cálculo da pontuação da Dimensão 2 para a UFPB, que abrange as questões 7 a 11 do instrumento de medição. A pontuação máxima para esta dimensão é de 75 pontos. A UFPB obteve uma pontuação bruta, calculada conforme a fórmula: $Q7*3 + Q8*3 + Q9*3 + Q10*3 + Q11*3$, resultando em 54 pontos.

Aplicou-se a equação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{54}{75} \right) \times 100 = 72 \text{ pontos}$$

Este resultado posiciona a UFPB na categoria "Avançado" na Dimensão 2, conforme os critérios e intervalos previamente estabelecidos no MMTDP. Essa classificação indica que a instituição está em um bom nível de maturidade nessa dimensão.

Análise

A análise da dimensão 2 evidencia avanços pontuais e significativos na maturidade da Universidade Federal da Paraíba em relação às políticas e processos de tratamento de dados pessoais. Apesar de progressos relevantes, como a identificação inicial de agentes de tratamento e a implementação de mecanismos abrangentes para garantir os direitos dos titulares, persistem lacunas que comprometem a consolidação de uma governança de dados plenamente estruturada e alinhada às exigências da LGPD e às normas internacionais, como a ABNT NBR ISO/IEC 27701:2019.

No que se refere à identificação das categorias de dados pessoais e respectivos titulares, a organização iniciou esse processo de forma documentada. Contudo, a abordagem limitada e incompleta restringe a aplicação de controles adequados e dificulta o cumprimento integral das exigências legais, comprometendo a abrangência e a eficiência das ações.

A documentação dos agentes de tratamento de dados pessoais representa um avanço relevante, mas a ausência de monitoramento contínuo limita a eficácia da governança e dificulta a adaptação a mudanças normativas ou organizacionais. Esse cenário, embora positivo como ponto de partida, exige medidas adicionais para alcançar um sistema robusto e sustentável.

A identificação dos processos e atividades operacionais que lidam com dados pessoais foi realizada parcialmente e de maneira informal, comprometendo a gestão eficaz desses dados. A ausência de um mapeamento completo representa um desafio para a implementação de políticas consistentes e alinhadas às boas práticas.

No que tange aos mecanismos formais para garantir os direitos dos titulares, a UFPB demonstra maturidade e abrangência. Esses mecanismos são bem implementados, revisados e continuamente aprimorados, reforçando a conformidade com as exigências legais e promovendo maior confiança dos titulares de dados.

Por fim, a instituição apresenta elevado nível de maturidade na aplicação de técnicas de mascaramento, pseudonimização e anonimização de dados sensíveis, com regras rigorosas e monitoramento regular. Essas práticas garantem a proteção contra acessos não autorizados e minimizam os riscos de vazamentos, atendendo às melhores práticas de segurança de dados.

Recomendações

Para elevar a maturidade institucional da UFPB na dimensão 2, recomenda-se a implementação das seguintes ações estratégicas:

- **Identificação das Categorias de Dados e Titulares:**
 - Ampliar o mapeamento das categorias de dados pessoais e respectivos titulares, documentando detalhadamente todas as informações.
 - Realizar auditorias regulares para verificar a completude e a precisão do mapeamento.
 - Criar um processo formal e contínuo de revisão e atualização das informações mapeadas.
- **Monitoramento de Agentes de Tratamento:**

- Implementar um sistema de monitoramento contínuo dos agentes de tratamento, assegurando sua conformidade com as diretrizes normativas.
- Estabelecer auditorias periódicas para avaliar o desempenho dos agentes e o alinhamento com as políticas internas e regulamentações aplicáveis.
- Promover treinamentos específicos para os agentes de tratamento, garantindo entendimento pleno das obrigações legais e operacionais.
- Mapeamento de Processos Operacionais:
 - Formalizar o mapeamento de processos e atividades que envolvam dados pessoais, documentando detalhadamente cada etapa e identificando áreas críticas.
 - Utilizar ferramentas de gestão e mapeamento de processos para facilitar a atualização e visualização das atividades.
 - Estabelecer uma governança centralizada para supervisionar e revisar continuamente os processos relacionados ao tratamento de dados.
- Direitos dos Titulares:
 - Manter a prática de revisão e melhoria contínua dos mecanismos formais que asseguram os direitos dos titulares.
 - Desenvolver um sistema de acompanhamento das solicitações feitas pelos titulares, garantindo respostas rápidas, precisas e adequadas.
 - Divulgar de maneira clara e acessível os canais de comunicação, ampliando a transparência e a confiança no tratamento de dados.
- Segurança de Dados Sensíveis:
 - Continuar investindo em tecnologias e práticas que assegurem a proteção de dados sensíveis, como criptografia avançada e anonimização.
 - Ampliar o monitoramento e a revisão periódica das técnicas utilizadas, acompanhando inovações tecnológicas e novas demandas regulatórias.
 - Promover treinamentos regulares para as equipes que lidam diretamente com dados sensíveis, assegurando a aplicação consistente das técnicas de proteção.
- Auditoria e Melhoria Contínua:

- Instituir um cronograma regular de auditorias para verificar a conformidade dos processos e práticas com a LGPD e normas internacionais.
- Estabelecer indicadores de desempenho para avaliar a evolução das práticas de tratamento de dados e sua eficácia.
- Realizar reuniões periódicas com as partes interessadas para discutir avanços, identificar lacunas e propor melhorias contínuas no sistema de governança.

6.3.2.3 Dimensão 3: Treinamento e Conscientização

A seguir, detalha-se o cálculo da pontuação da Dimensão 3 para a Universidade Federal da Paraíba, abrangendo as questões 12 a 15 do instrumento de medição. Com uma pontuação máxima de 60 pontos nesta dimensão, a UFPB alcançou uma pontuação bruta calculada pela fórmula: $Q12*3 + Q13*3 + Q14*3 + Q15*3$, totalizando 39 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{39}{60} \right) \times 100 = 65 \text{ pontos}$$

Este resultado posiciona a universidade no nível de maturidade "Intermediário" nesta dimensão, de acordo com os critérios do MMTDP.

Análise

A análise da dimensão 3 evidencia que a Universidade Federal da Paraíba apresenta avanços pontuais em capacitação e conscientização no tratamento de dados pessoais, embora persistam lacunas que comprometem a evolução para um nível de maturidade plena e sustentável.

No que se refere aos programas de capacitação, constatou-se que a UFPB implementou iniciativas que abordam aspectos pontuais do tratamento e proteção de dados pessoais. Contudo, essa abordagem limitada não abrange todos os envolvidos, o que dificulta a construção de uma cultura organizacional ampla e integrada em segurança da informação. A ausência de programas contínuos e detalhados para todos os colaboradores, conforme preconizado no art. 50 da LGPD

e na ABNT NBR ISO/IEC 27002:2022, reflete um nível de maturidade ainda em evolução.

Por outro lado, a UFPB demonstra maturidade avançada na conscientização dos agentes de tratamento. A existência de um programa abrangente e contínuo assegura que os agentes compreendam plenamente suas responsabilidades no tratamento de dados, alinhando-se aos requisitos normativos e às melhores práticas. Esse avanço é essencial para garantir a conformidade regulatória e a mitigação de riscos.

Entretanto, observou-se que os treinamentos direcionados para colaboradores e parceiros ainda apresentam abrangência limitada. Essa limitação compromete a uniformidade na aplicação das boas práticas de proteção de dados. O art. 50 da LGPD reforça a importância de capacitar todos os agentes envolvidos no tratamento de dados, tornando a ampliação dos treinamentos uma necessidade estratégica.

Quanto à conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, a universidade conta com um programa regular. Contudo, foram identificadas áreas que demandam melhorias para torná-lo mais completo e eficaz. Essa lacuna pode impactar negativamente a percepção dos riscos por parte dos colaboradores, reduzindo a eficácia das ações preventivas e a aderência às melhores práticas de mitigação.

De maneira geral, os avanços refletem o compromisso da UFPB com a proteção de dados. No entanto, a falta de uniformidade e abrangência nos programas de capacitação e conscientização limita o progresso em direção a um nível de maturidade institucional mais elevado.

Recomendações

Para fortalecer a maturidade institucional da UFPB na dimensão 3, recomenda-se a adoção das seguintes ações estratégicas:

- Expansão dos Programas de Capacitação:
 - Ampliar o escopo dos programas de capacitação para incluir todos os colaboradores, terceirizados e parceiros que lidam com dados pessoais.

- Desenvolver conteúdos abrangentes que contemplem o ciclo de vida dos dados, cobrindo coleta, armazenamento, compartilhamento e descarte.
- Incorporar estudos de caso, simulações práticas e exemplos reais de incidentes de segurança para aumentar a aplicabilidade dos treinamentos.
- Estabelecer cronogramas regulares para assegurar a continuidade e a atualização dos conteúdos, alinhando-os às mudanças regulatórias e tecnológicas.
- Fortalecimento da Conscientização dos Agentes de Tratamento:
 - Manter e aprimorar os programas de conscientização existentes, promovendo revisões periódicas para garantir alinhamento às melhores práticas e novas exigências normativas.
 - Desenvolver materiais de apoio, como guias, manuais e vídeos educativos, para reforçar o entendimento das responsabilidades dos agentes de tratamento.
 - Estabelecer indicadores de desempenho para avaliar o impacto das ações de conscientização e identificar oportunidades de melhoria.
- Abrangência dos Treinamentos:
 - Expandir os treinamentos para abranger todos os agentes envolvidos, promovendo uniformidade na aplicação das políticas de proteção de dados.
 - Criar módulos específicos para diferentes níveis de envolvimento com dados pessoais, assegurando maior relevância e eficácia.
 - Monitorar a participação nos treinamentos e avaliar seu impacto por meio de questionários e auditorias internas.
- Melhorias nos Programas de Conscientização sobre Riscos:
 - Atualizar continuamente os conteúdos dos programas de conscientização, incorporando novos riscos, ameaças e tendências de segurança.
 - Realizar palestras, workshops e campanhas de sensibilização para destacar as consequências legais e reputacionais do tratamento inadequado de dados pessoais.

- Personalizar as ações de conscientização para refletir os riscos específicos de cada área da instituição, aumentando a relevância e o impacto das iniciativas.
- Monitoramento e Auditoria:
 - Implementar auditorias periódicas para avaliar a eficácia dos programas de capacitação e conscientização.
 - Utilizar métricas, como taxas de participação, compreensão dos conteúdos e redução de incidentes, para medir os resultados das ações implementadas.
 - Realizar reuniões regulares com as equipes responsáveis para discutir avanços, identificar lacunas e propor ajustes nos programas de capacitação e conscientização.

6.3.2.4 Dimensão 4: Segurança da Informação e Tecnologia

A seguir, apresenta-se o cálculo da pontuação da Dimensão 4 para a Universidade Federal da Paraíba, que abrange as questões 16 a 21 do instrumento de medição. A pontuação máxima para esta dimensão é de 100 pontos. A UFPB obteve uma pontuação bruta, calculada conforme a fórmula: $Q16*5 + Q17*3 + Q18*3 + Q19*3 + Q20*3 + Q21*3$, resultando em 82 pontos.

Aplicando a equação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{82}{100} \right) \times 100 = 82 \text{ pontos.}$$

Este resultado posiciona a UFPB na categoria "Avançado" na Dimensão 4, conforme os critérios e intervalos previamente estabelecidos no MMTDP.

Análise

A análise da dimensão 4 evidencia um progresso da universidade no que diz respeito à segurança da informação e ao uso de tecnologias no tratamento de dados pessoais. Apesar dos avanços observados, a implementação ainda apresenta inconsistências em diversas áreas, apontando para a necessidade de monitoramento contínuo e uma maior integração entre as práticas de segurança e outras iniciativas institucionais.

A elaboração e implementação da Política de Segurança da Informação representam um marco importante para a organização. No entanto, a ausência de um monitoramento sistemático e de revisões regulares compromete sua atualização contínua e a capacidade de adaptação a novos desafios tecnológicos e regulatórios. Essa lacuna destaca a importância de maior vigilância e ajustes periódicos para garantir a eficácia e a relevância da política.

O uso da criptografia na proteção de dados pessoais demonstra um nível avançado de maturidade, com aplicação consistente em áreas críticas. Contudo, foram identificadas necessidades de aprimoramento no monitoramento dessas práticas, o que pode comprometer a segurança total dos dados armazenados ou transmitidos pela instituição.

No que se refere à gestão de backups e trilhas de auditoria, a UFPB apresenta um sistema bem estruturado. Entretanto, há necessidade de uma integração mais robusta com outras práticas de governança de dados, assegurando a proteção abrangente dos dados ao longo de todo o seu ciclo de vida. Quanto à coleta e análise de informações relacionadas a vulnerabilidades e ameaças, constatou-se que o processo estruturado existente ainda precisa ser expandido para abranger todas as áreas críticas de segurança da informação.

Em relação aos controles de acesso e autenticação segura, a UFPB adota medidas amplamente implementadas, mas que ainda exigem revisões regulares para garantir a conformidade com as normas vigentes. Da mesma forma, os mecanismos de monitoramento de eventos de violação e vazamento de dados estão bem estabelecidos, embora careçam de maior integração com outras práticas de segurança e de um aprimoramento contínuo.

De maneira geral, a UFPB demonstra um nível de maturidade avançado em várias frentes de segurança da informação. Contudo, a ausência de integração plena entre os diferentes aspectos e a falta de monitoramento contínuo em algumas áreas evidenciam oportunidades de melhoria que podem consolidar ainda mais a maturidade institucional da universidade.

Recomendações

Para elevar sua maturidade na dimensão de segurança da informação, recomenda-se à UFPB a adoção das seguintes ações estratégicas:

- Monitoramento e Revisão da Política de Segurança da Informação:

- Estabelecer um cronograma de revisões periódicas da política para assegurar alinhamento contínuo com os avanços tecnológicos e regulatórios.
- Incorporar feedback dos colaboradores e análises de incidentes para aperfeiçoar o conteúdo da política.
- Promover treinamentos regulares para reforçar a compreensão e a aplicação das diretrizes entre os colaboradores.
- **Aperfeiçoamento no Uso de Criptografia:**
 - Ampliar o monitoramento e a revisão das práticas de criptografia em todas as áreas críticas.
 - Adotar tecnologias de ponta para fortalecer a robustez das soluções de criptografia implementadas.
 - Capacitar as equipes responsáveis para acompanhar tendências e inovações no campo da proteção de dados.
- **Integração de Backups e Trilhas de Auditoria:**
 - Integrar os sistemas de backup e auditoria às demais práticas de governança de dados para criar um ambiente coeso e seguro.
 - Realizar testes periódicos para validar a confiabilidade dos backups e a rastreabilidade dos dados.
 - Documentar detalhadamente todos os processos relacionados ao ciclo de vida dos dados, garantindo transparência e conformidade.
- **Expansão da Gestão de Vulnerabilidades:**
 - Ampliar o alcance do processo de coleta e análise de vulnerabilidades, abrangendo todas as áreas críticas.
 - Implementar ferramentas de inteligência de ameaças para monitoramento contínuo e proativo.
 - Produzir relatórios regulares que orientem decisões estratégicas para mitigação de riscos.
- **Controle de Acesso e Autenticação:**
 - Fortalecer o monitoramento e a revisão dos controles de acesso e autenticação em todas as áreas sensíveis.
 - Adotar práticas avançadas, como autenticação multifator, para aumentar a segurança.

- Realizar auditorias frequentes para ajustar permissões e identificar falhas potenciais.
- Monitoramento de Incidentes e Integração de Práticas de Segurança:
 - Desenvolver uma política integrada para monitoramento de incidentes, alinhando-a às demais práticas de segurança.
 - Adotar ferramentas automatizadas para detecção e resposta rápida a incidentes de segurança.
 - Realizar simulações periódicas de incidentes, treinando as equipes para agir de forma eficaz em cenários reais.

6.3.2.5 Dimensão 5: Acesso à Informação e Transparência

A seguir, detalha-se o cálculo da pontuação da Dimensão 5 para a Universidade Federal da Paraíba, abrangendo as questões 22 a 25 do instrumento de medição. Com uma pontuação máxima de 70 pontos nesta dimensão, a UFPB alcançou uma pontuação bruta calculada pela fórmula: $Q22*3 + Q23*3 + Q24*5 + Q25*3$, totalizando 52 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{52}{70} \right) \times 100 = 74,29 \text{ pontos}$$

Este resultado posiciona a UFPB na categoria "Avançado" na Dimensão 5, de acordo com os critérios de maturidade organizacional do MMTDP.

Análise

A análise das respostas evidencia aspectos cruciais sobre a maturidade da organização no que tange à conformidade com os princípios de transparência e às boas práticas de tratamento de dados pessoais. Inicialmente, observa-se que a organização demonstra plena aderência ao princípio da transparência, ao disponibilizar informações claras, completas e acessíveis sobre o tratamento de dados. Essa prática denota alinhamento com os artigos 50 e 25 da Lei Geral de Proteção de Dados, promovendo confiança entre os titulares de dados. Além disso, o monitoramento contínuo dessas informações reforça a capacidade da organização de se adaptar a novas regulamentações e demandas, fortalecendo sua postura proativa e responsável.

Entretanto, identifica-se uma lacuna relevante: a inexistência de uma Política de Classificação da Informação ou de instrumento equivalente. Essa ausência compromete o tratamento adequado de diferentes categorias de dados, especialmente dados sensíveis e informações relacionadas a crianças e adolescentes. Tal cenário implica a não conformidade com o artigo 46 da LGPD, que exige medidas proporcionais à sensibilidade dos dados, além de infringir o artigo 14, que impõe cuidados específicos para dados de menores. Essa deficiência destaca a necessidade urgente de estruturar políticas que garantam segurança, organização e conformidade no tratamento das informações.

Em relação à publicização das informações do encarregado de proteção de dados (DPO), a organização demonstra maturidade ao assegurar ampla acessibilidade e monitoramento regular desses dados de contato. Essa iniciativa evidencia alinhamento com os requisitos do artigo 41 da LGPD, promovendo transparência e viabilizando o exercício dos direitos dos titulares. O monitoramento contínuo dessa acessibilidade reforça a confiança na instituição, garantindo a eficácia dos canais de comunicação.

Por fim, verifica-se que, embora a Política de Privacidade esteja publicizada, ainda apresenta limitações quanto à acessibilidade e clareza para todos os interessados. Essa situação compromete a conformidade com o artigo 6º, inciso IV, da LGPD, que exige práticas de tratamento de dados compreensíveis para o público em geral. Torna-se, portanto, essencial revisar detalhadamente o conteúdo dessa política, assegurando maior acessibilidade, clareza e transparência, de modo a atender plenamente às exigências legais e às expectativas dos titulares.

Recomendações

A partir da análise apresentada, propõe-se um conjunto de ações estratégicas e organizadas para elevar a maturidade da instituição nas práticas de tratamento e proteção de dados pessoais:

- Aprimorar a comunicação sobre o tratamento de dados pessoais:
 - Manter o monitoramento contínuo da conformidade das informações publicizadas, assegurando que estejam sempre atualizadas, claras e acessíveis.

- Incorporar feedbacks dos titulares como instrumento para identificar oportunidades de melhoria na transparência e no detalhamento das práticas de tratamento de dados.
- Realizar revisões periódicas das informações disponibilizadas, garantindo alinhamento com novas regulamentações e boas práticas do setor.
- Desenvolver e implementar uma Política de Classificação da Informação:
 - Elaborar um documento abrangente, categorizando dados pessoais, dados sensíveis e informações relacionadas a crianças e adolescentes.
 - Basear a estrutura da política nas normas ABNT NBR ISO/IEC 27701 e 27002, adotando padrões reconhecidos internacionalmente.
 - Promover treinamentos regulares para os colaboradores, garantindo o entendimento e a aplicação adequada da política.
 - Estabelecer um cronograma de revisões e atualizações periódicas, assegurando que a política acompanhe as mudanças legais e operacionais.
- Fortalecer a comunicação e o monitoramento contínuo das informações do DPO:
 - Expandir os canais de divulgação das informações de contato do DPO, garantindo ampla visibilidade e acessibilidade.
 - Implementar testes regulares de acessibilidade para verificar a atualização e a eficiência dos canais de comunicação.
 - Incorporar feedbacks dos titulares para ajustar os canais de comunicação às suas necessidades e expectativas.
- Revisar e tornar a Política de Privacidade mais acessível e compreensível:
 - Reescrever a Política de Privacidade em linguagem clara, objetiva e acessível, facilitando a compreensão por parte de todos os interessados.
 - Disponibilizar a política em locais de fácil acesso, como o site institucional e plataformas digitais amplamente utilizadas pela organização.

- Implementar um sistema de revisões regulares da Política de Privacidade, garantindo que ela reflita as práticas atuais de tratamento de dados e as mudanças nas regulamentações.
- Promover campanhas educativas para conscientizar os titulares sobre a importância da Política de Privacidade, destacando seus direitos e como podem exercê-los.

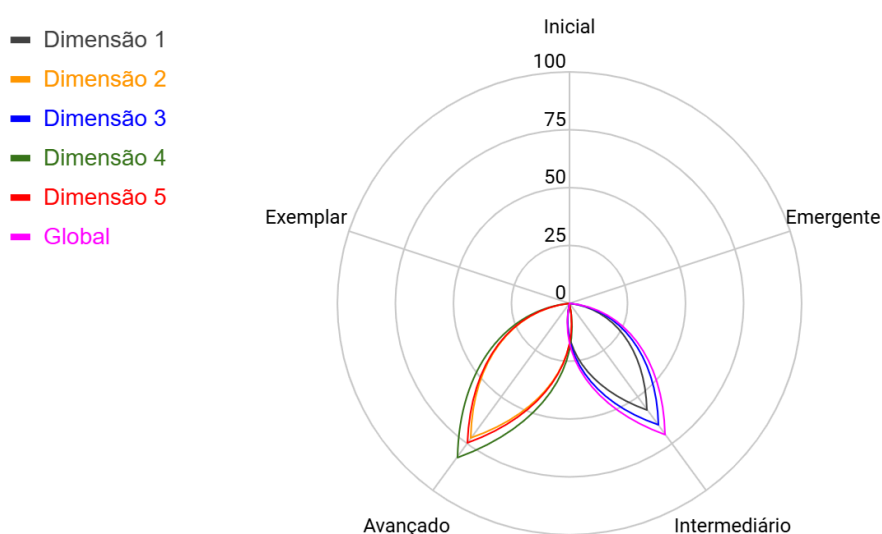
6.3.2.6 Análise Global da Instituição

A análise global dos resultados da Universidade Federal da Paraíba (UFPB) aponta que a instituição alcançou o estágio de maturidade **“Intermediário”** no tratamento de dados pessoais, conforme o cálculo descrito no item **5.3.7.4**, a fórmula aplicada foi a seguinte:

$$\text{Pontuação Global} = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

Os dados apurados revelaram as seguintes pontuações por dimensão: PND1 = 56,67 pontos, PND2 = 72 pontos, PND3 = 65 pontos, PND4 = 82 pontos e PND5 = 74,29 pontos, resultando em uma pontuação global de 69,99 pontos. Esse resultado reflete uma implementação parcial e estruturada de políticas de proteção de dados, assegurando conformidade inicial com legislações e normas relevantes. Contudo, revela a necessidade de aprimoramentos significativos para atingir uma governança plena.

Gráfico 9 - Níveis de maturidade da Universidade Federal da Paraíba



Fonte: elaborado pelo autor.

A Dimensão de Segurança da Informação e Tecnologia destacou-se como o melhor desempenho entre as áreas avaliadas, alcançando o nível intermediário. O Gráfico 9 evidencia a distribuição das capacidades organizacionais.

Os resultados indicam que a UFPB alcançou progressos importantes, como a criação de uma estrutura formal de governança de dados, que inclui a nomeação de um Encarregado de Proteção de Dados (DPO) e a formação de comitês especializados. Essas ações demonstram alinhamento com a Lei Geral de Proteção de Dados e normas como ABNT NBR ISO/IEC 27701:2019 e ISO/IEC 27014:2021. Entretanto, há necessidade de maior integração entre o DPO e áreas estratégicas, como Tecnologia da Informação (TI) e Jurídico, para fortalecer a governança por meio de abordagens multidisciplinares.

No ciclo de vida dos dados, observa-se a existência de políticas documentadas abrangendo etapas como coleta, armazenamento e descarte. Porém, o mapeamento de dados carece de maior formalização e abrangência para atender plenamente aos requisitos legais e normativos. Além disso, a gestão de consentimento e o controle de acesso demandam maior rigor, de forma a promover transparência e segurança e mitigar riscos associados ao tratamento de dados, especialmente os sensíveis e relacionados a menores.

Na área de segurança da informação, identificam-se boas práticas, como o uso de criptografia, backups regulares e auditorias. Contudo, a aplicação dessas práticas é desigual entre os setores da instituição. A implementação das normas ABNT NBR ISO/IEC 27005:2023, voltada à gestão de riscos, e ISO/IEC 27035:2023, que trata do monitoramento contínuo, é recomendada para promover revisões mais sistemáticas e abrangentes. Expansão do uso de autenticação forte e auditorias regulares também são necessárias para garantir uma proteção uniforme e eficaz.

Em termos de capacitação, a UFPB demonstra compromisso com treinamentos regulares voltados à proteção de dados e segurança da informação. Todavia, o alcance desses programas deve ser ampliado para assegurar que todos os colaboradores compreendam suas responsabilidades legais, normativas e éticas. A construção de uma cultura organizacional que valorize a proteção de dados é fundamental para incorporar as práticas de governança às rotinas institucionais e promover alinhamento estratégico.

A transparência também se apresenta como um ponto de atenção. Embora a UFPB disponibilize amplamente os contatos do DPO e informações relacionadas,

em conformidade com o art. 41 da LGPD, faz-se necessária a implementação de uma Política de Classificação da Informação, além de revisões na Política de Privacidade. Essas medidas garantirão maior clareza na comunicação institucional e promoverão um entendimento mais amplo sobre o tratamento de dados pessoais.

O posicionamento da UFPB no nível “Intermediário” reflete esforços relevantes na construção de uma estrutura de governança de dados. Contudo, as lacunas identificadas sugerem que a formalização de práticas, o fortalecimento da segurança da informação e a ampliação de programas de capacitação são indispensáveis para a consolidação de uma governança robusta e eficaz.

Ao investir no aprimoramento contínuo e no monitoramento de suas práticas, a UFPB estará apta a atender integralmente às exigências legais e normativas, fortalecendo sua posição como referência em governança de dados. Tais avanços consolidam a confiança dos titulares de dados e promoverão uma reputação institucional fundamentada na ética, responsabilidade e excelência.

6.3.3 Universidade Federal da Bahia (UFBA)

Criada em 1946, a Universidade Federal da Bahia (UFBA) possui campi nas cidades de Salvador, Vitória da Conquista e Barreiras. A UFBA é reconhecida por sua influência cultural e acadêmica na região Nordeste. Para assegurar a conformidade com a Lei Geral de Proteção de Dados, a instituição mantém um site com informações sobre o tema, que pode ser acessado em: <https://lgpd.ufba.br/>. A UFBA registrou suas respostas ao instrumento de medição de maturidade também na data de 10 de outubro de 2024, conforme as respostas registradas.

Quadro 34 - Respostas do instrumento de medição da UFBA

Questões	Respostas da UFBA
Questão 1	3
Questão 2	4
Questão 3	4
Questão 4	5
Questão 5	5
Questão 6	5
Questão 7	5
Questão 8	5
Questão 9	5
Questão 10	5

Questão 11	5
Questão 12	3
Questão 13	5
Questão 14	4
Questão 15	4
Questão 16	2
Questão 17	1
Questão 18	4
Questão 19	3
Questão 20	4
Questão 21	4
Questão 22	5
Questão 23	4
Questão 24	5
Questão 25	5

Fonte: elaborado pelo autor.

As respostas fornecidas pela UFBA foram utilizadas para o cálculo de maturidade, seguindo a metodologia detalhada no item **5.3.7** deste trabalho e fundamentando-se nos dados padronizados disponíveis no **Apêndice M**. O Quadro 35 sintetiza a classificação da UFBA em cada uma das dimensões avaliadas e apresenta o resultado da maturidade global da instituição.

Quadro 35 - Pontuação e classificação da UFBA

Dimensão	Pontuação	Nível de Maturidade
Dimensão 1	86,67	Avançado
Dimensão 2	100,00	Exemplar
Dimensão 3	80,00	Avançado
Dimensão 4	58,00	Intermediário
Dimensão 5	95,71	Exemplar
Global	82,82	Avançado

Fonte: elaborado pelo autor.

Esses resultados evidenciam os principais pontos de melhoria para que a UFBA eleve seus níveis de maturidade. O detalhamento da análise dessas classificações pode ser observado a seguir.

6.3.3.1 Dimensão 1: Governança de Dados e Boas Práticas

A seguir, apresenta-se o detalhamento do cálculo de pontuação da Dimensão 1 para a Universidade Federal da Bahia (UFBA), que abrange as questões 1 a 6 do instrumento de medição. A pontuação máxima possível para esta dimensão é de 120 pontos. A UFBA obteve uma pontuação bruta calculada conforme a fórmula: $Q1*3 + Q2*5 + Q3*5 + Q4*5 + Q5*3 + Q6*3$, resultando em 104 pontos.

Aplicando equação da pontuação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{104}{120} \right) \times 100 = 86,67 \text{ pontos}$$

Esse valor posiciona a UFBA no nível de maturidade "Avançado" na Dimensão 1. Essa avaliação revela um nível considerável de maturidade nas práticas de governança de dados, embora com algumas lacunas a serem preenchidas para alcançar maior efetividade e alinhamento com as melhores práticas.

Análise

A análise dos resultados evidencia avanços significativos e desafios persistentes na governança de dados da organização, destacando pontos fortes e áreas que necessitam de melhorias. A seguir, são apresentados os principais aspectos identificados.

Inicialmente, constatou-se que a organização já elaborou um programa ou plano de governança, mas sua implementação permanece parcial. Esse avanço demonstra um compromisso inicial com a proteção de dados, mas a execução incompleta compromete a eficácia das práticas e a credibilidade perante os titulares. Torna-se imprescindível formalizar e internalizar o programa para assegurar o pleno alinhamento às normativas, especialmente à LGPD e ao Decreto n. 10.046/2019.

Em relação ao Encarregado de Proteção de Dados (DPO), verificou-se que sua designação foi formalizada e sua atuação reconhecida. No entanto, a integração com áreas estratégicas, como Tecnologia da Informação (TI) e Jurídico, ainda apresenta lacunas. Essa integração é essencial para uma governança eficaz, conforme preconizado pela norma ISO/IEC 27701:2019, pois permite uma abordagem multidisciplinar para a proteção de dados pessoais.

A análise também demonstra que o comitê interno de governança de dados já possui funções bem definidas e integração com áreas relevantes. Contudo, há

margem para expandir sua atuação estratégica, o que fortalecerá sua eficácia na coordenação de ações e no acompanhamento das políticas de proteção de dados.

No que tange à Política de Privacidade, observa-se que esta está bem estruturada, amplamente divulgada e aplicada uniformemente. Esse nível de maturidade reflete um compromisso com a transparência e a conformidade legal, promovendo confiança entre os titulares de dados. No entanto, revisões regulares são indispensáveis para garantir que o documento permaneça atualizado e alinhado às mudanças normativas e práticas de mercado.

Ademais, a identificação, documentação e controle formal do compartilhamento de dados destacam um nível avançado de maturidade. A realização de monitoramentos contínuos e revisões regulares das práticas reforçam a transparência e garantem conformidade com os artigos 33 a 36 da LGPD, assegurando a proteção dos dados pessoais compartilhados com terceiros.

Por fim, verifica-se que a organização segue plenamente o princípio da segregação de funções, assegurando que o DPO tenha total autonomia e dedicação exclusiva à sua função. Essa prática reduz riscos de conflitos de interesse e promove maior eficácia na supervisão das atividades relacionadas à proteção de dados.

Recomendações

Com base na análise apresentada, sugere-se o seguinte conjunto de ações para elevar a maturidade institucional em governança de dados e proteção da privacidade:

- Formalizar e implementar plenamente o programa de governança de dados:
 - Estabelecer um plano de implementação detalhado, com prazos e responsáveis claramente definidos.
 - Criar um comitê de governança de dados para supervisionar a execução do programa e monitorar seu progresso.
 - Promover treinamentos para as equipes envolvidas, assegurando o entendimento das políticas e práticas estabelecidas.
- Fortalecer a integração do DPO com áreas estratégicas:
 - Instituir reuniões regulares entre o DPO e setores como TI, Jurídico e Recursos Humanos para alinhar ações e estratégias.

- Prover treinamentos contínuos ao DPO, garantindo sua atualização em legislações e boas práticas.
 - Implementar canais internos de comunicação para facilitar a troca de informações entre o DPO e as demais áreas.
- Ampliar a atuação estratégica do comitê de governança de dados:
 - Definir metas e indicadores de desempenho para o comitê, monitorando seu impacto nas práticas institucionais.
 - Documentar reuniões e decisões do comitê, assegurando transparência e rastreabilidade das ações.
 - Promover maior integração do comitê com as áreas operacionais, fortalecendo o alinhamento entre estratégia e execução.
- Revisar e aprimorar continuamente a Política de Privacidade:
 - Realizar revisões periódicas da Política de Privacidade para assegurar alinhamento com mudanças legais e avanços tecnológicos.
 - Incorporar feedbacks de titulares e colaboradores, ajustando a política às necessidades identificadas.
 - Divulgar amplamente as atualizações realizadas, reforçando a transparência e a confiança institucional.
- Aprimorar o controle e o monitoramento do compartilhamento de dados pessoais:
 - Realizar auditorias regulares para verificar a conformidade das transferências de dados com as regulamentações aplicáveis.
 - Atualizar continuamente os procedimentos de controle, incorporando práticas de segurança mais robustas.
 - Implementar relatórios periódicos para monitorar o compartilhamento de dados com terceiros.
- Manter a independência e eficácia do DPO:
 - Realizar auditorias periódicas para avaliar a independência do DPO e identificar possíveis interferências.

- Criar um canal de denúncia confidencial para que o DPO possa relatar interferências ou dificuldades em sua atuação.
- Promover treinamentos para a alta administração sobre a importância da autonomia do DPO, reforçando seu papel estratégico.

6.3.3.2 Dimensão 2: Políticas e Processos de Tratamento de Dados

A seguir, apresenta-se o cálculo da pontuação da Dimensão 2 para a Universidade Federal da Bahia, que abrange as questões 7 a 11 do instrumento de medição. A pontuação máxima para esta dimensão é de 75 pontos. A UFBA obteve uma pontuação bruta, calculada conforme a fórmula: $Q7*3 + Q8*3 + Q9*3 + Q10*3 + Q11*3$, resultando em 75 pontos.

Aplicando a equação da pontuação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{75}{75} \right) \times 100 = 100 \text{ pontos}$$

Este resultado posiciona a UFBA na categoria "Exemplar" na Dimensão 2, conforme os critérios e intervalos previamente estabelecidos para a avaliação da maturidade organizacional no MMTDP. Essa classificação indica que a instituição está atendendo todas as exigências que envolvem esta dimensão.

Análise

A análise das práticas da organização revela um elevado nível de maturidade nesta dimensão, evidenciando conformidade plena com os princípios legais e normativos aplicáveis e refletindo uma gestão bem estruturada e eficaz.

Verificou-se que a organização identificou, documentou e mantém um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação. Essa prática demonstra maturidade avançada, atendendo aos requisitos da LGPD, especialmente os artigos 17 e 50, bem como às normas ISO/IEC 27701:2019 e Resolução CONARQ n. 54/2023. Essa abordagem permite à organização gerenciar de forma eficiente os dados sob sua responsabilidade, assegurando conformidade regulatória e proteção contínua.

Além disso, a organização documenta e monitora formalmente os agentes de tratamento de dados, incluindo controladores e operadores. Esse controle reflete uma abordagem robusta e proativa na governança de dados, garantindo que papéis

e responsabilidades sejam claramente definidos e regularmente revisados. Esse alinhamento com os artigos 37 e 50 da LGPD e com os itens 7 e 8 da ISO/IEC 27701:2019 reforça a confiabilidade da gestão de dados e minimiza riscos regulatórios.

A organização também demonstra que identifica, documenta e mantém um processo contínuo para monitorar e melhorar as atividades operacionais relacionadas ao tratamento de dados pessoais. Essas práticas asseguram que o tratamento de dados seja realizado com segurança e eficiência, em conformidade com os artigos 3º e 50 da LGPD e as melhores práticas da ISO/IEC 27701. A integração de auditorias e revisões periódicas evidencia o compromisso com a melhoria constante e a proteção de informações sensíveis.

Adicionalmente, a organização dispõe de mecanismos formais e abrangentes para garantir os direitos dos titulares de dados pessoais, como acesso, correção, exclusão e portabilidade. Esses mecanismos são continuamente revisados e atualizados, assegurando conformidade com o artigo 51 da LGPD e o item 5.18 da ABNT NBR ISO/IEC 27002:2022. Essa abordagem fortalece a credibilidade institucional e promove a confiança dos titulares.

Por fim, destaca-se que a organização aplica rigorosamente regras operacionais para proteger dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização e anonimização. Essas práticas são monitoradas regularmente, assegurando proteção robusta contra acessos não autorizados e vazamento de informações. Essa abordagem demonstra alinhamento com os artigos 11 e 16 da LGPD e os itens 7.4.5 da ISO/IEC 27701:2019 e 8.11 da ISO/IEC 27002:2022, consolidando a posição da organização como referência em segurança de dados sensíveis.

Recomendações

Para assegurar a manutenção desse nível elevado de maturidade e promover a evolução contínua, são sugeridas as seguintes ações:

- Revisar e atualizar continuamente o mapeamento de categorias de dados e titulares:
 - Realizar auditorias periódicas para verificar a precisão e a abrangência da documentação.

- Atualizar os registros sempre que ocorrerem mudanças operacionais ou regulatórias.
 - Capacitar equipes para identificar e gerenciar alterações nas categorias de dados e titulares.
- Fortalecer o controle sobre os agentes de tratamento de dados:
 - Implementar revisões regulares das designações de controladores e operadores.
 - Realizar treinamentos periódicos para os agentes envolvidos, assegurando alinhamento com as regulamentações.
 - Documentar todas as alterações nas funções dos agentes para garantir rastreabilidade.
- Aprimorar os processos operacionais relacionados ao tratamento de dados:
 - Manter um cronograma de auditorias e revisões para identificar possíveis lacunas nos processos.
 - Investir em tecnologias que permitam o monitoramento automático das atividades que envolvem dados pessoais.
 - Promover treinamentos regulares com foco em melhores práticas e conformidade legal.
- Ampliar e divulgar os mecanismos de garantia de direitos dos titulares:
 - Realizar campanhas de conscientização para informar os titulares sobre seus direitos e os mecanismos disponíveis.
 - Monitorar a eficácia dos processos de atendimento às solicitações dos titulares e implementar melhorias quando necessário.
 - Estabelecer indicadores de desempenho para avaliar a qualidade do atendimento.
- Manter a robustez das práticas de proteção de dados sensíveis:
 - Revisar regularmente as regras operacionais e as técnicas aplicadas para mascaramento, pseudonimização e anonimização.
 - Adotar novas tecnologias para reforçar a proteção contra acessos não autorizados.
 - Promover workshops com as equipes operacionais para atualização em práticas de segurança.

6.3.3.3 Dimensão 3: Treinamento e Conscientização

A seguir, detalha-se o cálculo da pontuação da Dimensão 3 para a UFBA, abrangendo as questões 12 a 15 do instrumento de medição. Com uma pontuação máxima de 60 pontos nesta dimensão, a universidade alcançou uma pontuação bruta calculada pela fórmula: $Q12*3 + Q13*3 + Q14*3 + Q15*3$, totalizando 48 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{48}{60} \right) \times 100 = 80 \text{ pontos}$$

Este resultado posiciona a UFBA na categoria "Avançado" na Dimensão 3, de acordo com os critérios de maturidade organizacional do MMTDP.

Análise

A análise das práticas da organização revela uma maturidade significativa, embora ainda existam oportunidades de aprimoramento em áreas relacionadas à capacitação e conscientização no tratamento de dados pessoais. A seguir, são apresentados os principais aspectos identificados.

Observou-se que a organização possui um programa de capacitação que abrange questões essenciais sobre o tratamento e a proteção de dados pessoais, representando um progresso relevante. Contudo, a efetividade do programa ainda é limitada por lacunas em áreas específicas. A falta de uniformidade nos treinamentos pode comprometer a consistência das práticas e criar vulnerabilidades no cumprimento das exigências da LGPD. A norma ABNT NBR ISO/IEC 27701:2019 enfatiza a importância de treinamentos abrangentes, capazes de capacitar todos os colaboradores de maneira consistente.

A organização demonstra um elevado nível de maturidade ao implementar programas contínuos e robustos de conscientização voltados para os agentes de tratamento de dados pessoais. Tais programas asseguram que esses agentes compreendam plenamente seus papéis e responsabilidades, em conformidade com os requisitos da LGPD e normas correlatas. Esse nível de conscientização fortalece a segurança jurídica e a confiança nas práticas institucionais, consolidando uma cultura organizacional orientada para a proteção de dados.

Foi também identificado que a organização dispõe de programas de treinamento específicos para colaboradores, terceirizados e parceiros, abrangendo temas relevantes ao tratamento de dados pessoais. No entanto, pequenas lacunas nos programas indicam a necessidade de melhorias para atender plenamente às exigências legais e normativas. Essas deficiências podem impactar a uniformidade da aplicação das práticas de proteção de dados e comprometer a compreensão das responsabilidades por todos os envolvidos.

Por fim, verificou-se que a organização mantém um programa regular de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais. Embora esse programa represente um avanço considerável, ainda há espaço para melhorias, como a inclusão de conteúdos mais específicos e estudos de caso que ilustrem os impactos do tratamento inadequado. Para garantir sua relevância e eficácia, a conformidade com a LGPD e normas como a ABNT NBR ISO/IEC 27701:2019 exige monitoramento contínuo e atualização regular dos conteúdos.

Recomendações

Para sustentar e ampliar a maturidade nas práticas de treinamento e conscientização, recomenda-se a adoção das seguintes ações estratégicas:

- Revisar e aprimorar os programas de capacitação:
 - Realizar um diagnóstico detalhado das áreas que necessitam de aprimoramento nos treinamentos.
 - Desenvolver módulos específicos para abordar lacunas identificadas, incluindo temas como segurança de dados sensíveis e resposta a incidentes.
 - Garantir que todos os colaboradores tenham acesso a treinamentos completos e regulares, incorporando feedback dos participantes para melhoria contínua.
- Manter e evoluir os programas de conscientização de agentes de tratamento de dados:
 - Revisar periodicamente os conteúdos dos programas para assegurar alinhamento às melhores práticas e regulamentações.
 - Implementar mecanismos de coleta de feedback para identificar áreas de melhoria e ajustar os programas conforme necessário.

- Promover campanhas regulares de conscientização para reforçar os papéis e responsabilidades dos agentes de tratamento.
- Fortalecer os treinamentos para colaboradores, terceirizados e parceiros:
 - Monitorar continuamente a eficácia dos programas, assegurando que sejam abrangentes e aplicáveis a todos os envolvidos no tratamento de dados.
 - Adicionar módulos específicos sobre questões emergentes, como novas regulamentações e práticas de segurança.
 - Estabelecer indicadores de desempenho para avaliar o impacto dos treinamentos e identificar pontos de melhoria.
- Aprimorar o programa de conscientização sobre riscos associados ao tratamento inadequado de dados:
 - Revisar os conteúdos para incluir estudos de caso recentes e exemplos práticos que ilustram os impactos do tratamento inadequado.
 - Realizar avaliações regulares da eficácia do programa, ajustando os conteúdos com base nas necessidades identificadas.
 - Incorporar atualizações sobre novas ameaças e vulnerabilidades no cenário digital, garantindo que os colaboradores estejam preparados para mitigar riscos.
- Monitorar e integrar as iniciativas de capacitação e conscientização:
 - Criar um sistema centralizado para gestão e monitoramento dos programas, permitindo uma visão integrada e facilitando a identificação de lacunas.
 - Promover a integração dos programas de capacitação e conscientização com outras políticas organizacionais, como gestão de incidentes e auditorias internas.
 - Garantir que todas as iniciativas estejam alinhadas à estratégia geral de governança de dados da organização.

6.3.3.4 Dimensão 4: Segurança da Informação e Tecnologia

A seguir, apresenta-se o cálculo da pontuação da Dimensão 4 para a Universidade Federal da Bahia, que abrange as questões 16 a 21 do instrumento de medição. A pontuação máxima para esta dimensão é de 100 pontos. A universidade

obteve uma pontuação bruta, calculada conforme a fórmula: $Q16*5 + Q17*3 + Q18*3 + Q19*3 + Q20*3 + Q21*3$, resultando em 58 pontos.

Aplicando a equação da normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{58}{100} \right) \times 100 = 58 \text{ pontos.}$$

Este resultado posiciona a UFBA na categoria "Intermediário" na Dimensão 4, conforme os critérios e intervalos previamente estabelecidos no MMTDP.

Análise

A análise das práticas da organização evidencia avanços importantes em diversas dimensões relacionadas à segurança e proteção de dados pessoais, ao mesmo tempo que identifica lacunas que comprometem a conformidade plena com as normativas aplicáveis, como a LGPD e normas internacionais.

Inicialmente, constatou-se que a organização iniciou a elaboração de uma política de segurança, representando um progresso significativo. Contudo, a ausência de formalização limita a capacidade de alinhar as práticas de proteção de dados aos requisitos legais e normativos, como os previstos pela ABNT NBR ISO/IEC 27701:2019. Sem um documento formalizado, torna-se desafiador estabelecer diretrizes claras e acessíveis para os colaboradores.

A análise também revelou que a ausência de criptografia nos processos representa um risco elevado para a segurança dos dados pessoais. Sem essa medida essencial, informações sensíveis permanecem vulneráveis a acessos não autorizados, colocando a organização em desconformidade com a LGPD e a norma ABNT NBR ISO/IEC 27002:2022, que enfatizam a criptografia como um controle fundamental de segurança.

Identificou-se, ainda, que a organização possui sistemas bem estabelecidos de backup e auditoria, que asseguram a proteção e a recuperação de dados. Contudo, a integração dessas práticas com outras ações de gestão de dados ainda apresenta oportunidades de melhoria, especialmente para garantir um funcionamento mais eficiente e alinhado ao ciclo de vida dos dados.

Além disso, constatou-se que a coleta e a análise de vulnerabilidades são realizadas de forma parcial, o que evidencia um progresso inicial. Entretanto, a ausência de uma estrutura formal dificulta a priorização e a resolução eficaz de

problemas. Essa deficiência compromete a capacidade de resposta da organização a ameaças emergentes, conforme preconizado pela ABNT NBR ISO/IEC 27002:2022.

No que se refere aos controles de acesso, verificou-se que a organização implementa práticas sólidas, atendendo a grande parte dos requisitos do art. 26 da LGPD e das normas internacionais. Contudo, a ausência de revisões e monitoramentos constantes limita a eficácia dessas práticas a longo prazo, contrariando as recomendações de auditorias regulares para garantir a atualização e a adequação dos controles.

Por fim, constatou-se que o sistema de monitoramento de incidentes de segurança está bem implementado e alinhado aos requisitos legais e normativos, como o art. 46 da LGPD e o item 5.35 da ABNT NBR ISO/IEC 27002:2022. Entretanto, identificou-se a necessidade de maior integração com outras práticas de segurança, o que poderia otimizar a capacidade de detectar e responder a incidentes de forma proativa e preventiva.

Recomendações

Para promover a evolução da maturidade institucional em segurança e proteção de dados, recomenda-se a implementação das seguintes ações estratégicas:

- Formalizar e disseminar a política de segurança da informação:
 - Concluir a elaboração da política, assegurando que inclua diretrizes claras e abrangentes para todas as áreas da organização.
 - Tornar a política amplamente acessível aos colaboradores e realizar treinamentos específicos para garantir sua compreensão e aplicação.
 - Estabelecer um plano de monitoramento e revisão periódica para garantir que a política permaneça atualizada e eficaz.
- Implementar a criptografia como medida essencial de segurança:
 - Priorizar a implementação de criptografia para dados pessoais sensíveis, tanto em armazenamento quanto em transmissão.
 - Desenvolver políticas e diretrizes para regulamentar o uso da criptografia em todos os níveis organizacionais.
 - Capacitar equipes técnicas para gerenciar e monitorar os sistemas de criptografia de forma eficiente.

- Aprimorar a integração dos sistemas de backup e auditoria:
 - Integrar os sistemas de backup e auditoria com outras práticas de gestão de dados, garantindo maior eficiência na proteção e recuperação de informações.
 - Realizar auditorias regulares para verificar a integridade e a eficácia dos backups.
 - Automatizar processos críticos para minimizar falhas e otimizar recursos.
- Estruturar um processo formal de gestão de vulnerabilidades:
 - Implementar um processo estruturado que inclui identificação, priorização e correção de vulnerabilidades.
 - Desenvolver relatórios periódicos para acompanhamento das ações de mitigação.
 - Utilizar ferramentas tecnológicas avançadas para identificar ameaças emergentes e reduzir riscos.
- Estabelecer revisões regulares dos controles de acesso:
 - Criar um cronograma de auditorias para revisar periodicamente permissões de acesso e identificar inconsistências.
 - Automatizar o processo de monitoramento para aumentar a eficácia e reduzir erros manuais.
 - Alinhar os controles de acesso às mudanças organizacionais, garantindo que eles reflitam as necessidades e responsabilidades atuais.
- Integrar o monitoramento de incidentes a outras práticas de segurança:
 - Adotar ferramentas de inteligência que permitam detectar padrões e prever ameaças.
 - Realizar auditorias frequentes para avaliar a eficácia do sistema de monitoramento de incidentes.
 - Promover a comunicação entre as equipes responsáveis pelo monitoramento e outras áreas de segurança, garantindo respostas coordenadas e eficazes.

6.3.3.5 Dimensão 5: Acesso à Informação e Transparência

A seguir, o cálculo da pontuação da Dimensão 5 para a Universidade Federal da Bahia, abrangendo as questões 22 a 25 do instrumento de medição. Com uma pontuação máxima de 70 pontos nesta dimensão, a UFBA alcançou uma pontuação bruta calculada pela fórmula: $Q22*3 + Q23*3 + Q24*5 + Q25*3$, totalizando 67 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{67}{70} \right) \times 100 = 95,71 \text{ pontos}$$

Este resultado posiciona a UFBA na categoria "Exemplar" na Dimensão 5.

Análise

A análise das práticas da organização revela um nível elevado de maturidade no tratamento e na transparência das informações relacionadas à proteção de dados pessoais, evidenciando alinhamento com a LGPD e normas internacionais. Contudo, há pequenas oportunidades de aprimoramento que podem ser exploradas para consolidar e expandir esse nível de conformidade.

Constatou-se que a organização atende plenamente ao princípio da transparência, disponibilizando informações claras, completas e acessíveis sobre o tratamento de dados pessoais. O monitoramento contínuo dessas informações assegura atualizações regulares, garantindo conformidade com o art. 50 da LGPD e com o art. 4º da Lei n. 8.159/1991. Essa prática reforça a confiança dos titulares e a capacidade de resposta da organização frente a novas regulamentações. Contudo, a manutenção desse nível exige esforços contínuos para monitorar a conformidade e a qualidade das informações publicizadas.

Identificou-se, ainda, que a organização possui práticas consistentes de transparência na disponibilização de informações sobre o tratamento de dados pessoais, mas carece de um sistema de monitoramento contínuo. Essa ausência pode gerar inconsistências que comprometam a confiança e a completude das informações, contrariando o art. 20 da LGPD. A implementação de revisões regulares contribuiria para aprimorar a clareza e a confiabilidade das informações, fortalecendo a confiança institucional.

Verificou-se que a designação e a divulgação das informações do encarregado de proteção de dados (DPO) são realizadas de maneira clara e acessível. Essa prática está em conformidade com o art. 41 da LGPD e com os itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019. A acessibilidade dos contatos do DPO promove o diálogo direto com os titulares e fortalece a confiança na gestão de dados pessoais pela organização.

Por fim, constatou-se que a Política de Privacidade é amplamente divulgada, aplicada de forma consistente e revisada regularmente. Esse nível de maturidade assegura transparência e conformidade com as exigências legais, promovendo a confiança dos titulares e alinhando-se às melhores práticas de proteção de dados pessoais descritas na LGPD e na ABNT NBR ISO/IEC 27701:2019.

Recomendações

Para sustentar e aprimorar o nível de maturidade alcançado, são recomendadas as seguintes ações estratégicas:

- Monitorar e revisar continuamente as informações publicadas sobre o tratamento de dados:
 - Realizar auditorias regulares para verificar a completude e a clareza das informações disponibilizadas.
 - Coletar feedback dos titulares de dados para identificar pontos de melhoria na comunicação institucional.
 - Implementar um cronograma de revisões periódicas para garantir que as informações estejam sempre atualizadas e em conformidade com as regulamentações vigentes.
- Implementar um sistema de monitoramento contínuo das informações publicizadas:
 - Desenvolver um sistema automatizado para revisão e atualização regular das informações publicadas, minimizando inconsistências.
 - Capacitar equipes responsáveis pela comunicação e governança de dados para garantir alinhamento às exigências da LGPD.
 - Incorporar relatórios periódicos que documentem as alterações e ajustes realizados.
- Manter e fortalecer a acessibilidade das informações do DPO:

- Realizar auditorias regulares para garantir que os contatos do DPO sejam acessíveis e estejam devidamente atualizados.
- Ampliar os canais de divulgação das informações do DPO, utilizando plataformas digitais e físicas para alcançar um público mais abrangente.
- Promover treinamentos específicos para o DPO, assegurando que esteja preparado para atender às demandas dos titulares de forma eficiente.
- Revisar e aprimorar continuamente a Política de Privacidade:
 - Realizar revisões periódicas da Política de Privacidade para refletir alterações normativas e avanços tecnológicos.
 - Incorporar feedback dos titulares e colaboradores para garantir que a Política seja clara, acessível e compreensível por diferentes públicos.
 - Divulgar amplamente as atualizações realizadas, reforçando a transparência e promovendo campanhas educativas sobre a importância da Política de Privacidade.
- Promover uma abordagem integrada na gestão de transparência e proteção de dados:
 - Estabelecer um comitê interdisciplinar para supervisionar as práticas de transparência, monitoramento e proteção de dados.
 - Adotar ferramentas tecnológicas que facilitem a gestão integrada das informações publicadas e dos direitos dos titulares.
 - Investir em programas regulares de capacitação para os responsáveis pela governança de dados, assegurando alinhamento contínuo às melhores práticas.

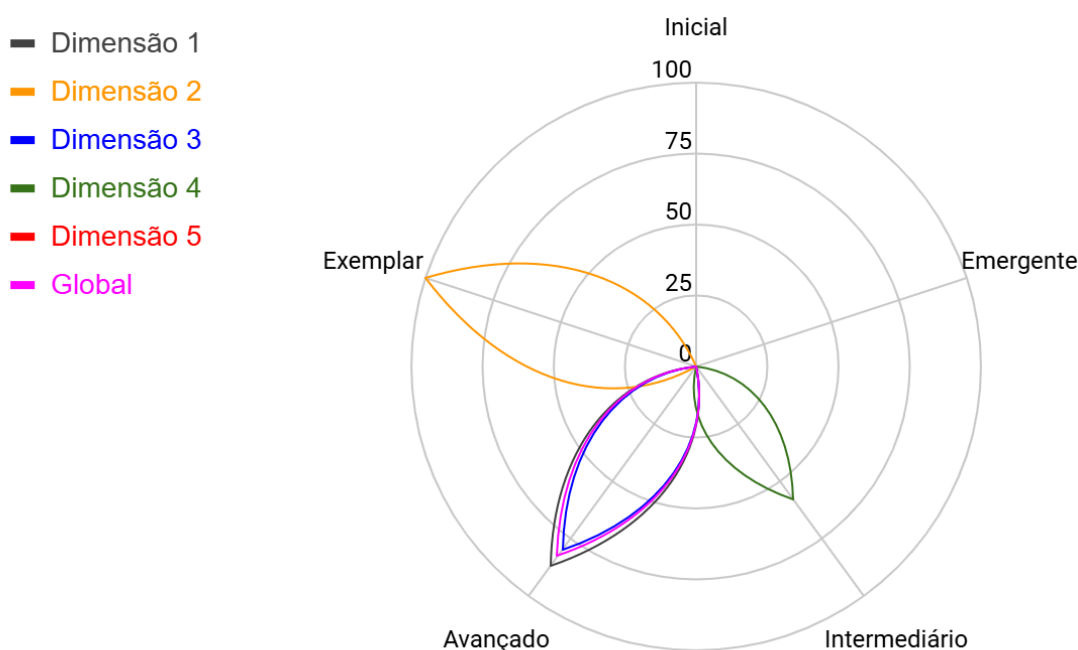
6.3.3.6 Análise Global da Instituição

A análise dos resultados obtidos pela Universidade Federal da Bahia (UFBA) revelou que a instituição alcançou o estágio de maturidade “**Avançado**” no tratamento de dados pessoais. Esse diagnóstico foi calculado com base na metodologia descrita no item **5.3.7.4**, utilizando a fórmula:

$$Pontuação\ Global = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

Os dados obtidos nas dimensões avaliadas foram: PND1 = 86,67 pontos, PND2 = 100 pontos, PND3 = 80 pontos, PND4 = 58 pontos e PND5 = 95,71 pontos, resultando em uma pontuação global de 82,82 pontos. O Gráfico 10 ilustra as capacidades organizacionais da universidade:

Gráfico 10 - Níveis de maturidade da Universidade Federal da Bahia



Fonte: elaborado pelo autor.

A dimensão de Políticas e Processos de Tratamento de Dados alcançou o melhor desempenho entre as dimensões avaliadas, atingindo o nível exemplar.

A UFBA destaca-se pela gestão robusta e bem estruturada de dados pessoais, posicionando-se como referência em governança e conformidade. A instituição apresenta avanços significativos na formulação de políticas e na implementação de programas voltados ao tratamento de dados, com processos claros de identificação, documentação e monitoramento. Essas práticas demonstram o compromisso da universidade com a proteção e a transparência no uso das informações, promovendo confiança tanto entre os titulares de dados quanto entre os stakeholders institucionais.

Contudo, algumas lacunas ainda precisam ser abordadas para maximizar a efetividade operacional e o alinhamento às melhores práticas. Apesar das políticas

abrangentes, é necessário intensificar a integração entre setores estratégicos, implementando um plano de execução detalhado e monitorado continuamente, a fim de assegurar uniformidade na aplicação das normativas. A adoção de técnicas avançadas, como pseudonimização e anonimização de dados sensíveis, é um ponto de destaque, mas a ampliação dessas iniciativas e sua integração com outros controles são essenciais para consolidar uma abordagem abrangente de proteção de dados.

O compromisso da UFBA com a capacitação dos colaboradores é evidente. A instituição realiza treinamentos regulares que promovem a conscientização sobre a importância do tratamento adequado de dados pessoais. Entretanto, aprimorar a abrangência dessas iniciativas, incorporando estudos de caso práticos e atualizações constantes, será crucial para fortalecer ainda mais a cultura organizacional de proteção de dados. Paralelamente, o investimento contínuo em tecnologias avançadas, como criptografia de dados em áreas sensíveis e autenticação forte, é indispensável para mitigar vulnerabilidades e elevar os padrões de segurança da informação.

As práticas de monitoramento e auditoria demonstram consistência e comprometimento com a melhoria contínua. Todavia, integrar essas atividades a uma análise proativa de riscos e eventos de segurança permitirá à instituição adotar uma abordagem preventiva mais robusta. Embora os controles de acesso eficazes e os processos de backup já implementados sejam diferenciais positivos, sua consolidação depende de maior integração com estratégias de inteligência e de resposta ágil a ameaças, ampliando a resiliência da universidade frente a incidentes.

Outro aspecto de destaque é o forte compromisso da UFBA com a transparência, evidenciado pela ampla divulgação de informações e pelo acesso facilitado ao Encarregado de Proteção de Dados (DPO). Essas práticas estão alinhadas às exigências da LGPD e contribuem para consolidar a confiança dos titulares. Contudo, a revisão e a atualização contínua das políticas de privacidade e classificação da informação são imprescindíveis para assegurar que a comunicação institucional permaneça clara, acessível e adaptada a um ambiente normativo e tecnológico em constante transformação.

De maneira geral, a Universidade Federal da Bahia posiciona-se como uma instituição madura no tratamento de dados pessoais, com políticas estruturadas, práticas consistentes e uma sólida cultura de governança e transparência. Manter

essa posição de destaque exigirá investimentos contínuos na modernização tecnológica, na ampliação das capacitações e na integração de práticas preventivas e proativas de segurança. Ao direcionar esforços para esses aprimoramentos, a UFBA estará apta a sustentar sua liderança, consolidar sua reputação e atender plenamente às exigências legais e normativas, reafirmando seu compromisso com a ética, a responsabilidade e a excelência na proteção de dados pessoais.

6.3.4 Universidade Federal do Rio Grande do Sul (UFRGS)

Fundada em 1934, a Universidade Federal do Rio Grande do Sul (UFRGS) possui seus principais campi localizados em Porto Alegre, além de unidades em Eldorado do Sul, Imbé e Tramandaí. Ao longo de sua trajetória, a UFRGS passou por diversas mudanças estruturais que a consolidaram como uma das instituições mais renomadas do sul do Brasil, destacando-se por sua forte tradição em pesquisa e inovação.

A universidade mantém um portal dedicado à Lei Geral de Proteção de Dados, no qual apresenta as políticas de proteção de dados adotadas pela instituição. Esse portal, acessível no endereço eletrônico <http://www.ufrgs.br/ufrgs/acessoainformacao/tratamento-de-dados-pessoais>, reúne diversas orientações, treinamentos e cartilhas informacionais sobre o tema, reforçando o compromisso da UFRGS com a transparência e a conformidade regulatória. As respostas da UFRGS ao instrumento de medição de maturidade foram registradas em 27 de setembro de 2024, conforme detalhado.

Quadro 36 - Respostas do instrumento de medição da UFRGS

Questões	Respostas da UFRGS
Questão 1	5
Questão 2	5
Questão 3	5
Questão 4	5
Questão 5	5
Questão 6	5
Questão 7	4
Questão 8	5
Questão 9	4
Questão 10	5

Questão 11	5
Questão 12	5
Questão 13	5
Questão 14	4
Questão 15	5
Questão 16	5
Questão 17	5
Questão 18	4
Questão 19	5
Questão 20	5
Questão 21	5
Questão 22	5
Questão 23	5
Questão 24	5
Questão 25	5

Fonte: elaborado pelo autor.

As respostas fornecidas pela UFRGS foram utilizadas para o cálculo de maturidade, seguindo a metodologia descrita no item **5.3.7** deste trabalho e com base nos dados padronizados apresentados no **Apêndice M**. O Quadro 37 sintetiza a classificação da UFRGS em cada uma das dimensões avaliadas, bem como o resultado da maturidade global da instituição.

Quadro 37 - Respostas do instrumento de medição da UFRGS

Dimensão	Pontuação	Classificação
Dimensão 1	100,00	Exemplar
Dimensão 2	92,00	Exemplar
Dimensão 3	95,00	Exemplar
Dimensão 4	97,00	Exemplar
Dimensão 5	100,00	Exemplar
Global	96,80	Exemplar

Fonte: elaborado pelo autor.

Esses resultados evidenciam os principais fatores de sucesso e demonstram como a UFRGS sustenta seus elevados níveis de maturidade. O detalhamento da análise dessas classificações é apresentado a seguir.

6.3.4.1 Dimensão 1: Governança de Dados e Boas Práticas

A seguir, apresenta-se o detalhamento do cálculo de pontuação referente à Dimensão 1 para a Universidade Federal do Rio Grande do Sul (UFRGS), que abrange as questões 1 a 6 do instrumento de medição. A pontuação máxima possível para essa dimensão é de 120 pontos. A UFRGS alcançou uma pontuação bruta calculada com base na fórmula: $Q1*3 + Q2*5 + Q3*5 + Q4*5 + Q5*3 + Q6*3$, resultando em 120 pontos.

Aplicando equação da pontuação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{120}{120} \right) \times 100 = 100 \text{ pontos}$$

Esse resultado, enquadrado nos intervalos predefinidos para a classificação de maturidade, posiciona a UFRGS na categoria "Exemplar" na Dimensão 1. Essa avaliação reflete um nível perfeito de maturidade nas práticas de governança de dados, evidenciando efetividade e alinhamento com as melhores práticas.

Análise

A organização demonstrou um elevado nível de maturidade na implementação de práticas relacionadas à governança de dados pessoais, conforme evidenciado pelas respostas fornecidas para cada uma das questões. A conformidade com as regulamentações estabelecidas pela Lei Geral de Proteção de Dados, bem como com as normas ISO/IEC, é uma prioridade dentro da organização. As práticas implementadas, como o desenvolvimento de programas de governança, a designação formal do Encarregado de Proteção de Dados (EPD), a criação de um comitê ativo, a implementação de uma Política de Privacidade e a gestão do compartilhamento de dados pessoais, revelam uma abordagem estruturada e bem integrada.

A organização atingiu um alto nível de maturidade com a elaboração e implementação completa do programa de governança, alinhando-se às melhores práticas e requisitos normativos, como os estabelecidos pela LGPD e pelas normas ISO/IEC 27701:2019 e 27014:2021. A manutenção de um programa bem estruturado e o monitoramento contínuo garantem que a organização esteja apta a se adaptar às mudanças legais e tecnológicas, promovendo uma proteção eficaz dos dados pessoais. No entanto, é fundamental que a organização continue a

investir em atualizações regulares do programa para garantir a continuidade da conformidade e a eficácia das práticas.

A designação formal do Encarregado de Proteção de Dados (EPD) e o reconhecimento do seu papel dentro da organização demonstram um compromisso significativo com a proteção de dados pessoais. O suporte da alta administração é crucial para garantir que o EPD possa atuar de forma efetiva, integrada e com autonomia, como recomendado pela LGPD e pela ISO/IEC 27701:2019. A organização deve manter o investimento em treinamento contínuo para o EPD e em práticas de comunicação eficientes para garantir a conformidade duradoura.

A criação de um comitê de governança de dados ativo e com funções bem definidas é um ponto forte da organização, permitindo uma abordagem estratégica e integrada na gestão da conformidade com as regulamentações de proteção de dados. A integração de diferentes áreas da organização no comitê é um aspecto positivo que assegura a aplicação de práticas de governança de dados em todos os níveis. A manutenção desse nível de maturidade requer a realização de reuniões regulares e auditorias periódicas para garantir que o comitê esteja sempre alinhado com as necessidades regulatórias e operacionais.

A Política de Privacidade é um dos pilares fundamentais para garantir a transparência no tratamento de dados pessoais, e a organização demonstrou seu compromisso com essa transparência por meio da elaboração de uma política amplamente divulgada, aplicada de forma consistente e regularmente revisada. Essa abordagem fortalece a confiança dos titulares e garante que a organização esteja em conformidade com a LGPD e a ABNT NBR ISO/IEC 27701:2019. No entanto, a organização deve continuar a realizar auditorias periódicas e atualizações regulares para garantir que a política permaneça alinhada com as mudanças legais e operacionais.

A organização atingiu um nível ideal de maturidade no gerenciamento do compartilhamento e transferência de dados pessoais. Com procedimentos documentados e formalizados, a organização assegura que todas as práticas de compartilhamento estão em conformidade com as regulamentações e são monitoradas de forma contínua. Isso reflete um compromisso com a transparência e a segurança dos dados pessoais. A manutenção dessa conformidade exigirá revisões contínuas e a adaptação dos procedimentos às novas regulamentações e melhores práticas do setor.

A organização assegura a total autonomia do Encarregado de Proteção de Dados, garantindo sua dedicação exclusiva à função, sem acumular outras responsabilidades que possam comprometer sua independência ou gerar conflitos de interesse. Esse é um nível ideal de maturidade, conforme exigido pela LGPD e pela Lei n. 14.133/2021. A independência do EPD é essencial para garantir a imparcialidade na supervisão das práticas de tratamento de dados pessoais. A manutenção desse nível requer auditorias periódicas e o monitoramento constante da autonomia do EPD, bem como uma atualização contínua sobre as mudanças regulatórias.

Recomendações

Para garantir a continuidade do alto nível de maturidade e o aprimoramento das práticas de governança de dados, a organização deve implementar as seguintes ações:

- Para a Governança de Dados:
 - Realizar revisões periódicas do programa de governança para garantir que ele esteja sempre alinhado com as mudanças nas regulamentações e com os avanços tecnológicos.
 - Investir em treinamentos contínuos para os responsáveis pela implementação do programa, garantindo que todos estejam atualizados sobre as melhores práticas de governança.
 - Estabelecer uma rotina de auditorias para monitorar a eficácia do programa de governança e identificar áreas de melhoria.
- Para o Encarregado de Proteção de Dados (EPD):
 - Manter e reforçar o suporte da alta administração ao EPD, assegurando que ele tenha os recursos necessários para desempenhar suas funções com eficácia.
 - Promover treinamentos regulares para o EPD, incluindo atualizações sobre as melhores práticas e mudanças nas regulamentações.
 - Estabelecer um processo de feedback contínuo para o EPD, permitindo a identificação de desafios e a implementação de melhorias nas práticas de proteção de dados.

- Para o Comitê de Governança de Dados:
 - Realizar reuniões regulares do comitê, garantindo que as discussões estejam sempre alinhadas com as mudanças regulatórias e as necessidades operacionais.
 - Estabelecer um sistema de monitoramento de desempenho para o comitê, utilizando indicadores que ajudem a avaliar a eficácia das ações tomadas.
 - Garantir a inclusão de representantes de todas as áreas relevantes da organização, promovendo uma abordagem multidisciplinar e integrada no processo de governança.

- Para a Política de Privacidade:
 - Realizar auditorias periódicas para avaliar a eficácia e a aplicação da Política de Privacidade, ajustando-a conforme necessário para manter sua relevância e conformidade.
 - Promover campanhas de conscientização sobre a Política de Privacidade entre os colaboradores e os titulares de dados, garantindo que todos compreendam suas responsabilidades e direitos.
 - Atualizar regularmente a política para refletir mudanças legais, tecnológicas e operacionais que possam afetar o tratamento de dados pessoais.

- Para o Compartilhamento de Dados Pessoais:
 - Continuar a realizar auditorias e revisões periódicas sobre os procedimentos de compartilhamento de dados, garantindo que todos os compartilhamentos de dados estejam documentados e em conformidade com as regulamentações.
 - Implementar um sistema de monitoramento contínuo que identifique e corrija quaisquer falhas ou desvios nos procedimentos de compartilhamento de dados.
 - Realizar treinamentos regulares com todos os funcionários envolvidos no processo de compartilhamento de dados, garantindo que compreendam as regulamentações e as melhores práticas de segurança.

- Para a Segregação das Funções do EPD:
 - Realizar auditorias periódicas para garantir que o EPD continue a desempenhar suas funções de forma independente e sem interferências externas.
 - Estabelecer uma política formal que assegure a dedicação exclusiva do EPD, proibindo a acumulação de funções que possam gerar conflitos de interesse.
 - Promover a revisão periódica das funções do EPD, garantindo que ele tenha a autonomia necessária para atuar de maneira imparcial e eficiente na supervisão do tratamento de dados pessoais.

6.3.4.2 Dimensão 2: Políticas e Processos de Tratamento de Dados

A seguir, apresenta-se o detalhamento do cálculo da pontuação referente à Dimensão 2 para a Universidade Federal do Rio Grande do Sul (UFRGS), que abrange as questões 7 a 11 do instrumento de medição. A pontuação máxima possível para essa dimensão é de 75 pontos. A UFRGS alcançou uma pontuação bruta, calculada com base na fórmula: $Q7*3 + Q8*3 + Q9*3 + Q10*3 + Q11*3$, resultando em 69 pontos.

Aplicando a equação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{69}{75} \right) \times 100 = 92 \text{ pontos}$$

Esse resultado posiciona a UFRGS na categoria "Exemplar" na Dimensão 2, conforme os critérios e intervalos previamente estabelecidos para a avaliação da maturidade organizacional no MMTDP.

Análise

A organização demonstrou um elevado nível de maturidade em várias áreas fundamentais no tratamento de dados pessoais, como a identificação das categorias de dados, o mapeamento dos agentes de tratamento, a documentação dos processos operacionais, a implementação de mecanismos para garantir os direitos dos titulares e o uso de técnicas de proteção de dados sensíveis. Essas práticas são essenciais para assegurar a conformidade com a Lei Geral de Proteção de Dados e

com as normas internacionais, como as estabelecidas pela ISO/IEC 27701:2019 e 27002:2022.

A organização alcançou um nível avançado ao identificar, documentar e manter um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação. Essa prática garante que os dados sejam tratados de acordo com as exigências da LGPD, especialmente em relação aos direitos dos titulares. A manutenção desse nível de maturidade exige revisões periódicas e monitoramento contínuo, a fim de refletir mudanças nas regulamentações e nas práticas operacionais.

A identificação dos agentes (controladores e operadores) de tratamento de dados pessoais também está avançada. A organização implementou um processo formal e contínuo para monitorar e atualizar essa identificação, demonstrando conformidade com os requisitos legais. Para garantir a eficácia a longo prazo, é imprescindível que a organização mantenha o monitoramento regular e ajuste o processo conforme necessário, refletindo as mudanças nas estruturas internas e nas regulamentações externas.

A organização identificou, documentou e mantém um processo contínuo para monitorar, revisar e melhorar os processos e atividades operacionais que lidam com dados pessoais. Esse nível de maturidade assegura que a organização tenha controle sobre como os dados são processados e protegidos. A revisão contínua e a atualização dessas práticas garantem a manutenção da conformidade, especialmente em um ambiente de rápidas mudanças regulatórias e tecnológicas.

A organização demonstrou um alto nível de maturidade na implementação de mecanismos formais e abrangentes para garantir os direitos dos titulares de dados pessoais. Esses mecanismos permitem que os titulares exerçam seus direitos de acesso, correção, exclusão e portabilidade de seus dados. A implementação de uma estrutura formal e a revisão contínua desses mecanismos são essenciais para garantir que a organização continue em conformidade com a LGPD.

A organização também aplicou rigorosamente técnicas como mascaramento, pseudonimização e anonimização de dados pessoais sensíveis, assegurando que esses dados sejam tratados de forma segura. O monitoramento contínuo e a aplicação consistente dessas técnicas são essenciais para proteger os dados contra acessos não autorizados e vazamentos de informações. Esse nível de maturidade reflete o compromisso da organização com a privacidade e a segurança dos dados

dados pessoais sensíveis, em conformidade com os requisitos da LGPD e as normas ISO/IEC.

Recomendações

Embora a organização tenha demonstrado avanços substanciais, há espaço para aprimorar ainda mais suas práticas de governança de dados, visando alcançar um nível superior de maturidade no tratamento de dados pessoais. A seguir, são apresentadas as ações recomendadas para garantir a evolução contínua das políticas e processos de governança de dados:

- Para a Identificação das Categorias de Dados e Titulares:
 - Realizar revisões periódicas do mapeamento das categorias de dados pessoais e dos titulares, garantindo que todas as categorias relevantes sejam identificadas e protegidas adequadamente.
 - Estabelecer um processo de monitoramento contínuo para adaptar as práticas de tratamento de dados às novas regulamentações e mudanças operacionais.
 - Implementar auditorias internas periódicas para garantir a conformidade e a precisão da documentação das categorias de dados e titulares.
- Para a Identificação dos Agentes de Tratamento:
 - Formalizar e documentar a identificação de todos os agentes de tratamento de dados pessoais, garantindo que todas as áreas e operadores externos estejam adequadamente registrados.
 - Estabelecer um protocolo de revisão contínua e atualização dos agentes de tratamento, de modo a refletir mudanças nas operações e nas relações contratuais.
 - Realizar auditorias regulares para verificar se os agentes de tratamento estão cumprindo com as exigências legais e com os compromissos assumidos em relação à proteção de dados.
- Para a Identificação dos Processos e Atividades Operacionais:
 - Formalizar e documentar todos os processos que envolvem o tratamento de dados pessoais, incluindo os fluxos de dados e os processos de segurança aplicados.

- Implementar um sistema de monitoramento contínuo e revisão dos processos operacionais, a fim de garantir que a conformidade seja mantida ao longo do tempo.
- Realizar revisões periódicas desses processos para identificar lacunas e garantir a adaptação contínua às novas regulamentações e práticas do setor.
- Para os Mecanismos de Garantia dos Direitos dos Titulares:
 - Expandir a cobertura dos mecanismos existentes para garantir que todos os direitos dos titulares de dados sejam atendidos de forma eficiente e dentro dos prazos exigidos pela LGPD.
 - Estabelecer canais de comunicação mais eficazes com os titulares de dados, a fim de garantir que suas solicitações sejam tratadas de forma transparente e rápida.
 - Implementar um sistema de feedback que permita à organização avaliar e melhorar continuamente a eficácia dos mecanismos de proteção dos direitos dos titulares.
- Para as Técnicas de Proteção de Dados Sensíveis:
 - Continuar a aplicação rigorosa de técnicas de proteção de dados sensíveis, garantindo que todas as categorias de dados sensíveis sejam adequadamente mascaradas, pseudonimizadas ou anonimizadas, conforme necessário.
 - Estabelecer uma rotina de revisão e atualização das técnicas de proteção de dados, garantindo que a organização esteja utilizando as melhores práticas disponíveis.
 - Monitorar continuamente o uso dessas técnicas e realizar auditorias regulares para identificar possíveis falhas e melhorar a eficácia das medidas de segurança.

6.3.4.3 Dimensão 3: Treinamento e Conscientização

A seguir, detalha-se o cálculo da pontuação referente à Dimensão 3 para a Universidade Federal do Rio Grande do Sul (UFRGS), abrangendo as questões 12 a 15 do instrumento de medição. Com uma pontuação máxima de 60 pontos nesta dimensão, a universidade alcançou uma pontuação bruta calculada com base na fórmula: $Q12*3 + Q13*3 + Q14*3 + Q15*3$, totalizando 95 pontos.

Aplicando a equação de normalização.

$$Pontuação Normalizada = \left(\frac{Pontuação Bruta}{Pontuação Máxima Possível na Dimensão} \right) \times 100$$

$$Pontuação Normalizada = \left(\frac{52}{60} \right) \times 100 = 95 \text{ pontos}$$

Esse resultado posiciona a UFRGS na categoria "Exemplar" na Dimensão 3, de acordo com os critérios de maturidade organizacional definidos pelo MMTDP. Essa classificação reflete o estágio avançado de desenvolvimento da instituição em práticas relacionadas a essa dimensão.

Análise

A organização demonstrou um elevado nível de maturidade nas práticas de treinamento e conscientização sobre o tratamento e a proteção de dados pessoais, conforme evidenciado pelas respostas fornecidas. A implementação de programas regulares e abrangentes para a capacitação de colaboradores, parceiros e terceirizados, juntamente com a conscientização contínua sobre os riscos associados ao tratamento inadequado de dados, são indicativos importantes de conformidade com LGPD e com as normas internacionais, como as estabelecidas pela ISO/IEC 27701:2019 e ISO/IEC 27002:2022.

A organização atingiu um nível avançado ao implementar programas de capacitação completos e regulares sobre o tratamento e a proteção de dados pessoais, com revisão e atualização contínuas. Esses programas garantem que os colaboradores estejam adequadamente preparados para lidar com as implicações legais e operacionais relacionadas à proteção de dados. O cumprimento do art. 50 da LGPD e dos requisitos da ABNT NBR ISO/IEC 27701:2019 e ISO/IEC 27002:2022 reforça a eficácia dessas iniciativas na organização.

Além disso, a organização demonstrou um alto nível de maturidade na conscientização dos agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades. O treinamento contínuo e abrangente assegurou que os agentes compreendessem plenamente suas obrigações, conforme as exigências da LGPD (arts. 42-48) e das normas ISO/IEC. A continuidade desse processo é crucial para garantir que a organização mantenha a conformidade e proteja adequadamente os dados pessoais.

A capacitação específica de colaboradores, terceirizados e parceiros está bem estruturada, com treinamentos regulares que cobrem todos os aspectos

relevantes do tratamento de dados pessoais. Esse nível de maturidade é fundamental para garantir que todos os envolvidos no tratamento de dados compreendam suas responsabilidades e estejam preparados para lidar com os riscos associados. As normas ISO/IEC 27701:2019 e ISO/IEC 27002:2022 orientam a necessidade de treinamentos contínuos, alinhados com as mudanças nas regulamentações.

A organização implementou um programa abrangente de conscientização sobre os riscos do tratamento inadequado de dados pessoais. A conscientização contínua e regular sobre esses riscos fortalece a cultura de proteção de dados na organização, capacitando os colaboradores a identificar e mitigar riscos relacionados ao tratamento inadequado de dados. O alinhamento com os arts. 42-45 e 50 da LGPD e com as normas ISO/IEC 27002:2022 demonstra o compromisso da organização com a segurança e a proteção dos dados pessoais.

Embora a organização tenha atingido um alto nível de maturidade, ainda existem oportunidades para aprimorar e consolidar esses processos. A evolução contínua das práticas de treinamento e conscientização é essencial para garantir que a organização mantenha sua conformidade com as regulamentações e se adapte a novas ameaças e melhores práticas do setor.

Recomendações

Para garantir a continuidade da maturidade organizacional e a evolução das práticas de treinamento e conscientização, as seguintes ações são recomendadas:

- Para a Identificação e Atualização dos Programas de Capacitação:
 - Realizar revisões periódicas do conteúdo dos programas de capacitação, assegurando que estes estejam sempre alinhados com as mudanças nas regulamentações e nos avanços tecnológicos.
 - Expandir o conteúdo dos treinamentos para cobrir todos os aspectos relevantes do tratamento e da proteção de dados, com ênfase nas práticas cotidianas.
 - Implementar avaliações periódicas para medir a eficácia dos programas de capacitação, promovendo ajustes contínuos baseados nos resultados obtidos.
- Para a Conscientização dos Agentes de Tratamento de Dados Pessoais:

- Ampliar a abrangência dos programas de conscientização para incluir mais aspectos do tratamento de dados pessoais, assegurando que todos os agentes compreendam plenamente suas responsabilidades legais e operacionais.
 - Estabelecer monitoramento contínuo da eficácia dos programas de conscientização, com feedback regular para ajustes rápidos e eficazes.
 - Promover treinamentos periódicos e workshops para manter os agentes atualizados sobre mudanças nas regulamentações e nas práticas de segurança de dados.
- Para o Treinamento de Colaboradores, Terceirizados e Parceiros:
 - Expandir a capacitação para incluir todos os colaboradores e parceiros envolvidos no tratamento de dados pessoais, assegurando uma abordagem uniforme e abrangente.
 - Desenvolver módulos específicos para diferentes tipos de dados e cenários de tratamento, garantindo uma aplicação prática e contextualizada do treinamento.
 - Estabelecer uma rotina de treinamentos regulares para colaboradores, terceirizados e parceiros, com o objetivo de manter a conformidade contínua com as exigências da LGPD e as melhores práticas de proteção de dados.
- Para a Conscientização sobre os Riscos do Tratamento Inadequado de Dados Pessoais:
 - Intensificar as atividades de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, com foco em identificar e mitigar falhas operacionais e incidentes de segurança.
 - Desenvolver campanhas de conscientização contínua, utilizando cenários práticos e exemplos reais de incidentes relacionados ao tratamento inadequado de dados, reforçando a importância de medidas preventivas.
 - Realizar avaliações regulares sobre o impacto das atividades de conscientização e implementar melhorias contínuas baseadas nos

resultados obtidos, garantindo que a organização esteja sempre à frente das novas ameaças.

6.3.4.4 Dimensão 4: Segurança da Informação e Tecnologia

A seguir, apresenta-se o detalhamento do cálculo da pontuação referente à Dimensão 4 para a Universidade Federal do Rio Grande do Sul (UFRGS), que abrange as questões 16 a 21 do instrumento de medição. A pontuação máxima para essa dimensão é de 100 pontos. A universidade alcançou uma pontuação bruta, calculada com base na fórmula: $Q16*5 + Q17*3 + Q18*3 + Q19*3 + Q20*3 + Q21*3$, resultando em 97 pontos.

Aplicando a equação normalizada.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{97}{100} \right) \times 100 = 97 \text{ pontos.}$$

Esse resultado posiciona a UFRGS na categoria "Exemplar" na Dimensão 4, conforme os critérios e intervalos previamente estabelecidos para a avaliação da maturidade organizacional no MMTDP. Essa classificação reflete um desempenho excelente, destacando a efetividade da instituição nas práticas relacionadas a essa dimensão.

Análise

A organização demonstrou um nível de maturidade avançado na implementação de práticas de segurança da informação e proteção de dados pessoais, conforme evidenciado pelas respostas fornecidas. A adoção de políticas e controles robustos, como o uso consistente de criptografia, a gestão de backups e trilhas de auditoria, o monitoramento contínuo de vulnerabilidades e ameaças, e a gestão rigorosa do controle de acesso, reflete uma conformidade sólida com a Lei Geral de Proteção de Dados e com as normas internacionais, como as estabelecidas pela ISO/IEC 27701:2019 e ISO/IEC 27002:2022.

A organização evidenciou um alto nível de maturidade ao definir, elaborar, implementar e monitorar regularmente sua Política de Segurança da Informação. A consistência e a revisão contínua dessa política demonstram um forte compromisso com a proteção dos dados e com a conformidade regulatória. Este processo está em total alinhamento com o art. 50 da LGPD e com as melhores práticas internacionais.

O uso consistente e abrangente de criptografia para proteger os dados pessoais é uma prática essencial que reflete uma abordagem madura de segurança. A criptografia, aliada a um monitoramento contínuo e a revisões regulares, garante que os dados pessoais sejam adequadamente protegidos contra acessos não autorizados e possíveis vazamentos, em conformidade com as exigências da LGPD e das normas ISO/IEC.

A organização também implementou um sistema robusto de gestão de backups e trilhas de auditoria, essencial para garantir a integridade e rastreabilidade dos dados pessoais. A existência de trilhas de auditoria oferece uma camada adicional de segurança, permitindo a identificação rápida de falhas ou incidentes. Esta prática é particularmente importante para garantir a conformidade contínua, especialmente em um ambiente de rápidas mudanças regulatórias e tecnológicas. Além disso, a organização adotou uma abordagem proativa ao monitorar e analisar informações sobre vulnerabilidades e ameaças à segurança da informação. A produção de inteligência de ameaças e a gestão de vulnerabilidades garantem que a organização esteja continuamente preparada para enfrentar riscos emergentes, refletindo uma cultura de segurança madura que está alinhada com os princípios da LGPD e com as diretrizes da ISO/IEC.

O controle de acesso rigoroso e a autenticação segura são fundamentais para proteger dados pessoais e garantir que apenas indivíduos autorizados tenham acesso a informações sensíveis. A organização demonstrou conformidade com a LGPD e com as normas ISO/IEC ao estabelecer controles adequados, revisar esses controles regularmente e implementar novas técnicas conforme necessário para aprimorar a segurança.

A organização implementou sistemas abrangentes de monitoramento e controle para lidar com violações e vazamentos de dados pessoais. O monitoramento contínuo, aliado a revisões e aprimoramentos regulares, assegura que a organização esteja pronta para responder a incidentes de segurança de forma eficiente e conforme as exigências legais, conforme os artigos 48 e 50 da LGPD.

Embora a organização tenha atingido um alto nível de maturidade em termos de segurança e proteção de dados, a evolução contínua desses processos é essencial. A adaptação às novas ameaças tecnológicas, bem como a incorporação de melhores práticas emergentes, permitirá que a organização se mantenha à frente

dos riscos de segurança e continue a promover a conformidade com a LGPD e outras regulamentações internacionais.

Recomendações

Para garantir a continuidade do alto nível de maturidade na proteção de dados pessoais e segurança da informação, a organização pode adotar as seguintes ações:

- Para a Política de Segurança da Informação:
 - Realizar revisões periódicas na Política de Segurança da Informação para garantir que ela se mantenha atualizada em relação às novas regulamentações e desafios tecnológicos.
 - Expandir o treinamento e a conscientização de todos os colaboradores sobre a política de segurança, garantindo que ela seja compreendida e aplicada de forma consistente em todas as áreas da organização.
 - Implementar métricas de avaliação contínua para monitorar a eficácia da política e realizar ajustes com base nos resultados obtidos e nas auditorias.
- Para o Uso de Criptografia:
 - Manter um ciclo regular de auditoria e avaliação dos processos de criptografia para garantir sua adequação às melhores práticas e às exigências regulamentares.
 - Incluir novas formas de criptografia conforme a evolução da tecnologia, adaptando-se a novos tipos de dados sensíveis e ameaças emergentes.
 - Estabelecer um plano de resposta rápida em caso de falha de criptografia ou incidentes relacionados ao acesso não autorizado a dados criptografados.
- Para a Gestão de Backup e Trilhas de Auditoria:
 - Aprimorar os sistemas de backup para garantir que todos os dados críticos estejam adequadamente protegidos e possam ser recuperados em caso de falhas.

- Fortalecer as trilhas de auditoria com o uso de ferramentas automatizadas para monitorar e relatar em tempo real atividades suspeitas ou não autorizadas.
- Realizar testes regulares de recuperação de dados e auditorias para garantir que o sistema de backup funcione de maneira eficaz quando necessário.
- Para o Monitoramento de Vulnerabilidades e Ameaças:
 - Expandir a inteligência de ameaças para incluir fontes externas, como feeds de informações sobre vulnerabilidades e eventos globais de segurança cibernética.
 - Realizar simulados de incidentes de segurança para treinar a equipe e garantir que a organização esteja preparada para lidar rapidamente com novas ameaças.
 - Desenvolver parcerias com especialistas em segurança para melhorar a capacidade de detectar e mitigar ameaças avançadas de forma mais eficaz.
- Para o Controle de Acesso e Autenticação Segura:
 - Revisar periodicamente os controles de acesso e as políticas de autenticação, assegurando que as permissões sejam adequadas e que não haja riscos de acessos indevidos.
 - Implementar autenticação multifatorial para proteger informações sensíveis, especialmente para sistemas críticos que lidam com dados pessoais.
 - Realizar auditorias regulares de acesso para garantir que os controles estejam sendo aplicados corretamente e que não existam brechas na segurança.
- Para o Monitoramento e Controle de Violação e Vazamento de Dados:
 - Desenvolver planos de resposta a incidentes mais robustos, incluindo protocolos claros para lidar com violações de dados, vazamentos e outros incidentes de segurança.

- Implementar uma plataforma automatizada de monitoramento de dados para detectar atividades suspeitas ou não autorizadas em tempo real.
- Realizar treinamentos contínuos para os colaboradores sobre como responder rapidamente a incidentes e garantir que os procedimentos de notificação e remediação estejam claros e sejam seguidos corretamente.

6.3.4.5 Dimensão 5: Acesso à Informação e Transparência

A seguir, detalha-se o cálculo da pontuação referente à Dimensão 5 para a Universidade Federal do Rio Grande do Sul (UFRGS), abrangendo as questões 22 a 25 do instrumento de medição. Com uma pontuação máxima de 70 pontos nesta dimensão, a UFRGS alcançou uma pontuação bruta, calculada com base na fórmula: $Q22*3 + Q23*3 + Q24*5 + Q25*3$, totalizando 70 pontos.

Aplicando a equação de normalização.

$$\text{Pontuação Normalizada} = \left(\frac{\text{Pontuação Bruta}}{\text{Pontuação Máxima Possível na Dimensão}} \right) \times 100$$

$$\text{Pontuação Normalizada} = \left(\frac{70}{70} \right) \times 100 = 100 \text{ pontos}$$

Esse resultado posiciona a UFRGS na categoria "Exemplar" na Dimensão 5, de acordo com os critérios de maturidade organizacional do MMTDP. Essa classificação reflete um desempenho exemplar, evidenciando o estágio avançado de desenvolvimento da instituição nessa dimensão.

Análise

A organização demonstrou um elevado nível de maturidade na governança e transparência no tratamento de dados pessoais, conforme evidenciado pelas respostas fornecidas. A implementação de políticas claras e acessíveis, como a Política de Segurança da Informação e a Política de Privacidade, a designação do encarregado de proteção de dados (DPO) e a transparência nas informações relacionadas ao tratamento de dados pessoais indicam uma conformidade sólida com a LGPD e com as melhores práticas internacionais, como as estabelecidas pela ISO/IEC 27701:2019 e ISO/IEC 27002:2022.

A organização cumpre plenamente o princípio da transparência, disponibilizando de forma clara e acessível todas as informações necessárias sobre

o tratamento de dados pessoais. A transparência é um dos pilares essenciais para a construção de uma cultura de confiança, refletindo o compromisso da organização em atender às exigências da LGPD, especialmente no que tange à acessibilidade e completude das informações. Esse nível de maturidade é fortalecido pelo monitoramento contínuo, que assegura que a organização se mantenha atualizada com as regulamentações e demandas dos titulares de dados.

A organização demonstrou um alto nível de maturidade ao elaborar e implementar uma Política de Classificação da Informação abrangente, que inclui dados pessoais sensíveis e dados relacionados a crianças e adolescentes. A existência de uma política robusta e constantemente revisada garante que a organização trate as informações com o devido cuidado, em conformidade com os requisitos do art. 11 da LGPD, que regula o tratamento de dados sensíveis. O processo de revisão regular reforça a capacidade da organização de se adaptar a novas exigências e contextos regulatórios.

A organização atendeu completamente à exigência de transparência, publicizando amplamente a designação do DPO e suas informações de contato. Essa abordagem facilita a comunicação com os titulares de dados e assegura que a organização esteja acessível para responder a quaisquer dúvidas ou preocupações sobre o tratamento de dados pessoais. O cumprimento do art. 41 da LGPD e a adoção de práticas recomendadas pela ISO/IEC 27701:2019 garantem que o DPO tenha um papel bem estabelecido e acessível dentro da organização.

A organização implementou uma Política de Privacidade bem estruturada, publicizada amplamente e regularmente revisada. Essa prática reflete a conformidade com a LGPD, especialmente com os artigos 9º e 50 da Lei, que exigem clareza e acessibilidade das informações sobre o tratamento de dados pessoais. A acessibilidade e a compreensão da política garantem que os titulares possam exercer seus direitos de forma efetiva, enquanto a revisão contínua assegura que a organização se mantenha atualizada com as mudanças na legislação e nas práticas de mercado.

Embora a organização tenha atingido um alto nível de maturidade, a evolução contínua dessas práticas é essencial para garantir que a instituição continue em conformidade com as regulamentações e se adapte às mudanças tecnológicas e normativas. A manutenção de uma cultura de transparência e a constante revisão

das políticas de governança e privacidade são fundamentais para o sucesso a longo prazo.

Recomendações

Para garantir a continuidade da maturidade organizacional e promover a evolução contínua das práticas de governança e transparência no tratamento de dados pessoais, a organização pode adotar as seguintes ações:

- Para o Princípio da Transparência:
 - Realizar revisões periódicas das práticas de transparência, ajustando-as conforme as mudanças nas regulamentações e nas necessidades dos titulares de dados.
 - Implementar um processo de feedback contínuo com os titulares de dados para garantir que a transparência seja mantida e que todas as informações estejam acessíveis e claras.
 - Expandir os canais de comunicação sobre o tratamento de dados pessoais, garantindo que todas as partes interessadas possam acessar facilmente as informações relevantes.
- Para a Política de Classificação da Informação:
 - Revisar e atualizar periodicamente a Política de Classificação da Informação para garantir que ela abranja todos os tipos de dados pessoais e seja aplicável a novos contextos regulatórios.
 - Promover treinamentos contínuos para colaboradores sobre a classificação de dados pessoais, assegurando que todos compreendam as categorias de dados e a importância de protegê-los adequadamente.
 - Realizar auditorias regulares para verificar a eficácia da política de classificação e garantir que todos os dados pessoais sejam corretamente classificados e protegidos.
- Para a Designação do Encarregado de Proteção de Dados (DPO):
 - Fortalecer a visibilidade e o apoio ao DPO dentro da organização, garantindo que ele tenha acesso a todas as áreas relevantes e a autonomia necessária para realizar suas funções de maneira eficaz.

- Revisar e atualizar periodicamente as informações de contato do DPO, garantindo que estejam sempre acessíveis e visíveis para os titulares de dados.
- Incluir o DPO em processos decisórios relacionados ao tratamento de dados pessoais, assegurando que a proteção de dados seja considerada desde a concepção de novos projetos e políticas.
- Para a Política de Privacidade:
 - Continuar revisando e aprimorando a Política de Privacidade, garantindo que ela esteja alinhada com as mudanças regulatórias e com as melhores práticas do setor.
 - Expandir a comunicação da Política de Privacidade para novos canais, como aplicativos móveis e interfaces digitais, garantindo que ela seja acessível em diferentes formatos.
 - Realizar treinamentos regulares para os colaboradores sobre a Política de Privacidade, assegurando que todos na organização compreendam a importância da privacidade dos dados e como aplicá-la nas suas funções diárias.

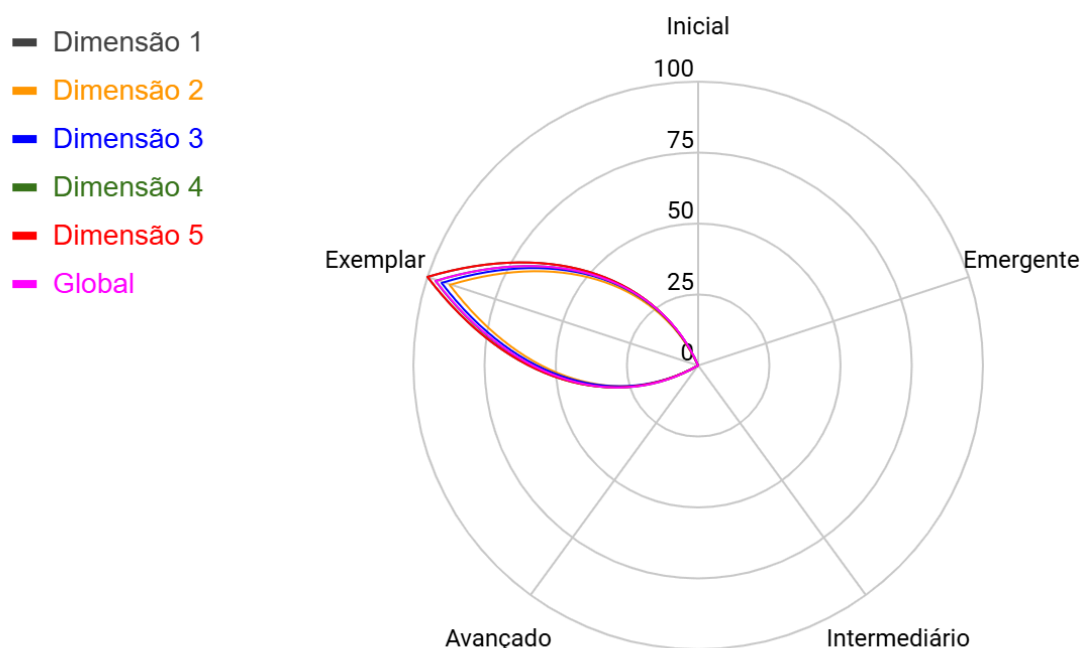
6.3.4.6 Análise Global da Instituição

A análise global dos resultados da Universidade Federal do Rio Grande do Sul (UFRGS) revelou que a instituição atingiu o estágio de maturidade **“Exemplar”** no tratamento de dados pessoais, conforme o Modelo de Maturidade para Tratamento de Dados Pessoais. Esse diagnóstico foi embasado no cálculo descrito no item **5.3.7.4**, utilizando a fórmula:

$$\text{Pontuação Global} = \left(\frac{PND1 + PND2 + PND3 + PND4 + PND5}{5} \right)$$

Os resultados das dimensões avaliadas foram os seguintes: PND1 = 100 pontos, PND2 = 92 pontos, PND3 = 95 pontos, PND4 = 97 pontos e PND5 = 100 pontos, resultando em uma pontuação global de 96,80 pontos. Essa classificação reflete uma implementação abrangente e avançada das políticas de proteção de dados, consolidando a UFRGS como referência nacional em governança e conformidade com a Lei Geral de Proteção de Dados e normas como a ABNT NBR ISO/IEC 27701 e ISO/IEC 27014. A seguir, apresenta-se uma representação visual das capacidades organizacionais avaliadas pela universidade:

Gráfico 11 - Níveis de maturidade da Universidade Federal do Rio Grande do Sul



Fonte: elaborado pelo autor.

O excelente desempenho da UFRGS em todas as dimensões avaliadas, alcançou um nível exemplar.

A UFRGS apresenta uma estrutura de governança robusta e bem articulada, integrando políticas detalhadas e amplamente implementadas ao longo de todo o ciclo de vida dos dados. Desde a coleta até o descarte, os processos institucionais são monitorados e documentados, garantindo alinhamento com padrões regulatórios e promovendo a transparência. A autonomia e a integração do Encarregado de Proteção de Dados (DPO) com áreas estratégicas, como Tecnologia da Informação (TI) e Jurídico, são pontos de destaque, assegurando uma governança de dados eficiente e responsiva.

A atuação proativa do comitê de governança de dados fortalece a capacidade da instituição de antecipar riscos e promover melhorias contínuas. Essa abordagem permite à UFRGS não apenas cumprir as exigências normativas, mas também adaptar-se rapidamente às transformações tecnológicas e regulatórias, consolidando um ambiente de confiança e segurança para os titulares de dados.

No âmbito da segurança da informação, a UFRGS adota práticas tecnológicas avançadas, incluindo criptografia robusta, autenticação multifatorial e

monitoramento contínuo de vulnerabilidades e incidentes. A revisão periódica da Política de Segurança da Informação assegura alinhamento com os padrões mais recentes, enquanto a integração de medidas como gestão eficiente de backup e auditorias regulares reforça a resiliência contra incidentes. Essa combinação de práticas reduz significativamente os riscos cibernéticos e amplia a proteção de dados sensíveis.

A transparência é um pilar central das práticas da UFRGS. A instituição disponibiliza informações claras e acessíveis sobre o tratamento de dados, promovendo atualizações regulares que fortalecem a confiança dos titulares. A Política de Privacidade e a Política de Classificação da Informação são amplamente divulgadas e revisadas periodicamente, garantindo aderência às melhores práticas e às exigências normativas. A comunicação direta com o DPO e os canais de atendimento acessíveis consolidam a relação de confiança com os titulares.

Para manter e aprimorar seu nível exemplar de maturidade, a UFRGS deve continuar revisando suas políticas e procedimentos regularmente, incorporando feedback dos titulares e antecipando-se às inovações tecnológicas e mudanças regulatórias. A realização de auditorias frequentes, simulações de incidentes e testes de acessibilidade pode fortalecer ainda mais a segurança e a transparência das operações. Investimentos contínuos em tecnologias avançadas e programas de capacitação assegurarão a evolução constante das práticas institucionais, consolidando a posição de liderança da UFRGS em governança de dados e proteção de informações pessoais.

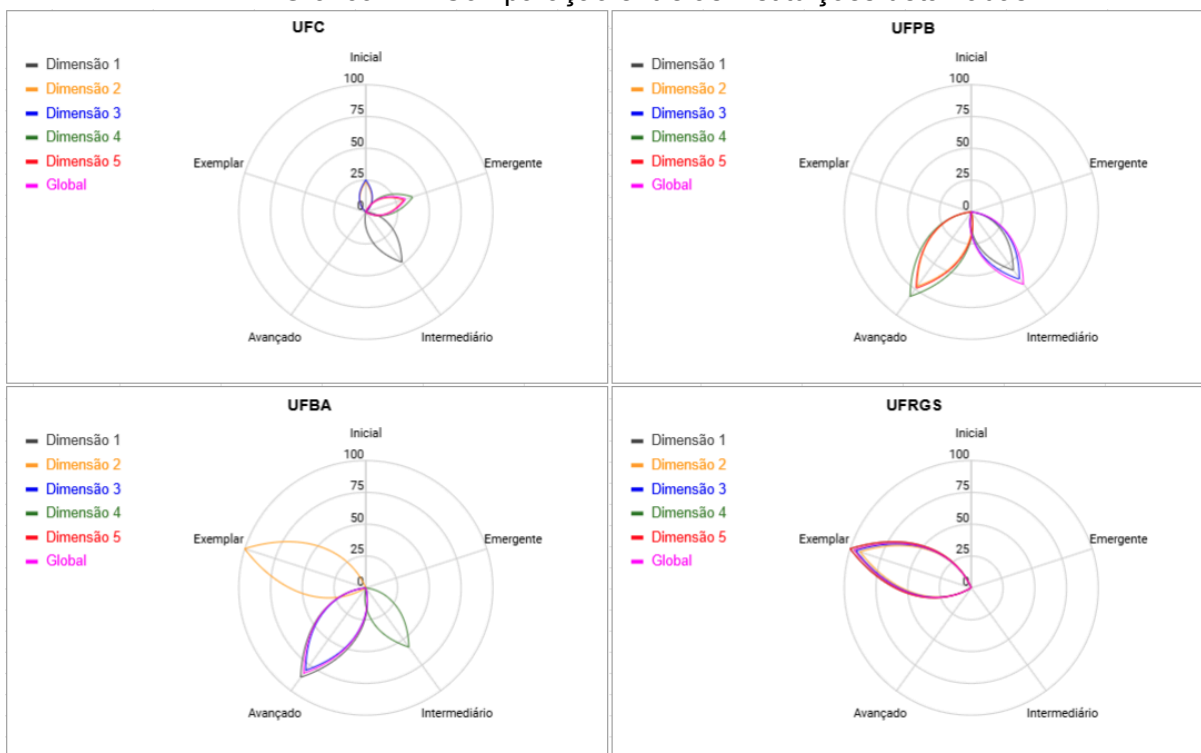
A Universidade Federal do Rio Grande do Sul destaca-se como uma instituição de excelência no tratamento de dados pessoais, demonstrando liderança e compromisso com as melhores práticas de governança, segurança e transparência. Com uma estrutura sólida e políticas bem implementadas, a UFRGS promove a confiança dos titulares e atende plenamente às exigências normativas. A continuidade no aprimoramento de suas práticas garantirá que a instituição permaneça na vanguarda da proteção de dados, reafirmando seu papel como referência nacional na área.

6.3.5 Comparando essas instituições

Conforme mencionado, devido ao tempo limitado para a execução desta pesquisa, tornou-se inviável realizar uma análise individualizada de todas as 66

universidades participantes. Optou-se, portanto, por uma análise detalhada de quatro instituições que apresentaram cenários significativamente distintos, conforme ilustrado no Gráfico 12.

Gráfico 12 - Comparação entre as instituições detalhadas



Fonte: elaborado pelo autor.

A análise dos gráficos evidencia disparidades notáveis nos níveis de maturidade das instituições avaliadas. A Universidade Federal do Ceará (UFC) apresenta o menor desempenho geral, com a maioria das dimensões concentradas nos níveis "Inicial" e "Emergente". Esse cenário indica que a UFC encontra-se em uma fase incipiente de desenvolvimento, demandando esforços estratégicos para estruturar políticas e práticas mais robustas, especialmente em áreas críticas como segurança da informação e treinamento de colaboradores.

Por outro lado, a Universidade Federal do Rio Grande do Sul (UFRGS) posiciona-se como referência, atingindo o nível "Exemplar" em todas as dimensões avaliadas. Esse desempenho reflete uma estrutura consolidada de governança, associada a práticas maduras de treinamento, segurança informacional e transparência.

Adicionalmente, ao analisar o desempenho intermediário da Universidade Federal da Paraíba (UFPB) e o desempenho avançado da Universidade Federal da

Bahia (UFBA), observa-se que ambas demonstram progressos significativos em determinadas áreas. Contudo, lacunas permanecem e demandam atenção. Essa comparação evidencia não apenas o progresso das instituições mais maduras, mas também as oportunidades de evolução para aquelas que ainda estão desenvolvendo suas práticas de governança e proteção de dados.

A UFRGS destaca-se como referência nacional no tratamento de dados pessoais, alcançando o nível "Exemplar" em todas as dimensões avaliadas. Esse resultado reflete uma estrutura de governança consolidada, fundamentada em práticas maduras de treinamento, segurança da informação e transparência, características que posicionam a instituição em um estágio avançado de gestão e conformidade. A maturidade alcançada pela UFRGS não apenas demonstra a eficácia de sua abordagem integrada, mas também reafirma o valor da análise de maturidade como uma ferramenta estratégica de gestão. Tal abordagem permite identificar e monitorar áreas críticas, assegurando que recursos sejam alocados de forma eficaz e alinhados às metas institucionais.

O contraste com instituições em estágios iniciais, como a UFC, destaca a importância dessa metodologia para direcionar esforços de melhoria. A UFC, cujas dimensões predominam nos níveis "Inicial" e "Emergente", encontra na análise de maturidade um diagnóstico claro de suas fragilidades e prioridades. Entre essas, destacam-se a necessidade de maior estruturação de políticas, integração de setores estratégicos e capacitação contínua. Já as Universidades Federais da Paraíba (UFPB) e da Bahia (UFBA), com desempenhos intermediários e progressos notáveis em áreas como Políticas e Processos e Transparência, demonstram que a análise de maturidade também funciona como um guia eficaz para consolidar avanços e superar lacunas, especialmente com maior investimento em tecnologia e treinamento.

Essa comparação demonstra que a análise de maturidade não se limita a um diagnóstico estático, mas configura-se como uma ferramenta de gestão dinâmica, essencial para traçar planos de ação e monitorar a evolução institucional. Essa metodologia possibilita não apenas identificar boas práticas em instituições de maior maturidade, como a UFRGS, mas também adaptar essas estratégias às realidades de instituições que enfrentam desafios estruturais. Assim, a análise de maturidade se consagra como um recurso indispensável para transformar dados em decisões

estratégicas, promovendo um ciclo contínuo de melhoria e alinhamento aos mais altos padrões de excelência em governança e proteção de dados pessoais.

7 CONSIDERAÇÕES FINAIS

O presente estudo evidenciou a necessidade premente de que as entidades públicas, especialmente as universidades federais brasileiras, atendam aos requisitos legais e regulamentares relacionados ao tratamento e à proteção de dados pessoais. A crescente demanda por conformidade com a Lei Geral de Proteção de Dados e outras normativas reforça a importância de práticas operacionais transparentes e alinhadas aos princípios de segurança e privacidade. Nesse contexto, o Modelo de Maturidade para Tratamento e Proteção de Dados Pessoais (MMTDP), desenvolvido nesta pesquisa, demonstrou ser uma ferramenta eficaz para diagnóstico e planejamento estratégico, possibilitando análises detalhadas das capacidades organizacionais.

Os resultados alcançados neste estudo reforçam a importância das legislações e normas, que estabelecem diretrizes fundamentais para a proteção e tratamento dos dados pessoais. A aplicação do MMTDP demonstrou alinhamento com esses marcos legais, sendo uma ferramenta que possibilita às universidades federais brasileiras operacionalizar esses princípios de maneira prática e estratégica, promovendo a conformidade legal e a governança de dados.

O MMTDP se baseia em elementos estruturantes discutidos no referencial teórico sobre modelos de maturidade, incluindo dimensões de análise, níveis de progresso e critérios de avaliação, que assegurem um diagnóstico preciso das capacidades organizacionais no tratamento de dados pessoais. A integração desses elementos foi essencial para garantir a aplicabilidade do modelo nos contextos institucionais, como demonstrado na análise realizada nas universidades federais brasileiras.

Os métodos e instrumentos de coleta empregados neste estudo foram adequados para atingir os objetivos propostos. O objetivo (a), relacionado à identificação das legislações e normas brasileiras que impactam o tratamento de dados pessoais, foi contemplado no item **5.3**. O objetivo (b), que tratou da análise dos elementos essenciais para a composição do modelo de maturidade aplicável às universidades federais, incluindo suas dimensões, níveis e inter-relações, foi desenvolvido na **Seção 5**. O objetivo (c), referente à elaboração do instrumento de medição do modelo de maturidade, está detalhado no **Apêndice O**. O objetivo (d),

que abordou a validação e estruturação do instrumento por meio do método *Delphi*, foi cumprido no item **5.3.6**. Por fim, o objetivo (e), relacionado à aplicação e teste do modelo nas universidades federais brasileiras, foi descrito no item **5.4** e na **Seção 6**.

A implementação do MMTDP gerou trocas enriquecedoras entre profissionais de diversas universidades, ampliando o impacto do modelo e sua capacidade de fomentar boas práticas. Um exemplo prático é a Universidade Federal de Viçosa (UFV), que utilizou o questionário como base para criar uma planilha de controle institucional, demonstrando a aplicabilidade do modelo como ferramenta de monitoramento contínuo.

A integração do MMTDP com ferramentas administrativas, como o ciclo PDCA, a matriz SWOT e o Balanced Scorecard (BSC), amplia seu potencial estratégico. O PDCA facilita ciclos de planejamento e melhoria contínua; a matriz SWOT auxilia na análise estratégica, identificando forças, fraquezas, oportunidades e ameaças; e o BSC promove o alinhamento das metas relacionadas ao tratamento de dados com os objetivos institucionais. Essas abordagens complementares fortalecem a governança de dados e impulsionam o alinhamento regulatório.

Recomenda-se a consulta regular ao site oficial da Autoridade Nacional de Proteção de Dados para acompanhar a evolução dos temas relacionados ao tratamento e à proteção de dados pessoais. O portal oferece acesso a atos normativos, como resoluções, portarias e enunciados, além de diversas publicações úteis, incluindo manuais, notas técnicas, relatórios e estudos técnicos. Esses materiais são essenciais para apoiar o planejamento estratégico e orientar a adoção de práticas adequadas. Os conteúdos estão disponíveis no seguinte endereço: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>.

Por fim, sugere-se expandir o MMTDP por meio do desenvolvimento de softwares que facilitem sua aplicação em diferentes contextos organizacionais. Assim, o modelo de maturidade consolida-se não apenas como um instrumento de conformidade, mas também como uma ferramenta estratégica para a gestão de dados pessoais, promovendo excelência e competitividade institucional em um ambiente regulatório desafiador.

REFERÊNCIAS

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos na graduação. 10 ed. São Paulo: Atlas, 2010.

ANPD aplica a primeira sanção por violação à Lei Geral Proteção de Dados.

Consultor Jurídico, 6 jul. 2023. Disponível em:

<https://www.conjur.com.br/2023-jul-06/anpd-aplica-primeira-sancao-violacao-lgpd>.

Acesso em: 14 jul. 2023.

ANTUNES, Ilídio. A problemática da avaliação e da maturidade nos processos de desenvolvimento de aplicações informáticas. **Informação & Informática**, v. 14, n. 26, p. 45-52, 2001.

ASSIS, Bruna Ferreira de Souza Pereira; MACHADO, Luciana Gonçalves; ANJOS, Mariana Couto; LIMA, Gilson Brito Alves. Metodologia para Análise de Maturidade de Inovações Sustentáveis. **Revista Sistemas & Gestão**, v. 7, n. 3, p. 416-427, 2012. Disponível em: <https://www.revistasg.uff.br/sg/article/view/V7N3A10/V7N3A10>. Acesso em: 12 jan. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2024** - Segurança da informação, segurança cibernética e proteção à privacidade - Sistema de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2024.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2023** - Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014:2021** - Segurança da informação, segurança cibernética e proteção à privacidade - Governança da segurança da informação. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27035:2023** - Tecnologia da informação - Gestão de incidentes de segurança da informação. Rio de Janeiro: ABNT, 2023.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29134:2024** - Tecnologia da informação - Técnicas de segurança - Orientações para avaliação de impacto de privacidade. Rio de Janeiro: ABNT, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 38500:2018** - Tecnologia da informação - Governança da TI para a organização. Rio de Janeiro: ABNT, 2018.

BATENBURG, Ronald; NEPPELENBROEK, Matthijs; SHAHIM, Abbas. A maturity model for governance, risk management and compliance in hospitals. **Journal of Hospital Administration**. Utrecht, v. 3, n. 4, 2014. Disponível em: https://www.researchgate.net/publication/314441258_A_maturity_model_for_governance_risk_management_and_compliance_in_hospitals#fullTextFileContent. Acesso em: 24 jan. 2023.

BECKER, Jörg; KNACKSTEDT, Ralf; PÖPPELBUß, Jens. Developing maturity models for IT management. **Business & Information Systems Engineering**, v. 3, p. 213-222, 2009. Disponível em: <https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf>. Acesso em: 17 ago. 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 ed. Rio de Janeiro: Forense, 2021.

BOBERG, Alice L; MONIS-KHOO, Sheryl. The delphi method: a review of methodology and an application in the evaluation of a higher education program. **The Canadian Journal of Program Evaluation**, v. 7, n. 1, p. 27-39, 1992. Disponível em: <https://www.proquest.com/scholarly-journals/delphi-method-review-methodology-application/docview/1011428076/se-2>. Acesso em: 11 set. 2023.

BRASIL. **Constituição da República Federal do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 05 set. 2020.

BRASIL. **Decreto n. 7.724, de 11 de maio de 2016**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 08 set. 2020.

BRASIL. **Decreto n. 8.771, de 11 de maio de 2016**. Regulamenta a Lei n. 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 08 set. 2020.

BRASIL. **Decreto n. 8.777, de 11 de maio de 2016**. Institui a Política de Dados

Abertos do Poder Executivo federal. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8777.htm. Acesso em: 08 set. 2020.

BRASIL. **Decreto n. 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 n. 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 08 set. 2020.

BRASIL. **Decreto n. 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. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 08 set. 2020.

BRASIL. **Decreto n. 11.226, de 25 de novembro de 2022**. Altera o Decreto n. 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11266.htm. Acesso em: 08 abr. 2023.

BRASIL. **Decreto-Lei n. 2.848, de 07 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 02 set. 2020.

BRASIL. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. 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. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 24 mar. 2022.

BRASIL. **Instrução Normativa n. 01, de 27 de maio de 2020**. Dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal (GSI). Brasília, DF, GSI/PR, 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Acesso em: 24 out. 2022.

BRASIL. **Instrução Normativa SGD/ME n. 117, de 19 de novembro de 2020**. Brasília, DF, SGD/ME, 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativasgd/me-n-117-de-19-de-nove>

mbro-de-2020-289515596. Acesso em: 09 jan. 2023.

BRASIL. **Lei n. 7.232, de 29 de outubro de 1984.** Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília, DF: Presidência da República, 1984. Disponível em: https://www.planalto.gov.br/CCivil_03/leis/L7232.htm. Acesso em: 07 set. 2020.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 07 set. 2020.

BRASIL. **Lei n. 8.159, de 08 de janeiro de 1991.** Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília, DF: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm. Acesso em: 04 set. 2020.

BRASIL. **Lei n. 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 04 set. 2023.

BRASIL. **Lei n. 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 04 set. 2023.

BRASIL. **Lei n. 9.784, de 29 de janeiro de 1999.** Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 04 set. 2023.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 10.741, de 1º de outubro de 2003.** Dispõe sobre o Estatuto da Pessoa Idosa e dá outras providências. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 08 set. 2023.

BRASIL. **Lei n. 12.414, de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011.** Regula o acesso a

informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019.** Altera a Lei n. 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.. Brasília, DF: Presidência da República, 2019. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 08 set. 2020.

BRASIL. **Lei n. 14.010, de 10 de junho de 2020.** Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidência da República, 2020. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm. Acesso em: 08 set. 2021.

CASTELLI, Tiago Machado. **Análise da metodologia Knowledge Development Process – Constructivist (Proknow-C) e suas contribuições à avaliação de desempenho organizacional:** um estudo à luz do apoio à decisão. 2018. 113 f. Dissertação (Mestrado em Administração) - Programa de Pós-Graduação em Administração, Instituto de Ciências Econômicas, Administrativas e Contábeis, Universidade Federal do Rio Grande, Rio Grande, 2018.

CASTRO, Jonathas Assunção Salvador Nery de. (2023). Prefácio: Prefácio à 4ª edição. In: PINHEIRO, P. P. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: SaraivaJur, 2023. 224p.

COLOMBO, Cristiano. **Decisões Automatizadas pela administração pública:** diálogos entre Leading Cases e Critérios para sua implementação à luz da Lei Geral de Dados Pessoais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves; RAMOS, Rafael (org.). Lei geral de proteção de dados e poder público. Porto Alegre: Tribunal de Contas do Estado, 2021, p. 57-66.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 54, de 8 de dezembro de 2023.** Estabelece diretrizes e regras para a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado. Diário Oficial da União: seção 1, Brasília, DF, 13 dez. 2023. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-54-de-8-de-dezembro-de-2023>. Acesso em: 6 jan. 2022.

COSTA, S. R.; RAMOS, Ana. F. B. Modelo de Maturidade em Gerenciamento de Projeto: Um Estudo de Caso Aplicado a Projetos de Petróleo e Energia. **Sistemas & Gestão**, [S. l.], v. 8, n. 3, p. 234–243, 2013. DOI: 10.7177/sg.2013.V8.N3.A2. Disponível em: <https://www.revistasg.uff.br/sg/article/view/V8N3A2>. Acesso em: 17 jan. 2023.

CMMI Product Team. CMMI for Systems Engineering, Version 1.1, Staged Representation (CMMI-SW, V1.1, Staged). **Software Engineering Institute**, Carnegie Mellon University, Report, Ago, 2002. Disponível em: <https://doi.org/10.1184/R1/6572408.v1>. Acesso em: 21 dez. 2022.
CRAWFORD, J. K. **Project Management Maturity Model:** Providing a proven path to project management excellence. 2002.

CROSBY, P. B. **Quality Is Free:** The Art of Making Quality Certain. McGraw-Hill, New York, 1979.

DAYCHOUM, Merhi. **Ferramentas e Técnicas de Gerenciamento:** 40+16. Rio de Janeiro: BRASPORT Livros. 6 ed., 2016.

DE BRUIN, Tonia; FREEZE, Ron; KULKARNI, Uday; ROSEMANN, Michael. Understanding the Main Phases of Developing a Maturity Assessment Model. Australasian Conference on Information Systems, **ACIS 2005**, Proceedings, 109, 2005. Disponível em: <https://aisel.aisnet.org/acis2005/109>. Acesso em: 04 set. 2023.

DIAS, Rita De Cássia Barros. **Método Delphi:** Uma descrição de seus principais conceitos e características. 2007. Monografia (Curso de especialização em Pesquisa de Mercado em Comunicação) - Escola de Comunicações e Artes - Departamento de Relações Públicas, Propaganda e Turismo - Universidade de São Paulo, São Paulo, 2007. Disponível em: <https://pospesquisa.eca.usp.br/monografias/rita%20dias%20maio.pdf>. Acesso em: 05 set. 2022.

DIAS, F. V. ; BOLESINA, I. Direito à proteção de dados pessoais no Brasil e os traços centrais de uma autoridade local de proteção. **E-CIVITAS** (BELO

HORIZONTE) , v. 10, p. 1-26, 2017. Disponível em:
<https://revistas.unibh.br/dcjpg/article/view/2165/1>. Acesso em: 11 out. 2022.

EHMS, K.; LANGEN, M. **Holistic development of knowledge management with KMMM**. [Local de publicação não informado]: Siemens, 2002.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, Vila Nova de Gaia, ano 2018, n. IV, ed. VII, p. 19-40, 2018. DOI 10.19135/revista.consinter.0007.01. Disponível em:
<https://revistaconsinter.com/wp-content/uploads/2019/02/ano-iv-numero-vii-direito-a-privacidade-e-novas-tecnologias-breves-consideracoes-acerca-da-protecao-de-dado-s-pessoais-no-brasil-e-na-europa.pdf>. Acesso em: 13 out. 2022.

FOGAÇA, A. B. **Um comparativo entre os Modelos de Maturidade para Gerenciamento De Projetos**: O caso de equipes ágeis no ambiente de Tecnologia da Informação. 2021. Disponível em:
 <<https://repositorio.ufsc.br/bitstream/handle/123456789/228251/Amanda%20Bressan%20Foga%c3%a7a%20-%20backup.pdf?sequence=1&isAllowed=y>>. Acesso em: 20 mar. 2023.

FONTANELLA, B. J. B.; RICAS, J.; TURATO, E. R. **Amostragem por saturação em pesquisas qualitativas em saúde**: contribuições teóricas. *Cad saúde pública*, v. 24, n. 1, p. 17-27, 2008. Disponível em:
<https://www.scielo.br/j/csp/a/Zbfsr8DcW5YNWVkyMVBByhrN/?lang=pt>. Acesso em: 08 de set. 2023.

FRANCE. **Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**. Disponível em:
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>. Acesso em: 13 out. 2022.

G1. **Megavazamento de dados de 223 milhões de brasileiros**: o que se sabe e o que falta saber. 28 jan. 2021. Disponível em:
<https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-d-e-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 19 set. 2023.

GERHARDT, T. E; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

GIBSON, Cyrus F.; NOLAN, Richard L. Managing the Four Stages of EDP Growth", **Harvard Business Review**, 1974. Disponível em:
https://www.researchgate.net/publication/239538731_Managing_the_Four_Stages_of_EDP_Growth. Acesso em: 05 out. 2022

GIL, A. C. **Métodos e técnicas em pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

HEPPER, Eduardo Luís. **Maturidade em sustentabilidade corporativa**: propondo

um framework para diagnóstico. Orientador: Profª Drª Maira de Cassia Petrini. 2017. 128 f. Dissertação (Mestrado em Administração e Negócios da Pontifícia) - Programa de Pós-Graduação em Administração - Universidade Católica do Rio Grande do Sul - PUCRS, Porto Alegre, 2017. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/7377/2/DIS_EDUARDO_LUIS_HEPPER_COMPLETO.pdf. Acesso em: 30 jan. 2023.

HUMPHREY, Watts S. Characterizing the software process: a maturity framework. **IEEE Software**, v. 5, n. 2, p. 73-79, mar. 1988. DOI: 10.1109/52.2014. Disponível em: <https://ieeexplore.ieee.org/document/2014>. Acesso em: 12 jan. 2023.

IESBIK VALMORBIDA, S. M.; ROLIM ENSSLIN, S. P.; ENSSLIN, L.; RIPOLL-FELIU, V. M. Rankings Universitários Mundiais. Que Dizem os Estudos Internacionais?. REICE. **Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación**, [S. l.], v. 14, n. 2, 2016. DOI: 10.15366/reice2016.14.2.001. Disponível em: <https://revistas.uam.es/reice/article/view/2744>. Acesso em: 25 nov. 2024.

KAYO, Eduardo Kazuo e SECURATO, José Roberto. Método *Delphi*: fundamentos, críticas e vieses. **Caderno de Pesquisas em Administração**, v. 1, n. 4, p. 51-61, 1997 Tradução. Disponível em: <https://silo.tips/download/metodo-delphi-fundamentos-criticas-e-vieses>. Acesso em: 30 ago. 2024.

KERZNER, H. **Strategic planning for project management using a project management maturity model**. New York: John Wiley & Sons, 2001.

KHATRI, V.; BROWN, C. V. Designing Data Governance. **Communications of the ACM**, 53(1), 148-152, 2010.

KIRKPATRICK, D. L. Techniques for Evaluation Training Programs. **Journal of the American Society of Training Directors**, 13, 21-26, 1959.

KIRKWOOD, David Allan; ALINAGHIAN, Leila Sadat; SRAI, Jagjit Singh. A maturity model for the strategic design of sustainable supply networks. 22nd. **Annual Conference of the Production and Operations Management Society**, Reno, USA, 2011.

KUZNETS, Simon. **Economic growth and structure**: selected essays. New York, W.W. Norton & Company, 1st ed., 1965, p. 213-216.

KWAK, Young Hoon; IBBS, C. William. **The Berkeley Project Management Process Maturity Model: measuring the value of project management**. Disponível em: https://www.researchgate.net/profile/Young-Kwak-3/publication/3865990_Berkeley_Project_Management_Process_Maturity_Model_Measuring_the_value_of_project_management/links/551bd96e0cf2fe6cbf75f281/Berkeley-Project-Management-Process-Maturity-Model-Measuring-the-value-of-project-management.pdf. Acesso em: 12 nov. 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de**

metodologia científica. 5. ed. São Paulo: Atlas, 2003.

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

LEAL, L. Q. Maturidade em Gerenciamento de Projetos: Uma Visão Analítica. **Engenharia de Software Magazine**, Rio de Janeiro, 15 dez. 2008, p. 32-37.

LIKERT, R. A technique for measurement of attitudes. **Archives of Psychology**, 140, 5-55, 1932. Disponível em: legacy.voteview.com/pdf/Likert_1932.pdf. Acesso em: 12 set. 2023.

MALDONADO, Viviane N; BLUM, Renato O. **LGPD** - Lei Geral de Proteção de Dados Pessoais - Comentada. 3 ed. São Paulo: Thomson Reuters Brasil, 2021.

MARQUES, Joana Brás Varanda; FREITAS, Denise de. Método *DELPHI*: caracterização e potencialidades na pesquisa em Educação. **Pro-Posições**, Campinas, v. 29, n. 2, p. 389-415, 01 ago. 2018. Dossiê "Desafios para a avaliação de contexto na educação infantil: Itália e Brasil". Disponível em: <http://dx.doi.org/10.1590/1980-6248-2015-0140>. Acesso em: 30 ago. 2024.

MASLOW, Abraham H. **Motivation and personality**, New York, Harper, 1954.

MATTAR, Fauze Najib; OLIVEIRA, Braulio; MOTTA, Sérgio Luís Stirbolov. **Pesquisa de marketing: metodologia, planejamento, execução e análise**. 7. ed. Rio de Janeiro: Elsevier, 2014.

MICHEL, M. H. **Metodologia e pesquisa científica em ciências sociais**. 2. ed. São Paulo: Atlas, 2009.

MINAYO, Maria Cecília de Souza; DESLANDES, Suely Ferreira; GOMES, Romeu. **Pesquisa Social: Teoria, Método e Criatividade**. Petrópolis: Vozes, 2016. 95 p. (Série Manuais Acadêmicos).

NASCIMENTO, Thiago Lucas Freire. **Ferramenta adaptável para auxílio no processo de coleta de dados em pesquisas estruturadas**. 2019. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Federal Rural de Pernambuco, Unidade Acadêmica de Serra Talhada, Serra Talhada, 2019.

NOLAN, Richard L. Managing the computer resource: a stage hypothesis: A practical approach for identifying opportunities for optimization. **Communications of the ACM**, New York, v. 16, n. 7, p. 339-405, 01 jul. 1973. DOI: 10.1145/362280.362284. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/362280.362284>. Acesso em: 10 jan. 2023.

OFFICE OF GOVERNMENT COMMERCE. **Portfolio, Programme and Project Management Maturity Model (P3M3)** Introduction and Guide to P3M3. OGC, 2010.

OFFICE OF GOVERNMENT COMMERCE. **PRINCE2 Maturity Model (P2MM)**. OGC, 2010.

PALAUER GARCIA, Deise. **Proposta de um modelo de maturidade em sustentabilidade para as instituições de ensino superior**. Ponta Grossa, Atena, 2021.

PATTON, M. Q. **Qualitative research e evaluation methods** (3a ed.). EUA: Sage Publications, Inc., 2001.

PEREIRA, Adriana Soares. **Metodologia da pesquisa científica**. Santa Maria, RS: UFSM, 2018. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/15824/Lic_Computacao_Metodologia-Pesquisa-Cientifica.pdf?sequence=1. Acesso em: 8 out. 2024.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: SaraivaJur, 2023. 224p.

PAULK, M. M; et al. Capability Maturity Model SM for software, version 1.1. **IEEE Software**, v. 10, n. 4, p. 18 – 27, ago/1993. Disponível em: https://www.researchgate.net/publication/3246910_Capability_Maturity_Model_Version_11/link/004635304db653a4a000000/download. Acesso em: 21 jul 2023.

PRADO, D. **Gerenciamento de Portfólios, Programas e Projetos nas Organizações**. 4ª ed. Nova Lima: INDG Tecs, 2004.

PROENÇA, Diogo; BORBINHA, José. **Maturity models for data and information management**: a state of the art. Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal. INESC-ID, Lisboa, Portugal, 2018. Disponível em: https://www.researchgate.net/publication/327431346_Maturity_Models_for_Data_and_Information_Management?enrichId=rgreq-265e9974ae266afc98c1f0ae8e90ee87-XX&enrichSource=Y292ZXJQYWdIOzMyNzQzM0NjBUzo2OTIxOTQyMDE1NzU0MzJAMTU0MjA0MzYwMA%3D%3D&el=1_x_3&_esc=publicationCoverPdf. Acesso em: 20 ago. 2023.

PROJECT MANAGEMENT INSTITUTE. **Organisational Project Management Maturity Model (OPM3)**. Maryland, USA: Project Management Institute Inc, 2003.

ROBREDO, J. Do documento impresso à informação nas nuvens: reflexões. **Liinc em Revista**, Rio de Janeiro, v.7, n.1, p.19-42, mar., 2011. Disponível em: <http://revista.ibict.br/liinc/article/view/3287/2903>. Acesso em: 03 set. 2021.

RÖGLINGER, Maximilian; PÖPPELBUß, Jens; BECKER, Jörg. Maturity models in business process management. **Business Process Management Journal**, v. 18, n. 2, p. 328-346, 2012. DOI: 10.1108/14637151211225225. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/14637151211225225/full/pdf?title=maturity-models-in-business-process-management>. Acesso em: 16 jan. 2023.

ROSEMANN, Michael; DE BRUIN, Tonia. Application of a holistic model for determining BPM maturity. **BPTrend**, [local de publicação não informado], fev., 2005.

Disponível em:

https://www.researchgate.net/publication/27481630_Application_of_a_Holistic_Model_for_Determining_BPM_Maturity. Acesso em: 31 ago. 2023.

ROSEMANN, Michael; DE BRUIN, Tonia. Towards a Business Process Management Maturity Model. **Proceedings of the Thirteenth European Conference on Information Systems (ECIS 2005)**, Regensburg, Germany, 2005.

RUARO, Regina Linden. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à LGPD (um exercício interpretativo). **Direitos Fundamentais e Justiça**. Belo Horizonte: Fórum, ano 14, n. 42, p. 219-249, jan./jun. 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/760/992>. Acesso em: 14 out. 2022.

SARSHAR, M.; HAIGH, R.; FINNEMORE, M.; AOUAD, G.; BARRETT, P.; BALDRY, D.; SEXTON, M. SPICE: a business process diagnostics tool for construction projects. **Engineering, Construction and Architectural Management**, v. 7, n. 3, p. 241-250, 2000.

SEN, A.; RAMAMURPHY, K.; SINHA, A. P. A model of data warehousing process maturity. **IEEE Transactions on Software Engineering**, vol. 38, n. 2, p. 336-353, mar./abr., 2012. DOI: 10.1109/TSE.2011.2. Disponível em: <https://ieeexplore.ieee.org/document/5680911>. Acesso em: 21 dez. 2022.

SILVA, E. L. da; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001. 121p.

SOARES, Gabriela Pereira. **Proposição de um modelo de maturidade voltado ao lean supply chain management com base nas práticas enxutas e desperdícios**. 2019. Orientadora, Marina Bouzon, Trabalho de Conclusão de Curso (Engenharia de Produção) - Universidade Federal de Santa Catarina, Centro Tecnológico, Florianópolis, 2019. 97 p.

SOFTWARE ENGINEERING INSTITUTE. **Capability Maturity Model SM for Software**, Version 1.1. Technical Report CMU/SEI-93-TR-024. Pittsburgh: SEI, 1993.

SOFTWARE ENGINEERING INSTITUTE. **Capability Maturity Model Integration for Systems Engineering**, Version 1.1, Staged Representation (CMMI-SW, V1.1, Staged). Pittsburgh: SEI, 2002.

SOFTEX. MPS.BR – Melhoria de Processo do Software Brasileiro: Guia Geral MPS de Software. **Sociedade Softex**, Brasil. 2021. Disponível em: <https://softex.br/download/guia-geral-de-software-2021/>. Acesso em: 23 jan. 2023.

TEIXEIRA, Elizabeth. **As três metodologias: acadêmica, da ciência e da pesquisa**. Petrópolis: Vozes, 2005.

Tribunal de Contas da União (TCU). **Acórdão n. 1384/2022**, de 15 de setembro de 2022. Plenário. Brasília, DF: TCU, 2022.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, 1995.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT>. Acesso em: 7 jan. 2025.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/EC (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 07 set. 2020.

VAN STEENBERGEN, M.; BOS, R.; BRINKKEMPER, S.; VAN DE WEERD, I.; BEKKERS, W. J. The design of focus area maturity models. In: WINTER, R.; ZHAO, J.; AIER, S. (Ed.). **Global perspectives on design science research**. [S.l.]: [s.n.], 2010. p. 317-332.

WANG, Guangbin; LIU, Huan; LI, Heng; LUO, Xiaochun; LIU, Jiayi. A building project-based industrialized construction maturity model involving organizational enablers: a multi-case study in China. **Sustainability**, [local de publicação não informado], v. 12, n. 10, 2020.

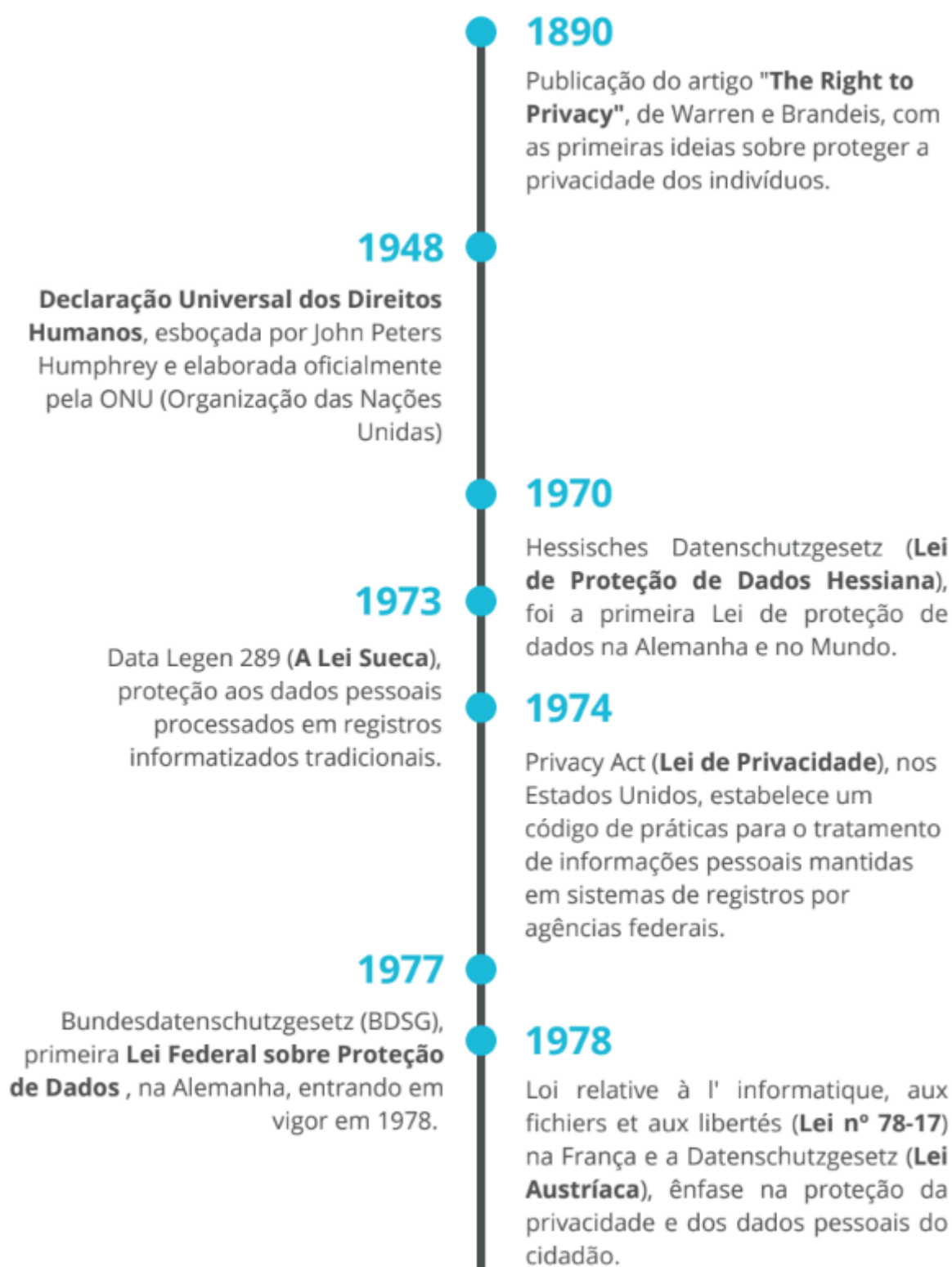
WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. **Harvard Law Review**, v. IV, n.5, dez, 1890. Disponível em: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3Af46a69247b8dc88be4a6a37a97b85262&ab_segments=&origin=. Acesso em: 11 out. 2022.

WILLIS, Christopher J.; RANKIN, Jeffrey H.. The construction industry macro maturity model (CIM3): theoretical underpinnings. **International Journal Of Productivity And Performance Management**, [local de publicação não informado], v. 61, n. 4, p. 382-402, 2012.

WINDER, D. **Personal Data From Entire 16.6M Population Of Ecuador Leaked Online**. Forbes, 16 set. 2019. Disponível em: <https://www.forbes.com/sites/daveywinder/2019/09/16/personal-data-from-entire-166m-population-of-ecuador-leaked-online/?sh=24652bfa3705>. Acesso em: 24 maio 2023.

ZIADY, H. **Meta slapped with record \$1.3 billion EU fine over data privacy**. CNN Business, 22 mai. 2023. Disponível em: <https://edition.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html>. Acesso em: 24 mai. 2023.

APÊNDICE A - Marcos históricos sobre privacidade, proteção e tratamento de dados pessoais



1983

Volkszählungsurteil (**Julgamento do Recenseamento**), parecer do Tribunal Constitucional Alemão, tornando constitucional a proteção dados pessoais na Alemanha.

1986-90

Lei de proteção de dados Austríaca (1986);

Lei Finlandesa de registro de pessoas (1987);

Disposição Constitucional **Holandesa** (1988);

Emenda Geral à **Lei Federal Alemã de Proteção de Dados** (1990).

1988

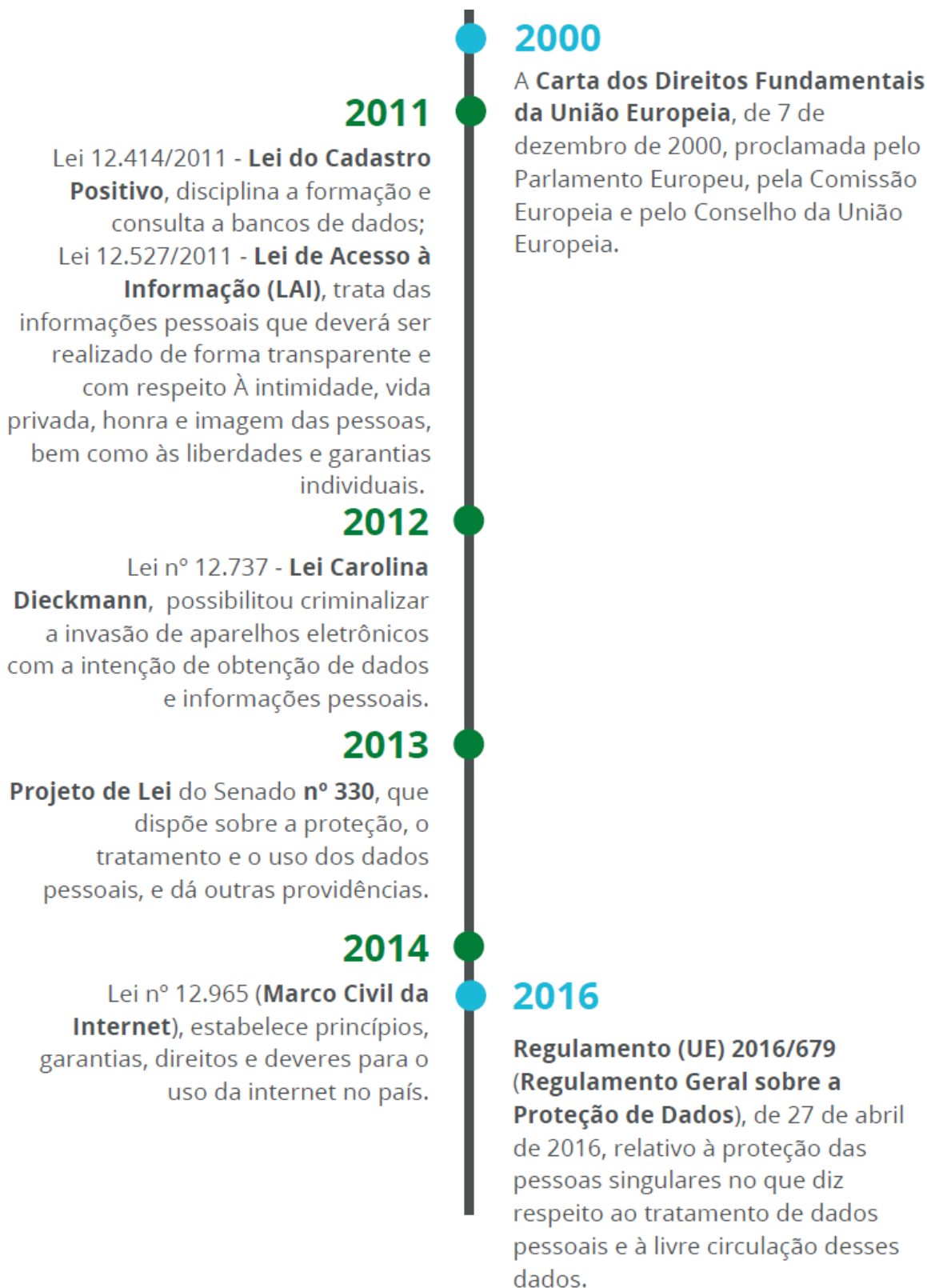
No Brasil é publicada a **Constituição Federal**, de 05 de outubro de 1988, podendo ser considerada um marco incipiente no tratamento dos dados pessoais no país, já que cita termos como privacidade, sigilo de dados e imagem.

1990-91

Lei nº 8.078 (1990), que dispõe sobre a proteção do consumidor e dá outras providências. **Lei nº 8.159** (1991), que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

1995

A **Diretiva 95/46/EC** do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, um código de conduta para a proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados.



2018

Lei nº 13.709 (Lei Geral de Proteção de Dados), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2022

Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixa a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Fonte: elaborado pelo autor.

APÊNDICE B - Questionário para identificação do encarregado pelo tratamento de dados pessoais nas universidades federais

Prezados (as),

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

Considerando o artigo Art. 23 da referida Lei, que diz que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. E seu inciso III que complementa a obrigatoriedade de indicar um encarregado da instituição para realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;

Considerando o artigo 5º, inciso VIII, desta Lei que define encarregado como a **pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).**

Considerando ainda que estou realizando uma pesquisa de doutorado na Universidade Federal da Paraíba, que irá abordar diversas discussões acerca da temática da Lei Geral de Proteção de Dados nas universidades federais do país;

Venho, respeitosamente, por meio deste, questionar:

1. A universidade já definiu quem será o encarregado da LGPD na instituição?

1.1 Caso já tenha definido, qual a portaria (ou outro documento normativo) que regularizou este profissional para a função de encarregado da instituição?

Quais são os contatos (telefone, email, etc) deste encarregado?

1.2 Caso a instituição ainda não tenha definido o seu encarregado. Qual é o posicionamento e prazo desta instituição para sanar essa pendência?

Qual é o setor, atualmente, que está trabalhando com estas demandas?

Quais são os contatos (telefones, emails, etc) desses profissionais?

APÊNDICE C - Diretrizes sobre o painel de especialistas

1. O "Painel de Especialistas" é de participação voluntária e não implica em qualquer risco à integridade física ou moral dos participantes. Garante-se aos participantes o direito de desistência a qualquer momento, sem necessidade de justificativa e sem que isso acarrete qualquer consequência negativa.
2. O "Painel de Especialistas" faz parte integrante da pesquisa de doutorado intitulada "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de modelo de maturidade sob a perspectiva dos marcos legais brasileiros", vinculada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba.
3. A equipe responsável pela coordenação do "Painel de Especialistas" e pela condução da pesquisa de doutorado é composta por Isaac Rozas Rios, doutorando (isaacrios@hotmail.com/ irr@academico.ufpb.br), e pelo Prof. Dr. Wagner Junqueira de Araújo, orientador (wagnerjunqueira.araujo@gmail.com).
4. O objetivo do "Painel de Especialistas" é contribuir para a elaboração e validação de um instrumento de medição do modelo de maturidade para o tratamento de dados pessoais nas Universidades Federais do Brasil, conforme a Lei Geral de Proteção de Dados e outros marcos legais brasileiros pertinentes. Esse processo será realizado a partir do consenso e das contribuições dos especialistas participantes. As dimensões contempladas no modelo incluem: i) governança de dados e boas práticas; ii) políticas e processos de tratamento de dados; iii) treinamento e conscientização; iv) segurança da informação e tecnologia; e v) acesso à informação e transparência.
5. Os resultados desta pesquisa têm fins exclusivamente acadêmicos, destinando-se à conclusão da tese de doutorado e à posterior divulgação em eventos científicos e publicações em periódicos especializados.
6. Esse processo resultará na habilitação e validação do questionário que irá compor o instrumento de medição do modelo de maturidade proposto, fundamentando-se na experiência e conhecimento dos especialistas participantes. Cada etapa do processo contribuirá para as fases subsequentes da pesquisa.
7. A realização deste "Painel de Especialistas" seguirá os requisitos essenciais para a aplicação do método *Delphi*, incluindo a garantia da confidencialidade dos participantes, a condução de interações sucessivas até a obtenção dos objetivos estabelecidos, a gestão de opiniões divergentes e o fornecimento de *feedback* controlado aos envolvidos.
8. O "Painel de Especialistas" será conduzido integralmente de forma online, ao longo de um período de quatro meses, de abril a agosto de 2024. Em cada etapa, os participantes (especialistas) terão um prazo de 20 dias para responder o questionário, podendo estender esse prazo por mais 10 dias, se o especialista solicitar prorrogação. O cronograma das etapas será o seguinte:

1ª etapa (18 de abril a 08 de maio de 2024): envio do questionário inicial aos especialistas para a avaliação de cada questão em relação às dimensões propostas no modelo. Nesta fase, os especialistas deverão fornecer suas análises quanto à relevância de cada questão e contribuir com sugestões para o aprimoramento do instrumento de mensuração, incluindo a proposição de novas questões, quando necessário.

2ª etapa (19 de junho a 09 de julho de 2024): envio de um questionário revisado, atualizado com as sugestões recebidas na rodada anterior, acompanhado de um relatório consolidado dos resultados da 1ª rodada. Durante esta fase, os especialistas deverão avaliar novamente as questões, considerando as alterações sugeridas, e fornecer contribuições conforme necessário.

3ª etapa (10 de julho a 25 de julho de 2024): consolidação dos resultados, incluindo o ranqueamento dos mesmos por dimensão do modelo. Nesta etapa, será avaliada a necessidade de realizar uma rodada adicional para aumentar o consenso ou proceder com a finalização do painel, seguido pela emissão do relatório final.

9. Após cada etapa, os facilitadores têm até 15 dias para preparar o relatório de feedback da rodada anterior, permitindo que os participantes acompanhem a evolução do processo. O envio desse relatório também informará a data de início da próxima rodada.

10. Após a conclusão da 3ª etapa, os facilitadores decidirão sobre: i) a realização de uma rodada adicional para aumentar o nível de coesão e consenso entre os participantes, ou ii) o encerramento do painel, considerando que o resultado alcançado seja satisfatório.

11. O acesso aos dados coletados será restrito à equipe de pesquisa, que se compromete a adotar todas as medidas necessárias para assegurar e preservar a confidencialidade das respostas dos participantes. Embora os resultados possam ser divulgados em eventos acadêmicos, conferências ou publicações científicas, qualquer informação proveniente do "Painel de Especialistas" será apresentada de forma codificada, garantindo o anonimato dos participantes.

12. Considerações adicionais: i) Todas as despesas relacionadas ao planejamento e execução do "Painel de Especialistas" serão desenvolvidas e custeadas integralmente pela equipe de pesquisa; ii) Não haverá qualquer forma de remuneração ou gratificação para os participantes do "Painel de Especialistas"; iii) Não serão concedidos reembolsos de quaisquer despesas decorrentes da participação no "Painel de Especialistas".

APÊNDICE D - Itens normativos envolvidos em cada uma das questões iniciais propostas para cada dimensão do modelo de maturidade

	Dimensão 1: Governança de Dados e Boas Práticas									
Normas/Questões	1	2	3	4	5	6	7	8	9	10
Lei n. 13.709/2018	art. 50 e art. 52, § 1º, inciso IX	art. 5º, inciso VIII, art. 23, inciso III e art. 41	art. 50	art. 7º, inciso II, art. 11, inciso II, alínea "a", art. 23, art. 26, inciso IV, art. 34, inciso I e art. 50	art. 6º, inciso I, art. 7º, art. 10, art. 15, art. 16, capítulo IV (arts. 23-32), art. 37 e art. 50	art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II	art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50	art. 50	art. 23, inciso I, art. 32, art. 50 e art. 51	art. 50, inciso I, alínea "h"
ABNT NBR ISO/IEC 27701:2019		item 6.3.1.1	item 6.3.1.1	itens 5.2.1 e 7.2.2	itens 7.2, 7.3, 7.4.1 e 8.2	itens 7.3, 7.4 e 8.3	itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5	itens 6.5.1, 6.5.3, 7.2.8 e 8.2.6	itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2	itens 5.7, 6.9.4, 6.9.7 e 6.15 e 8.2.6
ABNT NBR ISO/IEC 27002:2022				item 5.31		itens 5.34 e 6.6	item 5.14	itens 5.9, 5.10, 5.11 e 8.1.1	itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8	itens 5.22, 5.35, 5.36, 6.7, 8.15, 8.16 e 8.34
Resolução CONARQ n. 54/2023				art. 2º, parágrafo único	art. 2º, parágrafo único, arts. 4º-12 e art. 18	art. 4º, art. 13 e art. 20	art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V		art. 1º e art. 19	
Decreto n. 9.637/2018	X		art. 15							
Decreto n. 10.046/2019	X		X							
ABNT NBR ISO/IEC 27014:2021	X									
Lei n. 13.853/2019		x								
IN SGD/ME n. 117/2020		art. 1º								

Fonte: elaborado pelo autor.

	Dimensão 2: Políticas e Processos de Tratamento de Dados									
Normas/Questões	1	2	3	4	5	6	7	8	9	10

Lei n. 13.709/2018	art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII	art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50	art. 5º, inciso VI, art. 7º, incisos II e X, § 5, art. 9º, art. 10, art. 11, inciso II, art. 14, art. 37, art. 41, art. 42, art. 48 e art. 50	art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50	art. 2º, inciso I, art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso I, § 3º, inciso III, art. 32, art. 38 e art. 50, § 2º, inciso I, alíneas "a" e "d"	art. 7º, incisos III e V, art. 11, inciso I, alínea "d", art. 19, inciso II, § 3º, art. 26, incisos IV e V, art. 33, art. 35 e art. 50	art. 5º, incisos XV e XVI, art. 6º, art. 7º, inciso III e X (§5º), art. 9º, inciso V, art. 11, inciso II, alínea "b" e "g" (§3º e §4º), art. 16, inciso III, art. 18, inciso VII e inciso IX (§6º), arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50	art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51	art. 5º, inciso XII, art. 7º, incisos I e X, art. 8º, art. 9º, inciso VII, art. 11, inciso II, art. 14, art. 15, inciso III, art. 18, incisos VI, VIII e IX e art. 19, inciso II, § 3º, art. 27, inciso I e art. 33, inciso VIII, e art. 50	art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50
ABNT NBR ISO/IEC 27701:2019	itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6	itens 5.2.1, 5.2.2, 7 e 8	itens 5.2.2 e 7.2.7	itens 7.2, 7.4, 8.2 e 8.4	itens 6.2.1.1, 6.3.1.1, 6.11.2.1, 7.2.5 e 7.2.8	itens 6.15.1, 7.2.6, 7.2.7, 8.2.1, 8.3.1, 8.4.2 e 8.5	itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5	itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3	itens 7.2.2, 7.2.3, 7.2.4, 7.3 e 8.2.3	itens 7.4.2, 7.4.4 e 7.4.5
ABNT NBR ISO/IEC 27002:2022					itens 5.22 e 5.35	itens 5.20, 5.31, 6.2 e 6.5	item 5.14	item 5.18		item 8.11
Resolução CONARQ n. 54/2023	art. 13, inciso VI, e art. 17, inciso I	art. 3º, incisos I e IX, art. 13, inciso V	art. 2º, parágrafo único, art. 3º, inciso V, art. 9º, art. 14 e art. 16	art. 4º, incisos X e XII e art. 18, parágrafo único	art. 20	art. 16	art. 2º, parágrafo único, art. 10, inciso II, art. 13, inciso V, art. 22 e art. 23	capítulo IV (arts. 10-12)	art. 4º, inciso VII e art. 8º	art. 3º, incisos II e X, art. 9 e art. 18, inciso V
Decreto n. 9.637/2018									art. 3º, inciso XIII	
Lei n. 10.741/2003	art. 10, § 2º									
ABNT NBR ISO/IEC 29134:2024					Total					
Lei n. 7.232/1984 (PNI)								art. 2º, inciso IX		

Lei n. 8.159/1991								art. 4º		

Fonte: elaborado pelo autor.

Questões	Dimensão 3: Treinamento e Conscientização									
	1	2	3	4	5	6	7	8	9	10
Lei n. 13.709/2018	art. 50	art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50	art. 50	arts. 42-45, art. 50 e arts. 52-54	art. 50, arts. 52-54, art. 55-J, inciso IV, e art. 55-K	art. 48 e art. 50	art. 5º, inciso II, art. 11, art. 14, art. 38 e art. 50, § 2º, inciso I, alínea s "a" e "c"	art. 50	art. 50	art. 50
ABNT NBR ISO/IEC 27701:2019	itens 6.4.2.2 e 6.4.2.3	itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7	itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7	item 6.4.2.2	itens 6.4.2.3 e 6.15.1.1	item 6.13	itens 6.5.2.2, 7.2.2 e 7.2.3		itens 6.4.2.2 e 6.15	item 5.5.1
ABNT NBR ISO/IEC 27002:2022	item 6.3	itens 5.2, 5.4, 5.20, 5.27, 6.3, 6.4.2, 6.7, 8.7 e 8.8	itens 5.13, 5.2, 5.4, 5.20, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31	itens 5.2, 5.21, 5.4, 5.9 e 6.3	itens 6.3 e 6.4	itens 5.24, 5.25, 5.26, 5.27 e 6.3	itens 6.3, 6.6, 8.3, 8.10, 8.11 e 8.12	itens 5.35, 6.3 e 8.16	item 6.3	itens 6.3 e 8.6
Resolução CONARQ n. 54/2023		art. 3º, inciso		art. 17 e art. 25, parágrafo único		art. 15, parágrafo único	art. 4º, inciso VI			
Decreto n. 9.637/2018	art. 3º, inciso VII, e art. 15					art. 3º, incisos VII e IX				
Lei n. 7.232/1984 (PNI)	art. 4º, inciso V									
ABNT NBR ISO/IEC 27005:2023				Total						

Decreto-Lei n. 2.848/1940 (Código Civil)					art. 153, art. 305; art. 313A, art. 313B e art. 325					
ABNT NBR ISO/IEC 27035:2023						Total				

Fonte: elaborado pelo autor.

	Dimensão 4: Segurança da Informação e Tecnologia									
Questões	1	2	3	4	5	6	7	8	9	10
Lei n. 13.709/2018	art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º	art. 6º, incisos VII e VIII, arts. 46-47 e art. 50	art. 11, inciso II, alínea “g”, art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea ‘c’	art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50	art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50	art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, “g”, art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º	art. 6º, art. 31, art. 32, art. 48 e art. 50, inciso I, alínea “d”	art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea ‘g’, e art. 52, § 7º	art. 11, inciso II, alínea “g”, art. 20, art. 25, art. 46, § 2º, art. 49 e art. 50	art. 6º, inciso V, art. 18, art. 25, art. 26, inciso V, art. 31, art. 32 e art. 50
ABNT NBR ISO/IEC 27701:2019	itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15	itens 6.6.2.1, 6.6.2.2 e 6.6.3	itens 6.7 e 6.15.1.5	itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8	5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6	item 6.6	itens 5.7 e 6.13	itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6	itens 6.11, 7.4 e 8.4	itens 5.6.2, 5.7.1 e 7.4.3
ABNT NBR ISO/IEC 27002:2022	5.1 e 8.20	itens 5.16 e 8.1	item 8.24	itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25	itens 5.7, 8.7, 8.8, 8.23 e 8.28	itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5	itens 5.24, 5.26 e 5.27	itens 5.25, 5.35, 8.12, 8.16 e 8.23	itens 8.27, 8.28, 8.29 e 8.34	itens 5.12, 8.7 e 8.19

Resolução CONARQ n. 54/2023	art. 14					art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23	art. 15	art. 15 e art. 25, parágrafo único		art. 4º, inciso IX, art. 9º, art. 17, § 2º, e art. 25
Decreto n. 9.637/2018	x		art. 2º, inciso III		art. 2º, incisos II e III	art. 2º, incisos III e IV	art. 3º, inciso IX	art. 2º, inciso II, art. 3º, inciso X		art. 2º, inciso IV, e art. 3º, inciso VIII
Lei n. 7.232/1984 (PNI)	art. 4º, inciso V									
Instrução Normativa GSI/PR n. 1/2020	art. 9º									

Fonte: elaborado pelo autor.

	Dimensão 5: Acesso à Informação e Transparência									
Questões	1	2	3	4	5	6	7	8	9	10
Lei n. 13.709/2018	art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea "e"	art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas "a" e "d"	art. 5º, inciso VIII, art. 23, art. 41	art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º	art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52	art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso II, § 3º, art. 32, art. 38, art. 48 e art. 50	art. 6º, incisos VII e VIII, art. 31, art. 32, art. 46, art. 48, inciso II, § 3º, e art. 50	art. 6º, incisos VI e VII, art. 32, art. 46, art. 50	art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50	art. 32 e art. 50
ABNT NBR ISO/IEC 27701:2019		item 6.5.2	itens 6.3.1 e 8.5.5	itens 7.3.2, 7.3.3 e 8.5.5	itens 6.13, 7.3, 8.3 e 8.4.3	itens 6.1, 6.2, 7.2.5 e 8.5.5		item 6.13	itens 5.5.4, 8.4.3 e 8.5.5	itens 5.5.5, 6.9.1, 6.10 e 8.5.5

ABNT NBR ISO/IEC 27002:2022		itens 5.12 e 5.13		item 5.34	itens 5.24, 5.26 e 5.27		Itens 5.24, 5.26, 5.27, 5.28 e 5.33	itens 5.24, 5.27, 5.28 e 6.8	itens 6.6 e 6.8	itens 5.1, 5.31, 5.37 e 8.9
Resolução CONARQ n. 54/2023	art. 4º, inciso VIII, art. 18 e art. 24				art. 15		art. 14, art. 15 e art. 20	art. 15	art. 15 e art. 24	art. 19
Decreto n. 9.637/2018				art. 3º, inciso XI						
IN SGD/ME n. 117/2020			art. 1º							
Lei n. 7.232/1984 (PNI)				art. 2º , inciso VIII						
Lei n. 8.159/1991	art. 4									
Constituição Federal de 1988	art. 5, inciso XXXIII									
Lei n. 12.527/2011	Total	Total								
Decreto n. 7.724/2012	Total	Total								

Fonte: elaborado pelo autor.

APÊNDICE E – As 50 primeiras questões propostas para compor o instrumento de medição do Modelo de Maturidade para Tratamento de Dados Pessoais

Instruções: Utilize a escala a seguir com o propósito de atribuir uma pontuação de relevância a cada questão em relação à dimensão em análise. A escala de avaliação vai de **1 a 5**, onde:

- 1 - Irrelevante para a dimensão**
- 2 - Pouca relevância para a dimensão**
- 3 - Relevante para a dimensão**
- 4 - Muita relevância para a dimensão**
- 5 - Total relevância para a dimensão**

Dimensão 1: Governança de Dados e Boas Práticas (cor cinza)

1. A organização elaborou um **programa de governança, plano de governança ou documento equivalente** para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei n. 13.709/2018; Decreto n. 9.637/2018 e Decreto n. 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

() 1 () 2 () 3 () 4 () 5

2. A organização designou formalmente o **Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)**? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei n. 13.709/2018; Lei n. 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)

() 1 () 2 () 3 () 4 () 5

3. A organização estabeleceu **comitê interno ou equivalente** para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando *compliance* com todas as leis e regulamentações aplicáveis? (art. 50 da Lei n. 13.709/2018; art. 15 do Decreto n. 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto n. 10.046/2019)

() 1 () 2 () 3 () 4 () 5

4. A organização realizou **iniciativa sistemática para identificar outras legislações, normas ou regulamentos**, além da LGPD, que contenham requisitos relacionados ao tratamento de dados e informações pessoais? (art. 7º, inciso II, art. 11, inciso II, alínea “a”, art. 23, art. 26, inciso IV, art. 34, inciso I e art. 50 da Lei n. 13.709/2018; itens 5.2.1 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019 e item 5.31 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

5. A organização realizou a análise do **Legitimate Interests Assessment (LIA)**, considerando os quatro indicadores essenciais (**finalidade, necessidade, balanceamento e salvaguardas**), determinando assim as bases legais estratégicas que fundamentam o legítimo interesse no tratamento de dados pessoais na instituição? (art. 6º, inciso I, art. 7º, art. 10, art. 15, art. 16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei n. 13.709/2018; itens 7.2, 7.3, 7.4.1 e 8.2 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, arts. 4º-12 e art. 18 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

6. A instituição possui **Política de Privacidade ou documento equivalente** que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei n. 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, art. 13 e art. 20 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

7. A organização identificou se existe **compartilhamento ou transferência** de dados pessoais na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei n. 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

8. A organização faz **gestão de ativos** dos dados pessoais, **mapeando os fluxos (Personal Data Flow Map)** e o **inventário de dados pessoais**? (art. 50 da Lei n. 13.709/2018; itens 6.5.1, 6.5.3, 7.2.8 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.9, 5.10, 5.11 e 8.1.1 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

9. A organização **revisa e atualiza regularmente suas políticas e procedimentos institucionalizados** sobre o tratamento e proteção de dados e informações pessoais? (art. 23, inciso I, art. 32, art. 50 e art. 51 da Lei n. 13.709/2018; itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 1º e art. 19 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

10. A organização faz **compliance digital, monitoramento de indicadores específicos ou auditorias específicas**, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50, Inciso I, alínea “h” da Lei n. 13.709/2018; itens 5.7, 6.9.4, 6.9.7 e 6.15 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.22, 5.35, 5.36, 6.7, 8.15, 8.16 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela)

1. A organização realizou a **identificação das categorias de dados pessoais e dos titulares de dados pessoais** com os quais a instituição mantém relação? (art. 10, § 2º, da Lei n. 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

2. A organização realizou a **identificação dos agentes (controladores e operadores)** de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

3. A organização identificou se na instituição existe tratamento de dados que envolvam **controlador conjunto**, formalizando os papéis e responsabilidades de cada um? (art. 5º, inciso VI, art. 7º, incisos II e X, § 5, art. 9º, art. 10, art. 11, inciso II, art. 14, art. 37, art. 41, art. 42, art. 48 e art. 50 da Lei n. 13.709/2018; itens 5.2.2 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, art. 3º, inciso V, art. 9º, art. 14 e art. 16 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

4. A organização realizou a **identificação dos processos e atividades operacionais que lidam com dados pessoais**? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei n. 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

5. A organização gerencia os potenciais impactos por meio da **Análise ou Avaliação de Impacto de Privacidade ou PIA (Privacy Impact Assessment)**? (art. 2º, inciso I, art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso I, § 3º, inciso III, art. 32, art. 38 e art. 50, § 2º, inciso I, alíneas “a” e “d” da Lei n. 13.709/2018; itens 6.2.1.1, 6.3.1.1, 6.11.2.1, 7.2.5 e 7.2.8 da ABNT NBR ISO/IEC 27701:2019; itens 5.22 e 5.35 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 29134:2024 e art. 20 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

6. A organização **ajustou os contratos e convênios**, estabelecendo as diretrizes determinadas pelas legislações e normas, relacionadas ao tratamento e proteção dos dados pessoais? (art. 7º, incisos III e V, art. 11, inciso I, alínea “d”, art. 19, inciso II, § 3º, art. 26, incisos IV e V, art. 33, art. 35 e art. 50 da Lei n. 13.709/2018; itens 6.15.1, 7.2.6, 7.2.7, 8.2.1, 8.3.1, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.20, 5.31, 6.2 e 6.5 da ABNT NBR ISO/IEC 27002:2022 e art. 16 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

7. O **compartilhamento e transferência internacional de dados e informações pessoais com terceiros**, estão seguindo os critérios estabelecidos nas legislações? (art. 5º, incisos XV e XVI, art. 6º, art. 7º, inciso III e X (§5º), art. 9º, inciso V, art. 11, inciso II, alínea “b” e “g” (§3º e §4º), art. 16, inciso III, art. 18, inciso VII e inciso IX (§6º), arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei n. 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II, art. 13, inciso V, art. 22 e art. 23 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

8. Existem mecanismos formais na organização que garantam os **direitos dos titulares de dados pessoais**? (art. 2º, inciso IX, da Lei n. 7.232/1984; art. 4º da Lei n. 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei n. 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

9. A organização possui **gestão de consentimento dos titulares de dados pessoais**, estabelecendo procedimentos para gerenciar e documentar as revogações desse consentimento? (art. 5º, inciso XII, art. 7º, incisos I e X, art. 8º, art. 9º, inciso VII, art. 11, inciso II, art. 14, art. 15, inciso III, art. 18, incisos VI, VIII e IX e art. 19, inciso II, § 3º, art. 27, inciso I e art. 33, inciso VIII, e art. 50 da Lei n. 13.709/2018; art. 3º, inciso XIII, do Decreto n. 9.637/2018; itens 7.2.2, 7.2.3, 7.2.4, 7.3 e 8.2.3 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, inciso VII e art. 8º da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

10. A organização estabelece **regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados**, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei n. 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Dimensão 3: Treinamento e Conscientização (cor azul)

1. A organização possui **programas ou planos de capacitação** que abrangem treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei n. 7.232/1984; art. 50 da Lei n. 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto n. 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

2. A organização **conscientiza os seus agentes de tratamento de dados pessoais** sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei n. 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

3. Os **colaboradores (terceirizados e parceiros)** da organização que exercem atividades atreladas ao tratamento de dados pessoais, **recebem treinamentos e capacitações específicas sobre o tema**? (art. 50 da Lei n. 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

4. A organização **conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais?** (arts. 42-45, art. 50 e arts. 52-54 da Lei n. 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

5. A organização **capacita e conscientiza quanto às possíveis sanções administrativas aplicadas pela autoridade nacional?** (art. 153, art. 305; art. 313A, art. 313B e art. 325 do Decreto-Lei n. 2.848/1940; art. 50, arts. 52-54, art. 55-J, inciso IV, e art. 55-K, da Lei n. 13.709/2018; itens 6.4.2.3 e 6.15.1.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 6.4 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

6. A organização promove **capacitação quanto aos procedimentos adequados para a gestão de incidentes**, determinando a melhor forma de planejar, gerenciar e comunicar os incidentes de segurança da informação? (art. 48 e art. 50 da Lei n. 13.709/2018; art. 3º, incisos VII e IX, do Decreto n. 9.637/2018; item 6.13 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.25, 5.26, 5.27 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27035:2023; art. 15, parágrafo único, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

7. A organização possui **treinamentos específicos para o tratamento de dados e informações pessoais sensíveis, bem como de crianças e adolescentes?** (art. 5º, inciso II, art. 11, art. 14, art. 38 e art. 50, § 2º, inciso I, alíneas “a” e “c” da Lei n. 13.709/2018; itens 6.5.2.2, 7.2.2 e 7.2.3 da ABNT NBR ISO/IEC 27701:2019; itens 6.3, 6.6, 8.3, 8.10, 8.11 e 8.12 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso VI, da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

8. A organização realiza **avaliações periódicas ou monitoramento dos resultados (feedback) dos treinamentos e capacitações**, relacionados ao tratamento e proteção de dados e informações pessoais na instituição, aferindo a eficácia e o nível de compreensão? (art. 50 da Lei n. 13.709/2018 e itens 5.35, 6.3 e 8.16 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

9. A organização **promove regularmente, eventos, treinamentos, campanhas e/ou capacitações**, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50 da Lei n. 13.709/2018; itens 6.4.2.2 e 6.15 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

10. A organização, em seu planejamento orçamentário, disponibiliza **recursos específicos para fomentar capacitações e treinamentos**, direcionados ao tratamento e proteção de dados pessoais? (art. 50 da Lei n. 13.709/2018; item 5.5.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 8.6 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

Dimensão 4: Segurança da Informação e Tecnologia (cor verde)

1. A organização definiu e elaborou a **Política de Segurança da Informação (POSIC) ou instrumento similar**? (art. 4º, inciso V, da Lei n. 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei n. 13.709/2018; Decreto n. 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR n. 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022 e art. 14 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

2. A organização estabeleceu procedimentos para **registro, cancelamento e provisionamento de usuários nos sistemas** que realizam tratamento de dados pessoais? (art. 6º, incisos VII e VIII, arts. 46-47 e art. 50 da Lei n. 13.709/2018; itens 6.6.2.1, 6.6.2.2 e 6.6.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.16 e 8.1 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

3. A organização usa **criptografia** para proteger os dados pessoais? (art. 11, inciso II, alínea “g”, art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea ‘c’, da Lei n. 13.709/2018; art. 2º, inciso III, do Decreto n. 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

() 1 () 2 () 3 () 4 () 5

4. A organização possui **gestão de backup e trilhas de auditoria** para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei n. 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4,

6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

5. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a **inteligência de ameaças e a gestão de vulnerabilidades**? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei n. 13.709/2018; art. 2º, incisos II e III do Decreto n. 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

6. A organização estabelece **controle de acesso e autenticação segura** às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, “g”, art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei n. 13.709/2018; art. 2º, incisos III e IV, do Decreto n. 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

7. Existe **gestão de incidentes de segurança da informação** na instituição? (art. 6º, art. 31, art. 32, art. 48 e art. 50, inciso I, alínea “d” da Lei n. 13.709/2018; art. 3º, inciso IX, do Decreto n. 9.637/2018; itens 5.7 e 6.13 da ABNT NBR ISO/IEC 27701:2019 e itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

8. A organização faz **monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais**? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea ‘g’, e art. 52, § 7º, da Lei n. 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto n. 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

9. A organização implementou as abordagens **Privacy by Design e Privacy by Default** para garantir que os **sistemas institucionais sejam projetados de forma a restringir a coleta e o tratamento dos dados pessoais**, alinhando-se rigorosamente aos objetivos institucionais? (art. 11, inciso II, alínea “g”, art. 20, art. 25, art. 46, § 2º, art. 49 e art. 50 da Lei n. 13.709/2018; itens 6.11, 7.4 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e itens 8.27, 8.28, 8.29 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

10. A organização aplica a **risk assessment (avaliação de risco) para garantir confidencialidade, integridade e disponibilidade** dos dados pessoais? (art. 6º, inciso V, art. 18, art. 25, art. 26, inciso V, art. 31, art. 32 e art. 50 da Lei n. 13.709/2018; art. 2º, inciso IV, e art. 3º, inciso VIII, do Decreto n. 9.637/2018; itens 5.6.2, 5.7.1 e 7.4.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12, 8.7 e 8.19 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso IX, art. 9º; art. 17, § 2º, e art. 25 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Dimensão 5: Acesso à Informação e Transparência (cor vermelha)

1. A organização atende ao **princípio da transparência**? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei n. 8.159/1991; Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea “e”, da Lei n. 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

2. A organização possui **Política de Classificação da Informação ou instrumento similar**, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas “a” e “d”, da Lei n. 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

3. A identidade e as informações de contato, bem como a **nomeação do encarregado foram publicizadas em veículo de comunicação oficial**? (art. 5º, inciso VIII, art. 23, art. 41 da Lei n. 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

4. A **Política de Privacidade da instituição está publicizada?** (art. 2º, inciso VIII, da Lei n. 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei n. 13.709/2018; art. 3º, inciso XI, do Decreto n. 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

5. A organização estabeleceu **procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes de segurança**, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei n. 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

6. A organização implementou mecanismos para mitigar os riscos identificados no tratamento de dados pessoais por meio da **elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) ou Data Protect Impact Assessment (DPIA)?** (art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso II, § 3º, art. 32, art. 38, art. 48 e art. 50 da Lei n. 13.709/2018; itens 6.1, 6.2, 7.2.5 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

7. A organização **divulga os incidentes decorrentes de perdas, destruição, falsificação, acesso não autorizado ou liberação não autorizada?** (art. 6º, incisos VII e VIII, art. 31, art. 32, art. 46, art. 48, inciso II, § 3º, e art. 50 da Lei n. 13.709/2018; Itens 5.24, 5.26, 5.27, 5.28 e 5.33 da ABNT NBR ISO/IEC 27002:2022; art. 14, art. 15 e art. 20 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

8. A organização **promove e divulga mecanismos que incentivem relatos de incidentes e falhas de segurança** da informação? (art. 6º, incisos VI e VII, art. 32, art. 46, art. 50 da Lei n. 13.709/2018; item 6.13 da da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.27, 5.28 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ n. 54/2023)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

9. A organização possui **programa, plano de comunicação ou documento similar** que abarque as diretrizes das legislações e normas referentes ao tratamento e proteção de dados e informações pessoais? (art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50 da Lei n. 13.709/2018; itens 5.5.4, 8.4.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 6.6 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 24 da Resolução CONARQ n. 54/2023)

10. Os **procedimentos formalizados** relacionados ao tratamento e proteção dos dados e informações pessoais **estão documentados e disponibilizados**? (art. 32 e art. 50 da Lei n. 13.709/2018; itens 5.5.5, 6.9.1, 6.10 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.37 e 8.9 da ABNT NBR ISO/IEC 27002:2022 e art. 19 da Resolução CONARQ n. 54/2023)

() 1 () 2 () 3 () 4 () 5

Você gostaria de sugerir **novas questões ou indicar melhorias nas questões apresentadas** para uma melhor representatividade das dimensões abordadas? Caso sim, descreva suas sugestões abaixo. Para novas sugestões, destaque em qual dimensão ela se enquadraria, as dimensões possíveis são: Governança de Dados e Boas Práticas; Políticas e Processos de Tratamento de Dados; Treinamento e Conscientização; Segurança da Informação e Tecnologia; e Acesso à Informação e Transparência.

APÊNDICE F – Questionário inicial construído na plataforma questionpro e TCLE

PROPOSTA DO QUESTIONÁRIO PARA MEDIÇÃO DO MODELO DE MATURIDADE PARA TRATAMENTO DE DADOS PESSOAIS (MMTDP)

Introdução:

Prezado(a) Participante, antes de prosseguir com o preenchimento deste formulário, permita-me esclarecer o propósito e os termos associados a este estudo. Este questionário é uma parte integrante do "Painel de Especialistas" e constitui um componente crucial da pesquisa de doutorado intitulada "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de Modelo de Maturidade sob a perspectiva dos Marcos Legais Brasileiros".

Este trabalho está sendo desenvolvido no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. O propósito imediato deste questionário é identificar e selecionar as questões mais pertinentes que irão compor o instrumento de medição do modelo de maturidade para tratamento de dados pessoais, o qual está em fase de elaboração.

Equipe Responsável:

A equipe encarregada (facilitadores) pela condução desse "Painel de Especialistas" e pelo desenvolvimento integral da pesquisa de doutorado é composta pelos seguintes membros: Isaac Rozas Rios, doutorando (isaacrrios@hotmail.com/ irr@academico.ufpb.br) e o Prof. Dr. Wagner Junqueira de Araújo, orientador (wagnerjunqueira.araujo@gmail.com).

Contatos para esclarecimentos de dúvidas ou informações sobre a pesquisa:

Pesquisador Responsável: Isaac Rozas Rios - E-mail: isaacrrios@hotmail.com - Telefone: +55 (83) 99979-4530 ou Comitê de Ética do Centro de Ciências da Saúde Comitê de Ética em Pesquisa (CEP)- (1º andar) da Universidade Federal da Paraíba Campus I - Cidade Universitária / CEP: 58.051-900 - João Pessoa-PB - Telefone: +55 (83) 3216- 7791 - E-mail: comitedeetica@ccs.ufpb.br - Horário de Funcionamento: de 07h às 12h e de 13h às 16h. Homepage: <https://www.ccs.ufpb.br/eticaccsufp>.

Informamos que sua participação é voluntária e baseada em seu consentimento.

Termo de Consentimento Livre e Esclarecido:

A sua participação neste estudo é totalmente voluntária e não implica em nenhum custo financeiro. Todas as informações que você fornecer serão tratadas de forma anônima e confidencial, garantindo sua privacidade. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Para baixar este TCLE em formato PDF clique no link abaixo:

<https://drive.usercontent.google.com/u/0/uc?id=1C24oAbiIrLYWyMRaDqbCELG4xYbOHDzC&export=download>

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.

☐ **Sim**

☐ **Não**

Termo de Consentimento Livre e Esclarecido

Você está sendo convidado a participar da pesquisa intitulada "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de Modelo de Maturidade sob a perspectiva dos Marcos Legais Brasileiros", desenvolvida no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. O objetivo principal é propor um modelo de maturidade para o tratamento de dados pessoais nas Universidades Federais do Brasil, sob a perspectiva da Lei Geral de Proteção de Dados e demais marcos legais brasileiros sobre o tema. Este questionário tem como propósito identificar e selecionar as questões mais relevantes para compor o instrumento de medição do modelo de maturidade em fase de elaboração. Sua colaboração é muito importante, porém a participação é totalmente voluntária e não implica em custo financeiro. Para participar, você responderá a um questionário com matrizes de resposta única, incluindo uma pergunta aberta para sugestões. Todos os procedimentos para garantir a confidencialidade serão rigorosamente seguidos, mantendo suas informações anônimas e confidenciais. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Os benefícios esperados incluem o desenvolvimento da ferramenta administrativa para mapear as capacidades organizacionais no tratamento e proteção de dados e informações pessoais, promovendo transparência, controle e conformidade com as regulamentações. Os participantes terão acesso aos resultados, contribuindo para aprimorar a segurança e eficiência das atividades administrativas das instituições de ensino superior. Este estudo também servirá como referência para profissionais e pesquisas futuras sobre o tema. Reconhece-se a presença de riscos imprevisíveis, os quais são mitigados pela confidencialidade e anonimato assegurados aos participantes. Durante a coleta de dados, inclusive *on-line*, os participantes têm a liberdade de não responder sem prejuízo. Se houver dúvidas ou preocupações, entre em contato a qualquer momento com o Pesquisador Responsável: Isaac Rozas Rios - E-mail: isaacrios@hotmail.com - Telefone +55 (83) 99979-4530 ou Comitê de Ética do Centro de Ciências da Saúde Comitê de Ética em Pesquisa (CEP) - (1º andar) da Universidade Federal da Paraíba Campus I - Cidade Universitária / CEP: 58.051-900 - João Pessoa-PB - Telefone: +55 (83) 3216- 7791 - E-mail: comitedeetica@ccs.ufpb.br - Horário de Funcionamento: de 07h às 12h e de 13h às 16h. Homepage: <https://www.ccs.ufpb.br/eticaccsufpb>

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.

- ☐ Sim
- ☐ Não

Identificação do respondente (os dados pessoais não serão divulgados na pesquisa, serve apenas para controle interno dos pesquisadores)

* Nome da Instituição

* Nome do Encarregado de Dados Pessoais

* E-mail

Telefone

Instruções: Utilize a seguinte escala de relevância a cada questão com foco na dimensão em análise. A escala de avaliação vai de 1 a 5, onde:

- 1 - Irrelevante para a dimensão
- 2 - Pouca relevância para a dimensão
- 3 - Relevante para a dimensão
- 4 - Muita relevância para a dimensão
- 5 - Total relevância para a dimensão

Dimensão 1: Governança de Dados e Boas Práticas (cor cinza)

Esta dimensão avalia a forma como a organização estabelece sua estrutura de governança para lidar com dados e informações pessoais. Isso inclui aspectos estratégicos, como a nomeação de um Encarregado de Proteção de Dados, a constituição de comitês e programas de governança e a definição de responsabilidades de forma clara e precisa. Uma governança sólida é fundamental para garantir que uma instituição atue de maneira responsável e alinhada à legislação.

Dimensão 1: Governança de Dados e Boas Práticas

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei nº 13.709/2018; Decreto nº 9.637/2018 e Decreto nº 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

	1 - Irrelevante para dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou *Data Protection Officer* (DPO)? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei nº 13.709/2018; Lei nº 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

3. A organização estabeleceu **comitê interno ou equivalente** para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando *compliance* com todas as leis e regulamentações aplicáveis? (art. 50 da Lei nº 13.709/2018; art. 15 do Decreto nº 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto nº 10.046/2019)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

4. A organização realizou iniciativa sistemática para **identificar outras legislações, normas ou regulamentos**, além da LGPD, que contenham requisitos relacionados ao tratamento de dados e informações pessoais? (art. 7º, inciso II, art. 11, inciso II, alínea “a”, art. 23, art. 26, inciso IV, art. 34, inciso I e art. 50 da Lei nº 13.709/2018; itens 5.2.1 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019 e item 5.31 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

5. A organização realizou a análise do **Legitimate Interests Assessment (LIA)**, considerando os quatro indicadores essenciais (**finalidade, necessidade, balanceamento e salvaguardas**), determinando assim as bases legais estratégicas que fundamentam o legítimo interesse no tratamento de dados pessoais na instituição? (art. 6º, inciso I, art. 7º, art. 10, art. 15, art. 16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018; itens 7.2, 7.3, 7.4.1 e 8.2 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, arts. 4º-12 e art. 18 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

6. A instituição possui **Política de Privacidade ou documento equivalente** que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei nº 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, art. 13 e art. 20 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

7. A organização **identificou se existe compartilhamento ou transferência de dados pessoais** na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

8. A organização faz **gestão de ativos** dos dados pessoais, **mapeando os fluxos** (*Personal Data Flow Map*) e o **inventário de dados pessoais**? (art. 50 da Lei nº 13.709/2018; itens 6.5.1, 6.5.3, 7.2.8 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.9, 5.10, 5.11 e 8.1.1 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

9. A organização **revisa e atualiza regularmente** suas **políticas e procedimentos** institucionalizados sobre o tratamento e proteção de dados e informações pessoais? (art. 23, inciso I, art. 32, art. 50 e art. 51 da Lei nº 13.709/2018; itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 1º e art. 19 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

10. A organização faz **conformidade digital** (*compliance digital*), **monitoramento de indicadores específicos** ou **auditorias específicas**, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50, Inciso I, alínea “h” da Lei nº 13.709/2018; itens 5.7, 6.9.4, 6.9.7 e 6.15 e

8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.22, 5.35, 5.36, 6.7, 8.15, 8.16 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela)

Nesta dimensão, o foco recai sobre aspectos operacionais e técnicos, analisando a existência e eficácia das políticas, procedimentos e processos relacionados ao tratamento de dados. Avalia se as políticas estão bem definidas, abordando todos os aspectos do ciclo de vida dos dados e/ou informações pessoais, abrangendo coleta, armazenamento, tratamento e exclusão. Adicionalmente, avalia a capacidade da organização de identificar e avaliar os riscos inerentes ao tratamento de dados pessoais, à gestão dos dados pessoais sensíveis, aos dados de crianças e adolescentes e ao consentimento e direitos dos titulares de dados. Além disso, examina como a organização monitora a eficácia de suas práticas e busca continuamente aprimorá-las. O propósito é assegurar que os dados pessoais sejam tratados de maneira ética, legal e segura.

Dimensão 2: Políticas e Processos de Tratamento de Dados

1. A organização realizou a **identificação das categorias de dados pessoais e dos titulares de dados pessoais** com os quais a instituição mantém relação? (art. 10, § 2º, da Lei nº 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

2. A organização realizou a **identificação dos agentes (controladores e operadores)** de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

3. A organização identificou se existe tratamento de dados que envolvam atividades de "**controlador conjunto**", formalizando os papéis e responsabilidades de cada um? (art. 5º, inciso VI, art. 7º, incisos II e X, § 5, art. 9º, art. 10, art. 11, inciso II, art. 14, art. 37, art. 41, art. 42, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.2.2 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, art. 3º, inciso V, art. 9º, art. 14 e art. 16 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

4. A organização realizou a **identificação dos processos e atividades operacionais que lidam com dados pessoais**? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

5. A organização gerencia os potenciais impactos por meio da **Análise ou Avaliação de Impacto de Privacidade ou PIA (Privacy Impact Assessment)**? (art. 2º, inciso I, art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso I, § 3º, inciso III, art. 32, art. 38 e art. 50, § 2º, inciso I, alíneas “a” e “d” da Lei nº 13.709/2018; itens 6.2.1.1, 6.3.1.1, 6.11.2.1, 7.2.5 e 7.2.8 da ABNT NBR ISO/IEC 27701:2019; itens 5.22 e 5.35 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 29134:2023 e art. 20 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

6. A organização **ajustou os contratos e convênios**, estabelecendo as diretrizes determinadas pelas legislações e normas, relacionadas ao tratamento e proteção dos dados pessoais? (art. 7º, incisos III e V, art. 11, inciso I, alínea “d”, art. 19, inciso II, § 3º, art. 26, incisos IV e V, art. 33, art. 35 e art. 50 da Lei nº 13.709/2018; itens 6.15.1, 7.2.6, 7.2.7, 8.2.1, 8.3.1, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.20, 5.31, 6.2 e 6.5 da ABNT NBR ISO/IEC 27002:2022 e art. 16 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

7. O **compartilhamento e transferência internacional de dados e informações pessoais com terceiros**, estão **seguindo os critérios** estabelecidos nas legislações? (art. 5º, incisos XV e XVI, art. 6º, art. 7º, inciso III e X (§5º), art. 9º, inciso V, art. 11, inciso II, alínea “b” e “g” (§3º e §4º), art. 16, inciso III, art. 18, inciso VII e inciso IX (§6º), arts. 25-27, art. 30, Capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II, art. 13, inciso V, art. 22 e art. 23 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

8. Existem mecanismos formais na organização que garantam os **direitos dos titulares de dados pessoais**? (art. 2º, inciso IX, da Lei nº 7.232/1984; art. 4º da Lei nº 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei nº 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

9. A organização possui **gestão de consentimento dos titulares de dados pessoais**, estabelecendo procedimentos para gerenciar e documentar as revogações desse consentimento? (art. 5º, inciso XII, art. 7º, incisos I e X, art. 8º, art. 9º, inciso VII, art. 11, inciso II, art. 14, art. 15, inciso III, art. 18, incisos VI, VIII e IX e art. 19, inciso II, § 3º, art. 27, inciso I e art. 33, inciso VIII, e art. 50 da Lei nº 13.709/2018; art. 3º, inciso XIII, do Decreto nº 9.637/2018; itens 7.2.2, 7.2.3, 7.2.4, 7.3 e 8.2.3 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, inciso VII e art. 8º da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

10. A organização estabelece **regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados**, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei nº 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 3: **Treinamento e Conscientização** (cor azul)

Esta dimensão concentra-se no treinamento e na conscientização de colaboradores e partes interessadas sobre questões relacionadas à proteção de dados. Ela avalia o nível de instrução e conscientização dos colaboradores em relação à proteção de dados pessoais. O treinamento adequado e a conscientização são de importância crítica para garantir que todos na organização compreendam as implicações legais e éticas envolvidas no tratamento de dados e estejam preparados para agir conforme as políticas e procedimentos estabelecidos.

Dimensão 3: Treinamento e Conscientização

1. A organização possui **programas ou planos de capacitação** que abranjam treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei nº 7.232/1984; art. 50 da Lei nº 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto nº 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

2. A organização **conscientiza os seus agentes de tratamento de dados pessoais** sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei nº 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

3. Os **colaboradores (terceirizados e parceiros)** da organização que exercem atividades atreladas ao tratamento de dados pessoais, **recebem treinamentos e capacitações específicas** sobre o tema? (art. 50 da Lei nº 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

4. A organização **conscientiza regularmente quanto aos riscos associados ao tratamento inadequado** de dados pessoais? (arts. 42-45, art. 50 e arts. 52-54 da Lei nº 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

5. A organização **capacita e conscientiza quanto às possíveis sanções administrativas** aplicadas pela autoridade nacional? (art. 153, art. 305; art. 313A, art. 313B e art. 325 do Decreto-Lei nº 2.848/1940; art. 50, arts. 52-54, art. 55-J, inciso IV, e art. 55-K, da Lei nº 13.709/2018; itens 6.4.2.3 e 6.15.1.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 6.4 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

6. A organização promove **capacitação quanto aos procedimentos adequados para a gestão de incidentes**, determinando a melhor forma de planejar, gerenciar e comunicar os incidentes de segurança da informação? (art. 48 e art. 50 da Lei nº 13.709/2018; art. 3º, incisos VII e IX, do Decreto nº 9.637/2018; item 6.13 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.25, 5.26, 5.27 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27035:2023; art. 15, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

7. A organização possui **treinamentos específicos para o tratamento de dados e informações pessoais sensíveis, bem como de crianças e adolescentes**? (art. 5º, inciso II, art. 11, art. 14, art. 38 e art. 50, § 2º, inciso I, alíneas “a” e “c” da Lei nº 13.709/2018; itens 6.5.2.2, 7.2.2 e 7.2.3 da ABNT NBR ISO/IEC 27701:2019; itens 6.3, 6.6, 8.3, 8.10, 8.11 e 8.12 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso VI, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

8. A organização realiza **avaliações periódicas ou monitoramento dos resultados (feedback) dos treinamentos e capacitações**, relacionados ao tratamento e proteção de dados e informações pessoais na instituição, aferindo a eficácia e o nível de compreensão? (art. 50 da Lei nº 13.709/2018 e itens 5.35, 6.3 e 8.16 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

9. A organização **promove regularmente, eventos, treinamentos, campanhas e/ou capacitações**, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50 da Lei nº 13.709/2018; itens 6.4.2.2 e 6.15 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

10. A organização, em seu planejamento orçamentário, disponibiliza **recursos específicos para fomentar capacitações e treinamentos**, direcionados ao tratamento e proteção de dados pessoais? (art. 50 da Lei nº 13.709/2018; item 5.5.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 8.6 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 4: **Segurança da Informação e Tecnologia** (cor verde)

Nesta dimensão, o foco recai sobre as medidas de segurança implementadas pela organização para proteger dados e informações pessoais. Isso abrange a avaliação da segurança da infraestrutura de TI, as medidas de prevenção de violações de dados, a criptografia, a autenticação e outras práticas relacionadas à tecnologia, visando garantir confidencialidade e integridade dos dados. Além disso, examina-se a conformidade com as regulamentações de segurança e a eficácia das medidas de segurança implementadas nos sistemas da organização.

Dimensão 4: Segurança da Informação e Tecnologia

1. A organização definiu e elaborou a **Política de Segurança da Informação ou instrumento similar**? (art. 4º, inciso V, da Lei 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei nº 13.709/2018; Decreto nº 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022 e art. 14 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

2. A organização estabeleceu procedimentos para **registro, cancelamento e provisionamento de usuários** nos sistemas que realizam tratamento de dados pessoais? (art. 6º, incisos VII e VIII, arts. 46-47 e art. 50 da Lei nº 13.709/2018; itens 6.6.2.1, 6.6.2.2 e 6.6.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.16 e 8.1 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

3. A organização usa **criptografia para proteger os dados pessoais**? (art. 11, inciso II, alínea “g”, art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea ‘c’, da Lei nº 13.709/2018; art. 2º, inciso III, do Decreto nº 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

4. A organização possui **gestão de backup e trilhas de auditoria** para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei nº 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

5. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a **inteligência de ameaças e a gestão de vulnerabilidades**? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei nº 13.709/2018; art. 2º, incisos II e III do Decreto nº 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

6. A organização estabelece **controle de acesso e autenticação segura** às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, “g”, art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei nº 13.709/2018; art. 2º, incisos III e IV, do Decreto nº 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

7. Existe **gestão de incidentes de segurança da informação** na instituição? (art. 6º, art. 31, art. 32, art. 48 e art. 50, inciso I, alínea “d” da Lei nº 13.709/2018; art. 3º, inciso IX, do Decreto nº 9.637/2018; itens 5.7 e 6.13 da ABNT NBR ISO/IEC 27701:2019 e itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

8. A organização faz **monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais**? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea “g”, e art. 52, § 7º, da Lei nº 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto nº

9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

9. A organização implementou as abordagens **Privacy by Design e Privacy by Default** para garantir que os **sistemas institucionais** sejam **projetados de forma a restringir a coleta e o tratamento dos dados pessoais**, alinhando-se rigorosamente aos objetivos institucionais? (art. 11, inciso II, alínea “g”, art. 20, art. 25, art. 46, § 2º, art. 49 e art. 50 da Lei nº 13.709/2018; itens 6.11, 7.4 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e itens 8.27, 8.28, 8.29 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

10. A organização aplica a **avaliação de risco (risk assessment)** para **garantir confidencialidade, integridade e disponibilidade** dos dados pessoais? (art. 6º, inciso V, art. 18, art. 25, art. 26, inciso V, art. 31, art. 32 e art. 50 da Lei nº 13.709/2018; art. 2º, inciso IV, e art. 3º, inciso VIII, do Decreto nº 9.637/2018; itens 5.6.2, 5.7.1 e 7.4.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12, 8.7 e 8.19 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso IX, art. 9º; art. 17, § 2º, e art. 25 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência (cor vermelha)

Nesta dimensão, a avaliação concentra-se na disponibilidade e transparência das informações para as partes interessadas. Isso engloba a conformidade com as normas de acesso à informação e a capacidade de demonstrar transparência nas práticas de proteção de dados. Adicionalmente, avalia-se a capacidade de gerar relatórios precisos para garantir conformidade com regulamentações de privacidade e acesso à informação, bem como comunicar as partes afetadas, às autoridades regulatórias e outras partes interessadas sobre incidentes ocorridos, incluindo registros de como os incidentes foram tratados e as lições aprendidas.

Dimensão 5: Acesso à Informação e Transparência

1. A organização atende ao **princípio da transparência**? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei nº 8.159/1991; Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea “e”, da Lei nº 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

2. A organização possui **Política de Classificação da Informação ou instrumento similar**, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas “a” e “d”, da Lei nº 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

3. A **designação do encarregado e suas informações de contato, foram publicizadas** em algum meio de comunicação oficial?? (art. 5º, inciso VIII, art. 23, art. 41 da Lei nº 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

4. A **Política de Privacidade da instituição está publicizada?** (art. 2º, inciso VIII, da Lei 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei nº 13.709/2018; art. 3º, inciso XI, do Decreto nº 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

5. A organização estabeleceu **procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes** de segurança, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei nº 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

6. A organização implementou mecanismos para mitigar os riscos identificados no tratamento de dados pessoais por meio da elaboração do **Relatório de Impacto de Proteção de Dados Pessoais (RIPD) ou Data Protect Impact Assessment (DPIA)**? (art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso II, § 3º, art. 32, art. 38, art. 48 e art. 50 da Lei nº 13.709/2018; itens 6.1, 6.2, 7.2.5 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

7. A organização **divulga os incidentes decorrentes de perdas, destruição, falsificação, acesso não autorizado ou liberação não autorizada?** (art. 6º, incisos VII e VIII, art. 31, art. 32, art. 46, art. 48, inciso II, § 3º, e art. 50 da Lei nº 13.709/2018; Itens 5.24, 5.26, 5.27, 5.28 e 5.33 da ABNT NBR ISO/IEC 27002:2022; art. 14, art. 15 e art. 20 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

8. A organização **promove e divulga mecanismos que incentivem relatos de incidentes e falhas de segurança** da informação? (art. 6º, incisos VI e VII, art. 32, art. 46, art. 50 da Lei nº 13.709/2018; item 6.13 da da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.27, 5.28 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

9. A organização possui **programa, plano de comunicação ou documento similar** que abarque as diretrizes das legislações e normas referentes ao tratamento e proteção de dados e informações pessoais? (art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.5.4, 8.4.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 6.6 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 24 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

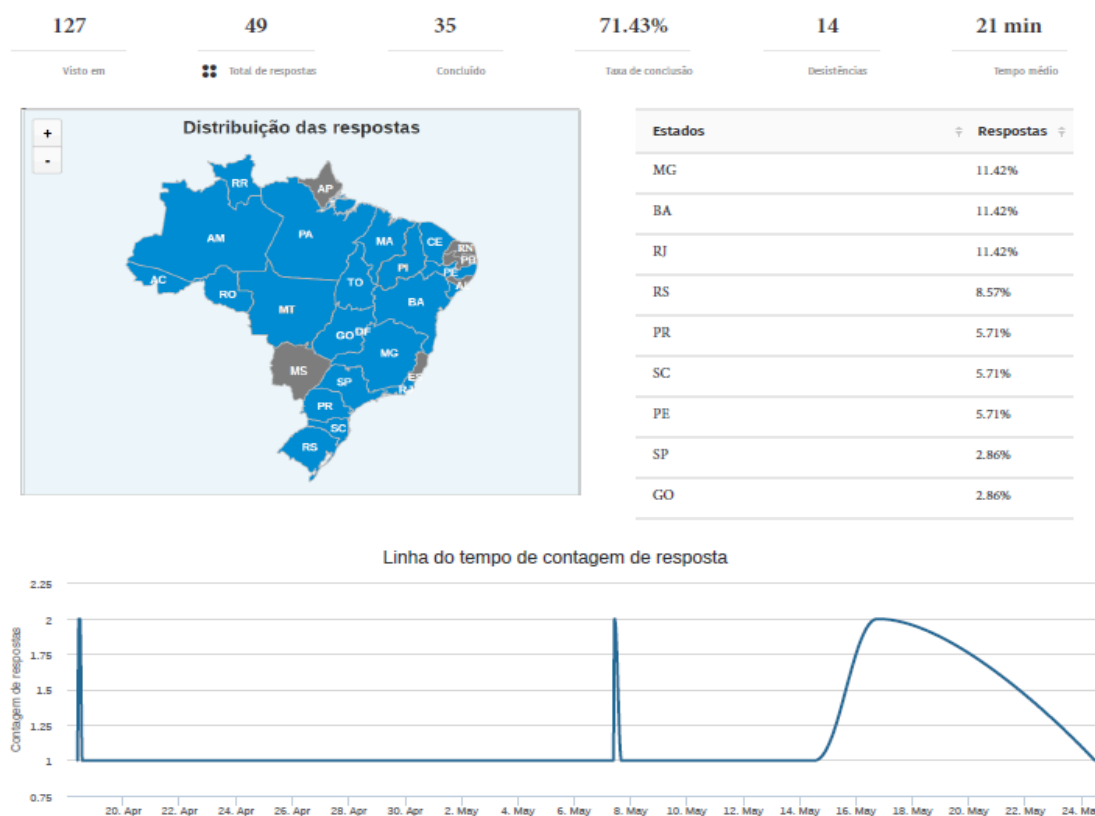
10. Os **procedimentos formalizados** relacionados ao tratamento e proteção dos dados e informações pessoais **estão documentados e disponibilizados**? (art. 32 e art. 50 da Lei nº 13.709/2018; itens 5.5.5, 6.9.1, 6.10 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.37 e 8.9 da ABNT NBR ISO/IEC 27002:2022 e art. 19 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Você teria alguma **sugestão de questão para acrescentar ao questionário**? Se sim, escreva abaixo a questão e em qual dimensão ela se enquadraria. As dimensões possíveis são: Governança de Dados e Boas Práticas; Políticas e Processos de Tratamento de Dados; Treinamento e Conscientização; Segurança da Informação e Tecnologia; e Acesso à Informação e Transparência.

APÊNDICE G – Relatório gerado pela plataforma questionpro após a primeira rodada do método *delphi*

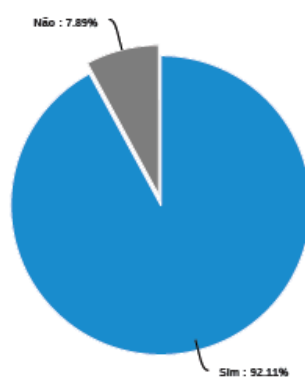
Relatório do Método Delphi - Resultado da 1ª rodada



Termo de Consentimento Livre e Esclarecido: A sua participação neste estudo é totalmente voluntária e não implica em nenhum custo financeiro. Todas as informações que você fornecer serão tratadas de forma anônima e confidencial, garantindo sua privacidade. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Para baixar este TCLE em formato PDF clique no link abaixo:

<https://drive.usercontent.google.com/u/0/uc?id=1C24oAbilrLYWyMRaDqbCELG4xYbOHDzC&export=download>

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
Sim	35	92.11%					
Não	3	7.89%					
Total	38	100 %					

Dimensão 1: Governança de Dados e Boas Práticas

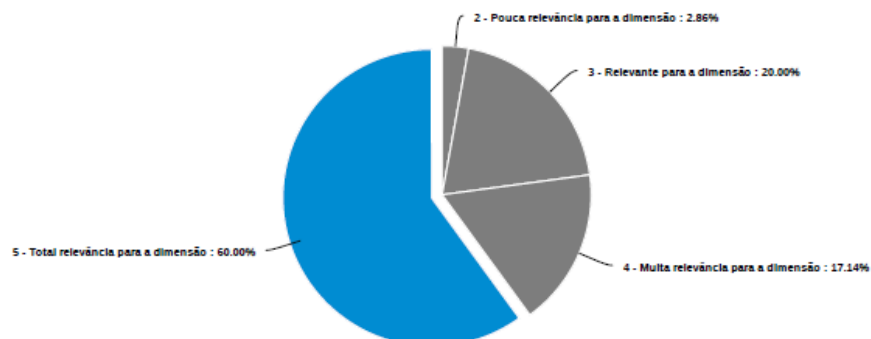
1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei nº 13.709/2018; Decreto nº 9.637/2018 e Decreto nº 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

Statement	1 - Irrelevante para dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	1 2.86%	7 20%	6 17.14%	21 60%	35 100%



Pergunta	Contagem	Pontuação	1 - Irrelevante para dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	4,34					
Média		4,34					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1 - Irrelevante para dimensão	0	0%					
2 - Pouca relevância para a dimensão	1	2.86%					
3 - Relevante para a dimensão	7	20%					
4 - Muita relevância para a dimensão	6	17.14%					
5 - Total relevância para a dimensão	21	60%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

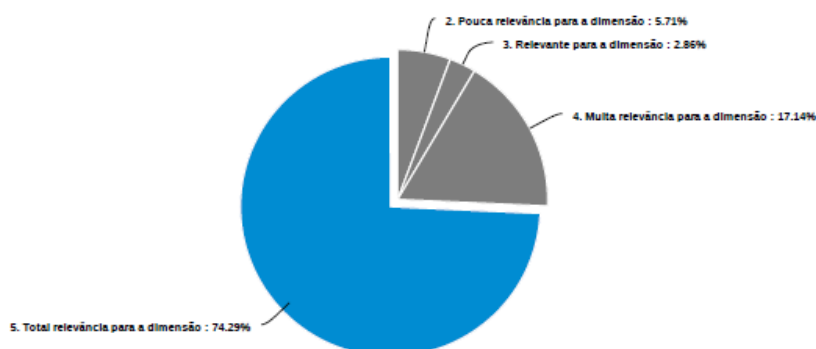
2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei nº 13.709/2018; Lei nº 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	2 5,71%	1 2,86%	6 17,14%	26 74,29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	4,6					
Média		4,6					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	1	2,86%					
4. Muita relevância para a dimensão	6	17,14%					
5. Total relevância para a dimensão	26	74,29%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

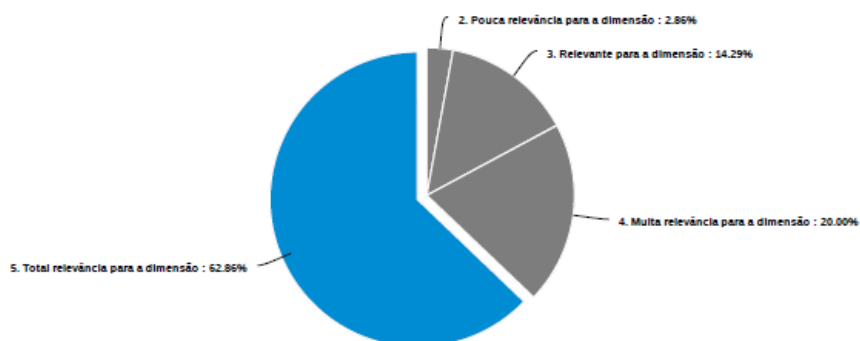
3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis? (art. 50 da Lei nº 13.709/2018; art. 15 do Decreto nº 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto nº 10.046/2019)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	1 2.86%	5 14.29%	7 20%	22 62.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	4,43					
Média		4,43					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	5	14.29%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	22	62.86%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

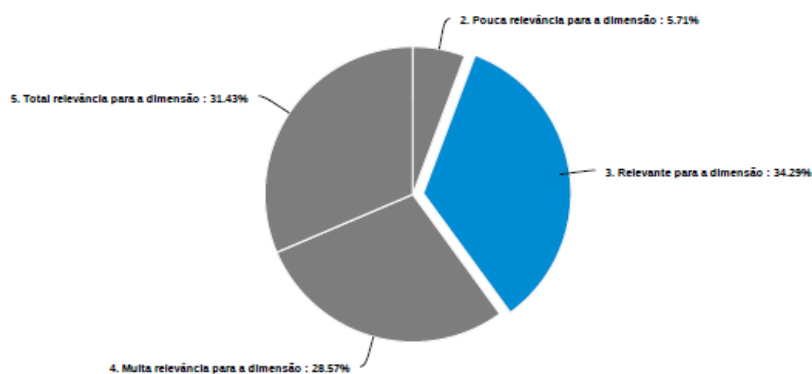
4. A organização realizou iniciativa sistemática para identificar outras legislações, normas ou regulamentos, além da LGPD, que contenham requisitos relacionados ao tratamento de dados e informações pessoais? (art. 7º, inciso II, art. 11, inciso II, alínea "a", art. 23, art. 26, inciso IV, art. 34, inciso I e art. 50 da Lei nº 13.709/2018; itens 5.2.1 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019 e item 5.31 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	2 5,71%	12 34,29%	10 28,57%	11 31,43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	3,86					
Média		3,86					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	12	34,29%					
4. Muita relevância para a dimensão	10	28,57%					
5. Total relevância para a dimensão	11	31,43%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

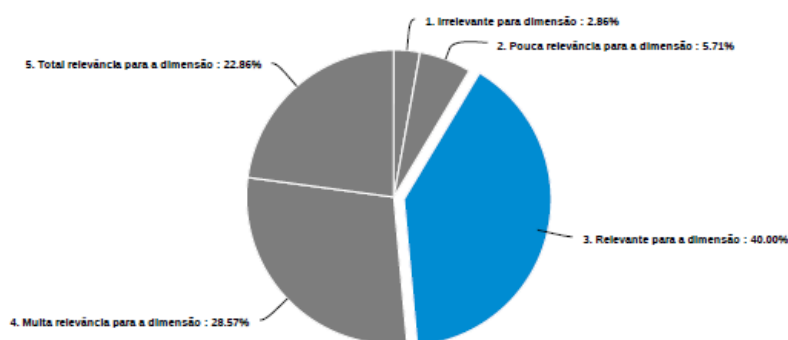
5. A organização realizou a análise do Legitimate Interests Assessment (LIA), considerando os quatro indicadores essenciais (finalidade, necessidade, balanceamento e salvaguardas), determinando assim as bases legais estratégicas que fundamentam o legítimo interesse no tratamento de dados pessoais na instituição? (art. 6º, inciso I, art. 7º, art. 10, art. 15, art. 16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018; itens 7.2, 7.3, 7.4.1 e 8.2 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, arts. 4º-12 e art. 18 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 2.86%	2 5.71%	14 40%	10 28.57%	8 22.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	3.63					
Média		3.63					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	14	40%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	8	22.86%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

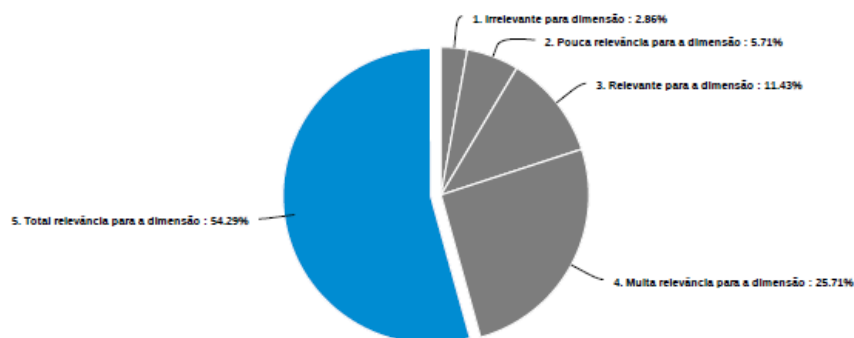
6. A instituição possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei nº 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, art. 13 e art. 20 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 2.86%	2 5.71%	4 11.43%	9 25.71%	19 54.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	4.23					
Média		4.23					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	19	54.29%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

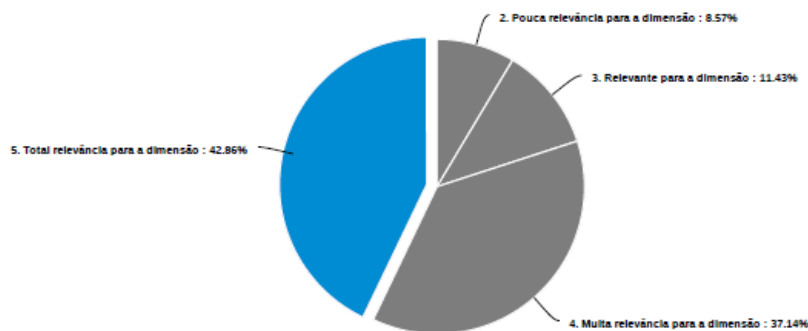
7. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	3 8.57%	4 11.43%	13 37.14%	15 42.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	13	37.14%					
5. Total relevância para a dimensão	15	42.86%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

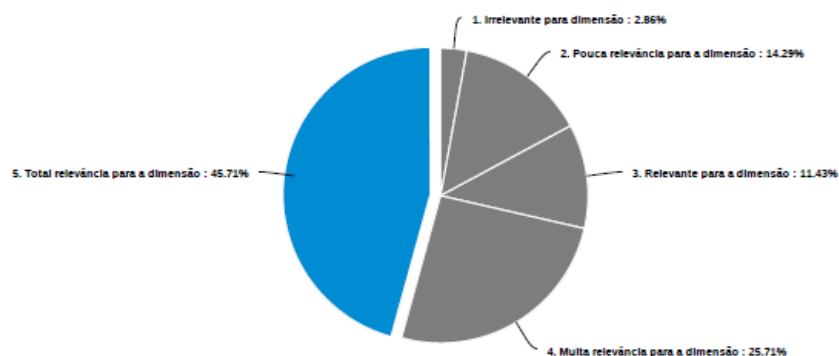
8. A organização faz gestão de ativos dos dados pessoais, mapeando os fluxos (Personal Data Flow Map) e o inventário de dados pessoais? (art. 50 da Lei nº 13.709/2018; itens 6.5.1, 6.5.3, 7.2.8 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.9, 5.10, 5.11 e 8.1.1 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 2.86%	5 14.29%	4 11.43%	9 25.71%	16 45.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	3.97					
Média		3.97					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	5	14.29%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	16	45.71%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

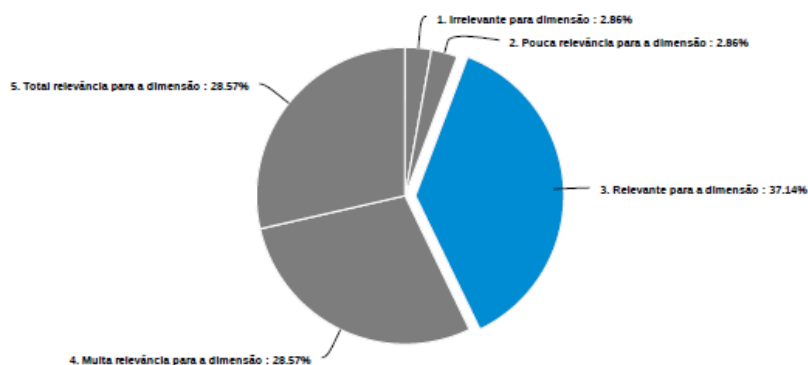
9. A organização revisa e atualiza regularmente suas políticas e procedimentos institucionalizados sobre o tratamento e proteção de dados e informações pessoais? (art. 23, inciso I, art. 32, art. 50 e art. 51 da Lei nº 13.709/2018; itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 1º e art. 19 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 2.86%	1 2.86%	13 37.14%	10 28.57%	10 28.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	3.77					
Média		3.77					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	13	37.14%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	10	28.57%					
Total	35	n = 35					

Dimensão 1: Governança de Dados e Boas Práticas

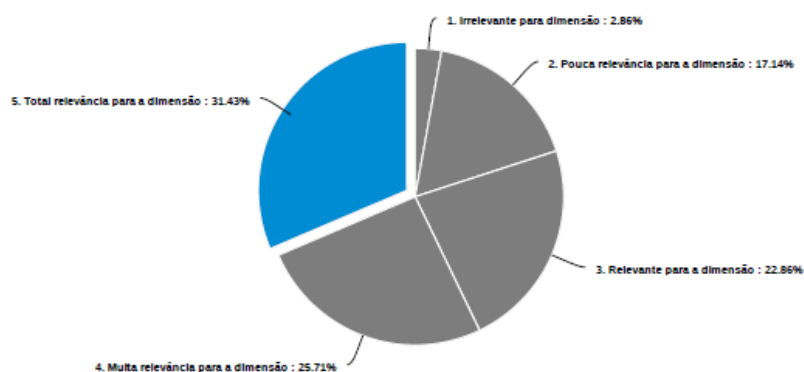
10. A organização faz conformidade digital (compliance digital), monitoramento de indicadores específicos ou auditorias específicas, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50, Inciso I, alínea "h" da Lei nº 13.709/2018; itens 5.7, 6.9.4, 6.9.7 e 6.15 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.22, 5.35, 5.36, 6.7, 8.15, 8.16 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 2.86%	6 17.14%	8 22.86%	9 25.71%	11 31.43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	35	3.66					
Média		3.66					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	11	31.43%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

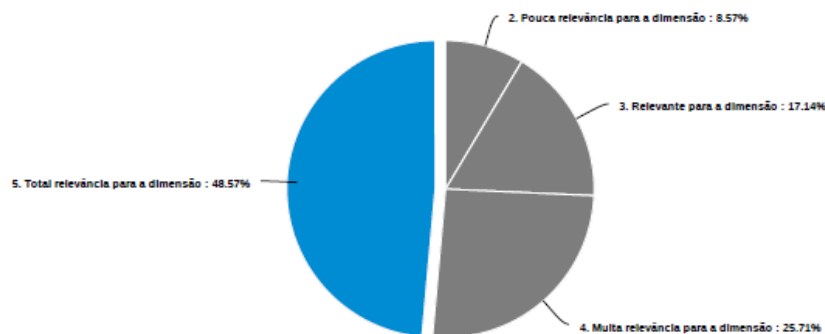
1. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação? (art. 10, § 2º, da Lei nº 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	3 8.57%	6 17.14%	9 25.71%	17 48.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	17	48.57%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

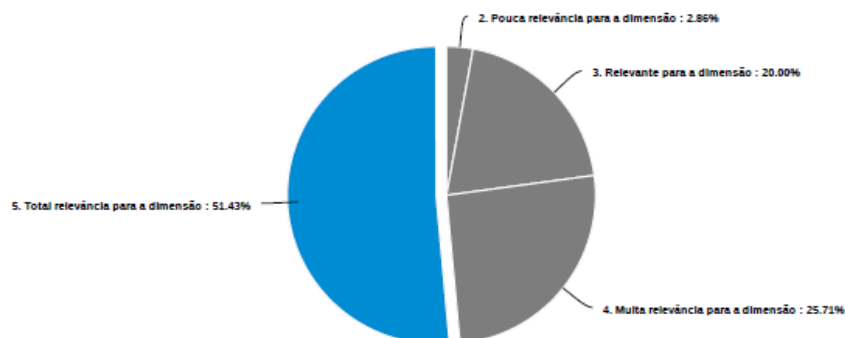
2. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	1 2.86%	7 20%	9 25.71%	18 51.43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4.26					
Média		4.26					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	18	51.43%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

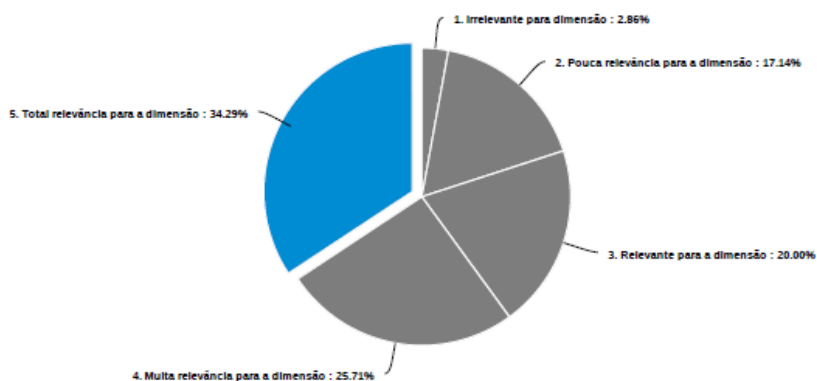
3. A organização identificou se existe tratamento de dados que envolvam atividades de "controlador conjunto", formalizando os papéis e responsabilidades de cada um? (art. 5º, inciso VI, art. 7º, incisos II e X, § 5, art. 9º, art. 10, art. 11, inciso II, art. 14, art. 37, art. 41, art. 42, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.2.2 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019 e art. 2º, parágrafo único, art. 3º, inciso V, art. 9º, art. 14 e art. 16 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	1 2.86%	6 17.14%	7 20%	9 25.71%	12 34.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	3.71					
Média		3.71					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	12	34.29%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

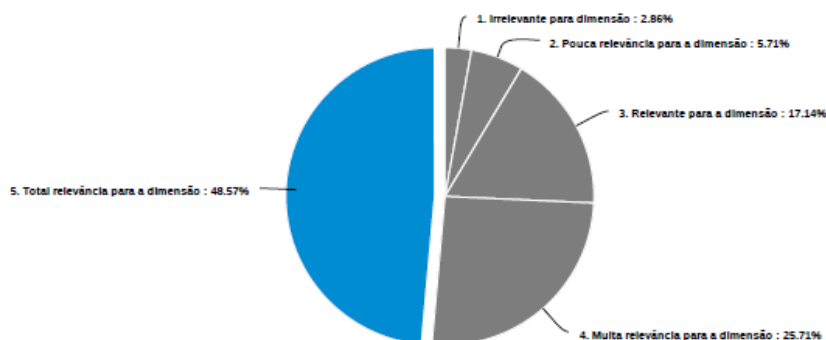
4. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	1 2.86%	2 5.71%	6 17.14%	9 25.71%	17 48.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4.11					
Média		4.11					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	17	48.57%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

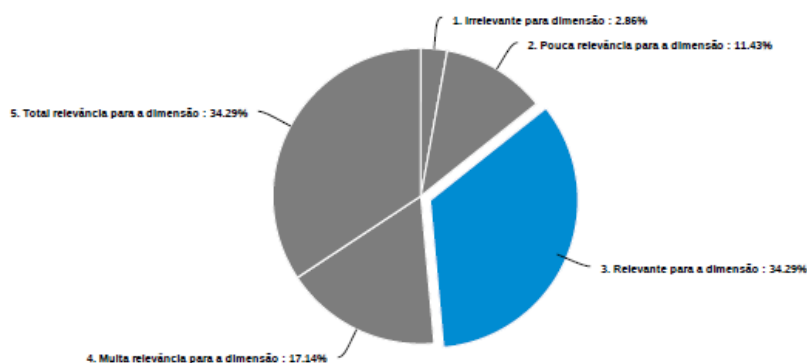
5. A organização gerencia os potenciais impactos por meio da Análise ou Avaliação de Impacto de Privacidade ou PIA (Privacy Impact Assessment)? (art. 2º, inciso I, art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso I, § 3º, inciso III, art. 32, art. 38 e art. 50, § 2º, inciso I, alíneas "a" e "d" da Lei nº 13.709/2018; itens 6.2.1.1, 6.3.1.1, 6.11.2.1, 7.2.5 e 7.2.8 da ABNT NBR ISO/IEC 27701:2019; itens 5.22 e 5.35 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 29134:2023 e art. 20 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	1 2.86%	4 11.43%	12 34.29%	6 17.14%	12 34.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	3.69					
Média		3.69					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	4	11.43%					
3. Relevante para a dimensão	12	34.29%					
4. Muita relevância para a dimensão	6	17.14%					
5. Total relevância para a dimensão	12	34.29%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

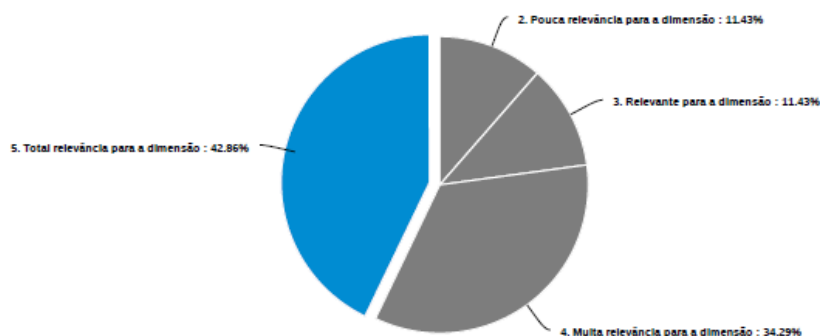
6. A organização ajustou os contratos e convênios, estabelecendo as diretrizes determinadas pelas legislações e normas, relacionadas ao tratamento e proteção dos dados pessoais? (art. 7º, incisos III e V, art. 11, inciso I, alínea "d", art. 19, inciso II, § 3º, art. 26, incisos IV e V, art. 33, art. 35 e art. 50 da Lei nº 13.709/2018; itens 6.15.1, 7.2.6, 7.2.7, 8.2.1, 8.3.1, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.20, 5.31, 6.2 e 6.5 da ABNT NBR ISO/IEC 27002:2022 e art. 16 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	4 11.43%	4 11.43%	12 34.29%	15 42.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4.09					
Média		4.09					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	4	11.43%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	12	34.29%					
5. Total relevância para a dimensão	15	42.86%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

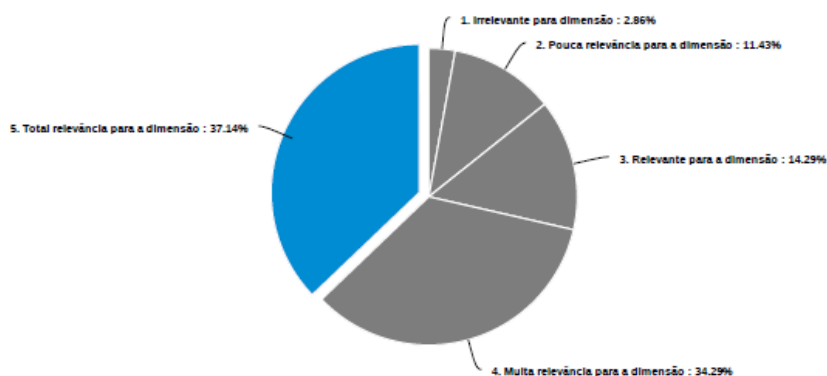
7. O compartilhamento e transferência internacional de dados e informações pessoais com terceiros, estão seguindo os critérios estabelecidos nas legislações? (art. 5º, incisos XV e XVI, art. 6º, art. 7º, inciso III e X (§5º), art. 9º, inciso V, art. 11, inciso II, alínea "b" e "g" (§3º e §4º), art. 16, inciso III, art. 18, inciso VII e inciso IX (§6º), arts. 25-27, art. 30, Capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II, art. 13, inciso V, art. 22 e art. 23 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	1 2.86%	4 11.43%	5 14.29%	12 34.29%	13 37.14%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	3.91					
Média		3.91					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	4	11.43%					
3. Relevante para a dimensão	5	14.29%					
4. Muita relevância para a dimensão	12	34.29%					
5. Total relevância para a dimensão	13	37.14%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

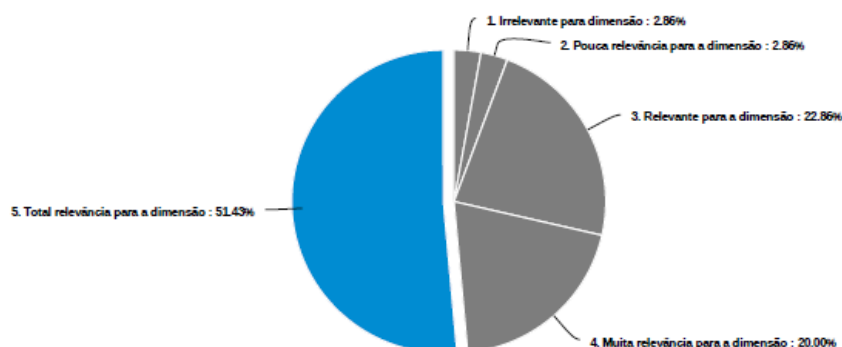
8. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais? (art. 2º, inciso IX, da Lei nº 7.232/1984; art. 4º da Lei nº 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei nº 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	1 2.86%	1 2.86%	8 22.86%	7 20%	18 51.43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	18	51.43%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

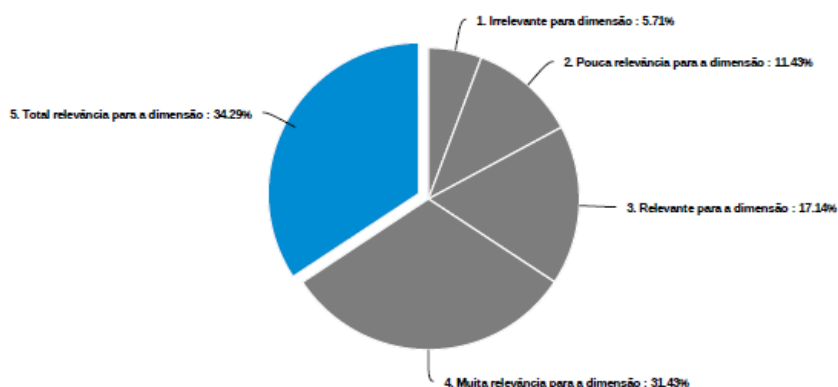
9. A organização possui gestão de consentimento dos titulares de dados pessoais, estabelecendo procedimentos para gerenciar e documentar as revogações desse consentimento? (art. 5º, inciso XII, art. 7º, incisos I e X, art. 8º, art. 9º, inciso VII, art. 11, inciso II, art. 14, art. 15, inciso III, art. 18, incisos VI, VIII e IX e art. 19, inciso II, § 3º, art. 27, inciso I e art. 33, inciso VIII, e art. 50 da Lei nº 13.709/2018; art. 3º, inciso XIII, do Decreto nº 9.637/2018; itens 7.2.2, 7.2.3, 7.2.4, 7.3 e 8.2.3 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, inciso VII e art. 8º da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	2 5,71%	4 11,43%	6 17,14%	11 31,43%	12 34,29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	3,77					
Média		3,77					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	2	5,71%					
2. Pouca relevância para a dimensão	4	11,43%					
3. Relevante para a dimensão	6	17,14%					
4. Muita relevância para a dimensão	11	31,43%					
5. Total relevância para a dimensão	12	34,29%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

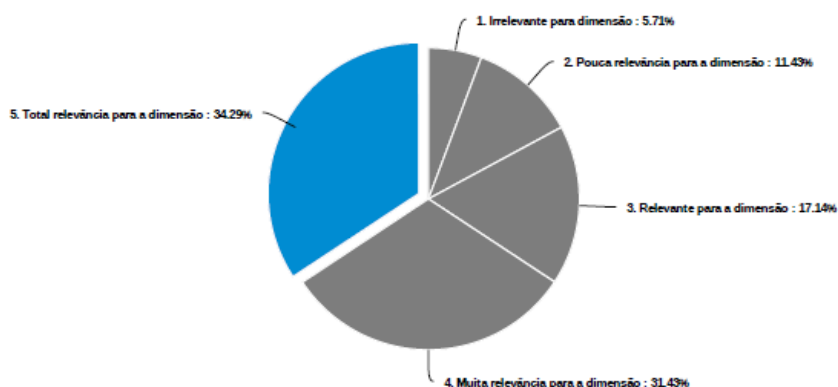
9. A organização possui gestão de consentimento dos titulares de dados pessoais, estabelecendo procedimentos para gerenciar e documentar as revogações desse consentimento? (art. 5º, inciso XII, art. 7º, incisos I e X, art. 8º, art. 9º, inciso VII, art. 11, inciso II, art. 14, art. 15, inciso III, art. 18, incisos VI, VIII e IX e art. 19, inciso II, § 3º, art. 27, inciso I e art. 33, inciso VIII, e art. 50 da Lei nº 13.709/2018; art. 3º, inciso XIII, do Decreto nº 9.637/2018; itens 7.2.2, 7.2.3, 7.2.4, 7.3 e 8.2.3 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, inciso VII e art. 8º da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	2 5,71%	4 11,43%	6 17,14%	11 31,43%	12 34,29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	3,77					
Média		3,77					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	2	5,71%					
2. Pouca relevância para a dimensão	4	11,43%					
3. Relevante para a dimensão	6	17,14%					
4. Muita relevância para a dimensão	11	31,43%					
5. Total relevância para a dimensão	12	34,29%					
Total	35	n = 35					

Dimensão 2: Políticas e Processos de Tratamento de Dados

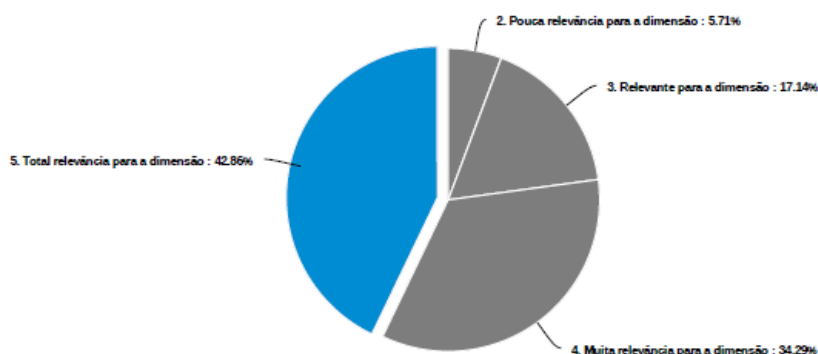
10. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei nº 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	2 5.71%	6 17.14%	12 34.29%	15 42.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	35	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	12	34.29%					
5. Total relevância para a dimensão	15	42.86%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

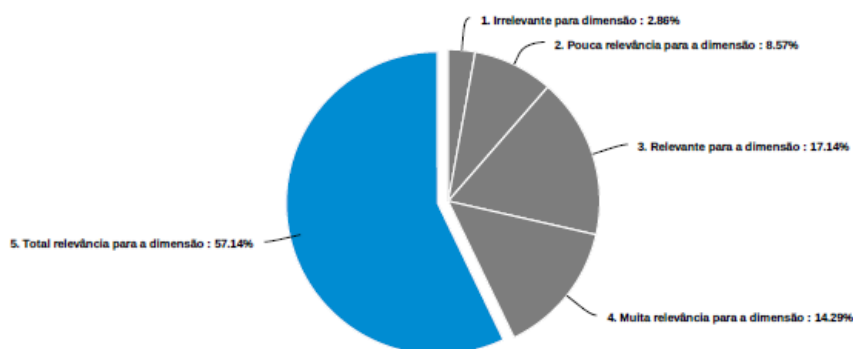
1. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei nº 7.232/1984; art. 50 da Lei nº 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto nº 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 2.86%	3 8.57%	6 17.14%	5 14.29%	20 57.14%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	5	14.29%					
5. Total relevância para a dimensão	20	57.14%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

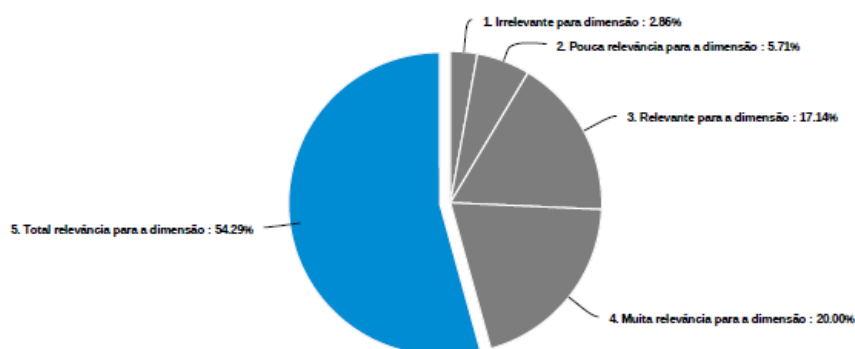
2. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei nº 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 2.86%	2 5.71%	6 17.14%	7 20%	19 54.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	4.17					
	Média	4.17					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	19	54.29%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

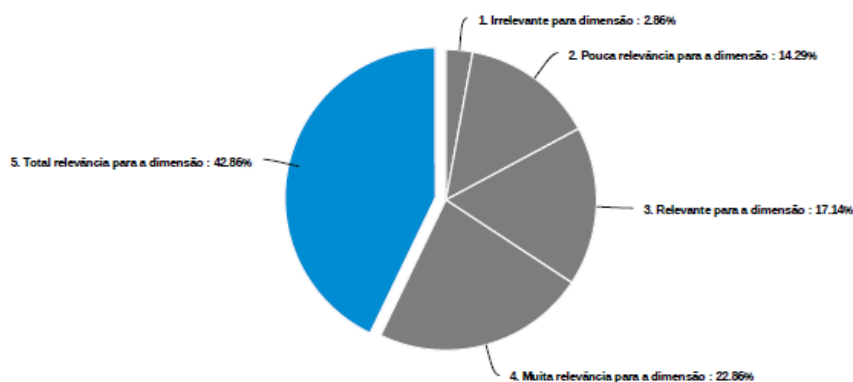
3. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais, recebem treinamentos e capacitações específicas sobre o tema? (art. 50 da Lei nº 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 2.86%	5 14.29%	6 17.14%	8 22.86%	15 42.86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3.89					
Média		3.89					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	1	2.86%					
2. Pouca relevância para a dimensão	5	14.29%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	15	42.86%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

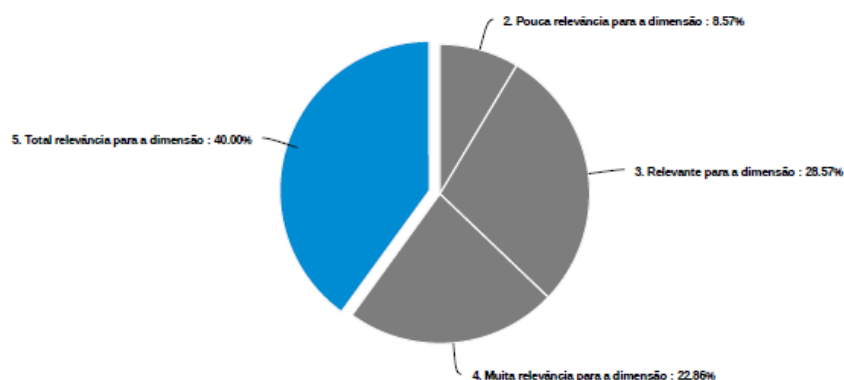
4. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais? (arts. 42-45, art. 50 e arts. 52-54 da Lei nº 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	0 0%	3 8.57%	10 28.57%	8 22.86%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3.94					
Média		3.94					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	10	28.57%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

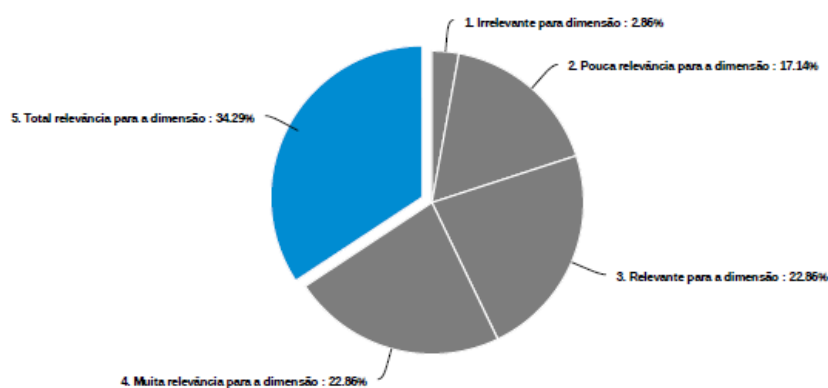
5. A organização capacita e conscientiza quanto às possíveis sanções administrativas aplicadas pela autoridade nacional? (art. 153, art. 305; art. 313A, art. 313B e art. 325 do Decreto-Lei nº 2.848/1940; art. 50, arts. 52-54, art. 55-J, inciso IV, e art. 55-K, da Lei nº 13.709/2018; itens 6.4.2.3 e 6.15.1.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 6.4 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 2.86%	6 17.14%	8 22.86%	8 22.86%	12 34.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3.69					
Média		3.69					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	12	34.29%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

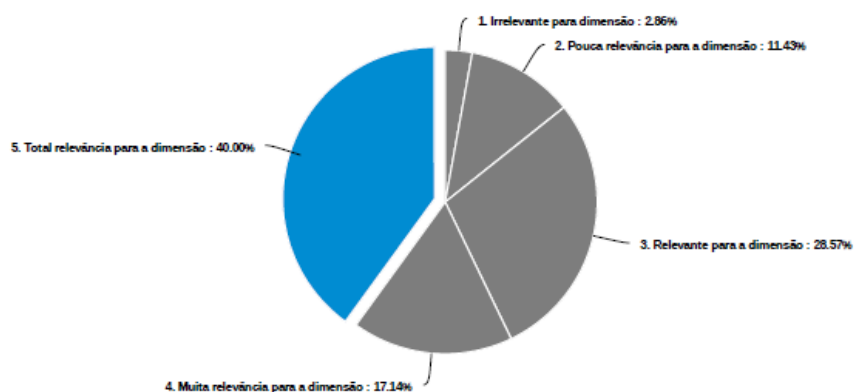
6. A organização promove capacitação quanto aos procedimentos adequados para a gestão de incidentes, determinando a melhor forma de planejar, gerenciar e comunicar os incidentes de segurança da informação? (art. 48 e art. 50 da Lei nº 13.709/2018; art. 3º, incisos VII e IX, do Decreto nº 9.637/2018; item 6.13 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.25, 5.26, 5.27 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27035:2023; art. 15, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 2.86%	4 11.43%	10 28.57%	6 17.14%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3.8					
Média		3.8					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	4	11.43%					
3. Relevante para a dimensão	10	28.57%					
4. Muita relevância para a dimensão	6	17.14%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

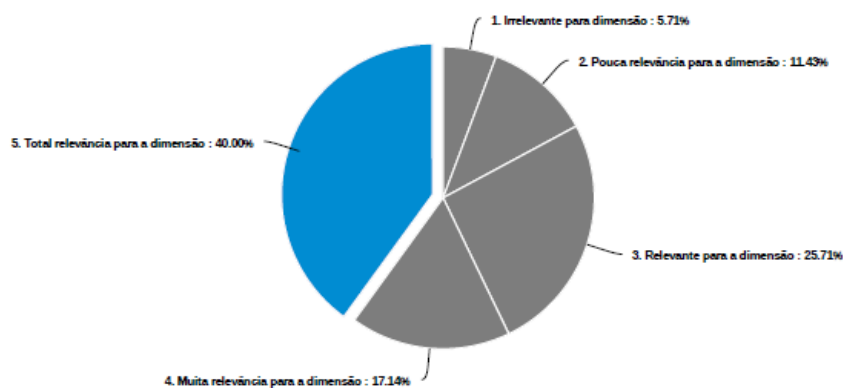
7. A organização possui treinamentos específicos para o tratamento de dados e informações pessoais sensíveis, bem como de crianças e adolescentes? (art. 5º, inciso II, art. 11, art. 14, art. 38 e art. 50, § 2º, inciso I, alíneas "a" e "c" da Lei nº 13.709/2018; itens 6.5.2.2, 7.2.2 e 7.2.3 da ABNT NBR ISO/IEC 27701:2019; itens 6.3, 6.6, 8.3, 8.10, 8.11 e 8.12 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso VI, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	2 5,71%	4 11,43%	9 25,71%	6 17,14%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3,74					
Média		3,74					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	2	5,71%					
2. Pouca relevância para a dimensão	4	11,43%					
3. Relevante para a dimensão	9	25,71%					
4. Muita relevância para a dimensão	6	17,14%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

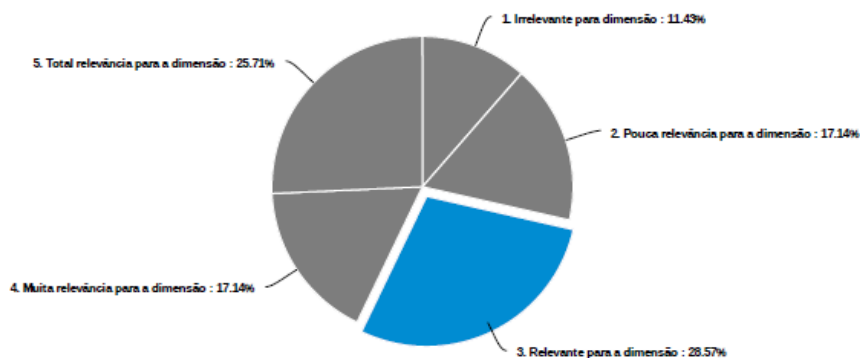
8. A organização realiza avaliações periódicas ou monitoramento dos resultados (feedback) dos treinamentos e capacitações, relacionados ao tratamento e proteção de dados e informações pessoais na instituição, aferindo a eficácia e o nível de compreensão? (art. 50 da Lei nº 13.709/2018 e itens 5.35, 6.3 e 8.16 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	4 11.43%	6 17.14%	10 28.57%	6 17.14%	9 25.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3.29					
Média		3.29					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	4	11.43%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	10	28.57%					
4. Muita relevância para a dimensão	6	17.14%					
5. Total relevância para a dimensão	9	25.71%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

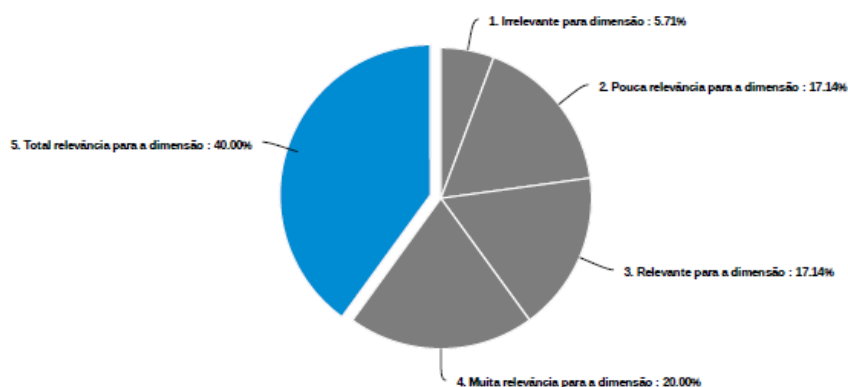
9. A organização promove regularmente, eventos, treinamentos, campanhas e/ou capacitações, relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 50 da Lei nº 13.709/2018; itens 6.4.2.2 e 6.15 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	2 5.71%	6 17.14%	6 17.14%	7 20%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3,71					
Média		3,71					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	2	5.71%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Dimensão 3: Treinamento e Conscientização

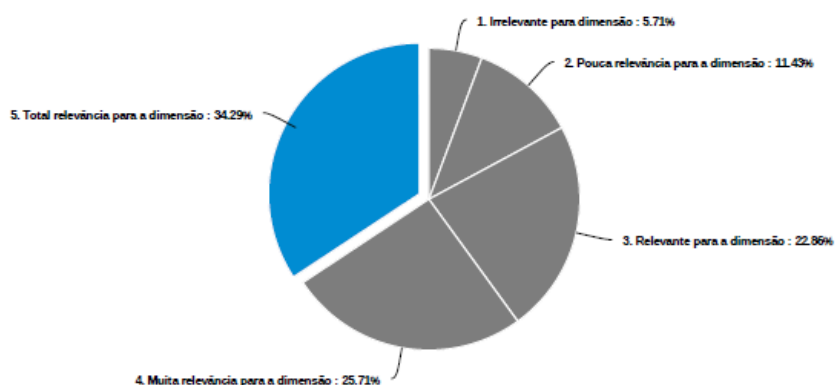
10. A organização, em seu planejamento orçamentário, disponibiliza recursos específicos para fomentar capacitações e treinamentos, direcionados ao tratamento e proteção de dados pessoais? (art. 50 da Lei nº 13.709/2018; item 5.5.1 da ABNT NBR ISO/IEC 27701:2019 e itens 6.3 e 8.6 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	2 5,71%	4 11,43%	8 22,86%	9 25,71%	12 34,29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	35	3,71					
Média		3,71					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	2	5,71%					
2. Pouca relevância para a dimensão	4	11,43%					
3. Relevante para a dimensão	8	22,86%					
4. Muita relevância para a dimensão	9	25,71%					
5. Total relevância para a dimensão	12	34,29%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

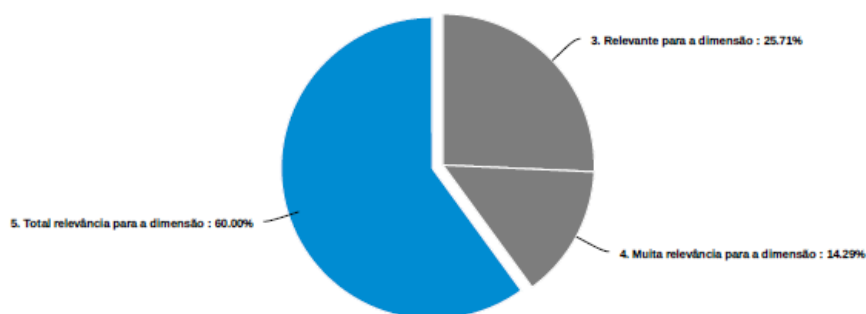
1. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar? (art. 4º, inciso V, da Lei 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei nº 13.709/2018; Decreto nº 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022 e art. 14 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	0 0%	9 25.71%	5 14.29%	21 60%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4.34					
Média		4.34					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	9	25.71%					
4. Muita relevância para a dimensão	5	14.29%					
5. Total relevância para a dimensão	21	60%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

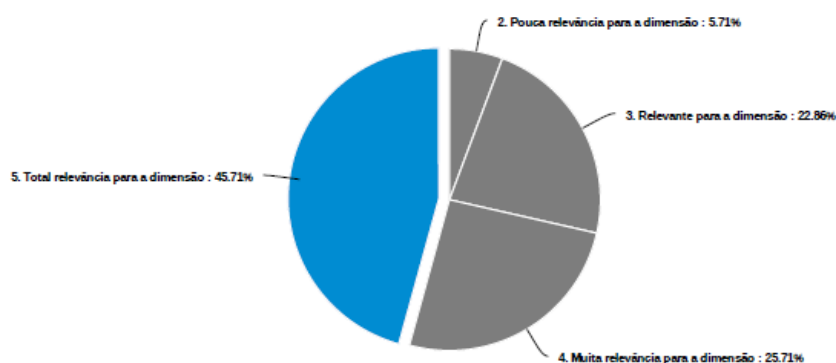
2. A organização estabeleceu procedimentos para registro, cancelamento e provisionamento de usuários nos sistemas que realizam tratamento de dados pessoais? (art. 6º, incisos VII e VIII, arts. 46-47 e art. 50 da Lei nº 13.709/2018; itens 6.6.2.1, 6.6.2.2 e 6.6.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.16 e 8.1 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	2 5,71%	8 22,86%	9 25,71%	16 45,71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,11					
Média		4,11					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	8	22,86%					
4. Muita relevância para a dimensão	9	25,71%					
5. Total relevância para a dimensão	16	45,71%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

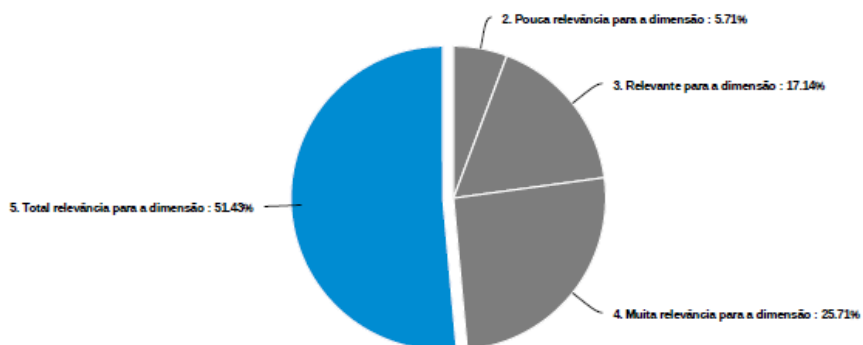
3. A organização usa criptografia para proteger os dados pessoais? (art. 11, inciso II, alínea "g", art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea "c", da Lei nº 13.709/2018; art. 2º, inciso III, do Decreto nº 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	2 5,71%	6 17,14%	9 25,71%	18 51,43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,23					
Média		4,23					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	6	17,14%					
4. Muita relevância para a dimensão	9	25,71%					
5. Total relevância para a dimensão	18	51,43%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

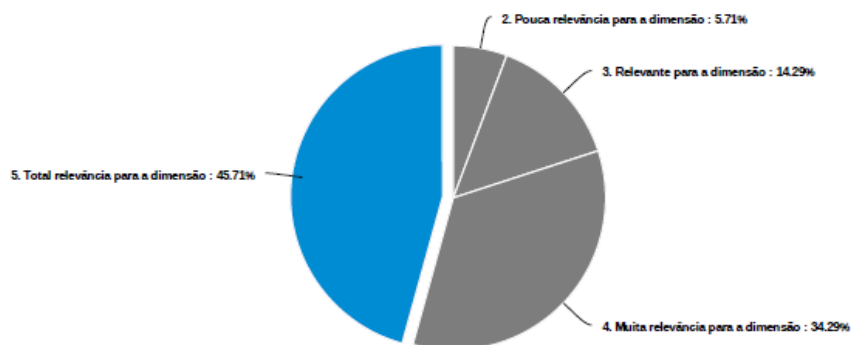
4. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei nº 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	2 5.71%	5 14.29%	12 34.29%	16 45.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4.2					
Média		4.2					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	5	14.29%					
4. Muita relevância para a dimensão	12	34.29%					
5. Total relevância para a dimensão	16	45.71%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

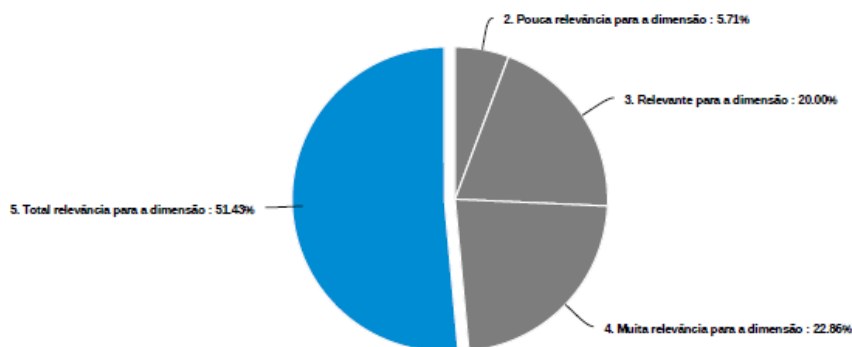
5. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei nº 13.709/2018; art. 2º, incisos II e III do Decreto nº 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	2 5,71%	7 20%	8 22,86%	18 51,43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,2					
Média		4,2					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	8	22,86%					
5. Total relevância para a dimensão	18	51,43%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

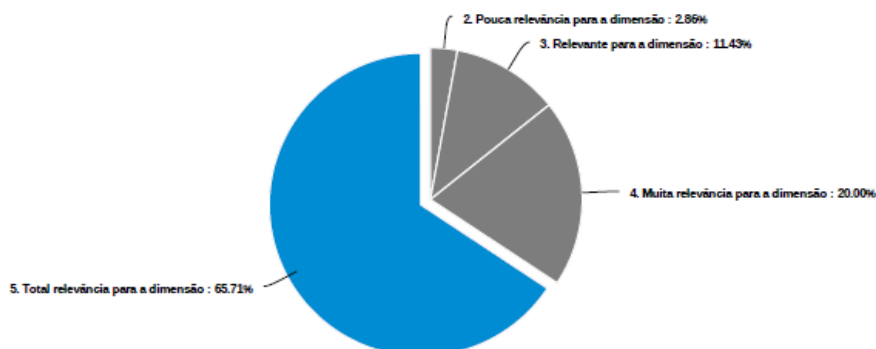
6. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, "g", art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei nº 13.709/2018; art. 2º, incisos III e IV, do Decreto nº 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	1 2.86%	4 11.43%	7 20%	23 65.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,49					
Média		4,49					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	23	65.71%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

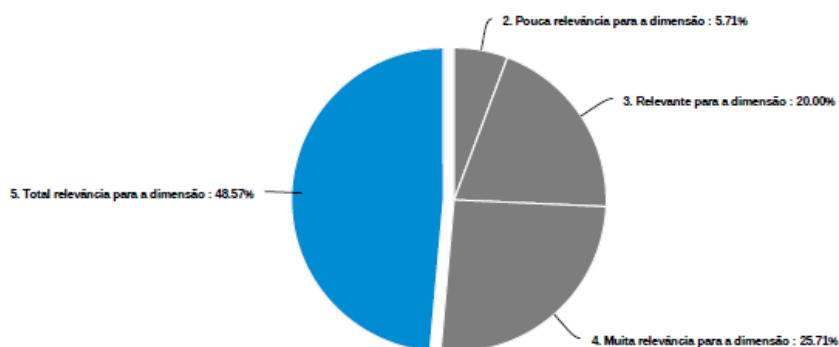
7. Existe gestão de incidentes de segurança da informação na instituição? (art. 6º, art. 31, art. 32, art. 48 e art. 50, inciso I, alínea "d" da Lei nº 13.709/2018; art. 3º, inciso IX, do Decreto nº 9.637/2018; itens 5.7 e 6.13 da ABNT NBR ISO/IEC 27701:2019 e itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	2 5,71%	7 20%	9 25,71%	17 48,57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,17					
Média		4,17					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	5,71%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	9	25,71%					
5. Total relevância para a dimensão	17	48,57%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

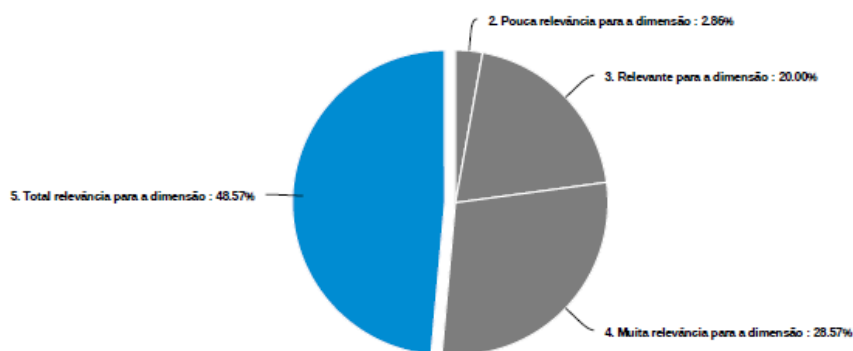
8. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea 'g', e art. 52, § 7º, da Lei nº 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto nº 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	1 2.86%	7 20%	10 28.57%	17 48.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4.23					
Média		4.23					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	17	48.57%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

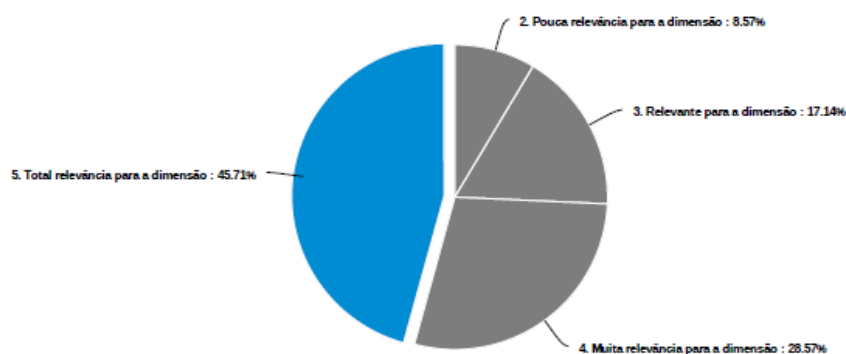
9. A organização implementou as abordagens Privacy by Design e Privacy by Default para garantir que os sistemas institucionais sejam projetados de forma a restringir a coleta e o tratamento dos dados pessoais, alinhando-se rigorosamente aos objetivos institucionais?(art. 11, inciso II, alínea "g", art. 20, art. 25, art. 46, § 2º, art. 49 e art. 50 da Lei nº 13.709/2018; itens 6.11, 7.4 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e itens 8.27, 8.28, 8.29 e 8.34 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	3 8.57%	6 17.14%	10 28.57%	16 45.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4,11					
Média		4,11					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	16	45.71%					
Total	35	n = 35					

Dimensão 4: Segurança da Informação e Tecnologia

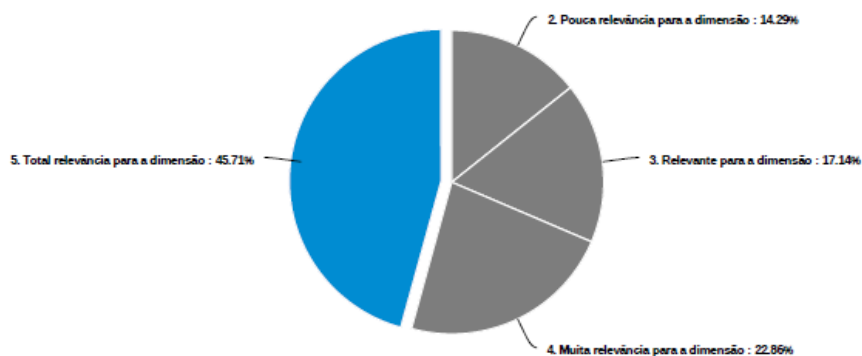
10. A organização aplica a avaliação de risco (risk assessment) para garantir confidencialidade, integridade e disponibilidade dos dados pessoais? (art. 6º, inciso V, art. 18, art. 25, art. 26, inciso V, art. 31, art. 32 e art. 50 da Lei nº 13.709/2018; art. 2º, inciso IV, e art. 3º, inciso VIII, do Decreto nº 9.637/2018; itens 5.6.2, 5.7.1 e 7.4.3 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12, 8.7 e 8.19 da ABNT NBR ISO/IEC 27002:2022 e art. 4º, inciso IX, art. 9º; art. 17, § 2º, e art. 25 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	5 14.29%	6 17.14%	8 22.86%	16 45.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	35	4					
Média		4					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	5	14.29%					
3. Relevante para a dimensão	6	17.14%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	16	45.71%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

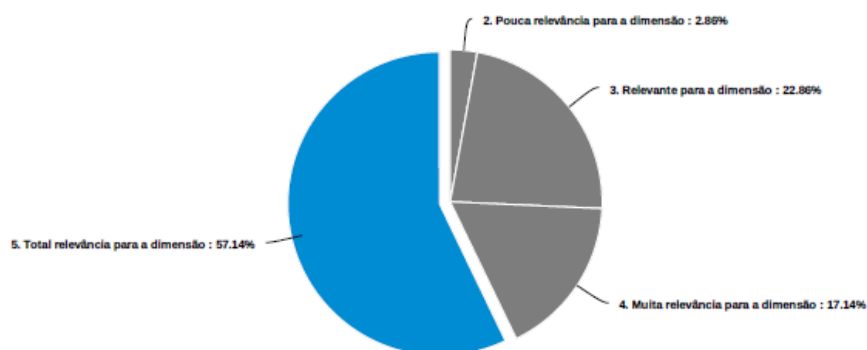
1. A organização atende ao princípio da transparência? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei nº 8.159/1991; Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea "e", da Lei nº 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	1 2.86%	8 22.86%	6 17.14%	20 57.14%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	4,29					
Média		4,29					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	1	2.86%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	6	17.14%					
5. Total relevância para a dimensão	20	57.14%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

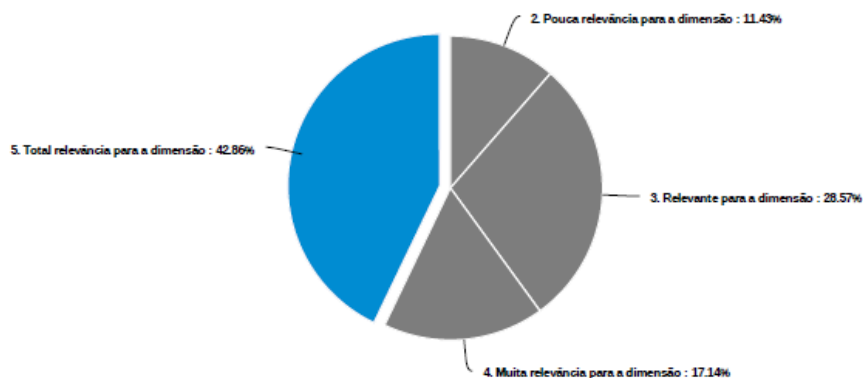
2. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas "a" e "d", da Lei nº 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	4 11,43%	10 28,57%	6 17,14%	15 42,86%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3,91					
Média		3,91					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	4	11,43%					
3. Relevante para a dimensão	10	28,57%					
4. Muita relevância para a dimensão	6	17,14%					
5. Total relevância para a dimensão	15	42,86%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

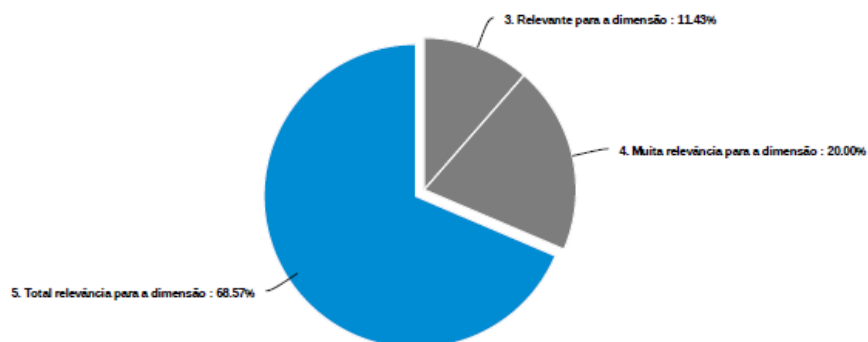
3. A designação do encarregado e suas informações de contato, foram publicizadas em algum meio de comunicação oficial?? (art. 5º, inciso VIII, art. 23, art. 41 da Lei nº 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	0 0%	4 11.43%	7 20%	24 68.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	4.57					
Média		4.57					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	4	11.43%					
4. Muita relevância para a dimensão	7	20%					
5. Total relevância para a dimensão	24	68.57%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

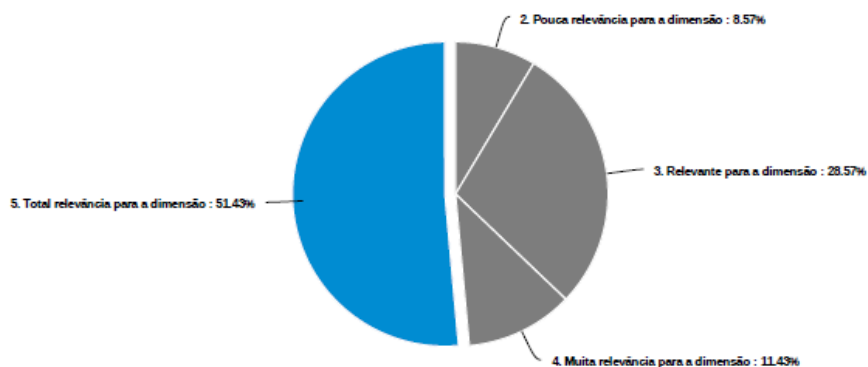
4. A Política de Privacidade da instituição está publicizada? (art. 2º, inciso VIII, da Lei 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei nº 13.709/2018; art. 3º, inciso XI, do Decreto nº 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	3 8.57%	10 28.57%	4 11.43%	18 51.43%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	4,06					
Média		4,06					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	8.57%					
3. Relevante para a dimensão	10	28.57%					
4. Muita relevância para a dimensão	4	11.43%					
5. Total relevância para a dimensão	18	51.43%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

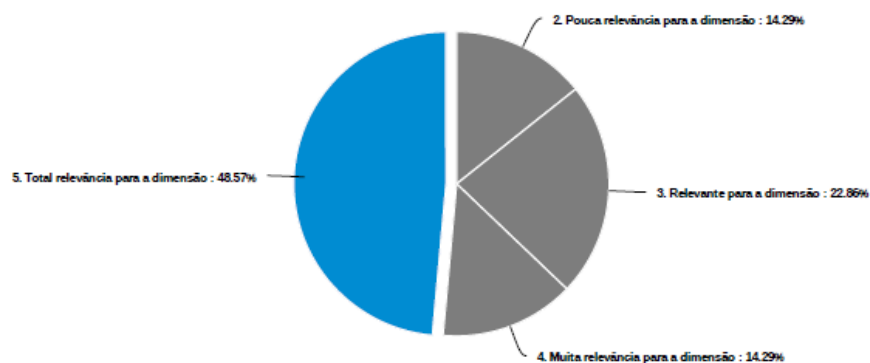
5. A organização estabeleceu procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes de segurança, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei nº 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	5 14.29%	8 22.86%	5 14.29%	17 48.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3.97					
Média		3.97					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	5	14.29%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	5	14.29%					
5. Total relevância para a dimensão	17	48.57%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

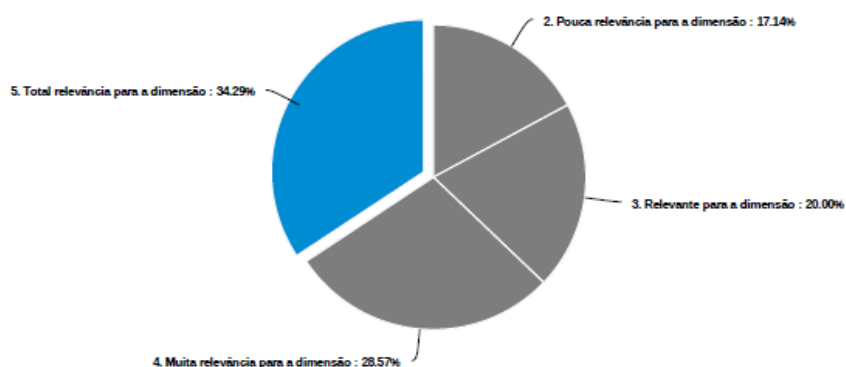
6. A organização implementou mecanismos para mitigar os riscos identificados no tratamento de dados pessoais por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) ou Data Protect Impact Assessment (DPIA)? (art. 4º, inciso IV, § 3º, art. 5º, inciso XVII, art. 10, inciso II, § 3º, art. 32, art. 38, art. 48 e art. 50 da Lei nº 13.709/2018; itens 6.1, 6.2, 7.2.5 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	6 17.14%	7 20%	10 28.57%	12 34.29%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3.8					
Média		3.8					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	12	34.29%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

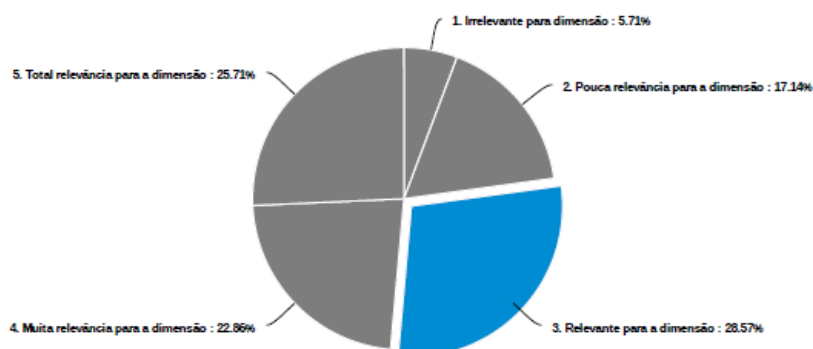
7. A organização divulga os incidentes decorrentes de perdas, destruição, falsificação, acesso não autorizado ou liberação não autorizada? (art. 6º, incisos VII e VIII, art. 31, art. 32, art. 46, art. 48, inciso II, § 3º, e art. 50 da Lei nº 13.709/2018; Itens 5.24, 5.26, 5.27, 5.28 e 5.33 da ABNT NBR ISO/IEC 27002:2022; art. 14, art. 15 e art. 20 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	2 5.71%	6 17.14%	10 28.57%	8 22.86%	9 25.71%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3,46					
Média		3,46					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	2	5.71%					
2. Pouca relevância para a dimensão	6	17.14%					
3. Relevante para a dimensão	10	28.57%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	9	25.71%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

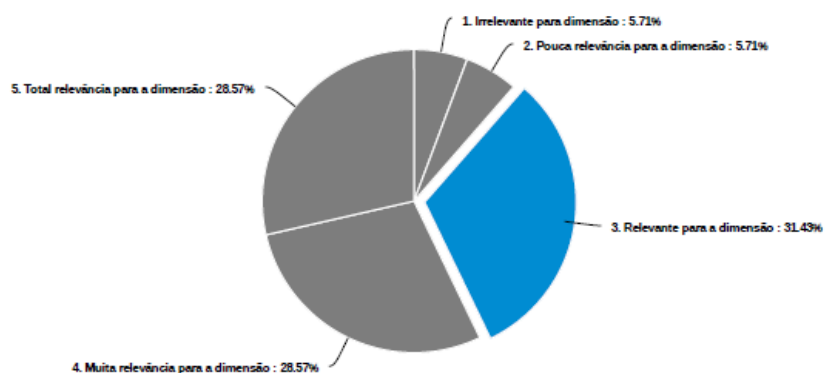
8. A organização promove e divulga mecanismos que incentivem relatos de incidentes e falhas de segurança da informação? (art. 6º, incisos VI e VII, art. 32, art. 46, art. 50 da Lei nº 13.709/2018; item 6.13 da da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.27, 5.28 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	2 5.71%	2 5.71%	11 31.43%	10 28.57%	10 28.57%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3.69					
Média		3.69					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	2	5.71%					
2. Pouca relevância para a dimensão	2	5.71%					
3. Relevante para a dimensão	11	31.43%					
4. Muita relevância para a dimensão	10	28.57%					
5. Total relevância para a dimensão	10	28.57%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

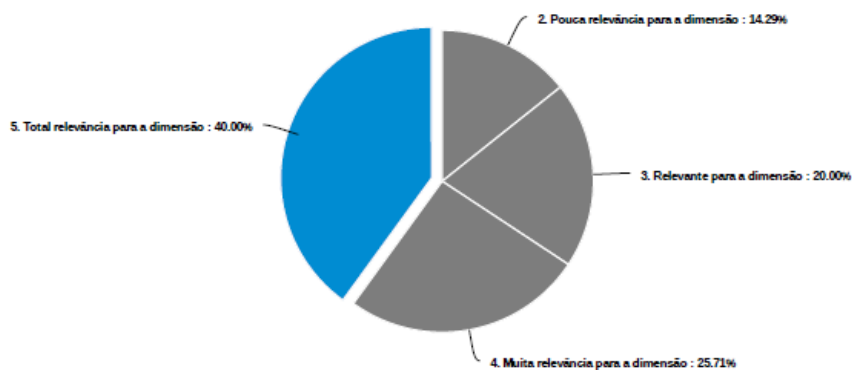
9. A organização possui programa, plano de comunicação ou documento similar que abarque as diretrizes das legislações e normas referentes ao tratamento e proteção de dados e informações pessoais? (art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.5.4, 8.4.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 6.6 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 24 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	5 14.29%	7 20%	9 25.71%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3.91					
Média		3.91					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	5	14.29%					
3. Relevante para a dimensão	7	20%					
4. Muita relevância para a dimensão	9	25.71%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Dimensão 5: Acesso à Informação e Transparência

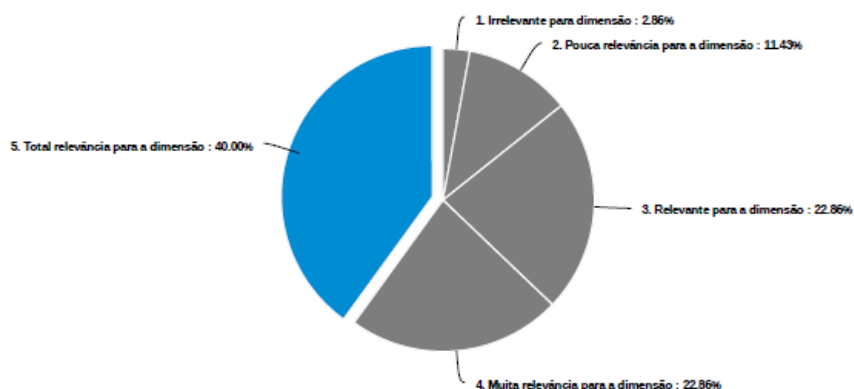
10. Os procedimentos formalizados relacionados ao tratamento e proteção dos dados e informações pessoais estão documentados e disponibilizados? (art. 32 e art. 50 da Lei nº 13.709/2018; itens 5.5.5, 6.9.1, 6.10 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.37 e 8.9 da ABNT NBR ISO/IEC 27002:2022 e art. 19 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	1 2.86%	4 11.43%	8 22.86%	8 22.86%	14 40%	35 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	35	3.86					
Média		3.86					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	2.86%					
2. Pouca relevância para a dimensão	4	11.43%					
3. Relevante para a dimensão	8	22.86%					
4. Muita relevância para a dimensão	8	22.86%					
5. Total relevância para a dimensão	14	40%					
Total	35	n = 35					

Você teria alguma sugestão de questão para acrescentar ao questionário? Se sim, escreva abaixo a questão e em qual dimensão ela se enquadraria. As dimensões possíveis são: Governança de Dados e Boas Práticas; Políticas e Processos de Tratamento de Dados; Treinamento e Conscientização; Segurança da Informação e Tecnologia; e Acesso à Informação e Transparência.

05/16/2024	132689831	Sim, tenho duas sugestões. Em "Políticas e Processos de Tratamento de Dados", adicionaria "a organização promove processo de atualização periódica dos cadastros pessoais haja vista a manutenção da qualidade dos dados (LGPD, art. 6º, V)?" Em Acesso à Informação e Transparência, adicionaria "a organização implementa canais de atendimento aos titulares dos dados pessoais?".
05/08/2024	131959790	Não ficou claro se o nível de relevância a ser atribuído a pergunta deveria observar critérios abstratos ou concretos, ou seja, não compreendi se a relevância da pergunta seria tão somente em relação à pergunta em si mesma, ou se em relação à aplicação ou não na realidade de minha instituição. De toda sorte, respondi observando critérios abstratos, ou seja, considerei a relevância da pergunta em relação ao tema geral "Proteção de Dados Pessoais", de forma dissociada da minha realidade concreta.
05/07/2024	131894205	A instituição segue as recomendações e está alinhada às iniciativas (Programa de Privacidade e Segurança da Informação (PPSI), Infraestrutura Nacional de Dados, etc) do governo federal no âmbito da Secretaria de Governo Digital do Ministério da Gestão e Inovação?
04/24/2024	130603011	NADA A DECLARAR
04/19/2024	130218111	Segurança da Informação: os treinamentos existentes atualmente são padrão e não específicos para realidade de cada instituição,
04/19/2024	130200243	Na dimensão Governança de Dados e Boas Práticas, sugiro que seja acrescentado algum tipo de indicador de maturidade em privacidade e segurança da informação
04/18/2024	130089630	Políticas e Processos de Tratamento de Dados: A instituição já implementou sua política de adequação à Lei Geral de Proteção de Dados?
04/18/2024	130066372	É imprescindível avaliar a aplicação do princípio da segregação das funções no que se refere ao usual acúmulo da atribuição de Encarregado com atribuições de acesso à informação em instituições públicas, bem como avaliar as suas implicações. Vislumbram-se eventuais conflitos na gestão dos princípios da privacidade e do acesso à informação caso sejam executados por um só indivíduo.

APÊNDICE H – Relatório de *feedback* da primeira rodada do método *delphi*

Relatório do Método Delphi - 1ª Rodada

1. Introdução

1.1 Objetivo do Relatório

Este relatório apresenta os resultados e o *feedback* da 1ª rodada do método *Delphi* aplicado ao estudo de doutorado intitulado "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: Proposta de Modelo de Maturidade sob a Perspectiva dos Marcos Legais Brasileiros".

1.2 Contexto

Este trabalho está sendo desenvolvido no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. O objetivo imediato do questionário é identificar e selecionar as questões mais pertinentes para compor o instrumento de medição do modelo de maturidade para tratamento de dados pessoais. A fase atual envolve a seleção e validação das questões do instrumento, conduzida pelo método *Delphi*, para obter a opinião dos especialistas sobre a relevância das questões propostas no instrumento.

2. Metodologia

2.1 Descrição do Método *Delphi*

O método *Delphi* representa um processo consultivo estruturado amplamente utilizado para alcançar consenso entre um grupo de especialistas. Este estudo adota um processo iterativo composto por múltiplas rodadas, durante as quais os especialistas oferecem suas opiniões e recebem *feedback* das respostas coletivas das rodadas anteriores. O objetivo aqui é utilizar o método *Delphi* para validar e selecionar as questões que integrarão o instrumento de medição do modelo de maturidade proposto para o tratamento de dados pessoais.

2.2 Fases do *Delphi* nesta pesquisa

Para a primeira rodada, o instrumento foi estruturado em cinco dimensões principais: Governança de Dados e Boas Práticas, Políticas e Processos de Tratamento de Dados, Treinamento e Conscientização, Segurança da Informação e Tecnologia, e Acesso à Informação e Transparência. Cada dimensão foi composta por 10 questões cuidadosamente selecionadas, alinhadas com legislações e normativas vigentes sobre o tratamento e proteção de dados pessoais no país.

A avaliação inicial consistiu em solicitar aos especialistas que ponderasse sobre a relevância de cada questão dentro de sua respectiva dimensão. As cinco questões de cada dimensão que obtiveram as avaliações médias mais elevadas foram selecionadas para avançar para a próxima fase do estudo. Em situações de empate, todas as questões empatadas foram igualmente consideradas para a rodada subsequente.

Além disso, foram aceitas sugestões adicionais dos especialistas, as quais foram criteriosamente analisadas quanto à sua pertinência e aderência aos objetivos da pesquisa. Tais sugestões consideradas serão incluídas na próxima etapa do estudo.

3. Participantes

3.1 Perfil dos Especialistas

Os participantes são os encarregados de proteção de dados das universidades federais do Brasil, profissionais com *know-how* no tema e nas práticas institucionais relacionadas ao tratamento de dados e informações pessoais dessas instituições.

3.2 Número de Participantes

Nesta primeira rodada 35 profissionais participaram.

4. Resultados da 1ª Rodada

4.1 Dados Coletados

Os especialistas avaliaram a relevância de 50 questões, divididas em 05 dimensões propostas para compor o instrumento de medição de maturidade. As respostas foram coletadas em uma escala de 1 a 5, onde 1 indica "Pouco Relevante" e 5 indica "Muito Relevante". Segue os dados coletados em cada dimensão.

Questões da Dimensão 1 (Governança de Dados e Boas Práticas)

Dimensão/Questão	Média	Moda	Mediana	Dp
D1Q2	4,6	5 (21)	4	0,72
D1Q3	4,43	5 (22)	4	0,91
D1Q1	4,34	5 (26)	4	1,14
D1Q6	4,23	5 (19)	4	1,08
D1Q7	4,14	5 (15)	4	0,97
D1Q8	3,97	5 (16)	4	0,88
D1Q4	3,86	3 (12)	3	0,95
D1Q9	3,77	3 (13)	3	0,78
D1Q10	3,66	5 (11)	3	1,04
D1Q5	3,63	3 (14)	3	1,17

Questões da Dimensão 2 (Políticas e Processos de Tratamento de Dados)

Dimensão/Questão	Média	Moda	Mediana	Dp
D2Q2	4,26	5 (18)	4	0,91
D2Q1	4,14	5 (17)	4	0,94

D2Q8	4,14	5 (18)	4	1,08
D2Q10	4,14	5 (15)	4	0,87
D2Q4	4,11	5 (17)	4	1,1
D2Q6	4,09	5 (15)	4	0,88
D2Q7	3,91	5 (13)	4	1,05
D2Q9	3,77	5 (12)	4	1,02
D2Q3	3,71	5 (12)	3	1,05
D2Q5	3,69	3 (12) e 5 (12)	3	1,07

Questões da Dimensão 3 (Treinamento e Conscientização)

Dimensão/Questão	Média	Moda	Mediana	Dp
D3Q2	4,17	5 (19)	5	1,06
D3Q1	4,14	5 (20)	5	1,07
D3Q4	3,94	5 (14)	4	1,17
D3Q3	3,89	5 (15)	4	1
D3Q6	3,8	5 (14)	4	1,06
D3Q7	3,74	5 (14)	4	1,19
D3Q9	3,71	5 (14)	4	1,09
D3Q10	3,71	5 (12)	4	1,03
D3Q5	3,69	5 (12)	4	1,15
D3Q8	3,29	3 (10)	3	0,95

Questões da Dimensão 4 (Segurança da Informação e Tecnologia)

Dimensão/Questão	Média	Moda	Mediana	Dp
D4Q6	4,49	5 (23)	5	0,88
D4Q1	4,34	5 (21)	5	0,81
D4Q3	4,23	5 (18)	5	0,95
D4Q8	4,23	5 (17)	4	0,9
D4Q4	4,2	5 (16)	4	0,84
D4Q5	4,2	5 (18)	5	0,97
D4Q7	4,17	5 (17)	4	0,92
D4Q2	4,11	5 (16)	4	0,98
D4Q9	4,11	5 (16)	4	0,9
D4Q10	4	5 (16)	4	0,96

Questões da Dimensão 5 (Acesso à Informação e Transparência)

Dimensão/Questão	Média	Moda	Mediana	Dp
D5Q3	4,57	5 (24)	5	0,69
D5Q1	4,29	5 (20)	4	0,95
D5Q4	4,06	5 (18)	4	0,96
D5Q5	3,97	5 (17)	4	1,17
D5Q2	3,91	5 (15)	4	0,98
D5Q9	3,91	5 (14)	4	1,19
D5Q10	3,86	5 (14)	4	1,17
D5Q6	3,8	5 (12)	4	0,92
D5Q8	3,69	3 (11)	4	0,99
D5Q7	3,46	3 (10)	4	0,86

4.2 Análise dos Dados

A análise dos dados revela uma predominância de percepções positivas. Entretanto, algumas questões destacam-se pela variabilidade nas respostas, indicando uma diversidade de opiniões. As questões com moda 5 e desvio padrão baixo sugerem um consenso mais forte entre os respondentes, enquanto aquelas com médias mais baixas e altos desvios padrão apontam para áreas de possíveis melhorias ou divergências nas percepções.

Conforme os critérios estabelecidos, após a análise das opiniões dos especialistas, as questões classificadas foram destacadas em verde e permanecerão no questionário para a próxima rodada. É importante ressaltar que houve empate nas dimensões 4 e 5, resultando na inclusão de ambas as questões na rodada seguinte. Por outro lado, as questões destacadas em vermelho foram removidas do questionário para a próxima rodada.

5. Feedback dos Participantes

5.1 Comentários Gerais

Os especialistas destacaram a importância significativa desta pesquisa, enfatizando que as questões formuladas abrangem tanto os aspectos técnicos quanto os aspectos legais do tratamento de dados pessoais. Eles também elogiaram a clareza e a objetividade das perguntas elaboradas.

5.2 Sugestões dos especialistas

Os especialistas contribuíram com sugestões de novas questões para serem incorporadas ao questionário na próxima rodada. Algumas dessas sugestões foram apresentadas de maneira genérica, sem um foco específico em uma das dimensões propostas, o que dificulta a aplicação da sugestão. Além disso, algumas sugestões já estavam contempladas por questões previamente propostas no questionário. Outras sugestões não deixaram claro a qual dimensão estariam relacionadas. Diante

desse cenário, os coordenadores desta pesquisa realizaram inferências e propuseram um alinhamento das sugestões com base no contexto que melhor se adequasse a cada uma delas.

A seguir, apresentam-se as propostas elaboradas pelos especialistas, as quais foram avaliadas quanto à sua inclusão no questionário para a rodada subsequente.

Para a Dimensão 1 - Governança de Dados e Boas Práticas:

Sugestão 1: Incluir um indicador de maturidade em privacidade e segurança da informação.

Análise: A sugestão foi refutada devido à falta de clareza sobre o tipo específico de indicador a ser utilizado, o que tornou a proposta subjetiva.

Para a Dimensão 2 - Políticas e Processos de Tratamento de Dados:

Sugestão 1: A organização promove processo de atualização periódica dos cadastros pessoais haja vista a manutenção da qualidade dos dados (LGPD, art. 6º, V)”?

Análise: Essa sugestão já está implementada na questão 2 da dimensão 2 e na questão 9 da dimensão 1. Segue as questões que já atende a sugestão.

D2Q1. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação? (art. 10, § 2o, da Lei no 10.741/2003; art. 5o, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei no 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ no 54/2023)

D1Q9. A organização revisa e atualiza regularmente suas políticas e procedimentos institucionalizados sobre o tratamento e proteção de dados e informações pessoais? (art. 23, inciso I, art. 32, art. 50 e art. 51 da Lei no 13.709/2018; itens 5.5.5, 6.2.1.2, 6.9.4 e 7.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.1, 5.31, 5.36, 5.9, 6.3, 6.6, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 1o e art. 19 da Resolução CONARQ no 54/2023)

Sugestão 2: A instituição já implementou sua política de adequação à Lei Geral de Proteção de Dados?

Análise: Essa sugestão é relevante, mas sua efetividade depende da realização prévia de um diagnóstico de maturidade. Este diagnóstico fornecerá uma compreensão detalhada do nível de preparação da organização em relação à LGPD e outras legislações e normas relacionadas. Com base nos resultados do diagnóstico, a instituição poderá elaborar e implementar uma política de adequação eficaz e personalizada às suas necessidades específicas. Por isso, a questão foi refutada.

Para a Dimensão 5 - Acesso à Informação e Transparência:

Sugestão 1: A organização implementa canais de atendimento aos titulares dos dados pessoais?

Análise: Essa sugestão já está implementada na questão 5 desta dimensão 5. Segue a questão que já atende a sugestão.

D5Q5. A organização estabeleceu procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes de segurança, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei n. 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ n. 54/2023)

Sugestões que não foram informada a dimensão:

Sugestão 1: A instituição segue as recomendações e está alinhada às iniciativas do governo federal, como o Programa de Privacidade e Segurança da Informação (PPSI) e a Infraestrutura Nacional de Dados, no âmbito da Secretaria de Governo Digital do Ministério da Gestão e Inovação?

Análise: A proposta é bastante relevante, especialmente pela conformidade com a Portaria SGD/MGI n. 852, de 28 de março de 2023. Entretanto, o tema proposto já está implementado, só que desmembrado em duas questões: na questão 6 da dimensão 1 e na questão 1 da dimensão 4. Por isso a portaria será acrescida no embasamento legal dessas duas questões. Segue como ficarão as questões atualizadas.

D1Q6. A instituição possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (artigos 1º, 2º, inciso I, 6º, incisos IV e VI, 8º, 9º, 17 a 22, 23, inciso I, e 50, § 2º, incisos I e II da Lei n. 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023; e artigos 4º, 13º e 20 da Resolução CONARQ n. 54/2023)

D4Q1. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar? (art. 4º, inciso V, da Lei n. 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas "b" e "g", art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei n. 13.709/2018; Decreto n. 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR n. 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023 e art. 14 da Resolução CONARQ n. 54/2023)

Sugestão 2: É essencial avaliar a aplicação do princípio da segregação das funções, especialmente no que se refere ao comum acúmulo de responsabilidades do Encarregado com o acesso à informação em instituições públicas, e considerar suas implicações. Há potenciais conflitos na gestão dos princípios da privacidade e do acesso à informação quando essas funções são desempenhadas por um único indivíduo.

Análise: A sugestão é relevante, alinhando-se ao disposto no artigo 5º da Lei 14.133/2021, que trata da segregação de funções como uma medida do Controle Interno para prevenir falhas e fraudes, além de evitar conflitos de interesse em contratações. A questão será incorporada à dimensão 1 da seguinte maneira:

D1Q12. A instituição segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados assuma outras funções que possam gerar conflitos de interesse? (Art. 50 da Lei 13.709/2018; Art. 5º e 7º, § 1º da Lei 14.133/2021)

6. Discussão

6.1 Interpretação dos Resultados

Embora a média aritmética simples seja o critério principal desta rodada, também foram analisados a moda, a mediana e o desvio padrão para proporcionar uma compreensão mais aprofundada dos resultados.

- **Média:**

As médias variaram de 3,29 a 4,6.

As questões com médias mais altas (>4.0) indicam uma percepção mais positiva ou um acordo mais forte.

As questões com médias mais baixas (<4.0) indicam uma percepção menos positiva.

- **Moda:**

A moda para a maioria das questões foi 5, indicando que a resposta mais frequente foi "concordo totalmente".

Algumas questões tiveram a moda 3, o que indica que a resposta foi mais "neutra" ou um grau de concordância/discordância mais moderado.

D2Q5 teve duas modas (3 e 5), indicando uma divisão clara das opiniões.

- **Mediana:**

A mediana é 4 para a maioria das questões, sugerindo que pelo menos metade dos respondentes escolheu 4 ou acima.

Algumas questões têm mediana 3, o que indica uma percepção mais moderada.

- **Desvio Padrão (Dp):**

O desvio padrão varia de 0,69 a 1,19.

Questões com Dp mais baixo têm respostas mais concentradas em torno da média. Questões com Dp mais alto têm respostas mais dispersas, indicando maior variabilidade nas opiniões.

Os resultados indicam que temas como a "designação" e "publicização do Encarregado de Proteção de Dados", a "identificação" e "Conscientização dos Agentes (operadores) de Tratamento de Dados Pessoais", bem como a "revisão e atualização regular das políticas e procedimentos institucionalizados", são assuntos extremamente importantes e foram consistentemente bem avaliados e com baixa variação entre as respostas. Em contrapartida, questões como "treinamentos específicos para o tratamento de dados pessoais sensíveis, incluindo dados de crianças e adolescentes", e "programa ou plano de comunicação", mostraram maior dispersão nas respostas, indicando diferentes percepções entre os especialistas. Perguntas relacionadas ao plano de governança, publicização do encarregado de

proteção de dados, controle de acesso e autenticação segura receberam altas avaliações e mostraram alto consenso entre os respondentes.

6.2 Comparação com Expectativas

A comparação dos resultados obtidos na primeira rodada do método *Delphi* com as expectativas iniciais demonstra um alinhamento satisfatório em relação aos objetivos estabelecidos. A identificação das questões mais relevantes para compor o modelo de maturidade no tratamento de dados pessoais nas universidades federais do Brasil foi alcançada de forma consistente. As dimensões que receberam maior pontuação média e consenso entre os especialistas, refletem a importância atribuída às práticas de governança de dados, políticas e processos de tratamento, treinamento e conscientização, segurança da informação e tecnologia, além do acesso à informação e transparência. A análise dos dados também revelou áreas de maior controvérsia ou dispersão de opiniões, especialmente em temas mais específicos como o tratamento de dados sensíveis e programas de comunicação.

7. Conclusão

7.1 Resumo

A primeira rodada do método *Delphi* proporcionou *insights* valiosos sobre as prioridades e desafios relacionados ao tratamento de dados pessoais nas universidades federais do Brasil. As questões mais bem avaliadas serão refinadas nas próximas rodadas, enquanto aquelas com menor avaliação foram revisadas ou eliminadas do instrumento de medição. Esses resultados serão fundamentais para o desenvolvimento de um modelo de maturidade robusto e adaptável às necessidades específicas dessas instituições de ensino superior.

O questionário será apresentado com a seguinte estrutura para a segunda rodada. Serão disponibilizadas 28 questões distribuídas em cinco dimensões.

Questão na 1ª rodada	Questão na 2ª rodada	Média	Temas
D1Q1	D1Q1	4,34	Programa ou Plano de Governança
D1Q2	D1Q2	4,6	Designação do Encarregado de Proteção de Dados
D1Q3	D1Q3	4,43	Comitê Interno para Tratamento de Dados e Informações Pessoais
D1Q6	D1Q4	4,23	Política de Privacidade, atualizado com a sugestão dos especialistas
D1Q7	D1Q5	4,14	Identificação de Compartilhamento e Transferência de Dados Pessoais
-	D1Q6	Sem nota	Princípio da segregação das funções, sugestão dos especialistas
D2Q1	D2Q1	4,14	Identificação das Categorias de Dados Pessoais e dos Titulares de Dados Pessoais
D2Q2	D2Q2	4,26	Identificação dos Agentes (operadores) de Tratamento de Dados Pessoais

D2Q4	D2Q3	4,11	Identificação dos Processos e Atividades Operacionais Relacionadas aos Dados Pessoais
D2Q8	D2Q4	4,14	Direitos dos Titulares de Dados Pessoais
D2Q10	D2Q5	4,14	Mascaramento, Pseudonimização ou Anonimização de Dados e Informações Pessoais
D3Q1	D3Q1	4,14	Programa ou Plano de Capacitação
D3Q2	D3Q2	4,17	Conscientização dos Agentes de Tratamento de Dados sobre seus Papéis e Responsabilidades
D3Q3	D3Q3	3,89	Treinamento e Capacitação dos Colaboradores (Terceirizados e Parceiros)
D3Q4	D3Q4	3,94	Capacitação Quanto aos Riscos Associados ao Tratamento Inadequado de Dados Pessoais
D3Q6	D3Q5	3,8	Capacitação Quanto aos Procedimentos Adequados para a Gestão de Incidentes
D4Q1	D4Q1	4,34	Política de Segurança da Informação, atualizado com a sugestão dos especialistas
D4Q3	D4Q2	4,23	Criptografia
D4Q4	D4Q3	4,2	Gestão de Backup e Trilhas de Auditoria
D4Q5	D4Q4	4,2	Inteligência de Ameaças e Gestão de Vulnerabilidades
D4Q6	D4Q5	4,49	Controle de Acesso e Autenticação Segura
D4Q8	D4Q6	4,23	Monitoramento e Controle de Eventos Associados à Violação e Vazamento de Dados Pessoais
D5Q1	D5Q1	4,29	Transparência
D5Q2	D5Q2	3,91	Política de Classificação da Informação
D5Q3	D5Q3	4,57	Publicização do Encarregado de Proteção de Dados
D5Q4	D5Q4	4,06	Publicização da Política de Privacidade
D5Q5	D5Q5	3,97	Procedimentos de Comunicação à ANPD e ao Titular de Dados em Caso de Ocorrência de Incidentes de Segurança
D5Q9	D5Q6	3,91	Programa ou Plano de Comunicação

7.2 Próximas Etapas

As próximas etapas do estudo envolvem a realização das rodadas subsequentes do método *Delphi*, com foco no refinamento das questões selecionadas. O objetivo é finalizar a construção e validação do instrumento de medição e iniciar a aplicação do modelo proposto, culminando na elaboração de recomendações para implementação nas universidades federais do Brasil.

APÊNDICE I – Questionário da segunda rodada na plataforma questionpro e TCLE

PROPOSTA DO QUESTIONÁRIO PARA MEDIÇÃO DO MODELO DE MATURIDADE PARA TRATAMENTO DE DADOS PESSOAIS (MMTDP) - 2ª RODADA

Introdução:

Prezado(a) Participante, antes de prosseguir com o preenchimento deste formulário, permita-me esclarecer o propósito e os termos associados a este estudo. Este questionário é uma parte integrante do "Painel de Especialistas" e constitui um componente crucial da pesquisa de doutorado intitulada "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de Modelo de Maturidade sob a perspectiva dos Marcos Legais Brasileiros". Esta é a **segunda rodada**, com as questões mais bem avaliadas e com sugestões dos especialistas aprovadas da primeira rodada.

Este trabalho está sendo desenvolvido no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. O propósito imediato deste questionário é refinar as questões mais pertinentes que irão compor o instrumento de medição do modelo de maturidade para tratamento de dados pessoais, o qual está em fase de elaboração.

Equipe Responsável:

A equipe encarregada (facilitadores) pela condução desse "Painel de Especialistas" e pelo desenvolvimento integral da pesquisa de doutorado é composta pelos seguintes membros: Isaac Rozas Rios, doutorando (isaacrrios@hotmail.com/ irr@academico.ufpb.br) e o Prof. Dr. Wagner Junqueira de Araújo, orientador (wagnerjunqueira.araujo@gmail.com).

Contatos para esclarecimentos de dúvidas ou informações sobre a pesquisa:

Pesquisador Responsável: Isaac Rozas Rios - E-mail: isaacrrios@hotmail.com - Telefone: +55 (83) 99979-4530 ou Comitê de Ética do Centro de Ciências da Saúde Comitê de Ética em Pesquisa (CEP)- (1º andar) da Universidade Federal da Paraíba Campus I - Cidade Universitária / CEP: 58.051-900 - João Pessoa-PB - Telefone: +55 (83) 3216- 7791 - E-mail: comitedeetica@ccs.ufpb.br - Horário de Funcionamento: de 07h às 12h e de 13h às 16h. Homepage: <https://www.ccs.ufpb.br/eticaccsufp>.

Informamos que sua participação é voluntária e baseada em seu consentimento.

Termo de Consentimento Livre e Esclarecido:

A sua participação neste estudo é totalmente voluntária e não implica em nenhum custo financeiro. Todas as informações que você fornecer serão tratadas de forma anônima e confidencial, garantindo sua privacidade. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Para baixar este TCLE em formato PDF clique no link abaixo:

https://drive.google.com/uc?export=download&id=1Ei35xuMbvb54nRycgxnNqj23O5zVAM_f

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.

☐ **Sim**

☐ **Não**

Termo de Consentimento Livre e Esclarecido

Você está sendo convidado a participar da pesquisa intitulada "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: proposta de Modelo de Maturidade sob a perspectiva dos Marcos Legais Brasileiros", desenvolvida no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. O objetivo principal é propor um modelo de maturidade para o tratamento de dados pessoais nas Universidades Federais do Brasil, sob a perspectiva da Lei Geral de Proteção de Dados e demais marcos legais brasileiros sobre o tema. Este questionário tem como propósito identificar e selecionar as questões mais relevantes para compor o instrumento de medição do modelo de maturidade em fase de elaboração. Sua colaboração é muito importante, porém a participação é totalmente voluntária e não implica em custo financeiro. Para participar, você responderá a um questionário com matrizes de resposta única, incluindo uma pergunta aberta para sugestões. Todos os procedimentos para garantir a confidencialidade serão rigorosamente seguidos, mantendo suas informações anônimas e confidenciais. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Os benefícios esperados incluem o desenvolvimento da ferramenta administrativa para mapear as capacidades organizacionais no tratamento e proteção de dados e informações pessoais, promovendo transparência, controle e conformidade com as regulamentações. Os participantes terão acesso aos resultados, contribuindo para aprimorar a segurança e eficiência das atividades administrativas das instituições de ensino superior. Este estudo também servirá como referência para profissionais e pesquisas futuras sobre o tema. Reconhece-se a presença de riscos imprevisíveis, os quais são mitigados pela confidencialidade e anonimato assegurados aos participantes. Durante a coleta de dados, inclusive *on-line*, os participantes têm a liberdade de não responder sem prejuízo. Se houver dúvidas ou preocupações, entre em contato a qualquer momento com o Pesquisador Responsável: Isaac Rozas Rios - E-mail: isaacrrios@hotmail.com - Telefone +55 (83) 99979-4530 ou Comitê de Ética do Centro de Ciências da Saúde Comitê de Ética em Pesquisa (CEP) - (1º andar) da Universidade Federal da Paraíba Campus I - Cidade Universitária / CEP: 58.051-900 - João Pessoa-PB - Telefone: +55 (83) 3216- 7791 - E-mail: comitedeetica@ccs.ufpb.br - Horário de Funcionamento: de 07h às 12h e de 13h às 16h. Homepage: <https://www.ccs.ufpb.br/eticaccsufp>

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.

- ☐ Sim
- ☐ Não

Identificação do respondente (os dados pessoais não serão divulgados na pesquisa, serve apenas para controle interno dos pesquisadores)

* Nome da Instituição

* Nome do Encarregado de Dados Pessoais

* E-mail

Telefone

Instruções: Utilize a seguinte escala de relevância a cada questão com foco na dimensão em análise. A escala de avaliação vai de 1 a 5, onde:

- 1 - Irrelevante para a dimensão
- 2 - Pouca relevância para a dimensão
- 3 - Relevante para a dimensão
- 4 - Muita relevância para a dimensão
- 5 - Total relevância para a dimensão

Dimensão 1: Governança de Dados e Boas Práticas (cor cinza)

Esta dimensão avalia a forma como a organização estabelece sua estrutura de governança para lidar com dados e informações pessoais. Isso inclui aspectos estratégicos, como a nomeação de um Encarregado de Proteção de Dados, a constituição de comitês e programas de governança e a definição de responsabilidades de forma clara e precisa. Uma governança sólida é fundamental para garantir que uma instituição atue de maneira responsável e alinhada à legislação.

Dimensão 1: Governança de Dados e Boas Práticas

1. A organização elaborou um **programa de governança, plano de governança ou documento equivalente** para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei nº 13.709/2018; Decreto nº 9.637/2018 e Decreto nº 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

	1 - Irrelevante para dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

2. A organização designou formalmente o **Encarregado de Proteção de Dados (EPD)** ou **Data Protection Officer (DPO)**? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei nº 13.709/2018; Lei nº 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

3. A organização estabeleceu **comitê interno ou equivalente** para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando *compliance* com todas as leis e regulamentações aplicáveis? (art. 50 da Lei nº 13.709/2018; art. 15 do Decreto nº 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto nº 10.046/2019)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

4. A instituição possui **Política de Privacidade ou documento equivalente** que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei nº 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI Nº 852/2023 e art. 4º, art. 13 e art. 20 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

5. A organização **identificou se existe compartilhamento ou transferência de dados pessoais** na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 1: Governança de Dados e Boas Práticas

6. A organização segue o **princípio da segregação das funções**, evitando que o Encarregado de Proteção de Dados assuma outras funções que possam gerar conflitos de interesse? (Art. 50 da Lei 13.709/2018; Art. 5º e 7º, § 1º da Lei 14.133/2021)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela)

Nesta dimensão, o foco recai sobre aspectos operacionais e técnicos, analisando a existência e eficácia das políticas, procedimentos e processos relacionados ao tratamento de dados. Avalia se as políticas estão bem definidas, abordando todos os aspectos do ciclo de vida dos dados e/ou informações pessoais, abrangendo coleta, armazenamento, tratamento e exclusão. Adicionalmente, avalia a capacidade da organização de identificar e avaliar os riscos inerentes ao tratamento de dados pessoais, à gestão dos dados pessoais sensíveis, aos dados de crianças e adolescentes e ao consentimento e direitos dos titulares de dados. Além disso, examina como a organização monitora a eficácia de suas práticas e busca continuamente aprimorá-las. O propósito é assegurar que os dados pessoais sejam tratados de maneira ética, legal e segura.

Dimensão 2: Políticas e Processos de Tratamento de Dados

1. A organização realizou a **identificação das categorias de dados pessoais e dos titulares de dados pessoais** com os quais a instituição mantém relação? (art. 10, § 2º, da Lei nº 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

2. A organização realizou a **identificação dos agentes (controladores e operadores)** de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

3. A organização realizou a **identificação dos processos e atividades operacionais que lidam com dados pessoais**? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

4. Existem mecanismos formais na organização que garantam os **direitos dos titulares de dados pessoais**? (art. 2º, inciso IX, da Lei nº 7.232/1984; art. 4º da Lei nº 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei nº 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 2: Políticas e Processos de Tratamento de Dados

5. A organização estabelece **regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados**, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei nº 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	☐	☐	☐	☐	☐

Dimensão 3: **Treinamento e Conscientização** (cor azul)

Esta dimensão concentra-se no treinamento e na conscientização de colaboradores e partes interessadas sobre questões relacionadas à proteção de dados. Ela avalia o nível de instrução e conscientização dos colaboradores em relação à proteção de dados pessoais. O treinamento adequado e a conscientização são de importância crítica para garantir que todos na organização compreendam as implicações legais e éticas envolvidas no tratamento de dados e estejam preparados para agir conforme as políticas e procedimentos estabelecidos.

Dimensão 3: Treinamento e Conscientização

1. A organização possui **programas ou planos de capacitação** que abranjam treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei nº 7.232/1984; art. 50 da Lei nº 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto nº 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

2. A organização **conscientiza os seus agentes de tratamento de dados pessoais** sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei nº 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

3. Os **colaboradores (terceirizados e parceiros)** da organização que exercem atividades atreladas ao tratamento de dados pessoais, **recebem treinamentos e capacitações específicas** sobre o tema? (art. 50 da Lei nº 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
	☐	☐	☐	☐	☐

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

4. A organização **conscientiza regularmente quanto aos riscos associados ao tratamento inadequado** de dados pessoais? (arts. 42-45, art. 50 e arts. 52-54 da Lei nº 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 3: Treinamento e Conscientização

5. A organização promove **capacitação quanto aos procedimentos adequados para a gestão de incidentes**, determinando a melhor forma de planejar, gerenciar e comunicar os incidentes de segurança da informação? (art. 48 e art. 50 da Lei nº 13.709/2018; art. 3º, incisos VII e IX, do Decreto nº 9.637/2018; item 6.13 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.25, 5.26, 5.27 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27035:2023; art. 15, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	☐	☐	☐	☐	☐

Dimensão 4: **Segurança da Informação e Tecnologia** (cor verde)

Nesta dimensão, o foco recai sobre as medidas de segurança implementadas pela organização para proteger dados e informações pessoais. Isso abrange a avaliação da segurança da infraestrutura de TI, as medidas de prevenção de violações de dados, a criptografia, a autenticação e outras práticas relacionadas à tecnologia, visando garantir confidencialidade e integridade dos dados. Além disso, examina-se a conformidade com as regulamentações de segurança e a eficácia das medidas de segurança implementadas nos sistemas da organização.

Dimensão 4: Segurança da Informação e Tecnologia

1. A organização definiu e elaborou a **Política de Segurança da Informação ou instrumento similar**? (art. 4º, inciso V, da Lei 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei nº 13.709/2018; Decreto nº 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI Nº 852/2023 e art. 14 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

2. A organização usa **criptografia para proteger os dados pessoais**? (art. 11, inciso II, alínea “g”, art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea ‘c’, da Lei nº 13.709/2018; art. 2º, inciso III, do

Decreto nº 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

3. A organização possui **gestão de backup e trilhas de auditoria** para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei nº 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

4. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a **inteligência de ameaças e a gestão de vulnerabilidades**? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei nº 13.709/2018; art. 2º, incisos II e III do Decreto nº 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

5. A organização estabelece **controle de acesso e autenticação segura** às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, “g”, art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei nº 13.709/2018; art. 2º, incisos III e IV, do Decreto nº 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 4: Segurança da Informação e Tecnologia

6. A organização faz **monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais**? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea ‘g’, e art. 52, § 7º, da Lei nº 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto nº 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência (cor vermelha)

Nesta dimensão, a avaliação concentra-se na disponibilidade e transparência das informações para as partes interessadas. Isso engloba a conformidade com as normas de acesso à informação e a capacidade de demonstrar transparência nas práticas de proteção de dados. Adicionalmente, avalia-se a capacidade de gerar relatórios precisos para garantir conformidade com regulamentações de privacidade e acesso à informação, bem como comunicar as partes afetadas, às autoridades regulatórias e outras partes interessadas sobre incidentes ocorridos, incluindo registros de como os incidentes foram tratados e as lições aprendidas.

Dimensão 5: Acesso à Informação e Transparência

1. A organização atende ao **princípio da transparência**? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei nº 8.159/1991; Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea “e”, da Lei nº 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

2. A organização possui **Política de Classificação da Informação ou instrumento similar**, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas “a” e “d”, da Lei nº 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

3. A **designação do encarregado e suas informações de contato, foram publicizadas** em algum meio de comunicação oficial?? (art. 5º, inciso VIII, art. 23, art. 41 da Lei nº 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

4. A **Política de Privacidade da instituição está publicizada?** (art. 2º, inciso VIII, da Lei 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei nº 13.709/2018; art. 3º, inciso XI, do Decreto nº 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

5. A organização estabeleceu **procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes** de segurança, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei nº 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

Dimensão 5: Acesso à Informação e Transparência

6. A organização possui **programa, plano de comunicação ou documento similar** que abarque as diretrizes das legislações e normas referentes ao tratamento e proteção de dados e informações pessoais? (art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.5.4, 8.4.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 6.6 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 24 da Resolução CONARQ nº 54/2023)

	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	☐	☐	☐	☐	☐

APÊNDICE J – Relatório de *feedback* da segunda rodada do método *delphi* (relatório final)

Relatório Final do Método *Delphi*

1. Introdução

1.1 Objetivo do Relatório

Este relatório apresenta os resultados da 2ª rodada do método *Delphi* aplicado ao estudo de doutorado intitulado "O TRATAMENTO DOS DADOS PESSOAIS NAS UNIVERSIDADES FEDERAIS DO BRASIL: Proposta de Modelo de Maturidade sob a Perspectiva dos Marcos Legais Brasileiros".

1.2 Contexto

Este estudo está sendo desenvolvido no âmbito do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, com o objetivo central de identificar e selecionar as questões mais relevantes para compor o instrumento de medição do modelo de maturidade no tratamento de dados pessoais. No momento, a pesquisa encontra-se na segunda rodada de seleção das questões, tendo como meta a identificação das 25 questões mais significativas. Esse objetivo foi plenamente alcançado nesta etapa, que, por ter cumprido integralmente os critérios estabelecidos, foi definida também como a fase final do método.

2. Metodologia

2.1 Descrição do Método *Delphi*

O método *Delphi* é um processo consultivo estruturado amplamente empregado para alcançar um consenso majoritário entre especialistas. Este estudo adota um processo iterativo, composto por múltiplas rodadas, em que os especialistas expressam suas opiniões e recebem feedback baseado nas respostas coletivas das rodadas anteriores. O objetivo central é utilizar o método *Delphi* para validar e selecionar as 25 questões que integrarão o instrumento de medição do modelo de maturidade proposto para o tratamento de dados pessoais.

2.2 Fases do *Delphi* nesta pesquisa

Na segunda rodada, o instrumento manteve sua estrutura com base em cinco dimensões principais: Governança de Dados e Boas Práticas, Políticas e Processos de Tratamento de Dados, Treinamento e Conscientização, Segurança da Informação e Tecnologia, e Acesso à Informação e Transparência. Cada dimensão foi composta por 5 a 6 questões, todas alinhadas com as legislações e normativas vigentes sobre o tratamento e a proteção de dados pessoais no país, e que receberam as avaliações mais elevadas pelos especialistas na primeira rodada. Adicionalmente, foram incorporadas as sugestões apresentadas pelos especialistas na fase anterior.

3. Participantes

3.1 Perfil dos Especialistas

Os participantes da pesquisa foram os encarregados de proteção de dados das universidades federais do Brasil que já haviam participado da primeira rodada. Esses profissionais possuem *expertise* no tema, bem como nas práticas institucionais relacionadas ao tratamento e à proteção de dados e informações pessoais nessas instituições.

3.2 Número de Participantes

Nesta segunda rodada 28 profissionais participaram.

4. Resultados da 2ª Rodada

4.1 Dados Coletados

Os especialistas avaliaram a relevância de 28 questões, distribuídas entre as 5 dimensões propostas para compor o instrumento de medição de maturidade. As respostas foram obtidas utilizando uma escala de 1 a 5, em que 1 representa "Pouco Relevante" e 5 "Muito Relevante". A seguir, apresentam-se os dados coletados em cada dimensão. Seguem os dados coletados.

Questões da Dimensão 1 (Governança de Dados e Boas Práticas)

Dimensão/Questão	Média	Moda	Mediana	Dp
D1Q2	4,79	5	5	0,5
D1Q3	4,54	5	5	0,69
D1Q4	4,5	5	5	0,75
D1Q6	4,25	5	5	1,08
D1Q1	4,21	5	5	1,07
D1Q5	4,04	5	4	1,1

Questões da Dimensão 2 (Políticas e Processos de Tratamento de Dados)

Dimensão/Questão	Média	Moda	Mediana	Dp
D2Q1	4,32	5	5	1,02
D2Q3	4,32	5	5	0,98
D2Q5	4,32	5	5	0,98
D2Q2	4,29	5	5	0,94
D2Q4	4,14	5	4,5	0,97

Questões da Dimensão 3 (Treinamento e Conscientização)

Dimensão/Questão	Média	Moda	Mediana	Dp
D3Q2	4,25	5	4,5	0,89
D3Q1	4,14	5	4	1,04

D3Q3	4,04	5	4	1,07
D3Q4	4,04	5	4	1,1
D3Q5	3,96	5	4	1,04

Questões da Dimensão 4 (Segurança da Informação e Tecnologia)

Dimensão/Questão	Média	Moda	Mediana	Dp
D4Q1	4,61	5	5	0,63
D4Q5	4,43	5	5	0,74
D4Q6	4,39	5	5	0,79
D4Q2	4,32	5	5	0,86
D4Q3	4,32	5	4,5	0,77
D4Q4	4,21	5	4	0,88

Questões da Dimensão 5 (Acesso à Informação e Transparência)

Dimensão/Questão	Média	Moda	Mediana	Dp
D5Q3	4,54	5	5	0,79
D5Q4	4,32	5	5	0,82
D5Q1	4,25	5	5	1,14
D5Q2	4,18	5	4,5	0,98
D5Q5	3,96	5	4	1,07
D5Q6	3,89	5	4	1,07

4.2 Análise dos Dados

A análise dos dados revela uma predominância de percepções positivas. De acordo com os critérios estabelecidos, as questões foram avaliadas até que o consenso dos especialistas determinasse as 25 mais representativas. Considerou-se que o consenso foi alcançado quando as médias das avaliações foram iguais ou superiores a 4, e quando as modas e medianas também se mantiveram acima de 4. Caso esses índices não fossem atingidos nessa rodada, uma nova rodada seria necessária. Contudo, 25 questões atenderam a esses critérios, permitindo que o método Delphi atingisse seu objetivo, definindo as questões que compõem o instrumento de medição do modelo de maturidade.

Após a análise das opiniões dos especialistas, as questões com as melhores avaliações foram destacadas em verde, enquanto aquelas que não atingiram os índices desejados foram marcadas em vermelho. Além de selecionar as questões que comporão o instrumento de medição do modelo, essa etapa permitiu categorizar as questões de acordo com seu peso na avaliação da respectiva dimensão. Questões com média aritmética superior a 4,5, assim como moda e mediana também acima de 4,5, foram classificadas como de alta relevância para a dimensão, identificando-as como aquelas que terão maior peso no processo de avaliação da capacidade das organizações.

Dimensão/Questão	Média	Moda	Mediana	DP	Classificação	Peso
D1Q2	4,79	5	5	0,50	Alta	5
D4Q1	4,61	5	5	0,63	Alta	5
D5Q3	4,54	5	5	0,79	Alta	5
D1Q3	4,54	5	5	0,69	Alta	5
D1Q4	4,50	5	5	0,75	Alta	5
D4Q5	4,43	5	5	0,74	Média	3
D4Q6	4,39	5	5	0,79	Média	3
D5Q4	4,32	5	5	0,82	Média	3
D4Q2	4,32	5	5	0,86	Média	3
D2Q5	4,32	5	5	0,98	Média	3
D2Q3	4,32	5	5	0,98	Média	3
D2Q1	4,32	5	5	1,02	Média	3
D4Q3	4,32	5	4,5	0,77	Média	3
D2Q2	4,29	5	5	0,94	Média	3
D5Q1	4,25	5	5	1,14	Média	3
D1Q6	4,25	5	5	1,08	Média	3
D3Q2	4,25	5	4,5	0,89	Média	3
D1Q1	4,21	5	5	1,07	Média	3
D4Q4	4,21	5	4	0,88	Média	3
D5Q2	4,18	5	4,5	0,98	Média	3
D2Q4	4,14	5	4,5	0,97	Média	3
D3Q1	4,14	5	4	1,04	Média	3
D3Q4	4,04	5	4	1,10	Média	3
D3Q3	4,04	5	4	1,07	Média	3
D1Q5	4,04	5	4	1,10	Média	3
D5Q5	3,96	5	4	1,07	Baixa	1
D3Q5	3,96	5	4	1,04	Baixa	1
D5Q6	3,89	5	4	1,07	Baixa	1

5. Feedback dos Participantes

5.1 Comentários Gerais

Nesta rodada, o foco dos especialistas foi avaliar a relevância das questões no contexto de cada dimensão. As sugestões para novas questões, feitas na rodada anterior, foram incorporadas nesta etapa. Alguns dos participantes da primeira rodada optaram por não participar.

6. Discussão

6.1 Interpretação dos Resultados

A análise dos dados apresentados indica um processo de avaliação de questões dentro de diferentes dimensões, em que os valores de média, moda, mediana, desvio-padrão (DP), classificação e peso foram utilizados para determinar a relevância de cada questão. A seguir, apresenta-se uma interpretação detalhada:

1. Questões com Classificação "Alta" (Peso 5):

- **D1Q2, D4Q1, D5Q3, D1Q3, D1Q4:** Estas questões se destacam por terem obtido médias muito próximas de 5 (entre 4,50 e 4,79), uma moda e mediana igual a 5, e um desvio-padrão relativamente baixo (variando de 0,50 a 0,79). Esses valores indicam que os especialistas concordaram fortemente sobre a relevância dessas questões, demonstrando pouca variabilidade nas respostas. Por conseguinte, essas questões foram classificadas como de alta relevância e receberam o peso máximo (5).

2. Questões com Classificação "Média" (Peso 3):

- **D4Q5 a D3Q4:** Algumas questões tiveram médias ligeiramente inferiores (variando de 4,04 a 4,43), com modas e medianas geralmente igual a 5, exceto em alguns casos onde a mediana é 4 ou 4,5. O desvio-padrão é um pouco mais elevado (entre 0,74 e 1,10), indicando uma maior variação nas opiniões dos especialistas. Elas foram classificadas como de "média relevância".

3. Questões com Classificação "Baixa" (Peso 1):

- **D5Q5, D3Q5, D5Q6:** Já essas questões possuem as médias mais baixas (entre 3,89 e 3,96), embora a moda permaneça em 5, o que sugere que, apesar de alguns especialistas considerarem essas questões muito importantes, houve uma maior dispersão nas avaliações (com medianas de 4 e desvios-padrão superiores a 1). A classificação como "baixa relevância" reflete essa dispersão e indica uma prioridade reduzida na consideração dessas questões dentro do contexto geral. Como um dos critérios seriam só permanecer questões de média ou alta relevância, essas questões foram retiradas do instrumento.

6.2 Comparação com Expectativas

A análise dos dados obtidos permitiu definir as 25 questões que irão compor o instrumento de medição de maturidade do modelo proposto. Os resultados demonstraram que as questões selecionadas apresentam classificações médias ou de alta relevância, indicando sua pertinência e alinhamento com os objetivos do estudo. É importante destacar que nenhuma das questões classificadas como de baixa relevância foi incluída entre as selecionadas.

7. Conclusão

7.1 Resumo

A segunda rodada do método *Delphi*, fundamentada na análise criteriosa dos especialistas, resultou na seleção das questões do instrumento de medição de maturidade no tratamento de dados pessoais nas universidades federais do Brasil. Essa seleção rigorosa assegura que o instrumento final esteja alinhado com os objetivos do estudo e reflita as áreas de maior relevância para as dimensões analisadas, segundo as opiniões dos especialistas.

Os temas das questões selecionadas e as respectivas dimensões, avaliações e classificações são as seguintes:

Tema	Dimensão	Média	Moda	Mediana	Peso
Designação do Encarregado de Proteção de Dados	Governança de Dados e Boas Práticas	4,79	5	5	5
Política de Segurança da Informação, atualizado com a sugestão dos especialistas	Segurança da Informação e Tecnologia	4,61	5	5	5
Publicização do Encarregado de Proteção de Dados	Acesso à Informação e Transparência	4,54	5	5	5
Comitê Interno para Tratamento de Dados e Informações Pessoais	Governança de Dados e Boas Práticas	4,54	5	5	5
Política de Privacidade, atualizado com a sugestão dos especialistas	Governança de Dados e Boas Práticas	4,50	5	5	5
Controle de Acesso e Autenticação Segura	Segurança da Informação e Tecnologia	4,43	5	5	3
Monitoramento e Controle de Eventos Associados à Violação e Vazamento de Dados Pessoais	Segurança da Informação e Tecnologia	4,39	5	5	3
Publicização da Política de Privacidade	Acesso à Informação e Transparência	4,32	5	5	3
Criptografia	Segurança da Informação e Tecnologia	4,32	5	5	3
Mascaramento, Pseudonimização ou Anonimização de Dados e Informações Pessoais	Políticas e Processos de Tratamento de Dados	4,32	5	5	3
Identificação dos Processos e Atividades Operacionais Relacionadas aos Dados Pessoais	Políticas e Processos de Tratamento de Dados	4,32	5	5	3
Identificação das Categorias de Dados Pessoais e dos Titulares de Dados Pessoais	Políticas e Processos de Tratamento de	4,32	5	5	3

	Dados				
Gestão de Backup e Trilhas de Auditoria	Segurança da Informação e Tecnologia	4,32	5	4,5	3
Identificação dos Agentes (operadores) de Tratamento de Dados Pessoais	Políticas e Processos de Tratamento de Dados	4,29	5	5	3
Transparência	Acesso à Informação e Transparência	4,25	5	5	3
Princípio da segregação das funções, sugestão dos especialistas	Governança de Dados e Boas Práticas	4,25	5	5	3
Conscientização dos Agentes de Tratamento de Dados sobre seus Papéis e Responsabilidades	Treinamento e Conscientização	4,25	5	4,5	3
Programa ou Plano de Governança	Governança de Dados e Boas Práticas	4,21	5	5	3
Inteligência de Ameaças e Gestão de Vulnerabilidades	Segurança da Informação e Tecnologia	4,21	5	4	3
Política de Classificação da Informação	Acesso à Informação e Transparência	4,18	5	4,5	3
Direitos dos Titulares de Dados Pessoais	Políticas e Processos de Tratamento de Dados	4,14	5	4,5	3
Programa ou Plano de Capacitação	Treinamento e Conscientização	4,14	5	4	3
Capacitação Quanto aos Riscos Associados ao Tratamento Inadequado de Dados Pessoais	Treinamento e Conscientização	4,04	5	4	3
Treinamento e Capacitação dos Colaboradores (Terceirizados e Parceiros)	Treinamento e Conscientização	4,04	5	4	3
Identificação de Compartilhamento e Transferência de Dados Pessoais	Governança de Dados e Boas Práticas	4,04	5	4	3

8. Anexos

8.1 Instrumentos de Medição do Modelo de Maturidade para Dados Pessoais

Anexo A: Questionário com as questões selecionadas do instrumento de medição do modelo de maturidade

DIMENSÃO 1

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei n. 13.709/2018; Decreto n. 9.637/2018 e Decreto n. 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)
2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei n. 13.709/2018; Lei n. 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)
3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis? (art. 50 da Lei n. 13.709/2018; art. 15 do Decreto n. 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto n. 10.046/2019)
4. A instituição possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei n. 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023 e art. 4º, art. 13 e art. 20 da Resolução CONARQ n. 54/2023)
5. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei n. 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ n. 54/2023)
6. A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados assuma outras funções que possam gerar conflitos de interesse? (Art. 50 da Lei 13.709/2018; Art. 5º e 7º, § 1º da Lei 14.133/2021)

DIMENSÃO 2

7. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação? (art. 10, § 2º, da Lei n. 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ n. 54/2023)
8. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI

(arts. 37-41), art. 50 da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ n. 54/2023)

9. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei n. 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ n. 54/2023)

10. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais? (art. 2º, inciso IX, da Lei n. 7.232/1984; art. 4º da Lei n. 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei n. 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ n. 54/2023)

11. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei n. 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ n. 54/2023)

DIMENSÃO 3

12. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei n. 7.232/1984; art. 50 da Lei n. 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto n. 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

13. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei n. 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ n. 54/2023)

14. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais, recebem treinamentos e capacitações específicas sobre o tema? (art. 50 da Lei n. 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

15. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais? (arts. 42-45, art. 50 e arts. 52-54 da Lei n. 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

DIMENSÃO 4

16. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar? (art. 4º, inciso V, da Lei n. 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas “b” e “g”, art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei n. 13.709/2018; Decreto n. 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR n. 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023 e art. 14 da Resolução CONARQ n. 54/2023)

17. A organização usa criptografia para proteger os dados pessoais? (art. 11, inciso II, alínea “g”, art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea ‘c’, da Lei n. 13.709/2018; art. 2º, inciso III, do Decreto n. 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

18. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei n. 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

19. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei n. 13.709/2018; art. 2º, incisos II e III do Decreto n. 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

20. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, “g”, art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei n. 13.709/2018; art. 2º, incisos III e IV, do Decreto n. 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ n. 54/2023)

21. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea ‘g’, e art. 52, § 7º, da Lei n. 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto n. 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

DIMENSÃO 5

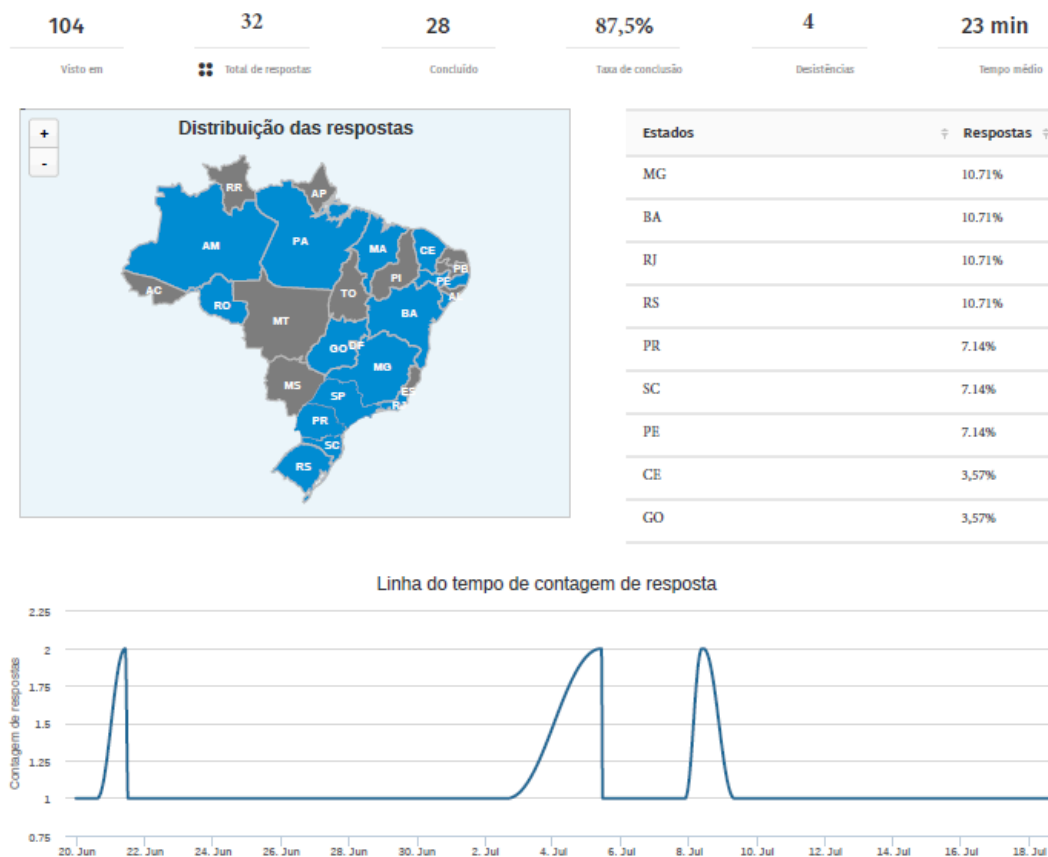
22. A organização atende ao princípio da transparência? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei n. 8.159/1991; Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea “e”, da Lei n. 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ n. 54/2023)

23. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas “a” e “d”, da Lei n. 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

24. A designação do encarregado e suas informações de contato, foram publicizadas em algum meio de comunicação oficial? (art. 5º, inciso VIII, art. 23, art. 41 da Lei n. 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)

25. A Política de Privacidade da instituição está publicizada? (art. 2º, inciso VIII, da Lei n. 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei n. 13.709/2018; art. 3º, inciso XI, do Decreto n. 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

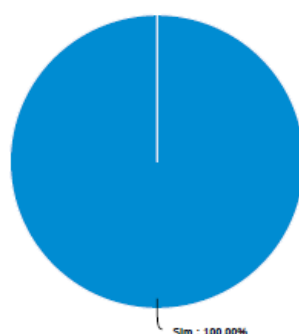
APÊNDICE K – Relatório gerado pela plataforma questionpro após a segunda rodada do método *delphi*



Termo de Consentimento Livre e Esclarecido: A sua participação neste estudo é totalmente voluntária e não implica em nenhum custo financeiro. Todas as informações que você fornecer serão tratadas de forma anônima e confidencial, garantindo sua privacidade. A pesquisa foi submetida ao Comitê de Ética sob o número de protocolo 78884624.3.0000.5188. Para baixar este TCLE em formato PDF clique no link abaixo:

https://drive.google.com/uc?export=download&id=1Ei35xuMbvb54nRycgxnNqj23O5zVAM_f

Ao assinalar "SIM" abaixo, você declara seu consentimento livre e esclarecido para participar deste estudo, atestando que compreendeu integralmente as informações fornecidas e concorda em colaborar voluntariamente. Ao assinalar "NÃO", você recusa a participação neste estudo.



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
Sim	28	100%					
Não	0	0%					
Total	28	100 %					

Dimensão 1: Governança de Dados e Boas Práticas

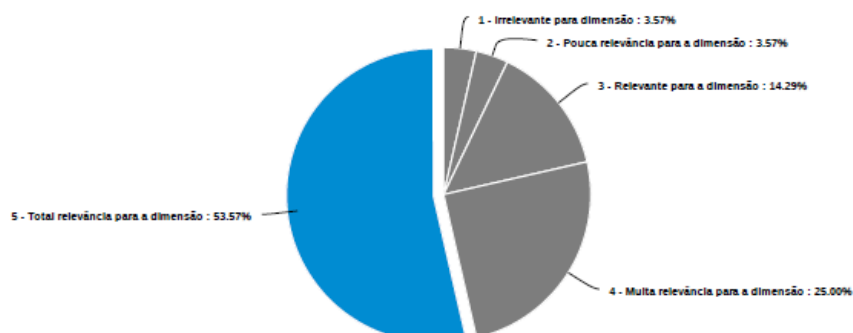
1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei nº 13.709/2018; Decreto nº 9.637/2018 e Decreto nº 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

Statement	1 - Irrelevante para a dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 3.57%	1 3.57%	4 14.29%	7 25%	15 53.57%	28 100%



Pergunta	Contagem	Pontuação	1 - Irrelevante para a dimensão	2 - Pouca relevância para a dimensão	3 - Relevante para a dimensão	4 - Muita relevância para a dimensão	5 - Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4,21					
Média		4.21					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1 - Irrelevante para a dimensão	1	3.57%					
2 - Pouca relevância para a dimensão	1	3.57%					
3 - Relevante para a dimensão	4	14.29%					
4 - Muita relevância para a dimensão	7	25%					
5 - Total relevância para a dimensão	15	53.57%					
Total	28	n = 28					

Dimensão 1: Governança de Dados e Boas Práticas

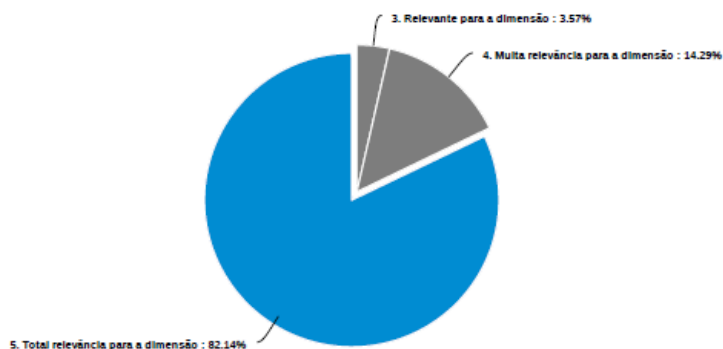
2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei nº 13.709/2018; Lei nº 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	0 0%	1 3.57%	4 14.29%	23 82.14%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4,79					
Média		4,79					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	1	3.57%					
4. Muita relevância para a dimensão	4	14.29%					
5. Total relevância para a dimensão	23	82.14%					
Total	28	n = 28					

Dimensão 1: Governança de Dados e Boas Práticas

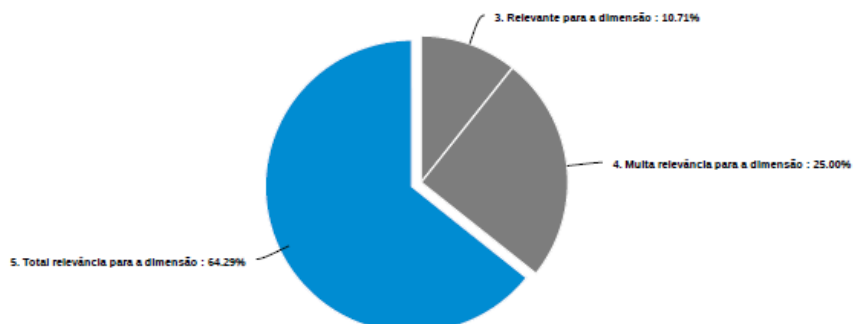
3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis? (art. 50 da Lei nº 13.709/2018; art. 15 do Decreto nº 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto nº 10.046/2019)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	0 0%	3 10.71%	7 25%	18 64.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4,54					
Média		4.54					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	3	10.71%					
4. Muita relevância para a dimensão	7	25%					
5. Total relevância para a dimensão	18	64.29%					
Total	28	n = 28					

Dimensão 1: Governança de Dados e Boas Práticas

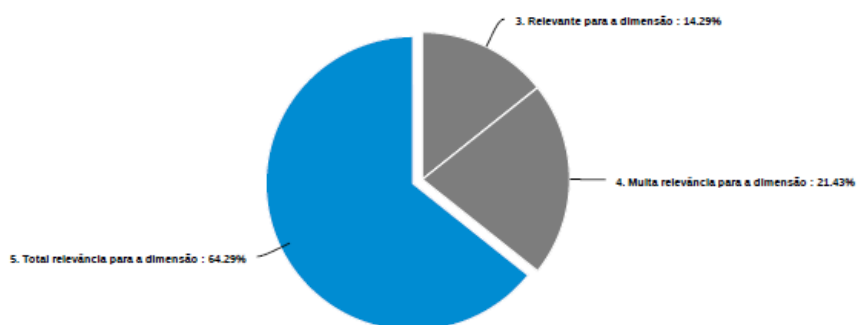
4. A instituição possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei nº 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI Nº 852/2023 e art. 4º, art. 13 e art. 20 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	0 0%	4 14.29%	6 21.43%	18 64.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4,5					
Média		4,5					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	6	21.43%					
5. Total relevância para a dimensão	18	64.29%					
Total	28	n = 28					

Dimensão 1: Governança de Dados e Boas Práticas

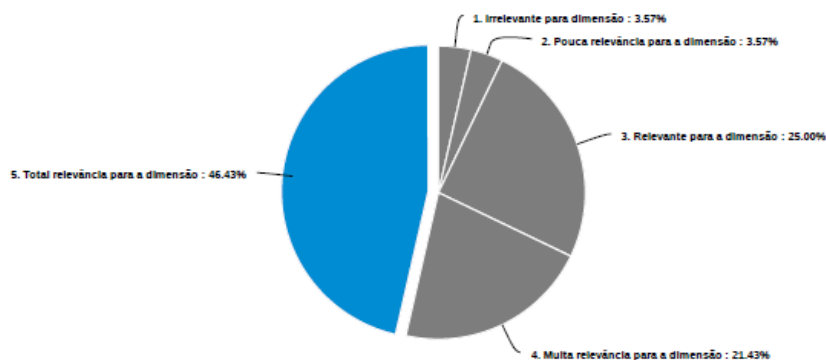
5. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei nº 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	1 3.57%	1 3.57%	7 25%	6 21.43%	13 46.43%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4,04					
Média		4,04					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	3.57%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	7	25%					
4. Muita relevância para a dimensão	6	21.43%					
5. Total relevância para a dimensão	13	46.43%					
Total	28	n = 28					

Dimensão 1: Governança de Dados e Boas Práticas

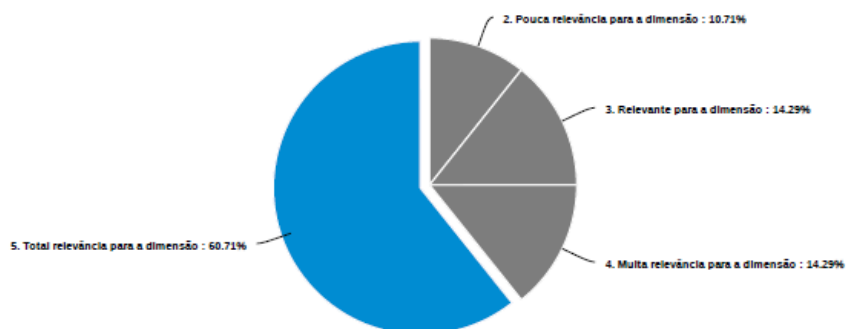
6. A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados assuma outras funções que possam gerar conflitos de interesse? (Art. 50 da Lei 13.709/2018; Art. 5º e 7º, § 1º da Lei 14.133/2021)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	0 0%	3 10.71%	4 14.29%	4 14.29%	17 60.71%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?	28	4.25					
Média		4.25					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Governança de Dados e Boas Práticas?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	10.71%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	4	14.29%					
5. Total relevância para a dimensão	17	60.71%					
Total	28	n = 28					

Dimensão 2: Políticas e Processos de Tratamento de Dados

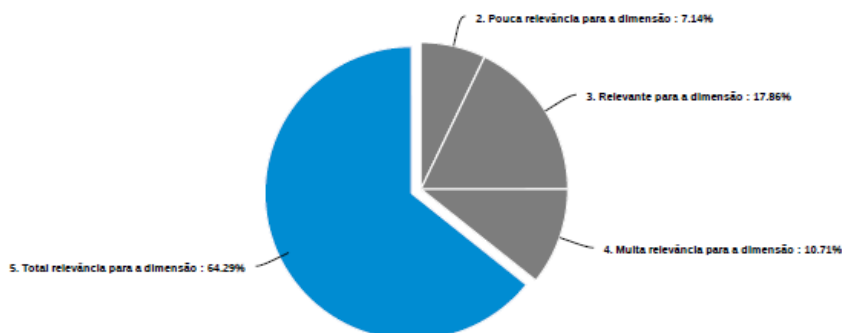
1. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação? (art. 10, § 2º, da Lei nº 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	2 7.14%	5 17.86%	3 10.71%	18 64.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	28	4.32					
Média		4.32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	7.14%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	3	10.71%					
5. Total relevância para a dimensão	18	64.29%					
Total	28	n = 28					

Dimensão 2: Políticas e Processos de Tratamento de Dados

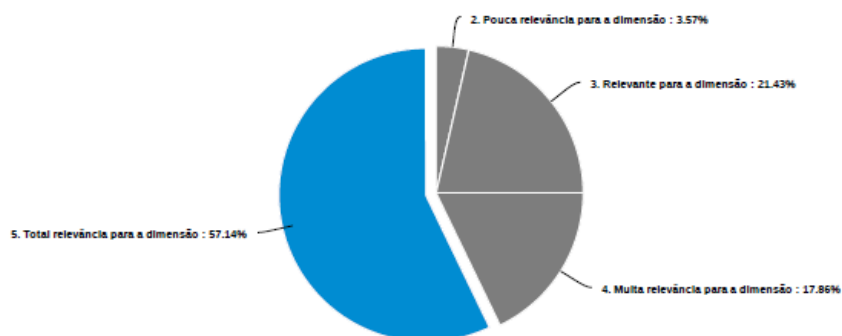
2. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei nº 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	1 3.57%	6 21.43%	5 17.86%	16 57.14%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	28	4,29					
Média		4,29					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	6	21.43%					
4. Muita relevância para a dimensão	5	17.86%					
5. Total relevância para a dimensão	16	57.14%					
Total	28	n = 28					

Dimensão 2: Políticas e Processos de Tratamento de Dados

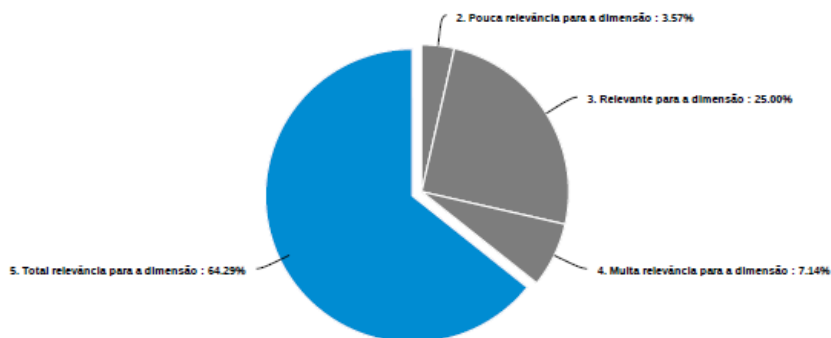
3. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei nº 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	1 3.57%	7 25%	2 7.14%	18 64.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	28	4.32					
Média		4.32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	7	25%					
4. Muita relevância para a dimensão	2	7.14%					
5. Total relevância para a dimensão	18	64.29%					
Total	28	n = 28					

Dimensão 2: Políticas e Processos de Tratamento de Dados

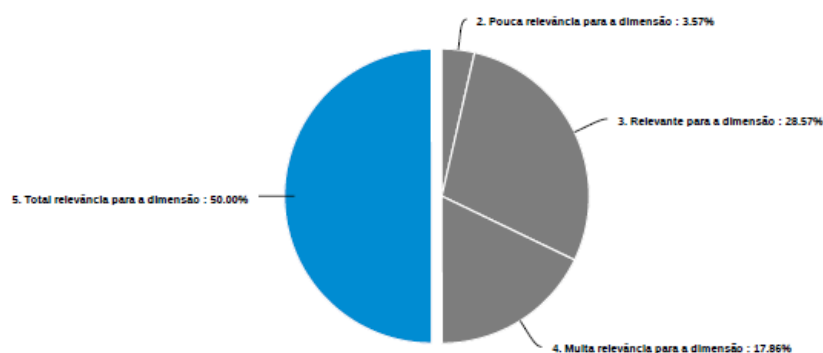
4. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais? (art. 2º, inciso IX, da Lei nº 7.232/1984; art. 4º da Lei nº 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei nº 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	1 3.57%	8 28.57%	5 17.86%	14 50%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	28	4,14					
Média		4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	8	28.57%					
4. Muita relevância para a dimensão	5	17.86%					
5. Total relevância para a dimensão	14	50%					
Total	28	n = 28					

Dimensão 2: Políticas e Processos de Tratamento de Dados

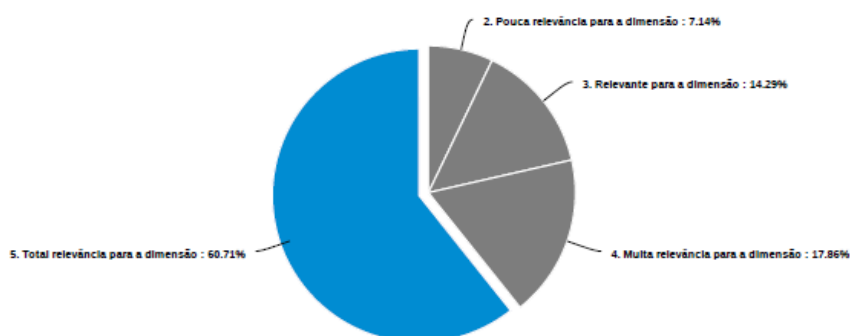
5. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei nº 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	0 0%	2 7.14%	4 14.29%	5 17.86%	17 60.71%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?	28	4.32					
Média		4.32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Políticas e Processos de Tratamento de Dados?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	7.14%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	5	17.86%					
5. Total relevância para a dimensão	17	60.71%					
Total	28	n = 28					

Dimensão 3: Treinamento e Conscientização

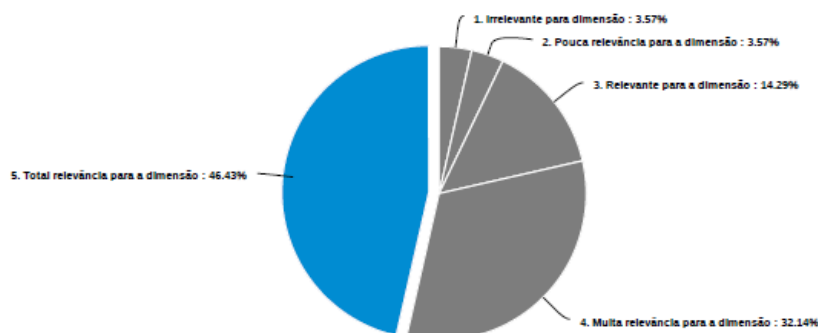
1. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização, sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei nº 7.232/1984; art. 50 da Lei nº 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto nº 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 3.57%	1 3.57%	4 14.29%	9 32.14%	13 46.43%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	28	4,14					
	Média	4,14					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	3.57%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	9	32.14%					
5. Total relevância para a dimensão	13	46.43%					
Total	28	n = 28					

Dimensão 3: Treinamento e Conscientização

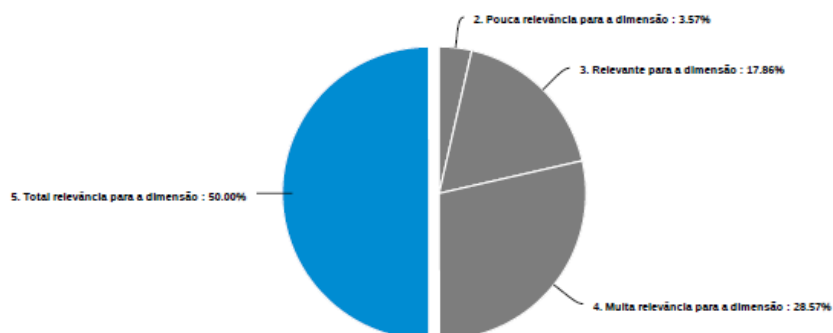
2. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei nº 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	0 0%	1 3.57%	5 17.86%	8 28.57%	14 50%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	28	4.25					
Média		4.25					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	8	28.57%					
5. Total relevância para a dimensão	14	50%					
Total	28	n = 28					

Dimensão 3: Treinamento e Conscientização

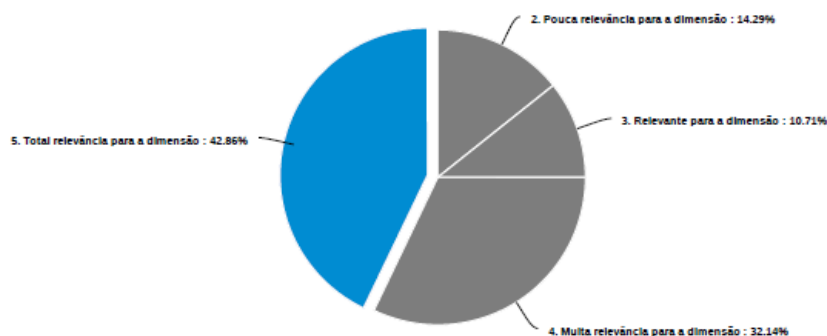
3. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais, recebem treinamentos e capacitações específicas sobre o tema? (art. 50 da Lei nº 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	0 0%	4 14.29%	3 10.71%	9 32.14%	12 42.86%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	28	4,04					
	Média	4,04					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	4	14.29%					
3. Relevante para a dimensão	3	10.71%					
4. Muita relevância para a dimensão	9	32.14%					
5. Total relevância para a dimensão	12	42.86%					
Total	28	n = 28					

Dimensão 3: Treinamento e Conscientização

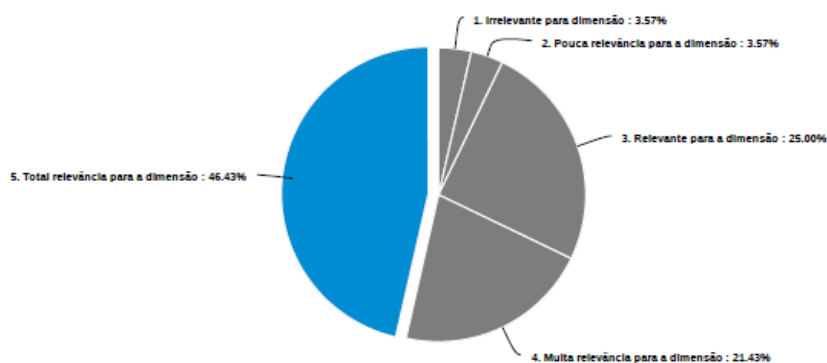
4. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais? (arts. 42-45, art. 50 e arts. 52-54 da Lei nº 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	1 3,57%	1 3,57%	7 25%	6 21,43%	13 46,43%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	28	4,04					
Média		4,04					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	3,57%					
2. Pouca relevância para a dimensão	1	3,57%					
3. Relevante para a dimensão	7	25%					
4. Muita relevância para a dimensão	6	21,43%					
5. Total relevância para a dimensão	13	46,43%					
Total	28	n = 28					

Dimensão 3: Treinamento e Conscientização

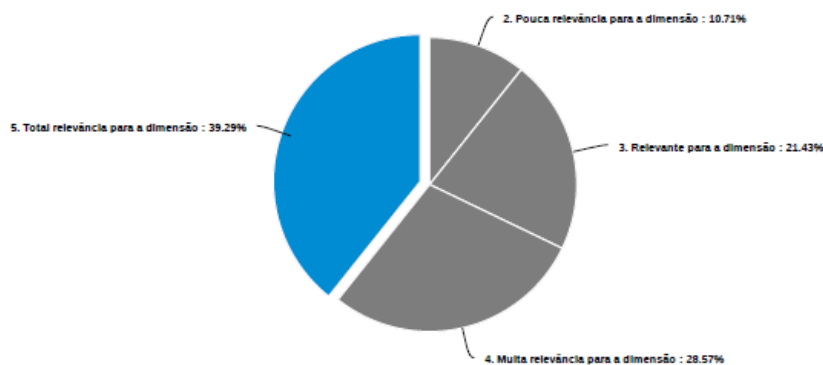
5. A organização promove capacitação quanto aos procedimentos adequados para a gestão de incidentes, determinando a melhor forma de planejar, gerenciar e comunicar os incidentes de segurança da informação? (art. 48 e art. 50 da Lei nº 13.709/2018; art. 3º, incisos VII e IX, do Decreto nº 9.637/2018; item 6.13 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.25, 5.26, 5.27 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27035:2023; art. 15, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	0 0%	3 10.71%	6 21.43%	8 28.57%	11 39.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?	28	3.96					
Média		3.96					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Treinamento e Conscientização?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	10.71%					
3. Relevante para a dimensão	6	21.43%					
4. Muita relevância para a dimensão	8	28.57%					
5. Total relevância para a dimensão	11	39.29%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

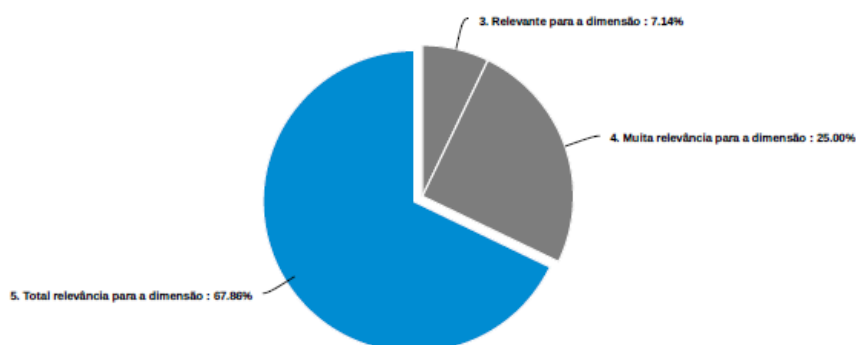
1. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar? (art. 4º, inciso V, da Lei 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas "b" e "g", art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei nº 13.709/2018; Decreto nº 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI Nº 852/2023 e art. 14 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	0 0%	2 7.14%	7 25%	19 67.86%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4,61					
Média		4,61					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	2	7.14%					
4. Muita relevância para a dimensão	7	25%					
5. Total relevância para a dimensão	19	67.86%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

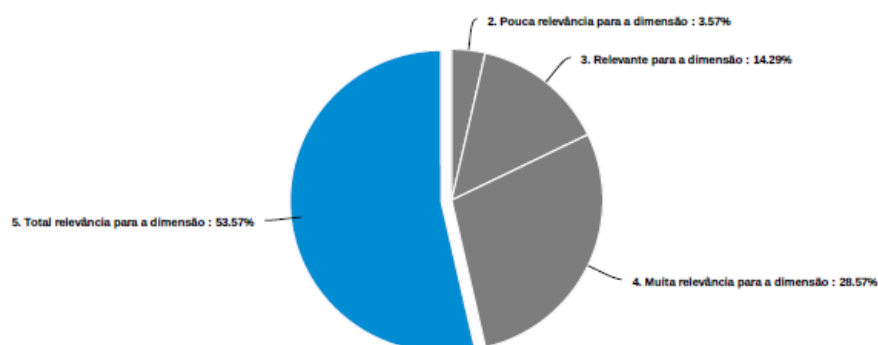
2. A organização usa criptografia para proteger os dados pessoais? (art. 11, inciso II, alínea "g", art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea 'c', da Lei nº 13.709/2018; art. 2º, inciso III, do Decreto nº 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	1 3.57%	4 14.29%	8 28.57%	15 53.57%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4.32					
Média		4.32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Percentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	8	28.57%					
5. Total relevância para a dimensão	15	53.57%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

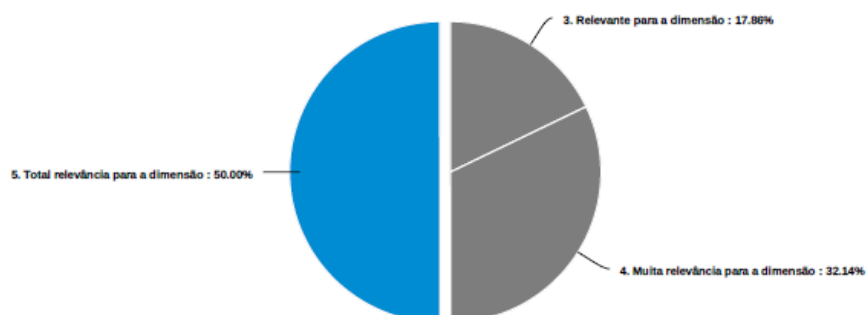
3. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei nº 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	0 0%	5 17.86%	9 32.14%	14 50%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4.32					
Média		4.32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	9	32.14%					
5. Total relevância para a dimensão	14	50%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

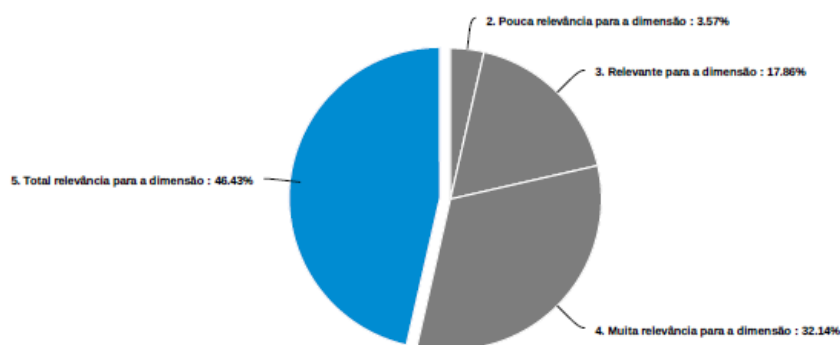
4. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei nº 13.709/2018; art. 2º, incisos II e III do Decreto nº 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	1 3.57%	5 17.86%	9 32.14%	13 46.43%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4.21					
Média		4.21					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	9	32.14%					
5. Total relevância para a dimensão	13	46.43%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

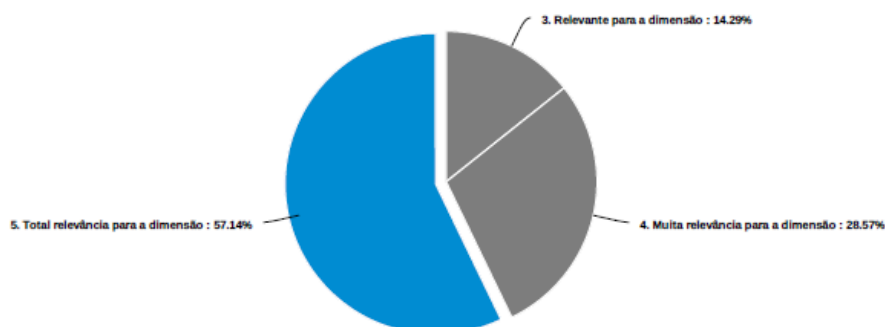
5. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, "g", art. 13, art. 18, art. 19, art. 25, art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei nº 13.709/2018; art. 2º, incisos III e IV, do Decreto nº 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	0 0%	4 14.29%	8 28.57%	16 57.14%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4,43					
Média		4,43					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	4	14.29%					
4. Muita relevância para a dimensão	8	28.57%					
5. Total relevância para a dimensão	16	57.14%					
Total	28	n = 28					

Dimensão 4: Segurança da Informação e Tecnologia

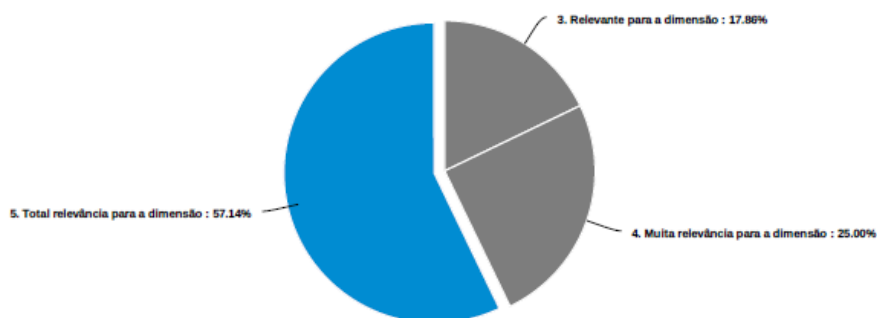
6. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea 'g', e art. 52, § 7º, da Lei nº 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto nº 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	0 0%	0 0%	5 17.86%	7 25%	16 57.14%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?	28	4.39					
Média		4.39					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Segurança da Informação e Tecnologia?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	7	25%					
5. Total relevância para a dimensão	16	57.14%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

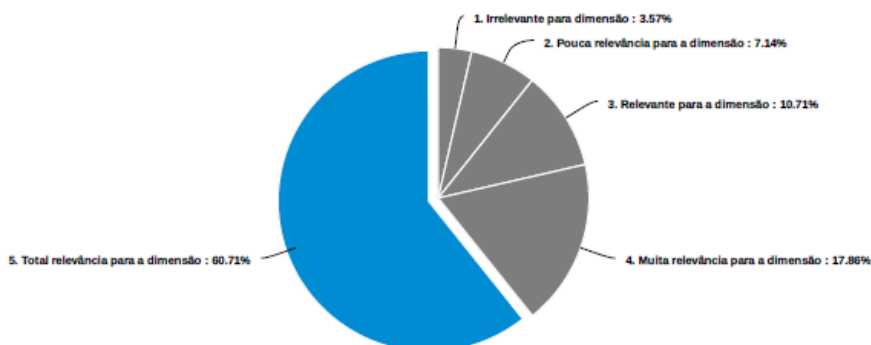
1. A organização atende ao princípio da transparência? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei nº 8.159/1991; Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea "e", da Lei nº 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	1 3.57%	2 7.14%	3 10.71%	5 17.86%	17 60.71%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	4.25					
Média		4.25					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	1	3.57%					
2. Pouca relevância para a dimensão	2	7.14%					
3. Relevante para a dimensão	3	10.71%					
4. Muita relevância para a dimensão	5	17.86%					
5. Total relevância para a dimensão	17	60.71%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

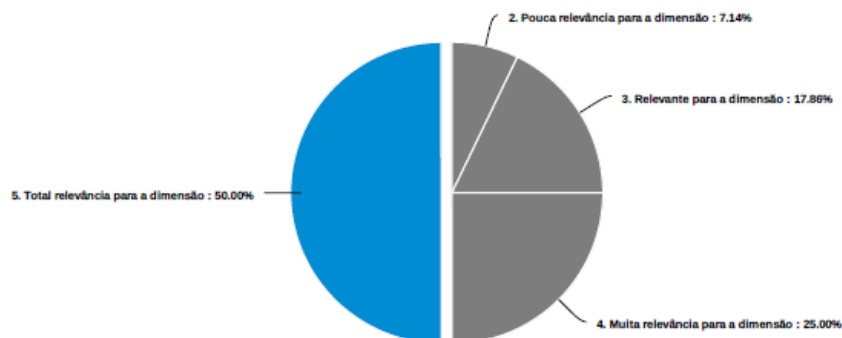
2. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei nº 12.527/2011; Decreto nº 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas "a" e "d", da Lei nº 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	2 7.14%	5 17.86%	7 25%	14 50%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	4.18					
Média		4.18					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	2	7.14%					
3. Relevante para a dimensão	5	17.86%					
4. Muita relevância para a dimensão	7	25%					
5. Total relevância para a dimensão	14	50%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

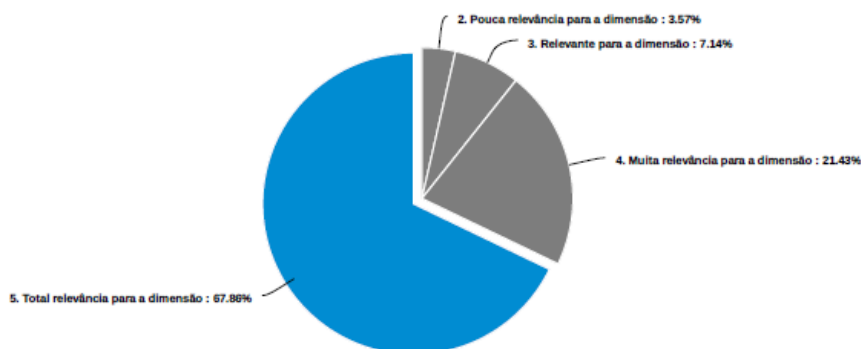
3. A designação do encarregado e suas informações de contato, foram publicizadas em algum meio de comunicação oficial?? (art. 5º, inciso VIII, art. 23, art. 41 da Lei nº 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME nº 117/2020)

Statement	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	1 3.57%	2 7.14%	6 21.43%	19 67.86%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	4,54					
Média		4,54					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	1	3.57%					
3. Relevante para a dimensão	2	7.14%					
4. Muita relevância para a dimensão	6	21.43%					
5. Total relevância para a dimensão	19	67.86%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

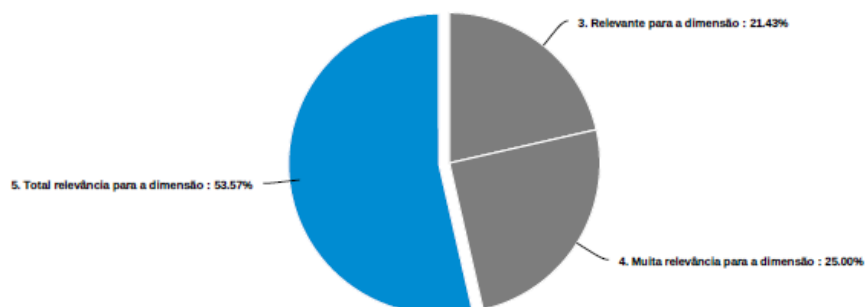
4. A Política de Privacidade da instituição está publicizada? (art. 2º, inciso VIII, da Lei 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei nº 13.709/2018; art. 3º, inciso XI, do Decreto nº 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	0 0%	6 21,43%	7 25%	15 53,57%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	4,32					
Média		4,32					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para dimensão	0	0%					
2. Pouca relevância para a dimensão	0	0%					
3. Relevante para a dimensão	6	21,43%					
4. Muita relevância para a dimensão	7	25%					
5. Total relevância para a dimensão	15	53,57%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

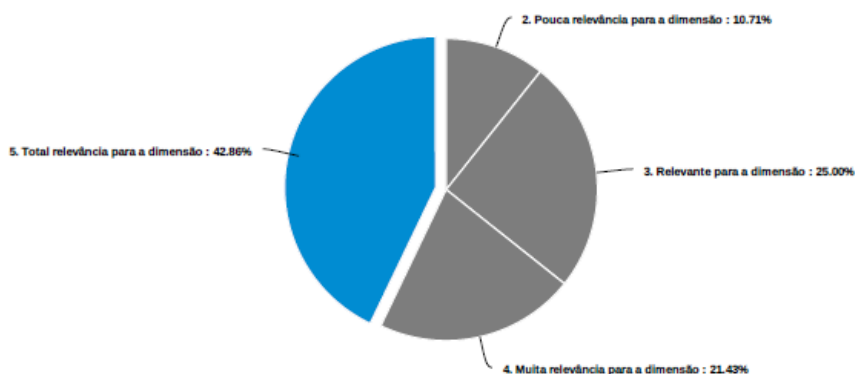
5. A organização estabeleceu procedimentos de comunicação com a Agência Nacional de Proteção de Dados (ANPD) e o titular de dados em caso de ocorrência de incidentes de segurança, que possam acarretar risco ou dano relevante aos titulares? (art. 7º, inciso X, § 5, art. 15, inciso III, art. 18, art. 19, art. 26, § 2º, art. 27, art. 29, arts. 30-32, art. 36, art. 41, art. 46, art. 48, art. 50, § 2º, inciso I, alínea 'g', art. 51 e art. 52 da Lei nº 13.709/2018; itens 6.13, 7.3, 8.3 e 8.4.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.24, 5.26 e 5.27 da ABNT NBR ISO/IEC 27002:2022 e art. 15 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	3 10.71%	7 25%	6 21.43%	12 42.86%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	3.96					
Média		3.96					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	10.71%					
3. Relevante para a dimensão	7	25%					
4. Muita relevância para a dimensão	6	21.43%					
5. Total relevância para a dimensão	12	42.86%					
Total	28	n = 28					

Dimensão 5: Acesso à Informação e Transparência

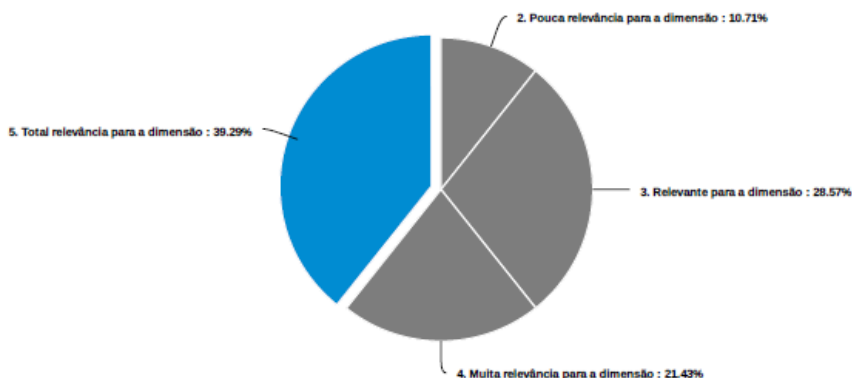
6. A organização possui programa, plano de comunicação ou documento similar que abarque as diretrizes das legislações e normas referentes ao tratamento e proteção de dados e informações pessoais? (art. 2º, art. 6º, inciso X, art. 18, art. 19, art. 27, arts. 29-32, art. 48 e art. 50 da Lei nº 13.709/2018; itens 5.5.4, 8.4.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019; itens 6.6 e 6.8 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 24 da Resolução CONARQ nº 54/2023)

Statement	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão	Overall
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	0 0%	3 10.71%	8 28.57%	6 21.43%	11 39.29%	28 100%



Pergunta	Contagem	Pontuação	1. Irrelevante para a dimensão	2. Pouca relevância para a dimensão	3. Relevante para a dimensão	4. Muita relevância para a dimensão	5. Total relevância para a dimensão
Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?	28	3.89					
Média		3.89					

Na sua opinião, qual a relevância dessa pergunta para a dimensão Acesso à Informação e Transparência?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Irrelevante para a dimensão	0	0%					
2. Pouca relevância para a dimensão	3	10.71%					
3. Relevante para a dimensão	8	28.57%					
4. Muita relevância para a dimensão	6	21.43%					
5. Total relevância para a dimensão	11	39.29%					
Total	28	n = 28					

APÊNDICE L – Instrumento de medição do MMTDP**TRATAMENTO DE DADOS E INFORMAÇÕES PESSOAIS
NA INSTITUIÇÃO**

Considerando a Constituição Federal de 1988;

Considerando a Lei nº 7.232/1984 (Política Nacional de Informática); a Lei nº 8.159/1991 (Lei de Arquivos); a Lei nº 10.741/2003 (Estatuto do Idoso); a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados);

Considerando o Decreto nº 7.724/2012, o Decreto nº 9.637/2018, o Decreto nº 10.046/2019 e o Decreto-Lei nº 2.848/1940 (Código Civil);

Considerando a Norma ABNT NBR ISO/IEC 27701:2019, a Norma ABNT NBR ISO/IEC 27014:2021, a Norma ABNT NBR ISO/IEC 27002:2022, a Norma ABNT NBR ISO/IEC 27005:2023, a Norma ABNT NBR ISO/IEC 27035:2023 e a Norma ABNT NBR ISO/IEC 29134:2023;

Considerando a Instrução Normativa GSI/PR 1/2020 e a Instrução Normativa SGD/ME nº 117/2020;

Considerando a Resolução CONARQ nº 54/2023;

Solicito, de forma objetiva, a esta instituição o fornecimento das informações pertinentes ao questionário abaixo, conforme as normativas mencionadas.

Nome da Universidade

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais?

- ☐ 1. Não, a organização ainda não elaborou um programa, plano de governança ou documento com esse direcionamento.
- ☐ 2. Sim, a organização está em fase inicial de elaboração do programa, plano de governança ou documento equivalente com esse direcionamento.

- ☐ 3. Sim, a organização já elaborou um programa, plano de governança ou documento equivalente com esse direcionamento, mas este ainda não foi totalmente implementado.
- ☐ 4. Sim, a organização elaborou e implementou o programa, plano de governança ou documento equivalente com esse direcionamento, mas este documento não é monitorado regularmente.
- ☐ 5. Sim, a organização elaborou e implementou completamente o programa, plano de governança ou documento equivalente com esse direcionamento, e está monitorando regularmente para garantir a conformidade contínua com as regulamentações sobre tratamento e proteção de dados pessoais.

2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)?

- ☐ 1. Não, a organização não designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO.
- ☐ 2. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas suas funções não estão claramente definidas.
- ☐ 3. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas sua atuação é limitada e/ou não é amplamente reconhecida internamente.
- ☐ 4. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, com papel reconhecido, mas ainda há lacunas na sua atuação ou na integração com outras áreas.
- ☐ 5. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, que atua de forma efetiva, integrada às áreas, e com reconhecimento e suporte da alta administração.

3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis?

- ☐ 1. Não, a organização não possui um comitê ou equivalente.
- ☐ 2. Sim, a organização possui um comitê, mas não está ativo ou não tem funções definidas.
- ☐ 3. Sim, a organização possui um comitê ativo, mas ele se concentra apenas em tarefas pontuais ou de suporte, sem uma atuação estratégica.

- ☐ 4. Sim, a organização possui um comitê ativo com funções bem definidas, e está desenvolvendo sua capacidade de atuação estratégica e integração com todas as áreas relevantes.
- ☐ 5. Sim, a organização possui um comitê ativo, com funções bem definidas, que cobre todas as áreas necessárias e está em plena operação.

4. A organização possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares?

- ☐ 1. Não, a organização ainda não possui uma Política de Privacidade.
- ☐ 2. Sim, a instituição está desenvolvendo uma Política de Privacidade, mas ela ainda está em fase de elaboração.
- ☐ 3. Sim, a instituição possui uma Política de Privacidade, mas não é aplicada de maneira consistente.
- ☐ 4. Sim, a instituição possui uma Política de Privacidade, que é aplicada e divulgada, mas ainda precisa de melhorias.
- ☐ 5. Sim, a instituição possui uma Política de Privacidade, que é divulgada, aplicada de forma consistente e regularmente revisada.

5. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição?

- ☐ 1. Não, a organização não identificou o compartilhamento ou transferência de dados pessoais.
- ☐ 2. Sim, a organização começou a mapear o compartilhamento ou transferência de dados pessoais, mas o processo é incompleto ou informal.
- ☐ 3. Sim, a organização identificou as principais áreas onde ocorre compartilhamento ou transferência de dados pessoais, mas ainda não há uma visão abrangente ou documentada.
- ☐ 4. Sim, a organização identificou e documentou o compartilhamento e a transferência de dados pessoais, mas faltam procedimentos formais para monitoramento ou controle.
- ☐ 5. Sim, a organização identificou, documentou e implantou procedimentos formais para monitorar e controlar o compartilhamento e a transferência de dados pessoais, com revisões regulares para garantir conformidade.

6. A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados (EPD) assuma outras funções que possam gerar conflitos de interesse?

- ☐ 1. Não, a organização não segue o princípio da segregação das funções, e o Encarregado de Proteção de Dados (EPD) acumula funções que claramente geram conflitos de interesse.
- ☐ 2. Sim, a organização reconhece a importância da segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda acumula outras funções que podem resultar em conflitos de interesse.
- ☐ 3. Sim, a organização implementa a segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda desempenha algumas atividades que podem potencialmente criar conflitos de interesse.
- ☐ 4. Sim, a organização implementou a segregação das funções, garantindo que o Encarregado de Proteção de Dados (EPD) tenha autonomia na função. Entretanto, interferências de órgãos superiores comprometem parcialmente essa autonomia.
- ☐ 5. Sim, a organização assegura que o Encarregado de Proteção de Dados (EPD) tenha total autonomia e dedicação exclusiva à sua função, sem acumular outras atividades que possam comprometer sua independência ou gerar conflitos de interesse, e sem interferências de órgãos superiores na tomada de decisões.

7. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação?

- ☐ 1. Não, a organização não realizou a identificação das categorias de dados pessoais nem dos titulares.
- ☐ 2. Sim, a organização identificou algumas categorias de dados pessoais e titulares, mas de forma limitada e incompleta.
- ☐ 3. Sim, a organização identificou as principais categorias de dados pessoais e titulares, mas ainda há lacunas ou falta de documentação completa.
- ☐ 4. Sim, a organização identificou e documentou as categorias de dados pessoais e titulares, mas há necessidade de revisões, monitoramento ou melhorias no processo.
- ☐ 5. Sim, a organização identificou, documentou e mantém um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação.

8. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento

de dados pessoais da instituição?

- ☐ 1. Não, a organização não identificou os agentes (controladores e operadores) de tratamento de dados pessoais.
- ☐ 2. Sim, a organização iniciou a identificação dos agentes de tratamento de dados pessoais, mas o processo é incompleto ou informal.
- ☐ 3. Sim, a organização identificou os principais agentes de tratamento de dados pessoais, mas ainda há áreas sem identificação clara ou documentação adequada.
- ☐ 4. Sim, a organização identificou e documentou os agentes de tratamento de dados pessoais, mas o processo de monitoramento ou revisão ainda precisa ser aprimorado.
- ☐ 5. Sim, a organização identificou, documentou e mantém um processo formal e contínuo para monitorar e revisar os agentes de tratamento de dados pessoais, garantindo conformidade com as normas.

9. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais?

- ☐ 1. Não, a organização não identificou os processos e atividades operacionais que lidam com dados pessoais.
- ☐ 2. Sim, a organização começou a identificar os processos e atividades operacionais que lidam com dados pessoais, mas o mapeamento é parcial ou informal.
- ☐ 3. Sim, a organização identificou os principais processos e atividades que lidam com dados pessoais, mas ainda faltam detalhes ou documentação completa.
- ☐ 4. Sim, a organização identificou e documentou os processos e atividades operacionais que lidam com dados pessoais, mas existem áreas que requerem revisões ou melhorias.
- ☐ 5. Sim, a organização identificou, documentou e mantém um processo contínuo para monitorar, revisar e melhorar os processos e atividades operacionais que lidam com dados pessoais.

10. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais?

- ☐ 1. Não, a organização não possui mecanismos formais para garantir os direitos dos titulares de dados pessoais.

- ☐ 2. Sim, a organização começou a desenvolver mecanismos para garantir os direitos dos titulares, mas estes ainda são limitados ou informais.
- ☐ 3. Sim, a organização possui mecanismos formais para garantir os direitos dos titulares, mas eles não são abrangentes ou totalmente implementados.
- ☐ 4. Sim, a organização possui mecanismos formais que garantem os direitos dos titulares, mas esses mecanismos existentes não são revisados ou monitorados regularmente.
- ☐ 5. Sim, a organização possui mecanismos formais, abrangentes e bem implementados que garantem os direitos dos titulares de dados pessoais, com revisões e melhorias contínuas.

11. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário?

- ☐ 1. Não, a organização não possui regras operacionais para esconder dados pessoais sensíveis, nem utiliza técnicas como mascaramento, pseudonimização ou anonimização.
- ☐ 2. Sim, a organização reconhece a importância de proteger dados sensíveis, mas as regras operacionais e técnicas de mascaramento, pseudonimização ou anonimização não são implementadas ou são aplicadas de forma inconsistente.
- ☐ 3. Sim, a organização desenvolveu regras operacionais e começou a aplicar técnicas de mascaramento, pseudonimização ou anonimização, mas a aplicação é parcial ou não abrange todos os dados sensíveis.
- ☐ 4. Sim, a organização possui regras operacionais bem estabelecidas para esconder dados pessoais sensíveis, utilizando técnicas adequadas, mas há áreas que necessitam de aprimoramento e monitoramento.
- ☐ 5. Sim, a organização estabelece e aplica rigorosamente regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de forma consistente, abrangente e monitorada regularmente.

12. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais?

- ☐ 1. Não, a organização não possui programas ou planos de capacitação sobre tratamento e proteção de dados e informações pessoais.

- ☐ 2. Sim, a organização possui programas ou planos de capacitação, mas estes atendem aspectos pontuais relacionados ao tratamento e proteção de dados e informações pessoais.
- ☐ 3. Sim, a organização tem programas ou planos de capacitação que cobrem questões essenciais sobre o tratamento e a proteção de dados e informações pessoais, mas algumas áreas ainda precisam ser aprimoradas para garantir a efetividade do treinamento.
- ☐ 4. Sim, a organização possui programas de capacitação bem estruturados, que abrangem as questões relevantes sobre o tratamento e a proteção de dados e informações pessoais, mas os programas não são atualizados nem monitorados regularmente.
- ☐ 5. Sim, a organização possui programas ou planos de capacitação completos e regulares, cobrindo o tratamento e a proteção de dados e informações pessoais, com revisão e atualização contínuas para garantir a eficácia.

13. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades?

- ☐ 1. Não, a organização não realiza conscientização dos agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades.
- ☐ 2. Sim, a organização começou a conscientizar seus agentes de tratamento de dados pessoais, mas as atividades são pontuais e não cobrem todas as responsabilidades.
- ☐ 3. Sim, a organização realiza atividades de conscientização sobre papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas ainda há lacunas na abrangência ou na frequência dessas atividades.
- ☐ 4. Sim, a organização possui programas de conscientização estabelecidos, que cobrem os papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas a aplicação não é monitorada regularmente.
- ☐ 5. Sim, a organização conscientiza plenamente seus agentes de tratamento de dados pessoais sobre todos os seus papéis e responsabilidades, com programas contínuos e abrangentes de capacitação.

14. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais recebem treinamentos e capacitações específicas sobre o tema?

- ☐ 1. Não, os colaboradores, terceirizados e parceiros não recebem treinamentos ou capacitações sobre tratamento e proteção de dados pessoais.
- ☐ 2. Sim, alguns colaboradores, terceirizados ou parceiros recebem treinamentos sobre tratamento de dados pessoais, mas de forma pontual e não abrange todos os envolvidos.
- ☐ 3. Sim, a organização começou a oferecer treinamentos específicos para colaboradores, terceirizados e parceiros sobre tratamento de dados pessoais, mas ainda não são abrangentes ou regulares.
- ☐ 4. Sim, a organização possui programas de treinamento específicos para colaboradores, terceirizados e parceiros, cobrindo assuntos relacionados ao tratamento e proteção de dados pessoais, mas ainda há melhorias necessárias nesse programa.
- ☐ 5. Sim, a organização oferece treinamentos e capacitações regulares e específicos para todos os colaboradores, terceirizados e parceiros, garantindo que todos estejam capacitados para tratar dados e informações pessoais de forma segura e conforme as regulamentações.

15. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais?

- ☐ 1. Não, a organização não realiza conscientização sobre esses riscos.
- ☐ 2. Sim, a organização começou a conscientizar sobre os riscos, mas as atividades são esporádicas e não cobrem todos os aspectos críticos.
- ☐ 3. Sim, a organização realiza conscientização sobre os riscos de forma regular, mas ainda há lacunas na cobertura de todos os riscos ou áreas específicas de tratamento de dados pessoais.
- ☐ 4. Sim, a organização possui um programa regular de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, mas com necessidade de melhorias em algumas áreas.
- ☐ 5. Sim, a organização realiza conscientização contínua e abrangente sobre todos os riscos associados ao tratamento inadequado de dados pessoais.

16. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar?

- ☐ 1. Não, a organização não definiu nem elaborou uma Política de Segurança da Informação ou documento similar.

- ☐ 2. Sim, a organização começou a elaborar uma Política de Segurança da Informação ou instrumento similar, mas ainda está em fase de elaboração.
- ☐ 3. Sim, a organização elaborou uma Política de Segurança da Informação ou instrumento similar, mas sua implementação é parcial ou não foi formalmente adotada.
- ☐ 4. Sim, a organização elaborou e implementou uma Política de Segurança da Informação ou instrumento similar, mas ainda não realiza monitoramento ou revisões regulares.
- ☐ 5. Sim, a organização elaborou, implementou e monitora regularmente a Política de Segurança da Informação ou instrumento similar, assegurando conformidade contínua com as normas e regulamentações aplicáveis.

17. A organização usa criptografia para proteger os dados pessoais?

- ☐ 1. Não, a organização não utiliza criptografia para proteger os dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância da criptografia, mas sua aplicação é limitada ou inconsistente.
- ☐ 3. Sim, a organização usa criptografia para proteger alguns dados pessoais, mas não de forma abrangente ou em todas as áreas necessárias.
- ☐ 4. Sim, a organização usa criptografia de maneira abrangente para proteger os dados pessoais, mas ainda existem áreas que necessitam de melhorias ou revisões.
- ☐ 5. Sim, a organização utiliza criptografia de forma consistente e abrangente para proteger todos os dados pessoais, com monitoramento contínuo e revisões regulares para garantir a segurança.

18. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais?

- ☐ 1. Não, a organização não possui gestão de backup nem trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais.
- ☐ 2. Sim, a organização começou a desenvolver um sistema de gestão de backup e trilhas de auditoria, mas de forma limitada ou informal.
- ☐ 3. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria, mas ele não cobre todas as áreas necessárias ou não é aplicado de forma consistente.

- ☐ 4. Sim, a organização possui gestão de backup e trilhas de auditoria abrangentes, mas ainda há necessidade de melhorias ou maior integração com as práticas de gestão de dados.
- ☐ 5. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria robusto e bem implementado, que garante a proteção e integridade dos dados e informações pessoais em todas as fases do ciclo de vida.

19. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades?

- ☐ 1. Não, a organização não coleta nem analisa informações relacionadas a vulnerabilidades e ameaças à segurança da informação.
- ☐ 2. Sim, a organização começou a coletar e analisar informações sobre vulnerabilidades e ameaças, mas o processo é informal ou limitado.
- ☐ 3. Sim, a organização coleta e analisa informações sobre vulnerabilidades e ameaças à segurança da informação, mas ainda não possui um processo estruturado para gestão de vulnerabilidades.
- ☐ 4. Sim, a organização possui um processo estruturado para coletar, analisar e gerir vulnerabilidades e ameaças à segurança da informação, mas precisa de melhorias ou maior abrangência.
- ☐ 5. Sim, a organização promove de forma contínua a coleta, análise e gestão de informações sobre vulnerabilidades e ameaças à segurança da informação, com produção de inteligência e ações preventivas robustas.

20. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes?

- ☐ 1. Não, a organização não possui controle de acesso nem autenticação segura às informações pessoais.
- ☐ 2. Sim, a organização reconhece a necessidade de controle de acesso e autenticação segura, mas a implementação é parcial ou inconsistente.
- ☐ 3. Sim, a organização estabeleceu controle de acesso e autenticação segura para algumas áreas, mas ainda existem lacunas ou áreas não cobertas.

- ☐ 4. Sim, a organização possui controle de acesso e autenticação segura para a maioria das áreas, mas ainda precisa monitorar e realizar revisões regulares.
- ☐ 5. Sim, a organização estabelece e mantém controle de acesso e autenticação segura em todas as áreas, com conformidade total às legislações e normas vigentes, e realiza revisões e aprimoramentos contínuos.

21. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais?

- ☐ 1. Não, a organização não faz monitoramento nem possui mecanismos de controle para eventos de violação e vazamento de dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância do monitoramento, mas os mecanismos para controle e resposta a eventos de violação e vazamento de dados pessoais são limitados ou não estão formalmente implementados.
- ☐ 3. Sim, a organização possui mecanismos de monitoramento e controle para alguns tipos de eventos de violação e vazamento de dados pessoais, mas eles não são abrangentes nem regularmente revisados.
- ☐ 4. Sim, a organização implementou mecanismos de monitoramento e controle para eventos de violação e vazamento de dados pessoais, mas ainda existem áreas que precisam de aprimoramento e maior integração com outras práticas de segurança.
- ☐ 5. Sim, a organização possui mecanismos robustos de monitoramento e controle, que cobrem todos os eventos de violação e vazamento de dados pessoais, e são revisados e aprimorados regularmente para garantir conformidade com as normas.

22. A organização atende ao princípio da transparência?

- ☐ 1. Não, a organização não atende ao princípio da transparência, e não disponibiliza informações claras e acessíveis sobre o tratamento de dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância da transparência, mas as informações disponibilizadas sobre o tratamento de dados pessoais são limitadas ou não estão acessíveis de maneira clara para todos os interessados.
- ☐ 3. Sim, a organização disponibiliza informações sobre o tratamento de dados pessoais, mas estas não cobrem todas as exigências legais ou carecem de clareza e acessibilidade.

- ☐ 4. Sim, a organização atende ao princípio da transparência, disponibilizando informações claras, acessíveis e abrangentes sobre o tratamento de dados pessoais, mas ainda existem áreas que podem ser aprimoradas, e o monitoramento dessas práticas não é realizado de forma contínua.
- ☐ 5. Sim, a organização atende plenamente ao princípio da transparência, disponibilizando de forma clara, acessível e completa todas as informações necessárias sobre o tratamento de dados pessoais, com monitoramento e controle contínuos para garantir conformidade com as regulamentações aplicáveis.

23. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes?

- ☐ 1. Não, a organização não possui uma Política de Classificação da Informação ou instrumento similar.
- ☐ 2. Sim, a organização possui uma Política de Classificação da Informação, mas ela não abrange todas as categorias de dados, especialmente os dados sensíveis e os relacionados a crianças e adolescentes.
- ☐ 3. Sim, a organização possui uma Política de Classificação da Informação, que abrange as principais categorias de dados, mas ainda há lacunas ou áreas que necessitam de revisão.
- ☐ 4. Sim, a organização possui uma Política de Classificação da Informação, abrangente e bem estruturada, mas que ainda necessita de aprimoramentos ou de monitoramento contínuo.
- ☐ 5. Sim, a organização possui uma Política de Classificação da Informação, abrangente e completamente implementada, cobrindo todas as categorias de dados, incluindo dados pessoais sensíveis e os relacionados a crianças e adolescentes, com revisões regulares para assegurar conformidade.

24. A designação do encarregado e suas informações de contato foram publicizadas em algum meio de comunicação oficial?

- ☐ 1. Não, a organização não publiciza a designação do encarregado de proteção de dados nem suas informações de contato.
- ☐ 2. Sim, a organização publiciza a designação do encarregado de proteção de dados, mas as informações de contato não estão facilmente acessíveis ou são limitadas.

- ☐ 3. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato, mas a divulgação não é ampla ou acessível a todos os interessados.
- ☐ 4. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato de forma adequada, mas não há monitoramento da acessibilidade para garantir que as informações estejam disponíveis e acessíveis a todos.
- ☐ 5. Sim, a organização publiciza amplamente a designação do encarregado de proteção de dados e suas informações de contato, garantindo fácil acesso e disponibilidade contínua para todos os interessados, com monitoramento regular dessa acessibilidade.

25. A Política de Privacidade da organização está publicizada?

- ☐ 1. Não, a organização não publiciza sua Política de Privacidade.
- ☐ 2. Sim, a organização publiciza sua Política de Privacidade, mas de forma limitada ou em meios de comunicação de difícil acesso.
- ☐ 3. Sim, a organização publiciza sua Política de Privacidade, mas ela não é facilmente acessível e compreensível para todos os interessados.
- ☐ 4. Sim, a organização publiciza sua Política de Privacidade de forma adequada e acessível, mas ainda há necessidade de melhorias na comunicação ou atualização regular.
- ☐ 5. Sim, a organização publiciza amplamente sua Política de Privacidade, garantindo que seja facilmente acessível, compreensível e regularmente revisada para garantir conformidade com as regulamentações aplicáveis.

APÊNDICE M – Base de análises e recomendações padronizadas para cada resposta possível do instrumento de medição

Dimensão 1: Governança de Dados e Boas Práticas (cor cinza) - Questões de 1 a 6.

Questão 1: A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais? (art. 50 e art. 52, § 1º, inciso IX, da Lei n. 13.709/2018; Decreto n. 9.637/2018 e Decreto n. 10.046/2019 e ABNT NBR ISO/IEC 27014:2021)

Resposta 1:

"Não, a organização ainda não elaborou um programa, plano de governança ou documento com esse direcionamento."

Análise:

A ausência de um programa de governança para dados pessoais representa uma lacuna crítica em termos de conformidade, expondo a organização a riscos regulatórios e operacionais significativos. Sem um documento que defina responsabilidades, políticas e processos para o tratamento de dados, a organização não possui mecanismos adequados para assegurar que suas práticas estejam alinhadas às normativas relevantes, como a LGPD (Lei n. 13.709/2018) e o Decreto n. 10.046/2019.

Recomendação para avanço ao Nível 2:

Recomenda-se iniciar o desenvolvimento de um programa de governança que identifique os principais riscos e requisitos legais da organização. Esse programa deve ser construído em parceria com a alta administração e o DPO, com um plano de ação de curto prazo que contemple a criação de políticas iniciais e procedimentos de conformidade.

Resposta 2:

"Sim, a organização está em fase inicial de elaboração do programa, plano de governança ou documento equivalente com esse direcionamento."

Análise:

A fase inicial de elaboração demonstra um progresso, mas a falta de um programa estruturado limita a efetividade das práticas de governança. Embora a intenção de conformidade esteja presente, a ausência de um planejamento concreto dificulta a implementação eficaz das políticas e procedimentos, como exigido pela LGPD (Lei n. 13.709/2018) e pela ABNT NBR ISO/IEC 27014:2021.

Recomendação para avanço ao Nível 3:

É necessário desenvolver um cronograma claro para a conclusão do programa, especificando os responsáveis e as áreas prioritárias. A organização também deve assegurar que o programa aborda as normas e boas práticas principais, sendo disseminado entre líderes e setores-chave para garantir adesão.

Resposta 3:

"Sim, a organização já elaborou um programa, plano de governança ou documento equivalente com esse direcionamento, mas este ainda não foi totalmente implementado."

Análise:

A elaboração do programa representa um avanço significativo. Entretanto, a implementação parcial reduz a eficácia e compromete a credibilidade do compromisso com a proteção de dados. A organização possui uma base sólida que necessita de formalização e internalização para garantir alinhamento total com as normativas, em especial a LGPD e o Decreto n. 10.046/2019.

Recomendação para avanço ao Nível 4:

Para evoluir, a organização deve estabelecer um plano de implementação com etapas e prazos definidos. Recomenda-se que o processo seja monitorado por um comitê de governança de dados, responsável por avaliar o progresso e assegurar que as práticas e políticas estabelecidas sejam seguidas.

Resposta 4:

"Sim, a organização elaborou e implementou o programa, plano de governança ou documento equivalente com esse direcionamento, mas este documento não é monitorado regularmente."

Análise:

A implementação do programa demonstra comprometimento com a conformidade, mas a ausência de monitoramento contínuo compromete a atualização e sustentabilidade das práticas de proteção de dados. A conformidade regular com a LGPD e a ABNT NBR ISO/IEC 27701:2019 exige monitoramento para garantir eficácia e adaptação a novas exigências.

Recomendação para avanço ao Nível 5:

A organização deve implementar mecanismos de monitoramento contínuos, como auditorias e revisões de compliance, para assegurar a atualização do programa conforme as legislações e normas aplicáveis. Isso garantirá a adequação contínua às regulamentações e reduzirá riscos.

Resposta 5:

"Sim, a organização elaborou e implementou completamente o programa, plano de governança ou documento equivalente com esse direcionamento, e está monitorando regularmente para garantir a conformidade contínua com as regulamentações sobre tratamento e proteção de dados pessoais."

Análise:

Esse nível representa uma maturidade elevada e alinhamento completo com as melhores práticas e requisitos normativos, como exigido pela LGPD e pelas normas ISO/IEC 27701:2019 e 27014:2021. A implementação integral e o monitoramento contínuo garantem que o programa de governança é adaptável a mudanças legais e tecnológicas, promovendo uma proteção eficaz dos dados pessoais.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve investir em atualizações regulares do programa, considerando as mudanças legislativas e os avanços tecnológicos. Revisões e treinamentos periódicos também são essenciais para manter o comprometimento dos colaboradores e a eficácia do programa.

Questão 2: A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)? (art. 5º, inciso VIII, art. 23, inciso III e art. 41 da Lei n. 13.709/2018; Lei n. 13.853/2019; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)

Resposta 1:

"Não, a organização não designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO."

Análise:

A ausência de um DPO representa uma falha significativa na governança de dados, visto que o DPO é essencial para supervisionar e garantir a conformidade com a LGPD. Sem esse profissional, a organização fica vulnerável ao risco de não conformidade e à falta de supervisão no tratamento de dados.

Recomendação para avanço ao Nível 2:

É recomendável iniciar o processo de seleção e designação formal de um DPO que possua a competência necessária para assegurar a conformidade com a legislação e regulamentações de proteção de dados.

Resposta 2:

"Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas suas funções não estão claramente definidas."

Análise:

A designação de um DPO indica um compromisso inicial com a conformidade. No entanto, a ausência de uma definição clara das responsabilidades do DPO limita a capacidade da organização de gerenciar eficazmente a proteção de dados. Conforme previsto no art. 41 da LGPD e na ABNT NBR ISO/IEC 27701:2019, item 6.3.1.1, é fundamental que o DPO tenha funções específicas, como supervisionar a conformidade com a legislação, gerenciar os incidentes de dados e realizar comunicações com as autoridades competentes.

Recomendação para avanço ao Nível 3:

Para avançar, a organização deve criar um documento que defina claramente as atribuições do DPO. Esse documento deve abranger as principais responsabilidades, como o monitoramento de conformidade, a revisão de políticas e o acompanhamento de incidentes, assegurando que o DPO tenha os recursos necessários para atuar de forma eficaz.

Resposta 3:

"Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas sua atuação é limitada e/ou não é amplamente reconhecida internamente."

Análise:

A formalização do DPO é um avanço importante; entretanto, uma atuação limitada ou pouco reconhecida internamente compromete a eficácia do DPO em garantir a conformidade com a LGPD e outras regulamentações. A falta de reconhecimento pode impedir que o DPO influencie práticas de proteção de dados em toda a organização, conforme indicado pela Instrução Normativa SGD/ME n. 117/2020 e a ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 4:

A organização deve adotar medidas para promover o papel do DPO internamente, garantindo que ele tenha acesso às áreas relevantes e o suporte necessário. Sessões de orientação e reuniões com líderes de outras áreas podem auxiliar a fortalecer o entendimento sobre a importância do papel do DPO e fomentar uma cultura de proteção de dados.

Resposta 4:

"Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, com papel reconhecido, mas ainda há lacunas na sua atuação ou na integração com outras áreas."

Análise:

O reconhecimento formal do DPO na organização é um avanço significativo, mas a falta de integração com outras áreas limita o alcance de suas ações. Para uma governança de dados eficaz, conforme a ISO/IEC 27701:2019, é fundamental que o DPO colabore com áreas como Tecnologia da Informação, Jurídico e Recursos Humanos, o que permite uma abordagem multidisciplinar no cumprimento das regulamentações de proteção de dados.

Recomendação para avanço ao Nível 5:

Para alcançar o nível mais elevado, a organização deve estabelecer rotinas regulares de interação entre o DPO e outros setores. Além disso, recomenda-se que o DPO receba treinamentos de atualização e apoio da alta administração, promovendo uma sinergia entre as áreas que facilite a conformidade.

Resposta 5:

"Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, que atua de forma efetiva, integrada às áreas, e com reconhecimento e suporte da alta administração."

Análise:

Neste nível, a organização demonstra maturidade elevada no tratamento de dados pessoais, com um DPO que atua de forma integrada e tem suporte da alta administração, conforme orientado pelo art. 23 da LGPD e a ISO/IEC 27701:2019. Esse reconhecimento interno fortalece a capacidade do DPO para monitorar e assegurar a conformidade e para agir de maneira proativa em situações de risco.

Recomendação para manutenção:

Para sustentar este nível de maturidade, é importante que a organização continue apoiando o DPO, com investimentos em treinamentos regulares e monitoramento das práticas de governança de dados. A manutenção de uma comunicação eficiente entre o DPO e as outras áreas é essencial para garantir uma conformidade duradoura.

Questão 3: A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis? (art. 50 da Lei n. 13.709/2018; art. 15 do Decreto n. 9.637/2018; item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019 e Decreto n. 10.046/2019)

Resposta 1:

"Não, a organização não possui um comitê ou equivalente."

Análise:

A ausência de um comitê interno indica que a organização não dispõe de uma estrutura formal para o acompanhamento e gerenciamento de questões relacionadas ao tratamento de dados pessoais, conforme previsto no art. 50 da LGPD. Esta falha prejudica a capacidade da organização em coordenar ações de conformidade e em responder adequadamente a incidentes de segurança, o que aumenta a exposição a riscos legais e operacionais.

Recomendação para avanço ao Nível 2:

Recomenda-se a criação de um comitê de governança de dados, composto por membros de diferentes áreas da instituição. Este comitê deve ser capacitado para oferecer uma visão multidisciplinar e atuar em prol da conformidade com as regulamentações.

Resposta 2:

"Sim, a organização possui um comitê, mas não está ativo ou não tem funções definidas."

Análise:

A existência de um comitê representa um avanço inicial. No entanto, a falta de atividades ou de uma definição clara das funções limita a eficácia desse órgão, comprometendo a governança e a conformidade com os requisitos da LGPD e da ABNT NBR ISO/IEC 27701:2019, item 6.3.1.1.

Recomendação para avanço ao Nível 3:

É necessário definir com clareza as responsabilidades e os objetivos do comitê, instituindo um plano de ação com reuniões regulares para supervisão das práticas de conformidade e segurança de dados.

Resposta 3:

"Sim, a organização possui um comitê ativo, mas ele se concentra apenas em tarefas pontuais ou de suporte, sem uma atuação estratégica."

Análise:

Um comitê ativo é positivo; contudo, quando a atuação se limita a tarefas pontuais, o impacto na governança e proteção de dados fica restrito. A falta de uma abordagem estratégica pode comprometer uma visão de longo prazo em conformidade com a legislação e as melhores práticas.

Recomendação para avanço ao Nível 4:

Recomenda-se que o comitê adote uma postura estratégica, estabelecendo metas e indicadores de desempenho para avaliar seu impacto, em conformidade com o art. 50 da LGPD.

Resposta 4:

"Sim, a organização possui um comitê ativo com funções bem definidas, e está desenvolvendo sua capacidade de atuação estratégica e integração com todas as áreas relevantes."

Análise:

O comitê já demonstra um nível avançado de maturidade, com funções definidas e integração com áreas relevantes. Contudo, ainda há espaço para desenvolver essa atuação e maximizar sua eficácia.

Recomendação para avanço ao Nível 5:

A organização deve aprimorar a integração entre o comitê e outras áreas, promovendo reuniões conjuntas e relatórios periódicos para registrar os avanços e desafios de *compliance*.

Resposta 5:

"Sim, a organização possui um comitê ativo, com funções bem definidas, que cobre todas as áreas necessárias e está em plena operação."

Análise:

Este é o nível ideal, onde o comitê atua de forma proativa e integrada, com uma visão abrangente e estratégica que assegura a conformidade plena com a legislação

e as melhores práticas de governança de dados, conforme exigido pelo art. 50 da LGPD.

Recomendação para manutenção:

Para manter este nível, é essencial realizar reuniões regulares e revisões da atuação do comitê, além de adaptações conforme mudanças regulatórias. Auditorias periódicas ajudam a manter a eficácia e a conformidade contínua.

Questão 4: A organização possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares? (art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 8º, art. 9º, arts. 17-22, art. 23, inciso I, e art. 50, § 2º, inciso I e II, da Lei n. 13.709/2018; itens 7.3, 7.4 e 8.3 da ABNT NBR ISO/IEC 27701:2019; itens 5.34 e 6.6 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023 e art. 4º, art. 13 e art. 20 da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização ainda não possui uma Política de Privacidade."

Análise:

A falta de uma Política de Privacidade reflete uma lacuna significativa na transparência e conformidade com a LGPD e demais normativas, como a ISO/IEC 27701:2019, que enfatiza a importância da comunicação clara sobre o tratamento de dados. Sem uma política formal, a organização compromete a confiança dos titulares e expõe-se a riscos de penalidades.

Recomendação para avanço ao Nível 2:

Recomenda-se o início da elaboração de uma Política de Privacidade, alinhada às melhores práticas e regulamentações. O documento deve definir os processos de coleta, armazenamento, processamento, compartilhamento e descarte de dados pessoais, orientando colaboradores e informando os titulares.

Resposta 2:

"Sim, a instituição está desenvolvendo uma Política de Privacidade, mas ela ainda está em fase de elaboração."

Análise:

A elaboração da Política de Privacidade demonstra um compromisso inicial com a transparência. No entanto, enquanto a política não for finalizada e implementada, não há garantia sobre o tratamento dos dados pessoais, o que pode gerar insegurança nos titulares.

Recomendação para avanço ao Nível 3:

Priorizar a conclusão da política, abrangendo todo o ciclo de vida dos dados e assegurando alinhamento às normas pertinentes. A implementação deve ser acompanhada de treinamentos e comunicações institucionais para facilitar a compreensão e o cumprimento.

Resposta 3:

"Sim, a instituição possui uma Política de Privacidade, mas não é aplicada de maneira consistente."

Análise:

A existência de uma Política de Privacidade é positiva, mas a falta de aplicação uniforme compromete a segurança dos dados. Conforme a LGPD e a ISO/IEC 27701:2019, a aplicação da política deve ser consistente para evitar falhas de

conformidade e assegurar a integridade dos dados.

Recomendação para avanço ao Nível 4:

Implementar mecanismos de monitoramento e realizar treinamentos regulares para garantir uma aplicação uniforme. Também se recomenda uma revisão periódica para verificar a efetividade e adequação da política.

Resposta 4:

"Sim, a instituição possui uma Política de Privacidade, que é aplicada e divulgada, mas ainda precisa de melhorias."

Análise:

A aplicação e divulgação da Política de Privacidade indicam um alto nível de compromisso com a conformidade e a transparência. Contudo, a necessidade de melhorias aponta que o documento pode não estar plenamente adaptado às mudanças legais ou às práticas de mercado.

Recomendação para avanço ao Nível 5:

Realizar revisões regulares, incorporando feedback de usuários e colaboradores para aprimorar a política continuamente. A inclusão de pesquisas de opinião pode auxiliar na adequação do documento às expectativas e necessidades dos titulares.

Resposta 5:

"Sim, a instituição possui uma Política de Privacidade, que é divulgada, aplicada de forma consistente e regularmente revisada."

Análise:

A Política de Privacidade é completa, aplicada uniformemente e está sujeita a revisões periódicas, em conformidade com a LGPD e a ABNT NBR ISO/IEC 27701:2019. Esse nível assegura transparência e mantém a confiança dos titulares de dados, promovendo a segurança dos dados e o cumprimento das exigências legais.

Recomendação para manutenção:

A manutenção desse nível requer revisões e atualizações regulares com base nas mudanças regulatórias e nas melhores práticas de proteção de dados. Realizar auditorias periódicas é essencial para assegurar que a política continue adequada e eficaz em todas as áreas da organização.

Questão 5: A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição? (art. 5º, incisos XV e XVI, art. 7º, inciso III, art. 11, inciso II, art. 16, inciso III, arts. 25-27, art. 30, capítulo V (arts. 33-36) e art. 50 da Lei n. 13.709/2018; itens 6.10.2, 7.5, 8.2.6, 8.4.2 e 8.5 da ABNT NBR ISO/IEC 27701:2019; item 5.14 da ABNT NBR ISO/IEC 27002:2022 e art. 2º, parágrafo único, art. 10, inciso II e art. 13, inciso V, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não identificou o compartilhamento ou transferência de dados pessoais."

Análise:

A ausência de identificação sobre o compartilhamento e transferência de dados deixa a organização vulnerável a falhas de segurança e compliance, especialmente quanto à transparência com os titulares e aos requisitos legais. Isso vai contra os princípios da Lei Geral de Proteção de Dados, especialmente os arts. 7º e 33-36,

que regulamentam o compartilhamento de dados. A falta de um mapeamento adequado também contraria a orientação da ABNT NBR ISO/IEC 27701:2019, item 6.10.2, que requer o monitoramento de dados compartilhados.

Recomendação para avanço ao Nível 2:

Recomenda-se que a organização inicie um mapeamento preliminar de compartilhamento de dados, incluindo revisões para entender onde dados pessoais são processados e com quais terceiros são compartilhados. Esse mapeamento deve estar documentado para assegurar conformidade com as regulamentações.

Resposta 2:

"Sim, a organização começou a mapear o compartilhamento ou transferência de dados pessoais, mas o processo é incompleto ou informal."

Análise:

Iniciar o mapeamento é positivo, mas um processo informal ou incompleto pode deixar áreas críticas sem supervisão adequada, o que não cumpre os requisitos estabelecidos nos arts. 7º e 33-36 da LGPD, que exigem o controle sobre o compartilhamento de dados pessoais. O item 8.2.6 da ABNT NBR ISO/IEC 27701:2019 destaca a necessidade de processos documentados para o compartilhamento e transferência de dados.

Recomendação para avanço ao Nível 3:

A organização deve formalizar o processo de mapeamento de compartilhamento de dados, assegurando que ele esteja em conformidade com as regulamentações mencionadas e que inclua um controle detalhado dos tipos de dados e das partes envolvidas.

Resposta 3:

"Sim, a organização identificou as principais áreas onde ocorre compartilhamento ou transferência de dados pessoais, mas ainda não há uma visão abrangente ou documentada."

Análise:

Com as principais áreas identificadas, a organização demonstra maturidade crescente, mas a ausência de documentação e de uma visão completa limita o controle e monitoramento eficazes, conforme exigido pela LGPD nos arts. 16 e 50. A falta de uma visão documentada também impede o cumprimento do item 8.5 da ABNT NBR ISO/IEC 27701:2019, que recomenda o monitoramento das operações de compartilhamento de dados.

Recomendação para avanço ao Nível 4:

Recomenda-se documentar detalhadamente o compartilhamento de dados, incluindo os tipos de dados, finalidades e processos específicos, para alcançar uma conformidade robusta e evitar riscos regulatórios.

Resposta 4:

"Sim, a organização identificou e documentou o compartilhamento e a transferência de dados pessoais, mas faltam procedimentos formais para monitoramento ou controle."

Análise:

A documentação é um avanço relevante, mas a falta de monitoramento contínuo pode resultar em desvios ou não conformidade em processos de compartilhamento. Essa situação desrespeita as orientações da LGPD, em particular o art. 50, e o item 7.5 da ABNT NBR ISO/IEC 27701:2019, que orienta o monitoramento regular das

transferências de dados.

Recomendação para avanço ao Nível 5:

A organização deve implementar mecanismos de monitoramento contínuos e regulares, como auditorias, para assegurar que o compartilhamento de dados seja feito em conformidade com as normas e regulamentações aplicáveis.

Resposta 5:

"Sim, a organização identificou, documentou e implantou procedimentos formais para monitorar e controlar o compartilhamento e a transferência de dados pessoais, com revisões regulares para garantir conformidade."

Análise:

Este é o nível ideal de maturidade, com monitoramento e controle contínuos que asseguram transparência e rigorosa conformidade com as regulamentações. A prática atende ao que é determinado nos arts. 33-36 e 50 da LGPD, além de estar alinhada com as normas da ABNT NBR ISO/IEC 27701:2019, especialmente os itens 7.5 e 8.2.6.

Recomendação para manutenção:

Para manter esse nível, a organização deve realizar revisões contínuas e atualizações dos procedimentos, alinhando-se às melhores práticas e mudanças regulatórias para garantir a sustentabilidade do sistema de governança de dados.

Questão 6: A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados (EPD) assuma outras funções que possam gerar conflitos de interesse? (Art. 50 da Lei 13.709/2018; Art. 5º e 7º, § 1º da Lei 14.133/2021)

Resposta 1:

"Não, a organização não segue o princípio da segregação das funções, e o Encarregado de Proteção de Dados (EPD) acumula funções que claramente geram conflitos de interesse."

Análise:

A ausência de segregação de funções expõe a organização a sérios riscos de conflito de interesse, comprometendo a independência do EPD na condução de suas atividades. Segundo a LGPD (art. 50), é essencial que o EPD atue de forma independente, o que é impedido quando acumula funções potencialmente conflitantes. A Lei n. 14.133/2021 também reforça a importância da autonomia funcional para assegurar que as decisões do EPD não sejam influenciadas por interesses conflitantes.

Recomendação para avanço ao Nível 2:

Recomenda-se que a organização revise as atribuições do EPD, eliminando funções adicionais que possam comprometer sua imparcialidade. A instituição deve iniciar um plano de reestruturação organizacional para garantir que o EPD tenha uma atuação independente e focada exclusivamente na proteção de dados.

Resposta 2:

"Sim, a organização reconhece a importância da segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda acumula outras funções que podem resultar em conflitos de interesse."

Análise:

O reconhecimento da importância da segregação é positivo e demonstra

compromisso com a conformidade. No entanto, a acumulação de funções por parte do EPD ainda representa um risco à independência de suas ações, limitando sua capacidade de supervisionar o tratamento de dados com total imparcialidade, conforme estabelece o art. 50 da LGPD e o art. 7º, § 1º, da Lei n. 14.133/2021, que ressaltam a necessidade de evitar conflitos de interesse em funções críticas.

Recomendação para avanço ao Nível 3:

A organização deve identificar as funções adicionais que o EPD exerce e avaliar como essas funções podem ser transferidas a outros membros da equipe. Este processo deve garantir que o EPD esteja livre de quaisquer responsabilidades que possam afetar sua neutralidade no cumprimento da governança de dados.

Resposta 3:

"Sim, a organização implementa a segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda desempenha algumas atividades que podem potencialmente criar conflitos de interesse."

Análise:

A implementação parcial da segregação é um indicativo de progresso, mas atividades adicionais ainda podem comprometer a independência plena do EPD. Embora a organização demonstre esforços para assegurar a imparcialidade, a LGPD (art. 50) e a Lei n. 14.133/2021 enfatizam a necessidade de autonomia total para funções de alta responsabilidade, como a do EPD.

Recomendação para avanço ao Nível 4:

É recomendável que a organização elimine qualquer atribuição adicional ao EPD que possa interferir em sua capacidade de atuar de forma independente. A formalização de um manual de funções, com responsabilidades exclusivas para o EPD, ajudará a estruturar uma atuação transparente e isenta.

Resposta 4:

"Sim, a organização implementou a segregação das funções, garantindo que o Encarregado de Proteção de Dados (EPD) tenha autonomia na função. Entretanto, interferências de órgãos superiores comprometem parcialmente essa autonomia."

Análise:

A implementação da segregação de funções é um avanço significativo. No entanto, interferências de superiores hierárquicos prejudicam a autonomia plena do EPD, o que pode limitar sua capacidade de decisão independente. Segundo o art. 50 da LGPD, o EPD deve operar com autonomia para garantir uma supervisão imparcial das práticas de proteção de dados.

Recomendação para avanço ao Nível 5:

Para garantir a independência do EPD, a organização deve instituir políticas que restrinjam as interferências de outras áreas e departamentos. A criação de um comitê de governança de dados, do qual o EPD seja membro autônomo, pode assegurar maior independência e transparência nas suas funções.

Resposta 5:

"Sim, a organização assegura que o Encarregado de Proteção de Dados (EPD) tenha total autonomia e dedicação exclusiva à sua função, sem acumular outras atividades que possam comprometer sua independência ou gerar conflitos de interesse, e sem interferências de órgãos superiores na tomada de decisões."

Análise:

Neste nível de maturidade, a organização garante a independência total do EPD,

com dedicação exclusiva e ausência de pressões externas que possam comprometer sua atuação. Essa estrutura de governança está em conformidade com as melhores práticas recomendadas pelo art. 50 da LGPD e pela Lei n. 14.133/2021, assegurando que o EPD desempenhe suas funções de forma imparcial e eficiente.

Recomendação para manutenção:

Para manter esse nível, é aconselhável que a organização realize auditorias periódicas para avaliar a independência do EPD. Além disso, o monitoramento contínuo das atividades do EPD, juntamente com uma atualização constante sobre legislações e normativas, contribuirá para que a função permaneça isenta de conflitos de interesse.

Dimensão 2: Políticas e Processos de Tratamento de Dados (cor amarela) - Questões de 7 a 11.

Questão 7: A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação? (art. 10, § 2º, da Lei n. 10.741/2003; art. 5º, incisos I a V, art. 11, arts. 12-14, art. 17, art. 29, art. 48, art. 50 e art. 55-J, inciso VIII, da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 6.5.2, 7.2.2, 7.2.7, 7.2.8, 7.3.2, 8.2.1 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e art. 13, inciso VI, e art. 17, inciso I, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não realizou a identificação das categorias de dados pessoais nem dos titulares."

Análise:

A falta de identificação das categorias de dados pessoais e dos respectivos titulares com os quais a organização interage constitui um risco relevante, pois compromete a conformidade com a LGPD e dificulta a implementação de práticas de proteção adequadas. Sem um mapeamento inicial, a organização não consegue garantir o tratamento seguro dos dados e o cumprimento de políticas de proteção conforme exigido pelos artigos 5º, 11 e 50 da LGPD, além dos itens da ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 2:

Recomenda-se que a organização inicie um mapeamento preliminar das categorias de dados e dos titulares. Esse levantamento básico estabelecerá uma fundação para a documentação e a gestão desses dados, permitindo que a organização desenvolva políticas específicas para diferentes tipos de dados e garanta proteção adequada.

Resposta 2:

"Sim, a organização identificou algumas categorias de dados pessoais e titulares, mas de forma limitada e incompleta."

Análise:

O início do processo de identificação demonstra progresso; no entanto, uma abordagem limitada e incompleta pode não contemplar todas as categorias de dados necessárias para a conformidade com a LGPD e demais normativas. Esse mapeamento parcial impede que a organização aplique integralmente os requisitos dos artigos 5º e 29 da LGPD e dos itens 7.2.7 e 7.3.2 da ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 3:

A organização deve ampliar seu mapeamento, garantindo a cobertura completa das categorias de dados e dos titulares. É recomendável detalhar as categorias e documentar as relações com os titulares, o que proporcionará uma base para políticas de proteção mais robustas e permitirá conformidade com as regulamentações aplicáveis.

Resposta 3:

"Sim, a organização identificou as principais categorias de dados pessoais e titulares, mas ainda há lacunas ou falta de documentação completa."

Análise:

A identificação das principais categorias e titulares é um avanço relevante, mas a falta de documentação abrangente limita o controle e a capacidade de monitoramento. A ausência de uma visão completa e documentada pode prejudicar a aplicação uniforme das práticas de proteção, como previsto no art. 50 da LGPD e nos itens 5.2.1 e 8.2.1 da ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 4:

Recomenda-se que a organização complete a documentação de todas as categorias de dados e respectivos titulares. A realização de uma auditoria interna para identificar lacunas no mapeamento e assegurar que todas as categorias relevantes estejam devidamente documentadas e protegidas fortalecerá a governança e reduzirá os riscos de não conformidade.

Resposta 4:

"Sim, a organização identificou e documentou as categorias de dados pessoais e titulares, mas há necessidade de revisões, monitoramento ou melhorias no processo."

Análise:

A identificação e documentação estão bem estabelecidas, mas a ausência de revisões e monitoramento regulares pode levar a inconsistências e desatualizações ao longo do tempo, especialmente em um ambiente de dados em constante evolução. A manutenção e atualização desse mapeamento são fundamentais para evitar desvio das práticas de conformidade com o art. 48 da LGPD e com os itens 7.2.8 e 8.2.6 da ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo contínuo de revisão e atualização do mapeamento, assegurando que esteja sempre alinhado com as legislações e com as necessidades operacionais. Esse monitoramento permitirá que a organização atue preventivamente frente a mudanças regulatórias ou estruturais, preservando a eficácia da proteção de dados.

Resposta 5:

"Sim, a organização identificou, documentou e mantém um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação."

Análise:

Esse nível representa uma maturidade elevada no tratamento de dados pessoais, com identificação, documentação e monitoramento contínuos das categorias de dados e titulares. A organização demonstra conformidade com as melhores práticas e os requisitos normativos da LGPD, especialmente com os artigos 17 e 50, e das normas ISO/IEC 27701:2019 e Resolução CONARQ n. 54/2023.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar com revisões periódicas e monitoramento. Além disso, é importante atualizar a documentação conforme necessário para refletir mudanças regulatórias ou operacionais, assegurando a conformidade e a eficácia contínua das práticas de proteção de dados.

Questão 8: A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição? (art. 5º, incisos VI a IX, capítulo VI (arts. 37-41), art. 50 da Lei n. 13.709/2018; itens 5.2.1, 5.2.2, 7 e 8 da ABNT NBR ISO/IEC 27701:2019 e art. 3º, incisos I e IX, art. 13, inciso V, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não identificou os agentes (controladores e operadores) de tratamento de dados pessoais."

Análise:

A ausência de identificação dos agentes responsáveis pelo tratamento de dados representa uma falha crítica na governança de dados, pois compromete a transparência, a responsabilidade e a conformidade com as normas de proteção de dados. Sem essa identificação, a organização encontra dificuldades em estabelecer controles adequados, deixando-se vulnerável a riscos de não conformidade e falhas de segurança, conforme exigido pelo art. 37 da LGPD e pela ISO/IEC 27701.

Recomendação para avanço ao Nível 2:

Recomenda-se que a organização inicie o processo de identificação dos agentes de tratamento de dados, documentando papéis e responsabilidades e estabelecendo uma base para a implementação de controles de segurança e conformidade mais eficazes.

Resposta 2:

"Sim, a organização iniciou a identificação dos agentes de tratamento de dados pessoais, mas o processo é incompleto ou informal."

Análise:

Iniciar a identificação é um avanço; no entanto, um processo informal ou incompleto deixa lacunas que podem comprometer a segurança e a responsabilização. A falta de um mapeamento abrangente impede a adoção de uma estrutura robusta de compliance, conforme delineado pelo art. 50 da LGPD e os itens 7 e 8 da ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 3:

A organização deve formalizar o processo de identificação, documentando adequadamente todos os agentes e suas funções, para garantir a inclusão de todas as áreas e melhorar a eficácia do monitoramento e da conformidade com a LGPD.

Resposta 3:

"Sim, a organização identificou os principais agentes de tratamento de dados pessoais, mas ainda há áreas sem identificação clara ou documentação adequada."

Análise:

A organização já identificou os agentes principais, o que representa um progresso; contudo, a falta de documentação abrangente impede um controle eficaz e contínuo. A ausência de uma visão completa compromete a conformidade e dificulta a

aplicação uniforme de práticas de proteção de dados, conforme especificado nos artigos 38 e 41 da LGPD e nos itens 5.2.1 e 7.2 da ISO/IEC 27701.

Recomendação para avanço ao Nível 4:

A organização deve completar a documentação dos agentes de tratamento, abrangendo todas as áreas e adotando uma rotina de revisões para assegurar que a informação permaneça atualizada e em conformidade com a regulamentação vigente.

Resposta 4:

"Sim, a organização identificou e documentou os agentes de tratamento de dados pessoais, mas o processo de monitoramento ou revisão ainda precisa ser aprimorado."

Análise:

A documentação completa dos agentes de tratamento é um avanço relevante; entretanto, a ausência de um monitoramento contínuo pode afetar a eficácia da governança de dados a longo prazo. Para atender às exigências normativas, como as dos itens 5.2.2 e 8 da ISO/IEC 27701, é necessário que o monitoramento seja parte do processo para garantir uma conformidade sustentável.

Recomendação para avanço ao Nível 5:

A organização deve implementar uma rotina de revisão e monitoramento, com auditorias periódicas, para assegurar que todos os agentes permaneçam em conformidade e que os processos de tratamento de dados sejam continuamente atualizados.

Resposta 5:

"Sim, a organização identificou, documentou e mantém um processo formal e contínuo para monitorar, revisar e atualizar os agentes de tratamento de dados pessoais."

Análise:

Esse nível demonstra maturidade avançada na governança de dados, com uma abordagem abrangente para monitoramento, revisão e atualização dos agentes responsáveis pelo tratamento de dados. A conformidade com as normas e legislações vigentes está garantida, assegurando um controle robusto e contínuo.

Recomendação para manutenção:

Para sustentar esse nível de maturidade, a organização deve realizar revisões periódicas das designações e realizar ajustes conforme necessário, acompanhando as melhores práticas e as mudanças regulatórias para garantir a adequação contínua.

Questão 9: A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais? (art. 3º, art. 5º, inciso X, art. 6º, art. 7º, art. 9º, inciso I, arts. 10-11, art. 13, arts. 15-16, capítulo IV (arts. 23-32), art. 37 e art. 50 da Lei n. 13.709/2018 e itens 7.2, 7.4, 8.2 e 8.4 da ABNT NBR ISO/IEC 27701:2019 e art. 4º, incisos X e XII e art. 18, parágrafo único, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não identificou os processos e atividades operacionais que lidam com dados pessoais."

Análise:

A falta de identificação dos processos que lidam com dados pessoais compromete o tratamento de dados, impedindo que a organização controle o uso, armazenamento e proteção dessas informações. Essa ausência expõe a organização a riscos de conformidade e segurança, contrários aos requisitos dos artigos 10, 23 e 50 da LGPD e das diretrizes da ISO/IEC 27701.

Recomendação para avanço ao Nível 2:

Recomenda-se que a organização inicie um mapeamento preliminar de atividades e processos que tratam dados pessoais, estabelecendo uma base para implementar controles que garantam a conformidade com a legislação e a segurança dos dados.

Resposta 2:

"Sim, a organização começou a identificar os processos e atividades operacionais que lidam com dados pessoais, mas o mapeamento é parcial ou informal."

Análise:

A identificação inicial representa um progresso, mas um mapeamento parcial e informal compromete a eficácia no tratamento de dados pessoais. A falta de uma visão abrangente dificulta a aplicação de políticas consistentes e impede o alinhamento com os padrões exigidos nos artigos 6º e 13 da LGPD e nos itens 7.4 e 8.2 da ISO/IEC 27701.

Recomendação para avanço ao Nível 3:

A organização deve formalizar o mapeamento, garantindo a inclusão de todos os processos e atividades relevantes e documentando-os adequadamente, o que fortalecerá o controle e o monitoramento desses processos.

Resposta 3:

"Sim, a organização identificou os principais processos e atividades que lidam com dados pessoais, mas ainda faltam detalhes ou documentação completa."

Análise:

A organização demonstra progresso ao identificar os processos principais, mas a ausência de uma documentação completa impede o controle efetivo e limita o monitoramento contínuo. Sem uma visão detalhada, a organização corre o risco de não cumprir totalmente os requisitos dos artigos 15 e 16 da LGPD e dos itens 7.2 e 8.4 da ISO/IEC 27701.

Recomendação para avanço ao Nível 4:

A organização deve finalizar o mapeamento, cobrindo todas as atividades de tratamento de dados e garantindo que o documento seja atualizado conforme necessário para manter a conformidade e a segurança dos dados.

Resposta 4:

"Sim, a organização identificou e documentou os processos e atividades operacionais que lidam com dados pessoais, mas existem áreas que requerem revisões ou melhorias."

Análise:

A documentação dos processos e atividades operacionais reflete um bom nível de controle; no entanto, a ausência de revisões contínuas pode resultar em desatualizações que afetam a eficácia do sistema de governança. Os requisitos do art. 50 da LGPD e os itens 7.2 e 8.4 da ISO/IEC 27701 sugerem que revisões periódicas são fundamentais.

Recomendação para avanço ao Nível 5:

Para alcançar o nível mais alto, a organização deve implementar uma rotina de

auditorias e revisões periódicas para atualizar e aprimorar continuamente os processos, assegurando que todos estejam alinhados com as melhores práticas e mudanças legais.

Resposta 5:

"Sim, a organização identificou, documentou e mantém um processo contínuo para monitorar, revisar e melhorar os processos e atividades operacionais que lidam com dados pessoais."

Análise:

Esse nível representa uma maturidade avançada na gestão de dados pessoais, com monitoramento constante e revisões contínuas que asseguram a conformidade e a segurança. A organização demonstra uma capacidade sólida de supervisão, alinhada com as melhores práticas e os requisitos normativos, conforme disposto nos artigos 3º e 50 da LGPD e nas diretrizes da ISO/IEC 27701.

Recomendação para manutenção:

Para sustentar esse nível de maturidade, a organização deve continuar realizando revisões periódicas e adaptações de seus processos, conforme surgirem novas regulamentações e melhores práticas. É essencial que a instituição mantenha auditorias regulares e atualize seus controles e políticas de proteção de dados para assegurar a conformidade contínua e a proteção eficaz dos dados pessoais.

Questão 10: Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais? (art. 2º, inciso IX, da Lei n. 7.232/1984; art. 4º da Lei n. 8.159/1991; art. 2º, inciso II, art. 4º, inciso IV, § 1º, art. 7º, inciso X, art. 9º, art. 14, art. 15, capítulo III (arts. 17-22), art. 23, inciso III, § 3º, art. 34, inciso III, art. 45, art. 50 e art. 51 da Lei n. 13.709/2018; itens 7.2.2, 7.2.3, 7.2.7, 7.3, 7.5.3 e 8.3 da ABNT NBR ISO/IEC 27701:2019; item 5.18 da ABNT NBR ISO/IEC 27002:2022 e capítulo IV (arts. 10-12) da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não possui mecanismos formais para garantir os direitos dos titulares de dados pessoais."

Análise:

A ausência de mecanismos formais para assegurar os direitos dos titulares, tais como acesso, correção, exclusão e portabilidade dos dados pessoais, reflete uma grave desconformidade com a Lei Geral de Proteção de Dados, que em seu capítulo III, especialmente nos arts. 17 a 22, assegura o direito de privacidade e proteção de dados dos titulares. Essa lacuna coloca a organização em risco de sanções e compromete a confiança dos titulares ao dificultar o exercício dos seus direitos.

Recomendação para avanço ao Nível 2:

A organização deve implementar processos básicos que assegurem os direitos dos titulares. Recomenda-se começar com um procedimento simplificado para que os titulares possam solicitar informações sobre seus dados pessoais, estabelecendo uma base para um sistema mais robusto no futuro.

Resposta 2:

"Sim, a organização começou a desenvolver mecanismos para garantir os direitos dos titulares, mas estes ainda são limitados ou informais."

Análise:

Embora a organização tenha iniciado o desenvolvimento de mecanismos para

proteger os direitos dos titulares, a falta de formalização e abrangência pode comprometer a segurança e a eficácia dessas medidas, conforme exigido pelo art. 18 da LGPD e o item 7.2.7 da ABNT NBR ISO/IEC 27701:2019. A ausência de um sistema formalizado limita a aplicabilidade e consistência dos direitos dos titulares, expondo a organização a riscos de não conformidade.

Recomendação para avanço ao Nível 3:

A organização deve formalizar esses mecanismos, documentando processos e expandindo-os para cobrir todos os direitos dos titulares conforme previsto na LGPD.

Resposta 3:

"Sim, a organização possui mecanismos formais para garantir os direitos dos titulares, mas eles não são abrangentes ou totalmente implementados."

Análise:

A presença de mecanismos formais indica progresso, mas a falta de abrangência e implementação completa limita a experiência dos titulares e pode comprometer a conformidade total com a LGPD, especialmente em relação ao art. 23, inciso III. Para garantir a segurança e transparência no tratamento de dados, é essencial que esses mecanismos sejam plenamente abrangentes e implementados, conforme orientado pelo item 7.3 da ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 4:

A organização deve expandir esses mecanismos para cobrir todos os direitos dos titulares e assegurar a aplicação consistente em todos os departamentos.

Resposta 4:

"Sim, a organização possui mecanismos formais que garantem os direitos dos titulares, mas esses mecanismos existentes não são revisados ou monitorados regularmente."

Análise:

A existência de mecanismos formais demonstra maturidade, mas a falta de revisão e monitoramento contínuos pode gerar deficiências na aplicação, especialmente em resposta às mudanças regulatórias. A manutenção da eficácia desses mecanismos requer processos regulares de monitoramento e auditoria, conforme estabelecido pelo art. 50 da LGPD e o item 8.3 da ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de revisão e monitoramento contínuo para assegurar a eficácia e conformidade dos mecanismos com as normas atuais e futuras.

Resposta 5:

"Sim, a organização possui mecanismos formais, abrangentes e bem implementados que garantem os direitos dos titulares de dados pessoais, com revisões e melhorias contínuas."

Análise:

A organização demonstra plena conformidade e maturidade, com mecanismos abrangentes e constantemente atualizados para assegurar os direitos dos titulares. Isso fortalece a confiança dos titulares e protege a organização de sanções regulatórias, conforme preconizado no art. 51 da LGPD e item 5.18 da ABNT NBR ISO/IEC 27002:2022.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve realizar revisões

periódicas e adaptar os mecanismos às novas demandas regulatórias e tecnológicas.

Questão 11: A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário? (art. 5º, inciso III e XI, art. 7º, inciso IV, arts. 11-13, art. 16, inciso IV, art. 18, inciso IV e IX (§ 6º e § 7º) e art. 50 da Lei n. 13.709/2018; itens 7.4.2, 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019; item 8.11 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, incisos II e X, art. 9 e art. 18, inciso V, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não possui regras operacionais para esconder dados pessoais sensíveis, nem utiliza técnicas como mascaramento, pseudonimização ou anonimização."

Análise:

A ausência de regras operacionais para a proteção de dados sensíveis representa um risco elevado de exposição de informações críticas, especialmente em relação aos dados pessoais sensíveis, conforme o art. 11 da LGPD e o item 7.4.2 da ABNT NBR ISO/IEC 27701:2019. A falta dessas técnicas deixa os dados vulneráveis a acessos não autorizados.

Recomendação para avanço ao Nível 2:

A organização deve começar a implementar regras básicas para o uso de técnicas de proteção de dados, como o mascaramento, priorizando os dados mais críticos e sensíveis.

Resposta 2:

"Sim, a organização reconhece a importância de proteger dados sensíveis, mas as regras operacionais e técnicas de mascaramento, pseudonimização ou anonimização não são implementadas ou são aplicadas de forma inconsistente."

Análise:

Embora a organização reconheça a importância da proteção de dados sensíveis, a aplicação inconsistente dessas técnicas compromete a conformidade e a segurança. A LGPD, no art. 16, inciso IV, e o item 8.11 da ABNT NBR ISO/IEC 27002:2022, orientam a aplicação consistente dessas técnicas em áreas que lidam com dados pessoais sensíveis.

Recomendação para avanço ao Nível 3:

A organização deve formalizar e documentar essas regras, garantindo que as técnicas de proteção de dados sejam aplicadas consistentemente em todas as áreas onde dados sensíveis são processados.

Resposta 3:

"Sim, a organização desenvolveu regras operacionais e começou a aplicar técnicas de mascaramento, pseudonimização ou anonimização, mas a aplicação é parcial ou não abrange todos os dados sensíveis."

Análise:

A existência de regras operacionais demonstra progresso, mas a aplicação parcial compromete a eficácia das medidas de segurança e conformidade. A LGPD, no art. 18, inciso IV, e os itens 7.4.4 e 7.4.5 da ABNT NBR ISO/IEC 27701:2019, exigem que todas as informações sensíveis sejam protegidas integralmente.

Recomendação para avanço ao Nível 4:

A organização deve expandir a aplicação dessas técnicas para abranger todos os dados sensíveis, garantindo conformidade e proteção.

Resposta 4:

"Sim, a organização possui regras operacionais bem estabelecidas para esconder dados pessoais sensíveis, utilizando técnicas adequadas, mas há áreas que necessitam de aprimoramento e monitoramento."

Análise:

A existência de regras operacionais bem estabelecidas para a proteção de dados sensíveis indica um nível avançado de conformidade e comprometimento com a privacidade e a segurança dos dados. No entanto, a falta de monitoramento e aprimoramento contínuos pode comprometer a eficácia a longo prazo dessas medidas, especialmente considerando as mudanças regulatórias e tecnológicas. A LGPD, no art. 50, exige que as organizações adotem práticas de governança que incluam a avaliação e atualização regular das políticas de proteção de dados, enquanto os itens 7.4.4 e 8.11 da ABNT NBR ISO/IEC 27002:2022 orientam sobre a importância do monitoramento e da revisão periódica das técnicas de proteção.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de monitoramento contínuo e auditoria dessas regras e práticas, assegurando que se mantenham eficazes e alinhadas com as melhores práticas e regulamentações de proteção de dados sensíveis. Recomenda-se ainda uma atualização periódica para garantir adequação às novas necessidades operacionais e avanços tecnológicos.

Resposta 5:

"Sim, a organização estabelece e aplica rigorosamente regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de forma consistente, abrangente e monitorada regularmente."

Análise:

Neste nível, a organização demonstra uma maturidade elevada em governança de dados sensíveis, com práticas robustas e monitoramento contínuo que garantem a segurança e a conformidade com as exigências legais e normativas. A aplicação rigorosa e a atualização frequente das técnicas de mascaramento, pseudonimização e anonimização reforçam a proteção contra acessos não autorizados e vazamento de informações, conforme os requisitos da LGPD nos arts. 11 e 16, que orientam a segurança e privacidade dos dados pessoais sensíveis. Além disso, o item 7.4.5 da ABNT NBR ISO/IEC 27701:2019 e o item 8.11 da ABNT NBR ISO/IEC 27002:2022 corroboram a necessidade de manter processos consistentes e monitorados para assegurar a conformidade com padrões internacionais.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar monitorando e revisando regularmente essas práticas, acompanhando inovações tecnológicas e atualizações regulatórias. Recomenda-se também coletar feedback dos colaboradores e áreas envolvidas para aprimorar continuamente a proteção de dados sensíveis e adaptar-se às necessidades emergentes do cenário de privacidade e segurança.

Questão 12: A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais? (art. 4º, inciso V da Lei n. 7.232/1984; art. 50 da Lei n. 13.709/2018; art. 3º, inciso VII, e art. 15 do Decreto n. 9.637/2018; itens 6.4.2.2 e 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 e item 6.3 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não possui programas ou planos de capacitação sobre tratamento e proteção de dados e informações pessoais."

Análise:

A ausência de programas de capacitação compromete a habilidade dos colaboradores em entender e aplicar corretamente as práticas de proteção de dados, aumentando o risco de não conformidade com a Lei Geral de Proteção de Dados. Sem treinamento, a organização fica mais exposta a erros e violações, o que pode gerar sanções e comprometer a confiança dos titulares de dados. O art. 50 da LGPD e o item 6.4.2.3 da ABNT NBR ISO/IEC 27701:2019 destacam a importância de um programa educacional contínuo para garantir a eficácia das políticas de segurança e conformidade.

Recomendação para avanço ao Nível 2:

A organização deve iniciar um programa básico de capacitação que aborde os princípios fundamentais da proteção de dados, proporcionando aos colaboradores uma base sólida para compreender as práticas de segurança e conformidade.

Resposta 2:

"Sim, a organização possui programas ou planos de capacitação, mas estes atendem aspectos pontuais relacionados ao tratamento e proteção de dados e informações pessoais."

Análise:

A capacitação pontual representa um avanço, mas uma abordagem limitada não é suficiente para preparar os colaboradores a lidarem de maneira abrangente com questões de segurança e proteção de dados. O art. 50 da LGPD e o item 6.3 da ABNT NBR ISO/IEC 27002:2022 indicam a necessidade de treinamentos contínuos e detalhados, abrangendo todos os aspectos de segurança e proteção dos dados.

Recomendação para avanço ao Nível 3:

A organização deve ampliar o escopo dos treinamentos para abordar de forma abrangente todos os aspectos relevantes do tratamento e proteção de dados. Recomenda-se incluir instruções práticas e orientações específicas para que os colaboradores possam responder a situações do dia a dia com segurança.

Resposta 3:

"Sim, a organização tem programas ou planos de capacitação que cobrem questões essenciais sobre o tratamento e a proteção de dados e informações pessoais, mas algumas áreas ainda precisam ser aprimoradas para garantir a efetividade do treinamento."

Análise:

A existência de um programa mais abrangente é um progresso relevante, mas, se algumas áreas ainda carecem de aprimoramento, a efetividade da capacitação é limitada. A falta de uniformidade nos treinamentos pode resultar em lacunas na

proteção de dados. De acordo com o item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019, é essencial que os treinamentos sejam abrangentes para garantir a consistência das práticas.

Recomendação para avanço ao Nível 4:

A organização deve revisar e aprimorar o conteúdo do programa de capacitação, adicionando módulos específicos para áreas críticas e garantindo que todos os colaboradores recebam treinamento adequado e completo.

Resposta 4:

"Sim, a organização possui programas de capacitação bem estruturados, que abrangem as questões relevantes sobre o tratamento e a proteção de dados e informações pessoais, mas os programas não são atualizados nem monitorados regularmente."

Análise:

Ter um programa estruturado é um avanço, mas a ausência de atualizações e monitoramento regular pode desatualizar o conteúdo frente a mudanças legais e melhores práticas. A LGPD (art. 50) e o item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019 destacam a necessidade de revisões e atualizações para garantir a relevância e a eficácia contínua dos treinamentos.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de atualização e monitoramento regular do programa de capacitação, incorporando mudanças regulatórias e avanços tecnológicos, além de realizar avaliações periódicas da eficácia dos treinamentos.

Resposta 5:

"Sim, a organização possui programas ou planos de capacitação completos e regulares, cobrindo o tratamento e a proteção de dados e informações pessoais, com revisão e atualização contínuas para garantir a eficácia."

Análise:

Neste nível, a organização demonstra um alto grau de maturidade, com um programa abrangente, atualizado e monitorado, assegurando que os colaboradores estejam bem preparados para lidar com questões de segurança e proteção de dados. O art. 50 da LGPD e o item 6.3 da ABNT NBR ISO/IEC 27002:2022 reforçam a importância da atualização constante para garantir a conformidade.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar realizando revisões periódicas e aprimoramentos no programa de capacitação, incorporando feedback dos participantes e novas tendências regulatórias e de segurança.

Questão 13: A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades? (art. 6º, inciso X, art. 9º, art. 37, art. 39, arts. 42-48 e art. 50 da Lei n. 13.709/2018; itens 5.3.3, 5.5.3, 6.2.1.1, 6.3.1.1, 6.4.2.1, 6.4.2.2, 6.9.1, 7.2.6 e 7.2.7 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.4, 5.20, 5.27, 6.3, 8.7 e 8.8 da ABNT NBR ISO/IEC 27002:2022 e art. 3º, inciso I, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não realiza conscientização dos agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades."

Análise:

A ausência de conscientização formal dos agentes de tratamento de dados pessoais dificulta a compreensão das obrigações e aumenta o risco de violações de dados. A LGPD (arts. 42-48) exige que todos os agentes compreendam suas responsabilidades para garantir a proteção dos dados.

Recomendação para avanço ao Nível 2:

A organização deve iniciar um programa básico de conscientização, fornecendo orientações sobre as responsabilidades legais dos agentes de tratamento de dados pessoais.

Resposta 2:

"Sim, a organização começou a conscientizar seus agentes de tratamento de dados pessoais, mas as atividades são pontuais e não cobrem todas as responsabilidades."

Análise:

A conscientização pontual é positiva, mas insuficiente para abranger todas as responsabilidades exigidas pela LGPD e normas como a ABNT NBR ISO/IEC 27701:2019 (item 6.4.2.2), deixando áreas críticas sem a devida orientação.

Recomendação para avanço ao Nível 3:

A organização deve ampliar as atividades de conscientização para cobrir todas as responsabilidades dos agentes, garantindo que compreendam completamente suas funções.

Resposta 3:

"Sim, a organização realiza atividades de conscientização sobre papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas ainda há lacunas na abrangência ou na frequência dessas atividades."

Análise:

A conscientização sobre papéis e responsabilidades está em progresso, mas as lacunas comprometem a consistência. A falta de abrangência limita o entendimento completo das obrigações de proteção de dados, conforme o art. 50 da LGPD.

Recomendação para avanço ao Nível 4:

A organização deve assegurar que a conscientização seja abrangente e regular, cobrindo todos os tipos de dados e cenários de tratamento.

Resposta 4:

"Sim, a organização possui programas de conscientização estabelecidos, que cobrem os papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas a aplicação não é monitorada regularmente."

Análise:

Embora os programas estejam bem estruturados, a ausência de monitoramento limita a eficácia. O art. 50 da LGPD e o item 5.3.3 da ABNT NBR ISO/IEC 27701:2019 indicam a importância da avaliação contínua dos programas.

Recomendação para avanço ao Nível 5:

Implementar um sistema de monitoramento e avaliação que garanta a aplicação consistente e atualização dos programas de conscientização.

Resposta 5:

"Sim, a organização conscientiza plenamente seus agentes de tratamento de dados pessoais sobre todos os seus papéis e responsabilidades, com programas contínuos e abrangentes de capacitação."

Análise: Este nível indica uma alta maturidade organizacional, com um programa robusto e contínuo que assegura que todos os agentes de tratamento compreendem plenamente suas responsabilidades no tratamento e proteção de dados. A prática está alinhada aos requisitos legais e normativos da LGPD (arts. 42-48 e art. 50) e aos itens da ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27002:2022, que ressaltam a importância da conscientização integral sobre responsabilidades para garantir a conformidade e segurança dos dados pessoais.

Recomendação para manutenção: Para manter esse nível, a organização deve continuar atualizando e revisando periodicamente os programas de conscientização e capacitação, garantindo que permaneçam relevantes e alinhados às melhores práticas e novas regulamentações. Recomenda-se coletar feedback dos agentes para identificar áreas de melhoria contínua e realizar ajustes sempre que necessário, promovendo um ambiente de aprendizagem ativa e contínua.

Questão 14: Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais recebem treinamentos e capacitações específicas sobre o tema? (art. 50 da Lei n. 13.709/2018; itens 5.5.2, 5.5.3, 5.5.4 e 6.11.2.7 da ABNT NBR ISO/IEC 27701:2019 e itens 5.13, 5.2, 5.4, 5.20, 5.24, 5.27, 6.3, 6.4.2, 6.7, 8.7, 8.12, 8.23, 8.25 e 8.31 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1: *"Não, os colaboradores, terceirizados e parceiros não recebem treinamentos ou capacitações sobre tratamento e proteção de dados pessoais."*

Análise: A ausência de treinamentos específicos para colaboradores e parceiros envolvidos no tratamento de dados compromete a segurança e conformidade com a LGPD, além de aumentar o risco de manipulação inadequada de dados. Segundo o art. 50 da LGPD, é essencial que todos os envolvidos no tratamento de dados pessoais sejam treinados para minimizar riscos operacionais e regulatórios.

Recomendação para avanço ao Nível 2: A organização deve iniciar treinamentos básicos para colaboradores e parceiros que lidam com dados, abordando práticas fundamentais de proteção e segurança de dados, conforme recomendado pelas normas ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27002:2022.

Resposta 2: *"Sim, alguns colaboradores, terceirizados ou parceiros recebem treinamentos sobre tratamento de dados pessoais, mas de forma pontual e não abrangem todos os envolvidos."*

Análise: A capacitação de alguns colaboradores é positiva, mas a abrangência limitada impede uma cultura uniforme de proteção de dados. O art. 50 da LGPD exige uma abordagem mais ampla para cobrir todos os responsáveis pelo tratamento de dados pessoais.

Recomendação para avanço ao Nível 3: A organização deve expandir os treinamentos para incluir todos os colaboradores e parceiros envolvidos no tratamento de dados, garantindo uma abordagem mais uniforme e abrangente, alinhada às normas relevantes.

Resposta 3: *"Sim, a organização começou a oferecer treinamentos específicos para colaboradores, terceirizados e parceiros sobre tratamento de dados pessoais, mas ainda não são abrangentes ou regulares."*

Análise: O oferecimento de capacitações específicas é um avanço significativo, mas a falta de regularidade e cobertura completa limita a aplicação prática e a

conscientização. A LGPD e normas como a ABNT NBR ISO/IEC 27002:2022 (item 6.4.2) destacam a importância de treinamentos contínuos para assegurar uma implementação consistente das políticas de proteção de dados.

Recomendação para avanço ao Nível 4: A organização deve tornar esses treinamentos regulares e garantir que eles abranjam todos os aspectos necessários, estabelecendo uma periodicidade para revisão e reforço dos conteúdos.

Resposta 4: *"Sim, a organização possui programas de treinamento específicos para colaboradores, terceirizados e parceiros, cobrindo assuntos relacionados ao tratamento e proteção de dados pessoais, mas ainda há melhorias necessárias nesse programa."*

Análise: A existência de programas específicos para capacitação demonstra maturidade, mas melhorias adicionais são necessárias para atender plenamente às exigências da LGPD e das normas aplicáveis. Pequenas lacunas no programa podem afetar a consistência da conscientização e proteção dos dados.

Recomendação para avanço ao Nível 5: A organização deve monitorar e revisar continuamente esses programas para garantir que sejam completos e efetivos para todos os envolvidos no tratamento de dados, fortalecendo a conformidade com as normas.

Resposta 5: *"Sim, a organização oferece treinamentos e capacitações regulares e específicos para todos os colaboradores, terceirizados e parceiros, garantindo que todos estejam capacitados para tratar dados."*

Análise: A organização demonstra alto nível de maturidade ao oferecer treinamentos específicos e regulares para todos os envolvidos no tratamento de dados pessoais, abrangendo colaboradores internos e externos. Esse comprometimento com capacitação fortalece a cultura de proteção de dados e assegura a conformidade contínua com a LGPD e as práticas estabelecidas pela ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27002:2022.

Recomendação para manutenção: Para manter esse nível de maturidade, a organização deve continuar monitorando a eficácia dos treinamentos e ajustando os conteúdos para incluir novas práticas e regulamentações. Coletar feedback dos participantes também é recomendável para identificar oportunidades de melhoria contínua e manter o alinhamento com as melhores práticas do setor.

Questão 15: **A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais?** (arts. 42-45, art. 50 e arts. 52-54 da Lei n. 13.709/2018; item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019; itens 5.2, 5.21, 5.4, 5.9 e 6.3 da ABNT NBR ISO/IEC 27002:2022; ABNT NBR ISO/IEC 27005:2023 e art. 17 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não realiza conscientização sobre esses riscos."

Análise: A ausência de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais representa uma vulnerabilidade significativa para a organização. Sem uma compreensão clara dos riscos, os colaboradores podem adotar práticas negligentes, expondo a organização a falhas operacionais, violações de privacidade e sanções regulatórias. A falta de conscientização também implica em descumprimento de requisitos como os dispostos nos arts. 42-45 e 50 da Lei n.

13.709/2018, que tratam das responsabilidades e das sanções em caso de incidentes com dados pessoais.

Recomendação para avanço ao Nível 2: Recomenda-se que a organização inicie um programa básico de conscientização para informar os colaboradores sobre os riscos do tratamento inadequado de dados pessoais. Esse programa deve enfatizar as responsabilidades legais e as potenciais consequências de violações de dados, alinhando-se a diretrizes como o item 6.4.2.2 da ABNT NBR ISO/IEC 27701:2019.

Resposta 2:

"Sim, a organização começou a conscientizar sobre os riscos, mas as atividades são esporádicas e não cobrem todos os aspectos críticos."

Análise: A conscientização esporádica é um passo positivo, porém a falta de consistência e abrangência pode fazer com que os colaboradores não compreendam plenamente a importância da proteção de dados e dos riscos específicos associados ao tratamento inadequado. Essa abordagem limitada pode prejudicar a capacidade de prevenção e resposta a incidentes de dados, conforme preconizado pela LGPD e normas associadas, como o item 5.21 da ABNT NBR ISO/IEC 27002:2022, que enfatiza a importância da capacitação constante.

Recomendação para avanço ao Nível 3: A organização deve intensificar a regularidade dessas atividades e expandir o conteúdo para cobrir todos os riscos críticos. Recomenda-se a criação de módulos de treinamento com exemplos práticos e ilustrações dos impactos de um tratamento inadequado de dados, de forma a reforçar a importância da proteção.

Resposta 3:

"Sim, a organização realiza conscientização sobre os riscos de forma regular, mas ainda há lacunas na cobertura de todos os riscos ou áreas específicas de tratamento de dados pessoais."

Análise: A realização regular de conscientização sobre os riscos representa um progresso significativo; entretanto, a cobertura incompleta limita a eficácia do programa e pode deixar áreas específicas do tratamento de dados vulneráveis. A abrangência insuficiente pode comprometer a consistência e eficácia na aplicação das práticas de proteção de dados exigidas pela LGPD e pelas normas ABNT NBR ISO/IEC 27005:2023, que destacam a avaliação de riscos como parte fundamental da segurança de dados.

Recomendação para avanço ao Nível 4: A organização deve revisar e ampliar o conteúdo da conscientização para garantir que todos os riscos e áreas de tratamento sejam devidamente abordados. Isso pode incluir módulos específicos para diferentes tipos de dados e cenários, assegurando que todos os colaboradores estejam informados e capacitados para lidar com os riscos.

Resposta 4:

"Sim, a organização possui um programa regular de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, mas com necessidade de melhorias em algumas áreas."

Análise: O programa de conscientização regular é um avanço considerável, mas ainda há oportunidades de melhorias que poderiam torná-lo mais completo e eficaz. Pequenas lacunas podem comprometer a percepção dos colaboradores sobre os riscos específicos e sobre as melhores formas de mitigá-los. A revisão e atualização do conteúdo, alinhada ao art. 50 da LGPD e ao item 6.4.2.2 da ABNT NBR ISO/IEC

27701:2019, são fundamentais para garantir que o programa esteja sempre em conformidade com as melhores práticas e mudanças legislativas.

Recomendação para avanço ao Nível 5: A organização deve reforçar o monitoramento e atualização dos conteúdos de conscientização para garantir que eles permaneçam relevantes e abrangentes. Recomenda-se a inclusão de estudos de caso recentes ou incidentes de segurança que ilustram a importância de tratar dados pessoais de maneira segura.

Resposta 5:

"Sim, a organização realiza conscientização contínua e abrangente sobre todos os riscos associados ao tratamento inadequado de dados pessoais."

Análise: A organização demonstra alto nível de maturidade ao implementar um programa contínuo e abrangente de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais. Esse programa promove uma cultura de segurança e proteção de dados, preparando os colaboradores para agirem de forma proativa e em conformidade com os requisitos legais e normativos, como os arts. 42-45 e 50 da LGPD, que abordam as responsabilidades e sanções relacionadas a dados pessoais, além dos itens 5.2 e 6.4.2.2 das normas ABNT NBR ISO/IEC 27002:2022 e ABNT NBR ISO/IEC 27701:2019.

Recomendação para manutenção: Para manter esse nível de maturidade, é essencial que a organização continue realizando atividades regulares de conscientização e busque novas formas de engajar os colaboradores sobre segurança de dados. A inclusão de atualizações sobre novas ameaças e riscos emergentes é recomendada para garantir que o conteúdo do programa permaneça relevante e eficaz.

Dimensão 4: Segurança da Informação e Tecnologia (cor verde) - Questões 16 a 21.

Questão 16: A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar? (art. 4º, inciso V, da Lei n. 7.232/1984; art. 6º, inciso VII e VIII, art. 7º, inciso III, art. 10, inciso II, art. 11, inciso II, alíneas "b" e "g", art. 50 e art. 52, incisos IX, X e XI, § 7º, da Lei n. 13.709/2018; Decreto n. 9.637/2018; itens 5.3.2, 6.2, 6.12.1.1, 6.14 e 6.15 da ABNT NBR ISO/IEC 27701:2019; art. 9º da Instrução Normativa GSI/PR n. 1/2020; itens 5.1 e 8.20 da ABNT NBR ISO/IEC 27002:2022; Portaria SGD/MGI n. 852/2023 e art. 14 da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não definiu nem elaborou uma Política de Segurança da Informação ou documento similar."

Análise:

A ausência de uma política de segurança da informação expõe a organização a riscos significativos, como violações de dados e incidentes de segurança, devido à falta de diretrizes claras para a proteção de dados pessoais. Sem esse documento, é improvável que os colaboradores compreendam suas responsabilidades em relação à segurança da informação, aumentando a vulnerabilidade da instituição. A ausência de uma política formal também indica não conformidade com o art. 50 da Lei n. 13.709/2018 e as diretrizes da ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a elaboração de uma política de segurança da informação que estabeleça princípios básicos e responsabilidades dos colaboradores. Essa política deve ser estruturada com base nas melhores práticas e requisitos legais, incluindo orientações sobre como os dados devem ser protegidos e as responsabilidades dos colaboradores.

Resposta 2:

"Sim, a organização começou a elaborar uma Política de Segurança da Informação ou instrumento similar, mas ainda está em fase de elaboração."

Análise:

O início da elaboração da política representa um progresso, mas a falta de formalização limita a capacidade da organização de assegurar a proteção dos dados pessoais de forma eficaz e sistemática. Sem um documento formalizado, é difícil alinhar as práticas de segurança com a legislação e com normas como a ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 3:

A organização deve concluir a elaboração da política, assegurando que todos os aspectos críticos de segurança estejam cobertos e que o documento esteja acessível aos colaboradores. Recomenda-se também estabelecer um plano de implementação e disseminação da política, garantindo a compreensão e o cumprimento por toda a organização.

Resposta 3:

"Sim, a organização elaborou uma Política de Segurança da Informação ou instrumento similar, mas sua implementação é parcial ou não foi formalmente adotada."

Análise:

A existência de uma política elaborada é um ponto positivo; no entanto, a implementação parcial dificulta que as diretrizes sejam aplicadas de forma consistente em toda a organização, deixando áreas vulneráveis. A falta de uma aplicação uniforme pode prejudicar a capacidade de proteção de dados e comprometer a conformidade com os requisitos legais.

Recomendação para avanço ao Nível 4:

A organização deve trabalhar para implementar a política de forma abrangente, estabelecendo prazos e etapas para aplicação em todas as áreas. É essencial também conscientizar os colaboradores sobre o conteúdo da política para assegurar sua efetividade.

Resposta 4:

"Sim, a organização elaborou e implementou uma Política de Segurança da Informação ou instrumento similar, mas ainda não realiza monitoramento ou revisões regulares."

Análise:

A implementação da política de segurança é um avanço importante, oferecendo uma base sólida para a proteção de dados. No entanto, a falta de monitoramento e revisão periódica pode tornar a política obsoleta diante de novos riscos e ameaças. Essa situação indica uma conformidade parcial com o art. 50 da Lei n. 13.709/2018 e a ABNT NBR ISO/IEC 27002:2022, que recomendam atualizações contínuas.

Recomendação para avanço ao Nível 5:

A organização deve estabelecer um cronograma de revisão e monitoramento

contínuos para garantir que a política de segurança da informação seja atualizada regularmente conforme mudanças tecnológicas e regulamentares.

Resposta 5:

"Sim, a organização elaborou, implementou e monitora regularmente a Política de Segurança da Informação ou instrumento similar, assegurando conformidade contínua com as normas e regulamentações aplicáveis."

Análise:

Este nível indica que a organização possui uma política de segurança madura, implementada e revisada continuamente, assegurando proteção e conformidade constantes com as normas. Esse nível de proteção reforça a confiança e prepara a organização para enfrentar novos riscos de segurança, além de estar alinhado aos padrões da ABNT NBR ISO/IEC 27002:2022.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar realizando revisões periódicas e incorporar feedback dos colaboradores e análises de incidentes para aprimorar continuamente a política de segurança.

Questão 17: A organização usa criptografia para proteger os dados pessoais?

(art. 11, inciso II, alínea "g", art. 46, art. 48, § 3º, art. 49 e art. 50, § 2º, inciso I, alínea 'c', da Lei n. 13.709/2018; art. 2º, inciso III, do Decreto n. 9.637/2018; itens 6.7 e 6.15.1.5 da ABNT NBR ISO/IEC 27701:2019 e item 8.24 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não utiliza criptografia para proteger os dados pessoais."

Análise:

A ausência de criptografia representa um risco elevado, pois dados pessoais sem essa proteção estão vulneráveis a acessos não autorizados. A criptografia é uma medida essencial para garantir a segurança dos dados, especialmente em situações de transmissão e armazenamento de informações sensíveis, como determinado pela LGPD (Lei n. 13.709/2018) e as diretrizes da ABNT NBR ISO/IEC 27002:2022.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a implementação de criptografia para dados pessoais sensíveis, priorizando áreas mais críticas. Além disso, é recomendável definir políticas para orientar o uso dessa tecnologia.

Resposta 2:

"Sim, a organização reconhece a importância da criptografia, mas sua aplicação é limitada ou inconsistente."

Análise:

A aplicação limitada da criptografia demonstra uma intenção positiva, mas a inconsistência na aplicação deixa dados pessoais expostos em determinadas áreas, o que pode gerar vulnerabilidades significativas. A falta de uma prática uniforme vai contra as orientações da LGPD e normas como a ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 3:

A organização deve padronizar a aplicação de criptografia para assegurar a proteção em todas as áreas que tratam de dados pessoais, garantindo que a prática seja abrangente e consistente.

Resposta 3:

"Sim, a organização usa criptografia para proteger alguns dados pessoais, mas não de forma abrangente ou em todas as áreas necessárias."

Análise:

O uso de criptografia em alguns dados pessoais é um progresso, mas a aplicação restrita limita a segurança geral, expondo certas áreas a riscos de interceptação e violação. A conformidade plena requer a aplicação uniforme da criptografia, conforme sugerido na ABNT NBR ISO/IEC 27002:2022.

Recomendação para avanço ao Nível 4:

A organização deve expandir o uso da criptografia para cobrir todos os dados pessoais e áreas necessárias, implementando processos formais para gerenciar e monitorar o uso da criptografia.

Resposta 4:

"Sim, a organização usa criptografia de maneira abrangente para proteger os dados pessoais, mas ainda existem áreas que necessitam de melhorias ou revisões."

Análise:

A aplicação abrangente da criptografia proporciona uma segurança significativa, mas algumas áreas que necessitam de ajustes ou monitoramento podem comprometer a segurança total dos dados. A revisão e o monitoramento contínuo são fundamentais para a conformidade com as normas de segurança.

Recomendação para avanço ao Nível 5:

A organização deve revisar continuamente o uso da criptografia, ajustando práticas para cobrir completamente todas as áreas e realizando auditorias regulares para identificar melhorias.

Resposta 5:

"Sim, a organização utiliza criptografia de forma consistente e abrangente para proteger todos os dados pessoais, com monitoramento contínuo e revisões regulares para garantir a segurança."

Análise:

Este nível reflete uma proteção robusta, com a aplicação plena e monitorada da criptografia, assegurando que os dados pessoais estejam protegidos contra acessos não autorizados. Essa prática assegura conformidade regulatória e é alinhada com as diretrizes da ABNT NBR ISO/IEC 27701:2019.

Recomendação para manutenção:

Para manter este nível de maturidade, a organização deve continuar realizando auditorias regulares e monitorando a eficácia da criptografia, além de acompanhar avanços tecnológicos para incorporar novas técnicas de proteção conforme necessário.

Questão 18: A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais? (art. 5º, art. 15, art. 23, art. 25, art. 32, arts. 46-49 e art. 50 da Lei n. 13.709/2018; itens 5.6, 5.7, 6.5.3, 6.9.3, 6.9.4, 6.9.7, 6.14, 7.2.8, 7.4.6, 7.4.7 e 7.4.8 da ABNT NBR ISO/IEC 27701:2019 e itens 5.23, 7.10, 8.10, 8.13, 8.14, 8.15 e 8.25 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não possui gestão de backup nem trilhas de auditoria para

garantir o ciclo de vida dos dados e informações pessoais."

Análise:

A falta de um sistema de backup e trilhas de auditoria compromete a segurança e a integridade dos dados, dificultando o monitoramento de seu ciclo de vida. Sem esses mecanismos, a organização fica vulnerável a perdas de dados em caso de incidentes ou falhas, o que impede uma recuperação eficaz e deixa a organização em não conformidade com as exigências de segurança e privacidade. A ausência desses sistemas contraria as recomendações da ABNT NBR ISO/IEC 27701:2019.

Recomendação para avanço ao Nível 2:

A organização deve implementar um sistema básico de backup e trilhas de auditoria para dados pessoais. É recomendável começar por áreas críticas, expandindo a implementação para assegurar a proteção em toda a organização.

Resposta 2:

"Sim, a organização começou a desenvolver um sistema de gestão de backup e trilhas de auditoria, mas de forma limitada ou informal."

Análise:

A implementação inicial de sistemas de backup e auditoria é um progresso, mas a falta de formalidade e abrangência deixa áreas críticas desprotegidas, o que compromete a segurança e a conformidade com a legislação de proteção de dados. A conformidade plena exige um sistema robusto e documentado.

Recomendação para avanço ao Nível 3:

A organização deve formalizar e documentar esses sistemas, garantindo que todos os dados pessoais críticos estejam incluídos no processo e que o sistema seja aplicado de forma consistente em toda a organização.

Resposta 3:

"Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria, mas ele não cobre todas as áreas necessárias ou não é aplicado de forma consistente."

Análise:

A presença de um sistema de backup e auditoria demonstra maturidade, mas a aplicação parcial pode deixar algumas áreas vulneráveis, o que compromete a segurança e a recuperação completa dos dados em caso de incidentes. A cobertura plena dos sistemas é essencial para assegurar a integridade dos dados.

Recomendação para avanço ao Nível 4:

A organização deve expandir a cobertura dos sistemas de backup e auditoria para abranger todas as áreas de dados pessoais, garantindo a consistência na sua aplicação e minimizando os riscos de perda ou exposição indevida de dados.

Resposta 4:

"Sim, a organização possui gestão de backup e trilhas de auditoria abrangentes, mas ainda há necessidade de melhorias ou maior integração com as práticas de gestão de dados."

Análise:

O sistema de backup e auditoria está bem estabelecido, mas a integração com outras práticas de gestão de dados poderia fortalecer a proteção e recuperação de informações pessoais, garantindo que o sistema funcione de forma otimizada e sem falhas.

Recomendação para avanço ao Nível 5:

A organização deve integrar completamente as práticas de backup e auditoria às demais práticas de gestão de dados, criando um ambiente mais seguro e eficiente para a proteção dos dados ao longo de seu ciclo de vida.

Resposta 5:

"Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria robusto e bem implementado, que garante a proteção e integridade dos dados e informações pessoais em todas as fases do ciclo de vida."

Análise:

Este nível reflete uma gestão de dados avançada, com sistemas robustos de backup e auditoria que protegem a integridade dos dados e garantem sua rastreabilidade. A presença de trilhas de auditoria reforça a transparência e a capacidade de identificar e corrigir problemas de maneira eficaz.

Recomendação para manutenção:

Para sustentar esse nível de maturidade, a organização deve realizar auditorias regulares nos sistemas de backup e auditoria, acompanhando avanços tecnológicos e assegurando a conformidade contínua com normas de segurança e privacidade.

Questão 19: A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades? (art. 5º, inciso XVII, art. 31, art. 32, art. 38, parágrafo único, art. 48 e art. 50 da Lei n. 13.709/2018; art. 2º, incisos II e III do Decreto n. 9.637/2018; itens 5.4.1, 5.7.1, 6.9.2, 6.9.6 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019 e itens 5.7, 8.7, 8.8, 8.23 e 8.28 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não coleta nem analisa informações relacionadas a vulnerabilidades e ameaças à segurança da informação."

Análise:

A ausência de coleta e análise de informações relacionadas a vulnerabilidades e ameaças deixa a organização exposta a riscos evitáveis. Sem esse processo, a organização não possui uma base para identificar e mitigar ameaças à segurança, aumentando a probabilidade de incidentes. A conformidade com a ABNT NBR ISO/IEC 27701:2019 e a Lei n. 13.709/2018 requer uma abordagem estruturada para gestão de vulnerabilidades.

Recomendação para avanço ao Nível 2:

A organização deve iniciar um processo básico de coleta e análise de vulnerabilidades, focando nas áreas de maior risco e elaborando relatórios preliminares sobre ameaças para embasar as ações de mitigação.

Resposta 2:

"Sim, a organização começou a coletar e analisar informações sobre vulnerabilidades e ameaças, mas o processo é informal ou limitado."

Análise:

O início da coleta de informações sobre vulnerabilidades representa um avanço, mas a informalidade e limitação desse processo impedem a organização de obter uma visão clara dos riscos, o que pode resultar em ameaças não mitigadas.

Recomendação para avanço ao Nível 3:

A organização deve formalizar esse processo e ampliar sua abrangência,

implementando o monitoramento contínuo das áreas críticas de segurança e um sistema de documentação para os resultados das análises.

Resposta 3:

"Sim, a organização coleta e analisa informações sobre vulnerabilidades e ameaças à segurança da informação, mas ainda não possui um processo estruturado para gestão de vulnerabilidades."

Análise:

A coleta e análise de vulnerabilidades são indicativos de progresso, mas a falta de uma estrutura formal dificulta a resposta e resolução efetiva de problemas. Um processo estruturado permite priorizar e mitigar ameaças de maneira mais eficaz, conforme recomendado pela ABNT NBR ISO/IEC 27002:2022.

Recomendação para avanço ao Nível 4:

A organização deve estabelecer um processo estruturado de gestão de vulnerabilidades, incluindo identificação, priorização e correção de vulnerabilidades, bem como a criação de relatórios detalhados que facilitem o acompanhamento e a tomada de decisão.

Resposta 4:

"Sim, a organização possui um processo estruturado para coletar, analisar e gerir vulnerabilidades e ameaças à segurança da informação, mas precisa de melhorias ou maior abrangência."

Análise:

A existência de um processo estruturado para gestão de vulnerabilidades é positiva, mas a necessidade de melhorias e uma maior abrangência podem deixar certas áreas desprotegidas, comprometendo a segurança total dos dados pessoais.

Recomendação para avanço ao Nível 5:

A organização deve expandir a abrangência do processo de gestão de vulnerabilidades, garantindo a inclusão de todas as áreas de segurança da informação, além de adotar uma abordagem proativa e de inteligência de ameaças para monitoramento contínuo.

Resposta 5:

"Sim, a organização promove de forma contínua a coleta, análise e gestão de informações sobre vulnerabilidades e ameaças à segurança da informação, com produção de inteligência e ações preventivas robustas."

Análise:

Este nível reflete uma maturidade avançada, com uma abordagem proativa de inteligência de ameaças que permite à organização antecipar e mitigar riscos, além de realizar ações preventivas baseadas em dados sólidos e atualizados. Essa prática fortalece a segurança e assegura uma resposta ágil a ameaças emergentes.

Recomendação para manutenção:

Para manter este nível, a organização deve continuar monitorando novas ameaças e adaptando suas práticas de inteligência e gestão de vulnerabilidades. Recomenda-se também acompanhar as inovações tecnológicas para reforçar ainda mais as defesas de segurança da informação.

Questão 20: A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes? (art. 6º, incisos IV e VII, art. 9º, art. 11, inciso II, "g", art. 13, art. 18, art. 19, art. 25,

art. 26, art. 40, art. 46, art. 50, art. 52, § 7º, e art. 53, § 7º, da Lei n. 13.709/2018; art. 2º, incisos III e IV, do Decreto n. 9.637/2018; item 6.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.15, 5.16, 5.17, 5.18, 5.33, 8.2, 8.3, 8.4 e 8.5 da ABNT NBR ISO/IEC 27002:2022 e art. 1º, art. 2º, parágrafo único, art. 4º, art. 10, art. 14, art. 17, inciso IV, art. 18, art. 20, art. 21 e art. 23 da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não possui controle de acesso nem autenticação segura às informações pessoais."

Análise:

A falta de controle de acesso e autenticação segura para dados pessoais representa uma não conformidade com o art. 46 da Lei Geral de Proteção de Dados, que exige a adoção de medidas de segurança para a proteção de dados. Além disso, os itens 8.2 e 8.3 da ABNT NBR ISO/IEC 27002:2022 especificam a necessidade de controles de acesso apropriados para garantir a segurança dos dados.

Recomendação para avanço ao Nível 2:

Para melhorar a segurança, recomenda-se que a organização comece a implementar controles básicos de acesso e autenticação, especialmente em áreas que lidam com informações pessoais sensíveis, em alinhamento com o item 6.6 da ABNT NBR ISO/IEC 27701:2019 e o art. 25 da LGPD, que estabelece a importância de medidas preventivas de proteção.

Resposta 2:

"Sim, a organização reconhece a necessidade de controle de acesso e autenticação segura, mas a implementação é parcial ou inconsistente."

Análise:

Embora a organização reconheça a necessidade de controle de acesso, a implementação parcial ou inconsistente deixa algumas áreas vulneráveis e não atende plenamente ao art. 50 da LGPD, que exige a aplicação de medidas adequadas de segurança para o tratamento de dados pessoais. Além disso, o item 5.17 da ABNT NBR ISO/IEC 27002:2022 recomenda controles uniformes e consistentes para minimizar riscos de acessos não autorizados.

Recomendação para avanço ao Nível 3:

A organização deve expandir e padronizar a aplicação de controles de acesso e autenticação para todas as áreas de dados pessoais, em conformidade com o art. 46 da LGPD e com o item 8.4 da ABNT NBR ISO/IEC 27002:2022, que recomenda a aplicação consistente desses controles para aumentar a segurança.

Resposta 3:

"Sim, a organização estabeleceu controle de acesso e autenticação segura para algumas áreas, mas ainda existem lacunas ou áreas não cobertas."

Análise:

A implementação parcial de controle de acesso demonstra que a organização está avançando no cumprimento dos requisitos do art. 13 e do art. 25 da LGPD, que tratam da necessidade de proteção dos dados pessoais. Contudo, o art. 18 da LGPD exige proteção integral dos dados, e os itens 5.15 a 5.18 da ABNT NBR ISO/IEC 27002:2022 enfatizam a cobertura completa em todas as áreas que tratam de dados pessoais.

Recomendação para avanço ao Nível 4:

A organização deve expandir a cobertura dos controles de acesso e autenticação

para todas as áreas sensíveis, conforme exigido pelo art. 40 da LGPD e pelo item 5.33 da ABNT NBR ISO/IEC 27002:2022, que recomenda a aplicação de autenticação segura em todas as áreas de dados pessoais.

Resposta 4:

"Sim, a organização possui controle de acesso e autenticação segura para a maioria das áreas, mas ainda precisa monitorar e realizar revisões regulares."

Análise:

A prática de controle de acesso em grande parte da organização é positiva e demonstra conformidade com o art. 26 da LGPD e o item 5.16 da ABNT NBR ISO/IEC 27002:2022. No entanto, a falta de revisões e monitoramento constante contraria o item 8.5 da mesma norma, que recomenda auditorias regulares para garantir a eficácia contínua desses controles.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de monitoramento e revisão contínua, de acordo com o art. 52, § 7º, da LGPD e o item 5.18 da ABNT NBR ISO/IEC 27002:2022. Isso garante que os acessos e permissões sejam continuamente revisados, ajustando-se a novas exigências de segurança.

Resposta 5:

"Sim, a organização estabelece e mantém controle de acesso e autenticação segura em todas as áreas, com conformidade total às legislações e normas vigentes, e realiza revisões e aprimoramentos contínuos."

Análise:

Este nível demonstra conformidade integral com a LGPD, especialmente com o art. 50, que exige uma abordagem proativa e contínua para a proteção de dados pessoais. A prática de revisões regulares também está de acordo com o item 8.3 da ABNT NBR ISO/IEC 27002:2022, que recomenda a atualização constante dos controles de acesso.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar monitorando e aprimorando os controles de acesso e autenticação, conforme o item 5.16 da ABNT NBR ISO/IEC 27002:2022, garantindo que os processos de segurança estejam sempre atualizados e em conformidade com novos avanços tecnológicos.

Questão 21: A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais? (art. 15, inciso IV, art. 31, art. 32, arts. 42-45, art. 46, art. 48 e art. 50, § 2º, inciso I, alínea 'g', e art. 52, § 7º, da Lei n. 13.709/2018; art. 2º, inciso II, art. 3º, inciso X, do Decreto n. 9.637/2018; itens 5.7, 5.8, 6.9.4, 6.13 e 8.2.6 da ABNT NBR ISO/IEC 27701:2019; itens 5.25, 5.35, 8.12, 8.16 e 8.23 da ABNT NBR ISO/IEC 27002:2022 e art. 15 e art. 25, parágrafo único, da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não faz monitoramento nem possui mecanismos de controle para eventos de violação e vazamento de dados pessoais."

Análise:

A ausência de monitoramento e controle de incidentes de segurança é uma grave falha de conformidade com a Lei Geral de Proteção de Dados, especialmente com os artigos 46 e 48, que exigem medidas de proteção e a comunicação de incidentes

que comprometam dados pessoais. Esse cenário também contraria as orientações dos itens 5.7 e 8.12 da ABNT NBR ISO/IEC 27002:2022, que destacam a importância do monitoramento para prevenir e detectar vazamentos de dados.

Recomendação para avanço ao Nível 2:

A organização deve implementar um monitoramento básico para identificar atividades suspeitas e potenciais vazamentos. Isso pode incluir a criação de alertas e relatórios preliminares de segurança, conforme orientado no art. 32 da LGPD e no item 8.16 da ABNT NBR ISO/IEC 27002:2022, que recomendam a vigilância contínua e a resposta imediata a ameaças.

Resposta 2:

"Sim, a organização reconhece a importância do monitoramento, mas os mecanismos para controle e resposta a eventos de violação e vazamento de dados pessoais são limitados ou não estão formalmente implementados."

Análise:

Embora a organização tenha começado a reconhecer a importância do monitoramento, a implementação informal e limitada não atende plenamente ao art. 48 da LGPD, que exige a comunicação imediata de incidentes de segurança. Os itens 5.8 e 8.16 da ABNT NBR ISO/IEC 27002:2022 recomendam a formalização desses processos para garantir uma resposta rápida e consistente a eventos de violação.

Recomendação para avanço ao Nível 3:

A organização deve formalizar o monitoramento e expandir os controles para cobrir todas as áreas críticas, seguindo as diretrizes do item 6.13 da ABNT NBR ISO/IEC 27701:2019 e os requisitos do art. 31 da LGPD. A criação de um plano de resposta a incidentes, com responsáveis designados e processos documentados, é recomendada para assegurar uma resposta eficaz a incidentes.

Resposta 3:

"Sim, a organização possui mecanismos de monitoramento e controle para alguns tipos de eventos de violação e vazamento de dados pessoais, mas eles não são abrangentes nem regularmente revisados."

Análise:

Os mecanismos de monitoramento e controle existentes indicam progresso, mas a cobertura parcial e a ausência de revisões regulares deixam lacunas de segurança, contrariando o art. 46 da LGPD, que exige medidas adequadas de segurança para proteção dos dados. Os itens 5.25 e 8.23 da ABNT NBR ISO/IEC 27002:2022 destacam a importância de uma abordagem abrangente e atualizada para o monitoramento de incidentes de segurança.

Recomendação para avanço ao Nível 4:

A organização deve expandir a cobertura dos controles de monitoramento para abranger todos os tipos de dados e áreas sensíveis, conforme o art. 32 da LGPD, que trata da necessidade de medidas de prevenção. Além disso, recomenda-se instituir uma política de revisões periódicas para garantir a eficácia contínua, conforme orientado pelo item 8.16 da ABNT NBR ISO/IEC 27002:2022.

Resposta 4:

"Sim, a organização implementou mecanismos de monitoramento e controle para eventos de violação e vazamento de dados pessoais, mas ainda existem áreas que precisam de aprimoramento e maior integração com outras práticas de segurança."

Análise:

A implementação de um sistema de monitoramento para eventos de segurança indica um bom nível de maturidade, alinhado ao art. 46 da LGPD e ao item 5.35 da ABNT NBR ISO/IEC 27002:2022, que recomenda controles de monitoramento eficazes. No entanto, a necessidade de maior integração com outras práticas de segurança aponta uma oportunidade para otimizar a proteção dos dados.

Recomendação para avanço ao Nível 5:

A organização deve trabalhar para integrar totalmente o monitoramento de incidentes com outras práticas de segurança, conforme o art. 50 da LGPD, que incentiva uma abordagem proativa e preventiva. Essa integração pode incluir a adoção de auditorias e o uso de ferramentas de inteligência para detectar padrões de ameaças, conforme recomendado pelo item 8.2.6 da ABNT NBR ISO/IEC 27701:2019.

Resposta 5:

"Sim, a organização possui mecanismos robustos de monitoramento e controle, que cobrem todos os eventos de violação e vazamento de dados pessoais, e são revisados e aprimorados regularmente para garantir conformidade com as normas."

Análise:

Neste nível, a organização demonstra plena conformidade com o art. 48 da LGPD, ao manter um sistema abrangente e atualizado de monitoramento de incidentes de segurança. A prática regular de revisões e aprimoramentos também está alinhada com os itens 5.7 e 8.23 da ABNT NBR ISO/IEC 27002:2022, que enfatizam a necessidade de uma supervisão contínua e ajustada conforme novos riscos e ameaças emergem.

Recomendação para manutenção:

Para sustentar esse nível de maturidade, a organização deve continuar realizando revisões periódicas e incorporando novas tecnologias e metodologias para fortalecer o monitoramento. A realização de simulações de incidentes, conforme sugerido pelo item 8.16 da ABNT NBR ISO/IEC 27002:2022, pode contribuir para garantir que a resposta da organização seja rápida e eficaz em cenários reais.

Dimensão 5: Acesso à Informação e Transparência (cor vermelha) - Questões 22 a 25.

Questão 22: A organização atende ao princípio da transparência? (art. 5º, inciso XXXIII, da Constituição Federal de 1988, art. 4º da Lei n. 8.159/1991; Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 6, inciso VI, art. 9º, inciso VII, § 1º, art. 10, inciso II, § 2º, art. 20, art. 23, art. 25, art. 40 e art. 50, inciso I, alínea "e", da Lei n. 13.709/2018 e art. 4º, inciso VIII, art. 18 e art. 24 da Resolução CONARQ n. 54/2023)

Resposta 1:

"Não, a organização não atende ao princípio da transparência, e não disponibiliza informações claras e acessíveis sobre o tratamento de dados pessoais."

Análise:

A ausência de transparência quanto ao tratamento de dados pessoais representa uma desconformidade com a Lei Geral de Proteção de Dados, em especial com o art. 6º, inciso VI, que exige transparência como princípio essencial no tratamento de dados. Esse cenário compromete a confiança dos titulares e viola direitos

assegurados no art. 5º, inciso XXXIII, da Constituição Federal de 1988 e na Lei de Acesso à Informação (Lei n. 12.527/2011), que estabelecem o direito de acesso a informações públicas. Sem transparência, os titulares desconhecem como seus dados são utilizados, gerando insegurança e desconfiança.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a disponibilização de informações básicas sobre o tratamento de dados pessoais, de forma clara e acessível, conforme o art. 50, inciso I, da LGPD, que incentiva práticas de transparência. O art. 4º, inciso VIII, da Resolução CONARQ n. 54/2023 também recomenda que as informações fornecidas sejam compreensíveis para os titulares, assegurando o entendimento de como seus dados são utilizados e protegidos.

Resposta 2:

"Sim, a organização reconhece a importância da transparência, mas as informações disponibilizadas sobre o tratamento de dados pessoais são limitadas ou não estão acessíveis de maneira clara para todos os interessados."

Análise:

Embora a organização esteja ciente da necessidade de transparência, a limitação das informações ou sua dificuldade de acesso contraria o objetivo do art. 23 da LGPD, que exige a disponibilização clara e acessível de informações aos titulares. Essa falta de clareza limita a compreensão dos direitos dos titulares e do uso de seus dados, indo de encontro ao art. 10 do Decreto n. 7.724/2012, que orienta a disponibilização de informações públicas de forma que seja compreensível a todos.

Recomendação para avanço ao Nível 3:

A organização deve ampliar a acessibilidade e clareza das informações, seguindo o art. 9º, inciso VII, da LGPD e o art. 24 da Resolução CONARQ n. 54/2023, que recomendam a adoção de práticas que promovam a transparência e facilitem o entendimento dos titulares sobre como seus dados são tratados. A apresentação das informações de maneira direta e acessível é essencial para assegurar a conformidade com o princípio da transparência.

Resposta 3:

"Sim, a organização disponibiliza informações sobre o tratamento de dados pessoais, mas estas não cobrem todas as exigências legais ou carecem de clareza e acessibilidade."

Análise:

A disponibilização de informações demonstra um compromisso inicial com a transparência, mas a falta de completude e clareza limita a conformidade com o art. 50, inciso I, alínea "e", da LGPD, que exige transparência completa e acessível aos titulares. Esse contexto pode prejudicar a organização na prática de uma transparência efetiva, conforme recomendado no art. 18 da Resolução CONARQ n. 54/2023, que sugere uma comunicação clara e detalhada sobre as práticas de tratamento de dados.

Recomendação para avanço ao Nível 4:

A organização deve revisar as informações fornecidas aos titulares, de forma a atender plenamente as exigências legais. As orientações do art. 10, § 2º, da LGPD incentivam o uso de uma linguagem clara e acessível, essencial para assegurar a compreensão do público em geral. Oferecer essas informações em formatos acessíveis e de fácil entendimento garante que todos os interessados compreendam as práticas de tratamento de dados.

Resposta 4:

"Sim, a organização atende ao princípio da transparência, disponibilizando informações claras, acessíveis e abrangentes sobre o tratamento de dados pessoais, mas ainda existem áreas que podem ser aprimoradas, e o monitoramento dessas práticas não é realizado de forma contínua."

Análise:

A disponibilização de informações claras e abrangentes indica que a organização está bem posicionada quanto ao princípio da transparência. No entanto, a ausência de um monitoramento contínuo contraria o art. 20 da LGPD, que exige a atualização das informações para garantir sua veracidade e completude. Isso pode resultar em inconsistências que comprometam a confiança e o entendimento dos titulares.

Recomendação para avanço ao Nível 5:

A organização deve implementar um sistema de monitoramento e revisão contínua das informações disponibilizadas, conforme o art. 50 da LGPD, que exige práticas contínuas de conformidade. A adoção de mecanismos regulares de revisão garante que as informações permaneçam atualizadas e acessíveis ao público, mantendo a transparência e alinhamento com as práticas recomendadas pela Resolução CONARQ n. 54/2023.

Resposta 5:

"Sim, a organização atende plenamente ao princípio da transparência, disponibilizando de forma clara, acessível e completa todas as informações necessárias sobre o tratamento de dados pessoais, com monitoramento e controle contínuos para garantir conformidade com as regulamentações aplicáveis."

Análise:

Neste nível, a organização demonstra plena conformidade com o princípio da transparência, alinhando-se ao art. 50 da LGPD e ao art. 4º da Lei n. 8.159/1991, que reforçam a necessidade de acessibilidade e completude nas informações. O monitoramento contínuo assegura que as informações sobre o tratamento de dados sejam constantemente atualizadas, atendendo ao art. 9º da LGPD, e reforça a confiança dos titulares e a capacidade de resposta da organização a novas regulamentações.

Recomendação para manutenção:

Para manter este nível de maturidade, a organização deve continuar monitorando a conformidade e a qualidade das informações, conforme o art. 25 da LGPD, que exige a atualização regular das práticas de tratamento. Incorporar feedbacks dos titulares e realizar revisões periódicas garantem que a organização permaneça em conformidade com as normas e mantenha a transparência contínua.

Questão 23: A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes? (Lei n. 12.527/2011; Decreto n. 7.724/2012; art. 5º, inciso II, art. 11, art. 14, art. 46 e art. 50, § 2º, inciso I, alíneas "a" e "d", da Lei n. 13.709/2018; item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 e itens 5.12 e 5.13 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não possui uma Política de Classificação da Informação ou instrumento similar."

Análise:

A ausência de uma Política de Classificação da Informação compromete a capacidade da organização de tratar adequadamente diferentes categorias de dados, como os dados pessoais sensíveis e dados de crianças e adolescentes. A falta de classificação de dados coloca a organização em risco de não conformidade com o art. 46 da Lei n. 13.709/2018 (LGPD), que estabelece a necessidade de proteger dados pessoais de forma adequada ao seu nível de sensibilidade. Além disso, o art. 14 da LGPD determina o cuidado especial com dados de crianças e adolescentes, reforçando a importância de uma política de classificação que permita diferenciar e proteger esses dados de forma apropriada.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a elaboração de uma política de classificação, abordando categorias como dados pessoais, dados sensíveis e dados de crianças e adolescentes. O item 6.5.2 da ABNT NBR ISO/IEC 27701:2019 recomenda uma estrutura para o tratamento e a segurança de dados pessoais, enquanto o Decreto n. 7.724/2012 orienta a classificação de informações para fins de transparência e segurança. A criação de uma política específica garantirá que os dados mais críticos recebam o tratamento adequado.

Resposta 2:

"Sim, a organização possui uma Política de Classificação da Informação, mas ela não abrange todas as categorias de dados, especialmente os dados sensíveis e os relacionados a crianças e adolescentes."

Análise:

A existência de uma Política de Classificação representa um avanço, mas a falta de cobertura para dados sensíveis e dados de menores compromete a conformidade com o art. 11 da LGPD, que exige maior cuidado com informações sensíveis. A proteção de dados relacionados a crianças e adolescentes é reforçada pelo art. 14 da mesma lei, enquanto a Resolução CONARQ n. 54/2023 também recomenda uma abordagem abrangente para a classificação e proteção desses dados.

Recomendação para avanço ao Nível 3:

A organização deve expandir sua política de classificação para incluir dados pessoais sensíveis e de menores, garantindo que as medidas de segurança e proteção sejam adequadas para esses tipos de dados. Conforme o item 5.12 da ABNT NBR ISO/IEC 27002:2022, uma classificação abrangente auxilia na proteção e no gerenciamento de dados críticos.

Resposta 3:

"Sim, a organização possui uma Política de Classificação da Informação, que abrange as principais categorias de dados, mas ainda há lacunas ou áreas que necessitam de revisão."

Análise:

A cobertura das principais categorias de dados é um passo positivo, mas lacunas ou inconsistências limitam a eficácia da política, especialmente em relação à proteção de dados sensíveis e de crianças. A conformidade com o art. 50 da LGPD exige que as políticas de segurança de dados sejam abrangentes e consistentes. A ABNT NBR ISO/IEC 27701:2019 (item 6.5.2) também recomenda que a política de classificação seja revisada regularmente para assegurar que todas as áreas de dados estejam cobertas de forma adequada.

Recomendação para avanço ao Nível 4:

A organização deve revisar sua política de classificação para garantir uma cobertura completa e precisa de todas as categorias de dados. Essa prática é alinhada com o art. 46 da LGPD, que destaca a importância de medidas adequadas para proteção de dados. O uso de um sistema de revisão regular ajuda a identificar e corrigir lacunas na política de classificação.

Resposta 4:

"Sim, a organização possui uma Política de Classificação da Informação, abrangente e bem estruturada, mas que ainda necessita de aprimoramentos ou de monitoramento contínuo."

Análise:

A política de classificação é abrangente, indicando uma sólida estrutura para o tratamento de dados pessoais. No entanto, a falta de monitoramento contínuo pode levar a desatualizações, prejudicando a conformidade com o princípio da transparência exigido pelo art. 6º, inciso VI, da LGPD e a proteção completa prevista pelo art. 50. A atualização e o monitoramento contínuos são fundamentais para garantir que a política de classificação se mantenha eficaz e atualizada.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de monitoramento e revisão contínua da política de classificação, conforme indicado pelo item 5.13 da ABNT NBR ISO/IEC 27002:2022, que sugere revisões periódicas para refletir mudanças na regulamentação e nas práticas recomendadas. Isso assegura que a política esteja sempre atualizada e em conformidade.

Resposta 5:

"Sim, a organização possui uma Política de Classificação da Informação, abrangente e completamente implementada, cobrindo todas as categorias de dados, incluindo dados pessoais sensíveis e os relacionados a crianças e adolescentes, com revisões regulares para assegurar conformidade."

Análise:

Esse nível de maturidade demonstra conformidade plena com as regulamentações de proteção de dados, com uma política abrangente e continuamente revisada, em conformidade com os requisitos do art. 50 da LGPD e do art. 11, que rege o tratamento de dados sensíveis. O monitoramento regular garante que a política de classificação se adapte a novas exigências e melhore continuamente, assegurando o cumprimento das melhores práticas e regulamentos relevantes, como o Decreto n. 7.724/2012.

Recomendação para manutenção:

Para manter este nível de maturidade, a organização deve continuar revisando e aprimorando sua política de classificação, incorporando novas regulamentações e práticas recomendadas. A conformidade contínua é sustentada pela atualização periódica dos processos, conforme sugerido pela ABNT NBR ISO/IEC 27002:2022 e pelo art. 18 da Resolução CONARQ n. 54/2023.

Questão 24: A designação do encarregado e suas informações de contato foram publicizadas em algum meio de comunicação oficial? (art. 5º, inciso VIII, art. 23, art. 41 da Lei n. 13.709/2018; itens 6.3.1 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e art. 1º da IN SGD/ME n. 117/2020)

Resposta 1:

"Não, a organização não publiciza a designação do encarregado de proteção de dados nem suas informações de contato."

Análise:

A ausência de publicização da designação e das informações de contato do encarregado de proteção de dados (DPO) compromete a transparência e dificulta o acesso dos titulares aos canais de comunicação com o responsável pela proteção de seus dados. Segundo o art. 41 da Lei n. 13.709/2018 (LGPD), a organização tem a obrigação de nomear um encarregado e divulgar suas informações de contato. A falta dessa comunicação indica descumprimento da legislação, prejudicando o direito dos titulares de dados de obter informações sobre o tratamento de seus dados.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a publicização das informações básicas de contato do encarregado, garantindo que estejam acessíveis em um meio de comunicação oficial. Isso possibilitará que os titulares de dados exerçam seus direitos e ajuda a cumprir os requisitos legais conforme o art. 1º da IN SGD/ME n. 117/2020, que estabelece a divulgação do contato do DPO para fins de transparência.

Resposta 2:

"Sim, a organização publiciza a designação do encarregado de proteção de dados, mas as informações de contato não estão facilmente acessíveis ou são limitadas."

Análise:

Embora a designação do DPO esteja disponível, a acessibilidade limitada das informações de contato dificulta a comunicação entre o responsável e os titulares de dados, comprometendo parcialmente o princípio da transparência definido pelo art. 6º, inciso VI, da LGPD. Além disso, a falta de facilidade de acesso não atende integralmente o item 6.3.1 da ABNT NBR ISO/IEC 27701:2019, que enfatiza a importância de uma comunicação clara e acessível.

Recomendação para avanço ao Nível 3:

A organização deve tornar as informações de contato do DPO mais visíveis e acessíveis em locais onde os titulares possam facilmente encontrá-las, como em seu site institucional ou em áreas de fácil acesso. Isso garante maior transparência e conformidade com a LGPD e a norma ISO/IEC 27701.

Resposta 3:

"Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato, mas a divulgação não é ampla ou acessível a todos os interessados."

Análise:

A divulgação das informações do DPO indica progresso, mas a limitação de acesso a todos os interessados sugere uma falha na transparência completa. O art. 41, §1º da LGPD, prevê que as informações de contato do encarregado sejam de fácil acesso, assegurando que todos os titulares possam exercer seus direitos. A falta de visibilidade para um público amplo pode reduzir a conformidade com a legislação.

Recomendação para avanço ao Nível 4:

A organização deve expandir os canais de comunicação e tornar as informações do DPO amplamente acessíveis. Conforme as diretrizes da ABNT NBR ISO/IEC 27701:2019, item 8.5.5, a transparência deve estar alinhada à necessidade de acesso fácil aos contatos do DPO, assegurando conformidade com as normas e regulamentos.

Resposta 4:

"Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato de forma adequada, mas não há monitoramento da acessibilidade para garantir que as informações estejam disponíveis e acessíveis a todos."

Análise:

A publicização adequada do DPO é um avanço significativo, mas a falta de monitoramento contínuo para assegurar a disponibilidade das informações representa um risco de desatualização. A IN SGD/ME n. 117/2020 e o art. 41 da LGPD requerem que os dados do DPO estejam sempre acessíveis para assegurar comunicação contínua e transparente com os titulares.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de monitoramento contínuo para verificar a acessibilidade e atualidade das informações de contato do DPO, assegurando que os titulares possam sempre acessá-las quando necessário. Esse monitoramento contínuo assegura que a comunicação seja eficaz e conforme as exigências legais.

Resposta 5:

"Sim, a organização publiciza amplamente a designação do encarregado de proteção de dados e suas informações de contato, garantindo fácil acesso e disponibilidade contínua para todos os interessados, com monitoramento regular dessa acessibilidade."

Análise:

A organização demonstra alto nível de maturidade e conformidade com a LGPD, assegurando total transparência e acessibilidade. O monitoramento contínuo das informações do DPO reflete o compromisso com o art. 41 da LGPD, que exige clareza e fácil acesso. Além disso, o item 6.3.1 da ABNT NBR ISO/IEC 27701:2019 reforça a importância de manter canais de comunicação claros e acessíveis, garantindo que os titulares de dados possam facilmente obter informações e assistência.

Recomendação para manutenção:

A organização deve continuar monitorando e atualizando as informações de contato do DPO regularmente, conforme novas regulamentações ou alterações internas. Além disso, recomenda-se que testes periódicos de acessibilidade sejam realizados para garantir que as informações do DPO permaneçam acessíveis e atualizadas para todos os interessados, reforçando a confiança e a transparência.

Questão 25: A Política de Privacidade da organização está publicizada? (art. 2º, inciso VIII, da Lei n. 7.232/1984; art. 1º, art. 2º, inciso I, art. 6º, incisos IV e VI, art. 9º, art. 23, inciso I e § 1º, e art. 50, inciso II, § 3º da Lei n. 13.709/2018; art. 3º, inciso XI, do Decreto n. 9.637/2018; itens 7.3.2, 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019 e item 5.34 da ABNT NBR ISO/IEC 27002:2022)

Resposta 1:

"Não, a organização não publiciza sua Política de Privacidade."

Análise:

A falta de publicização da Política de Privacidade compromete o cumprimento do princípio de transparência previsto no art. 6º, inciso VI, da Lei n. 13.709/2018

(LGPD), que assegura aos titulares de dados o direito de entender como seus dados são tratados. Sem a publicização, os titulares ficam impossibilitados de obter informações sobre o uso e a proteção de seus dados pessoais, o que prejudica a confiança e a conformidade da organização com a LGPD e as normas ISO aplicáveis.

Recomendação para avanço ao Nível 2:

A organização deve iniciar a publicização da Política de Privacidade, disponibilizando-a em um meio de fácil acesso, como o site institucional, para que os titulares possam consultá-la facilmente. Isso ajudará a organização a cumprir o art. 23, inciso I, da LGPD, que exige transparência e acessibilidade sobre as práticas de tratamento de dados pessoais.

Resposta 2:

"Sim, a organização publiciza sua Política de Privacidade, mas de forma limitada ou em meios de comunicação de difícil acesso."

Análise:

Embora a Política de Privacidade esteja disponível, sua visibilidade limitada compromete a acessibilidade para os titulares de dados. A dificuldade de acesso ou localização indica um cumprimento parcial das exigências de transparência da LGPD e dos itens 7.3.2 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019, que ressaltam a importância de uma comunicação acessível sobre o tratamento de dados pessoais.

Recomendação para avanço ao Nível 3:

A organização deve tornar a Política de Privacidade mais visível e facilmente acessível, publicizando-a em canais de fácil acesso para o público. Essa melhoria é necessária para garantir que os titulares possam consultar a política sempre que necessário, em conformidade com o art. 9º da LGPD e com as melhores práticas estabelecidas nas normas ISO.

Resposta 3:

"Sim, a organização publiciza sua Política de Privacidade, mas ela não é facilmente acessível e compreensível para todos os interessados."

Análise:

Apesar de estar publicizada, a Política de Privacidade ainda apresenta dificuldades de acessibilidade ou compreensão, o que limita o entendimento do público sobre o uso e proteção dos dados pessoais. O art. 6º, inciso IV, da LGPD, enfatiza a necessidade de clareza nas práticas de tratamento de dados, e os titulares devem ser capazes de entender suas implicações sem dificuldades.

Recomendação para avanço ao Nível 4:

A organização deve revisar a Política de Privacidade para assegurar que seu conteúdo seja claro, acessível e compreensível, disponibilizando-a em um formato adequado para o público. Essa melhoria ajudará a organização a cumprir as exigências de transparência e a atender aos requisitos do item 5.34 da ABNT NBR ISO/IEC 27002:2022, que incentiva a simplicidade na comunicação de políticas.

Resposta 4:

"Sim, a organização publiciza sua Política de Privacidade de forma adequada e acessível, mas ainda há necessidade de melhorias na comunicação ou atualização regular."

Análise:

A Política de Privacidade está disponível e acessível, mas a falta de atualizações

regulares pode comprometer a conformidade e a confiança dos titulares. A LGPD, em seu art. 50, inciso II, § 3º, exige que as políticas de privacidade sejam mantidas atualizadas conforme as práticas e regulamentações vigentes.

Recomendação para avanço ao Nível 5:

A organização deve implementar um processo de atualização regular da Política de Privacidade, assegurando que ela acompanhe as mudanças legais e operacionais e seja sempre comunicada de maneira clara e acessível aos titulares. Esse processo contínuo é importante para garantir a conformidade e a confiança dos titulares na proteção de seus dados pessoais.

Resposta 5:

"Sim, a organização publiciza amplamente sua Política de Privacidade, garantindo que seja facilmente acessível, compreensível e regularmente revisada para garantir conformidade com as regulamentações aplicáveis."

Análise:

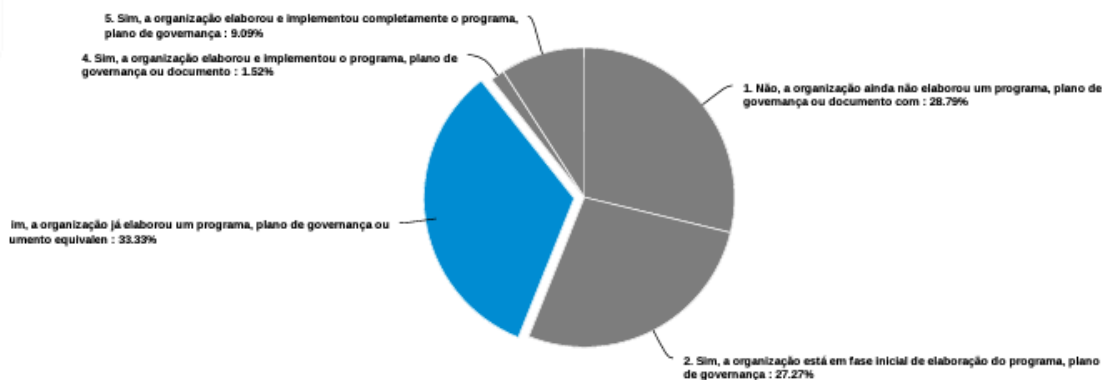
A organização demonstra alto nível de conformidade com a LGPD e os padrões de proteção de dados, publicizando amplamente uma Política de Privacidade acessível e compreensível, que é regularmente revisada para refletir as práticas de tratamento de dados. Essa abordagem é consistente com o art. 50, inciso II, § 3º, da LGPD e com os itens 7.3.3 e 8.5.5 da ABNT NBR ISO/IEC 27701:2019, assegurando transparência e confiança no tratamento de dados pessoais.

Recomendação para manutenção:

Para manter esse nível de maturidade, a organização deve continuar revisando e publicizando a Política de Privacidade regularmente, ajustando-a conforme necessário para garantir que permaneça acessível e em conformidade com as regulamentações aplicáveis. A coleta de feedback dos titulares de dados pode ajudar a identificar pontos de melhoria contínua.

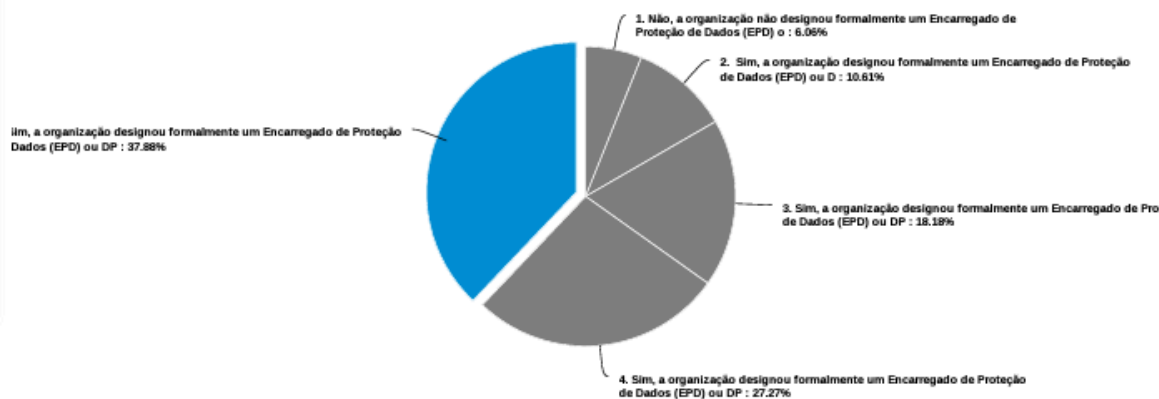
APÊNDICE N – Relatório gerado pelo questionpro após o teste do modelo de maturidade

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais?



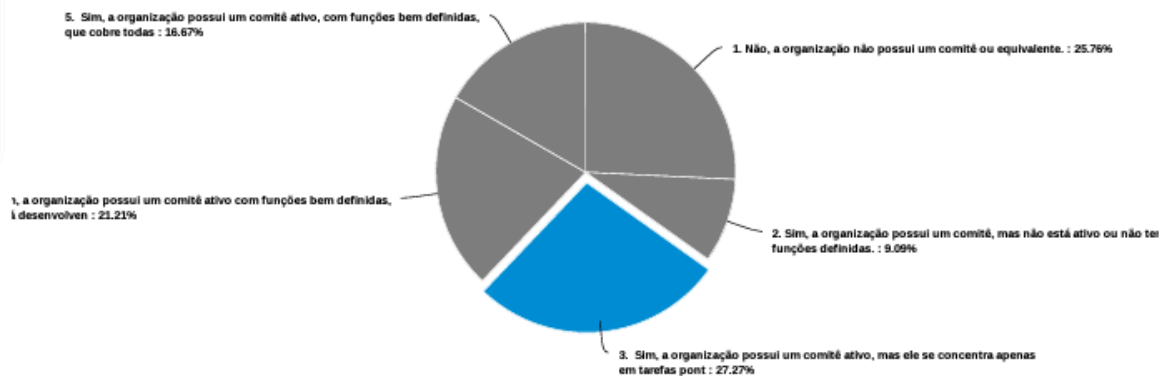
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização ainda não elaborou um programa, plano de governança ou documento com esse direcionamento.	19	28.79%					
2. Sim, a organização está em fase inicial de elaboração do programa, plano de governança ou documento equivalente com esse direcionamento.	18	27.27%					
3. Sim, a organização já elaborou um programa, plano de governança ou documento equivalente com esse direcionamento, mas este ainda não foi totalmente implementado.	22	33.33%					
4. Sim, a organização elaborou e implementou o programa, plano de governança ou documento equivalente com esse direcionamento, mas este documento não é monitorado regularmente.	1	1.52%					
5. Sim, a organização elaborou e implementou completamente o programa, plano de governança ou documento equivalente com esse direcionamento, e está monitorando regularmente para garantir a conformidade contínua com as regulamentações sobre tratamento e proteção de dados pessoais.	6	9.09%					
Total	66	n = 66					

2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)?



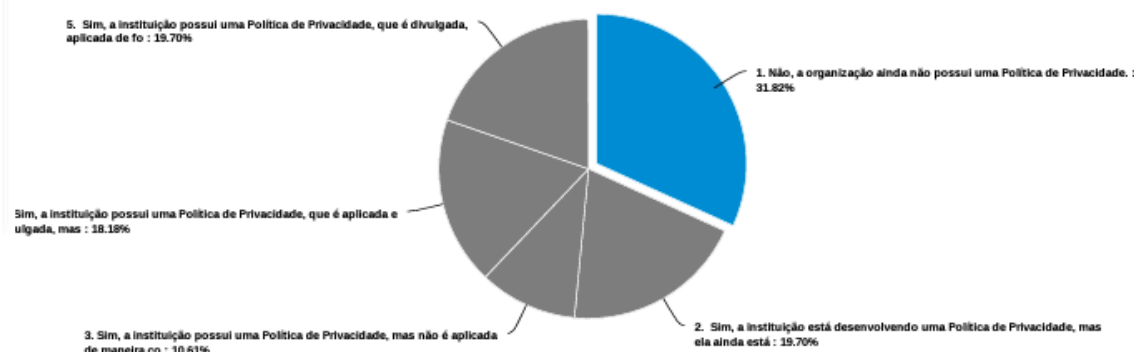
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO.	4	6.06%					
2. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas suas funções não estão claramente definidas.	7	10.61%					
3. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas sua atuação é limitada e/ou não é amplamente reconhecida internamente.	12	18.18%					
4. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, com papel reconhecido, mas ainda há lacunas na sua atuação ou na integração com outras áreas.	18	27.27%					
5. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, que atua de forma efetiva, integrada às áreas, e com reconhecimento e suporte de alta administração.	25	37.88%					
Total	66	n = 66					

3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis?



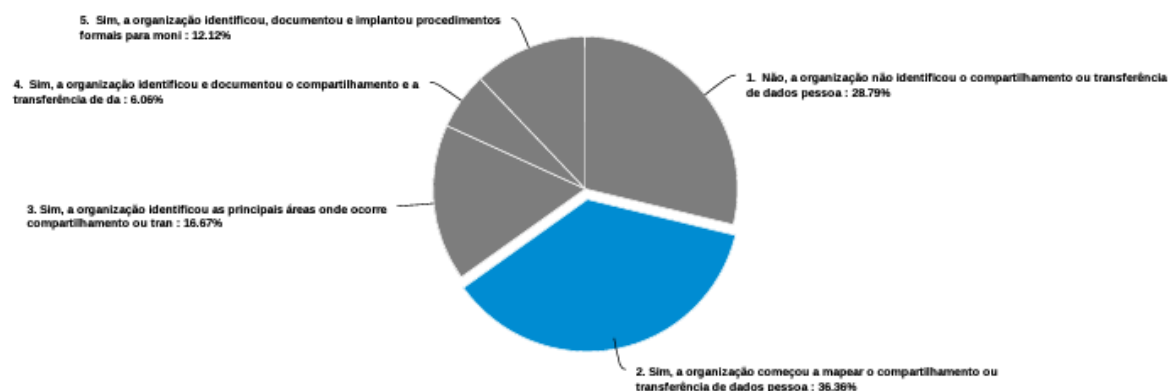
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui um comitê ou equivalente.	17	25.76%					
2. Sim, a organização possui um comitê, mas não está ativo ou não tem funções definidas.	6	9.09%					
3. Sim, a organização possui um comitê ativo, mas ele se concentra apenas em tarefas pontuais ou de suporte, sem uma atuação estratégica.	18	27.27%					
4. Sim, a organização possui um comitê ativo com funções bem definidas, e está desenvolvendo sua capacidade de atuação estratégica e integração com todas as áreas relevantes.	14	21.21%					
5. Sim, a organização possui um comitê ativo, com funções bem definidas, que cobre todas as áreas necessárias e está em plena operação.	11	16.67%					
Total	66	n = 66					

4. A organização possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares?



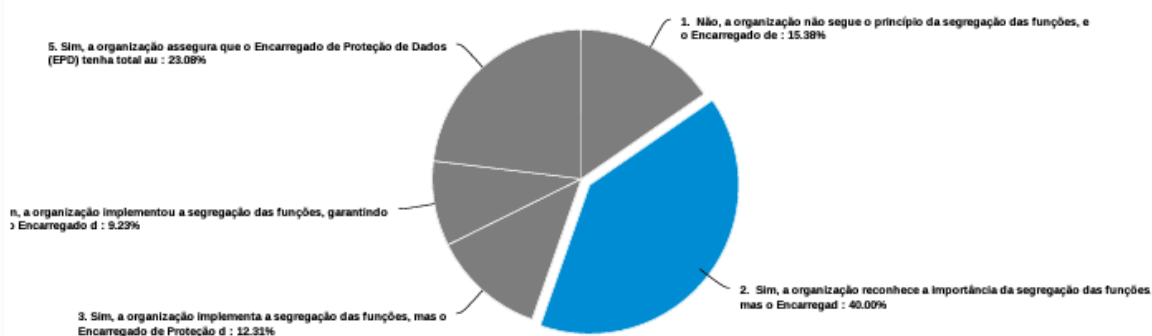
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização ainda não possui uma Política de Privacidade.	21	31.82%					
2. Sim, a instituição está desenvolvendo uma Política de Privacidade, mas ela ainda está em fase de elaboração.	13	19.7%					
3. Sim, a instituição possui uma Política de Privacidade, mas não é aplicada de maneira consistente.	7	10.61%					
4. Sim, a instituição possui uma Política de Privacidade, que é aplicada e divulgada, mas ainda precisa de melhorias.	12	18.18%					
5. Sim, a instituição possui uma Política de Privacidade, que é divulgada, aplicada de forma consistente e regularmente revisada.	13	19.7%					
Total	66	n = 66					

5. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição?



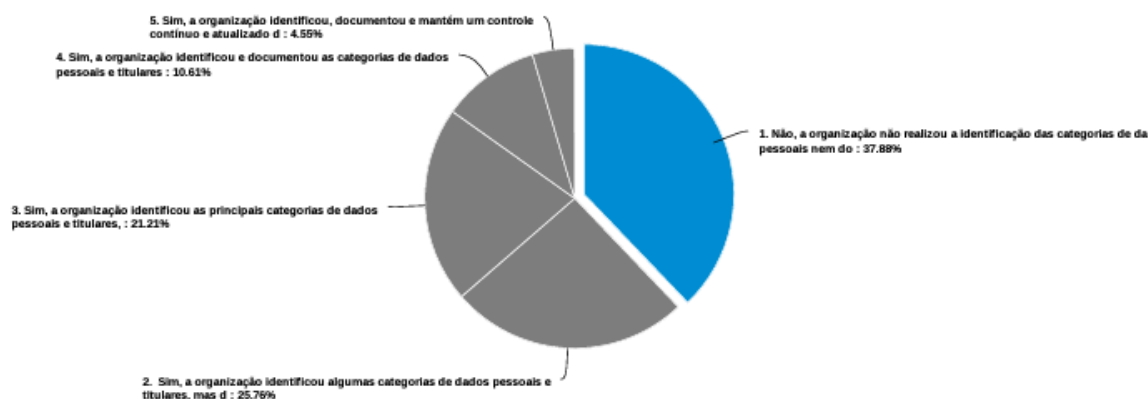
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não identificou o compartilhamento ou transferência de dados pessoais.	19	28.79%					
2. Sim, a organização começou a mapear o compartilhamento ou transferência de dados pessoais, mas o processo é incompleto ou informal.	24	36.36%					
3. Sim, a organização identificou as principais áreas onde ocorre compartilhamento ou transferência de dados pessoais, mas ainda não há uma visão abrangente ou documentada.	11	16.67%					
4. Sim, a organização identificou e documentou o compartilhamento e a transferência de dados pessoais, mas faltam procedimentos formais para monitoramento ou controle.	4	6.06%					
5. Sim, a organização identificou, documentou e implantou procedimentos formais para monitorar e controlar o compartilhamento e a transferência de dados pessoais, com revisões regulares para garantir conformidade.	8	12.12%					
Total	66	n = 66					

6. A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados (EPD) assuma outras funções que possam gerar conflitos de interesse?



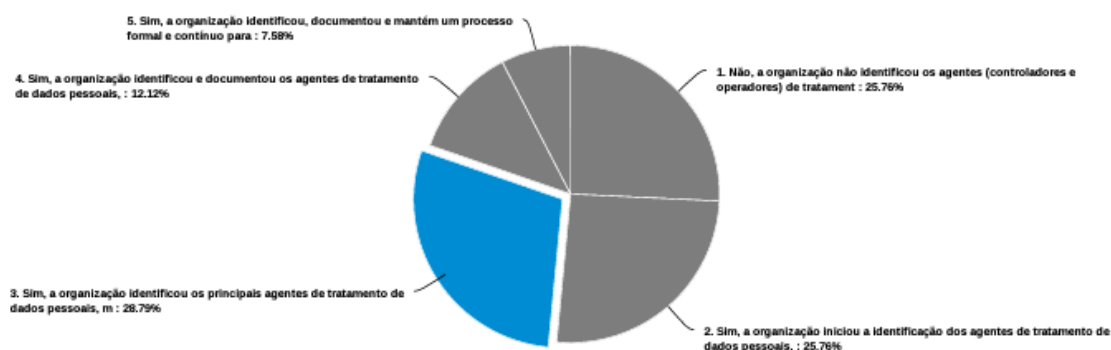
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não segue o princípio da segregação das funções, e o Encarregado de Proteção de Dados (EPD) acumula funções que claramente geram conflitos de interesse.	10	15.38%					
2. Sim, a organização reconhece a importância da segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda acumula outras funções que podem resultar em conflitos de interesse.	26	40%					
3. Sim, a organização implementa a segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda desempenha algumas atividades que podem potencialmente criar conflitos de interesse.	8	12.31%					
4. Sim, a organização implementou a segregação das funções, garantindo que o Encarregado de Proteção de Dados (EPD) tenha autonomia na função. Entretanto, interferências de órgãos superiores comprometem parcialmente essa autonomia.	6	9.23%					
5. Sim, a organização assegura que o Encarregado de Proteção de Dados (EPD) tenha total autonomia e dedicação exclusiva à sua função, sem acumular outras atividades que possam comprometer sua independência ou gerar conflitos de interesse, e sem interferências de órgãos superiores na tomada de decisões.	15	23.08%					
Total	65	n = 65					

7. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não realizou a identificação das categorias de dados pessoais nem dos titulares.	25	37.88%					
2. Sim, a organização identificou algumas categorias de dados pessoais e titulares, mas de forma limitada e incompleta.	17	25.76%					
3. Sim, a organização identificou as principais categorias de dados pessoais e titulares, mas ainda há lacunas ou falta de documentação completa.	14	21.21%					
4. Sim, a organização identificou e documentou as categorias de dados pessoais e titulares, mas há necessidade de revisões, monitoramento ou melhorias no processo.	7	10.61%					
5. Sim, a organização identificou, documentou e mantém um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação.	3	4.55%					
Total	66	n = 66					

8. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição?



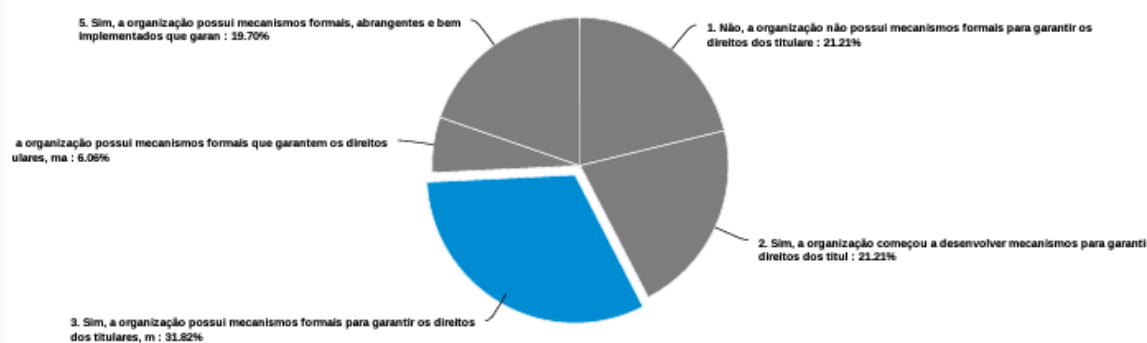
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não identificou os agentes (controladores e operadores) de tratamento de dados pessoais.	17	25.76%					
2. Sim, a organização iniciou a identificação dos agentes de tratamento de dados pessoais, mas o processo é incompleto ou informal.	17	25.76%					
3. Sim, a organização identificou os principais agentes de tratamento de dados pessoais, mas ainda há áreas sem identificação clara ou documentação adequada.	19	28.79%					
4. Sim, a organização identificou e documentou os agentes de tratamento de dados pessoais, mas o processo de monitoramento ou revisão ainda precisa ser aprimorado.	8	12.12%					
5. Sim, a organização identificou, documentou e mantém um processo formal e contínuo para monitorar e revisar os agentes de tratamento de dados pessoais, garantindo conformidade com as normas.	5	7.58%					
Total	66	n = 66					

9. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não identificou os processos e atividades operacionais que lidam com dados pessoais.	20	30.3%					
2. Sim, a organização começou a identificar os processos e atividades operacionais que lidam com dados pessoais, mas o mapeamento é parcial ou informal.	19	28.79%					
3. Sim, a organização identificou os principais processos e atividades que lidam com dados pessoais, mas ainda faltam detalhes ou documentação completa.	17	25.76%					
4. Sim, a organização identificou e documentou os processos e atividades operacionais que lidam com dados pessoais, mas existem áreas que requerem revisões ou melhorias.	6	9.09%					
5. Sim, a organização identificou, documentou e mantém um processo contínuo para monitorar, revisar e melhorar os processos e atividades operacionais que lidam com dados pessoais.	4	6.06%					
Total	66	n = 66					

10. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais?



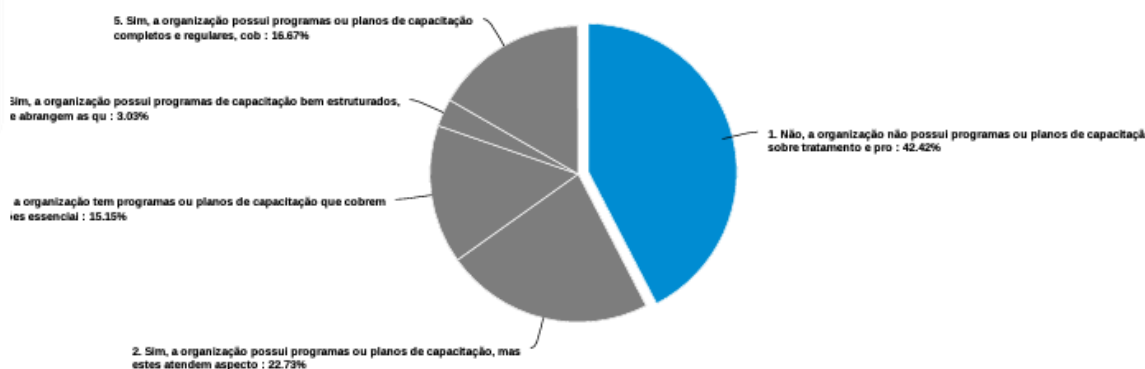
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui mecanismos formais para garantir os direitos dos titulares de dados pessoais.	14	21.21%					
2. Sim, a organização começou a desenvolver mecanismos para garantir os direitos dos titulares, mas estes ainda são limitados ou informais.	14	21.21%					
3. Sim, a organização possui mecanismos formais para garantir os direitos dos titulares, mas eles não são abrangentes ou totalmente implementados.	21	31.82%					
4. Sim, a organização possui mecanismos formais que garantem os direitos dos titulares, mas esses mecanismos existentes não são revisados ou monitorados regularmente.	4	6.06%					
5. Sim, a organização possui mecanismos formais, abrangentes e bem implementados que garantem os direitos dos titulares de dados pessoais, com revisões e melhorias contínuas.	13	19.7%					
Total	66	n = 66					

11. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário?



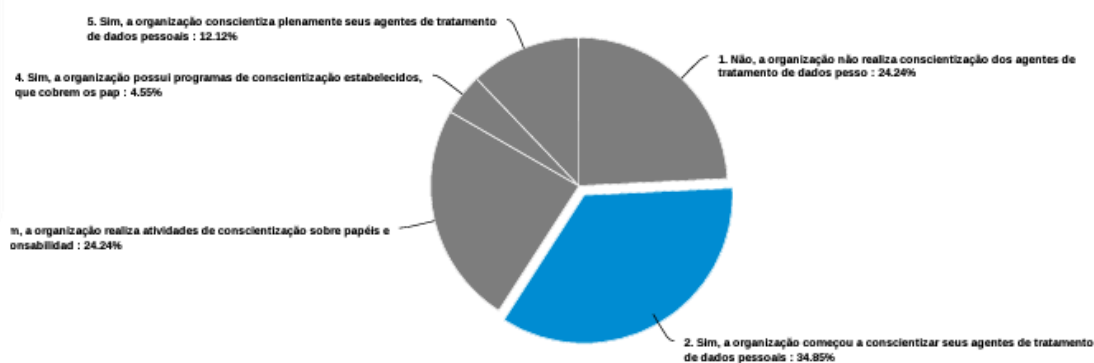
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui regras operacionais para esconder dados pessoais sensíveis, nem utiliza técnicas como mascaramento, pseudonimização ou anonimização.	10	15.38%					
2. Sim, a organização reconhece a importância de proteger dados sensíveis, mas as regras operacionais e técnicas de mascaramento, pseudonimização ou anonimização não são implementadas ou são aplicadas de forma inconsistente.	20	30.77%					
3. Sim, a organização desenvolveu regras operacionais e começou a aplicar técnicas de mascaramento, pseudonimização ou anonimização, mas a aplicação é parcial ou não abrange todos os dados sensíveis.	16	24.62%					
4. Sim, a organização possui regras operacionais bem estabelecidas para esconder dados pessoais sensíveis, utilizando técnicas adequadas, mas há áreas que necessitam de aprimoramento e monitoramento.	14	21.54%					
5. Sim, a organização estabelece e aplica rigorosamente regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de forma consistente, abrangente e monitorada regularmente.	5	7.69%					
Total	65	n = 65					

12. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais?



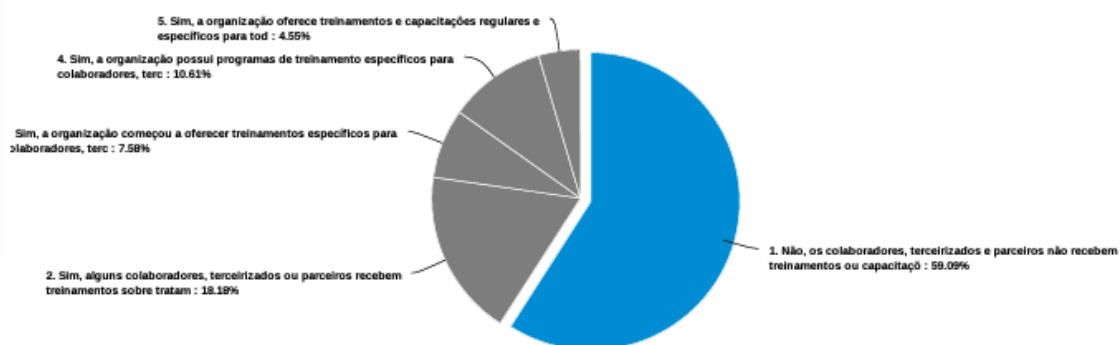
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui programas ou planos de capacitação sobre tratamento e proteção de dados e informações pessoais.	28	42.42%					
2. Sim, a organização possui programas ou planos de capacitação, mas estes atendem aspectos pontuais relacionados ao tratamento e proteção de dados e informações pessoais.	15	22.73%					
3. Sim, a organização tem programas ou planos de capacitação que cobrem questões essenciais sobre o tratamento e a proteção de dados e informações pessoais, mas algumas áreas ainda precisam ser aprimoradas para garantir a efetividade do treinamento.	10	15.15%					
4. Sim, a organização possui programas de capacitação bem estruturados, que abrangem as questões relevantes sobre o tratamento e a proteção de dados e informações pessoais, mas os programas não são atualizados nem monitorados regularmente.	2	3.03%					
5. Sim, a organização possui programas ou planos de capacitação completos e regulares, cobrindo o tratamento e a proteção de dados e informações pessoais, com revisão e atualização contínuas para garantir a eficácia.	11	16.67%					
Total	66	n = 66					

13. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não realiza conscientização dos agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades.	16	24.24%					
2. Sim, a organização começou a conscientizar seus agentes de tratamento de dados pessoais, mas as atividades são pontuais e não cobrem todas as responsabilidades.	23	34.85%					
3. Sim, a organização realiza atividades de conscientização sobre papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas ainda há lacunas na abrangência ou na frequência dessas atividades.	16	24.24%					
4. Sim, a organização possui programas de conscientização estabelecidos, que cobrem os papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas a aplicação não é monitorada regularmente.	3	4.55%					
5. Sim, a organização conscientiza plenamente seus agentes de tratamento de dados pessoais sobre todos os seus papéis e responsabilidades, com programas contínuos e abrangentes de capacitação.	8	12.12%					
Total	66	n = 66					

14. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais recebem treinamentos e capacitações específicas sobre o tema?



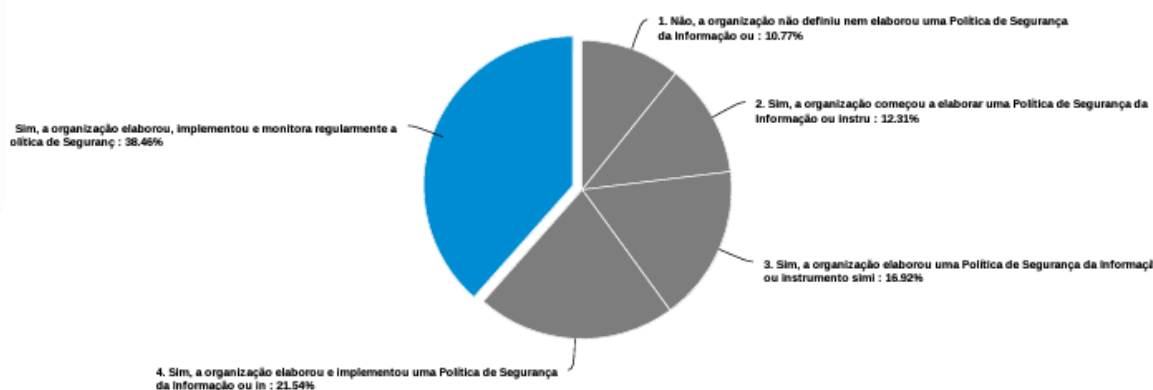
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, os colaboradores, terceirizados e parceiros não recebem treinamentos ou capacitações sobre o tema e proteção de dados pessoais.	39	59.09%					
2. Sim, alguns colaboradores, terceirizados ou parceiros recebem treinamentos sobre o tratamento de dados pessoais, mas de forma pontual e não abrangendo todos os envolvidos.	12	18.18%					
3. Sim, a organização começou a oferecer treinamentos específicos para colaboradores, terceirizados e parceiros sobre o tratamento de dados pessoais, mas ainda não são abrangentes ou regulares.	5	7.58%					
4. Sim, a organização possui programas de treinamento específicos para colaboradores, terceirizados e parceiros, cobrindo assuntos relacionados ao tratamento e proteção de dados pessoais, mas ainda há melhorias necessárias nesse programa.	7	10.61%					
5. Sim, a organização oferece treinamentos e capacitações regulares e específicos para todos os colaboradores, terceirizados e parceiros, garantindo que todos estejam capacitados para tratar dados e informações pessoais de forma segura e conforme as regulamentações.	3	4.55%					
Total	66	n = 66					

15. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais?



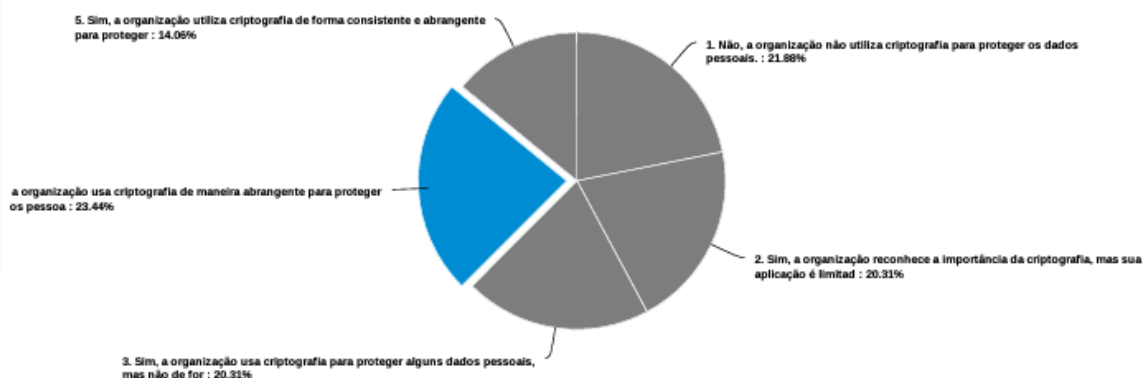
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não realiza conscientização sobre esses riscos.	22	33.33%					
2. Sim, a organização começou a conscientizar sobre os riscos, mas as atividades são esporádicas e não cobrem todos os aspectos críticos.	22	33.33%					
3. Sim, a organização realiza conscientização sobre os riscos de forma regular, mas ainda há lacunas na cobertura de todos os riscos ou áreas específicas de tratamento de dados pessoais.	13	19.7%					
4. Sim, a organização possui um programa regular de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, mas com necessidade de melhorias em algumas áreas.	5	7.58%					
5. Sim, a organização realiza conscientização contínua e abrangente sobre todos os riscos associados ao tratamento inadequado de dados pessoais.	4	6.06%					
Total	66	n = 66					

16. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar?



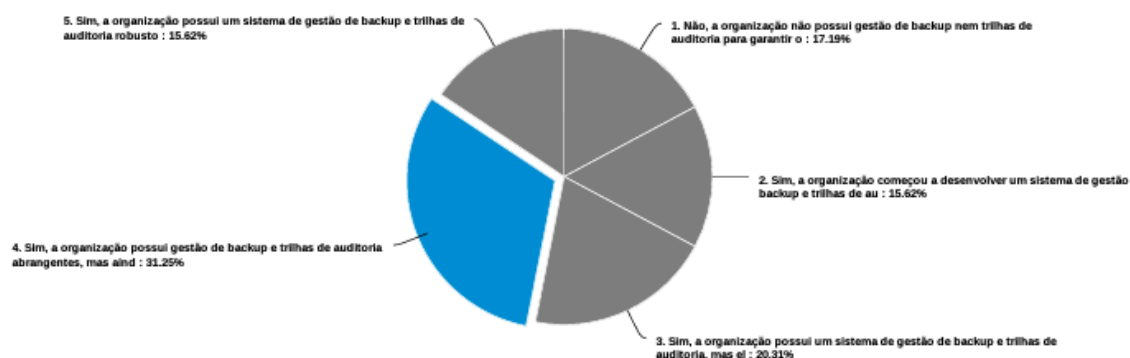
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não definiu nem elaborou uma Política de Segurança da Informação ou documento similar.	7	10.77%					
2. Sim, a organização começou a elaborar uma Política de Segurança da Informação ou instrumento similar, mas ainda está em fase de elaboração.	8	12.31%					
3. Sim, a organização elaborou uma Política de Segurança da Informação ou instrumento similar, mas sua implementação é parcial ou não foi formalmente adotada.	11	16.92%					
4. Sim, a organização elaborou e implementou uma Política de Segurança da Informação ou instrumento similar, mas ainda não realiza monitoramento ou revisões regulares.	14	21.54%					
5. Sim, a organização elaborou, implementou e monitora regularmente a Política de Segurança da Informação ou instrumento similar, assegurando conformidade contínua com as normas e regulamentações aplicáveis.	25	38.46%					
Total	65	n = 65					

17. A organização usa criptografia para proteger os dados pessoais?



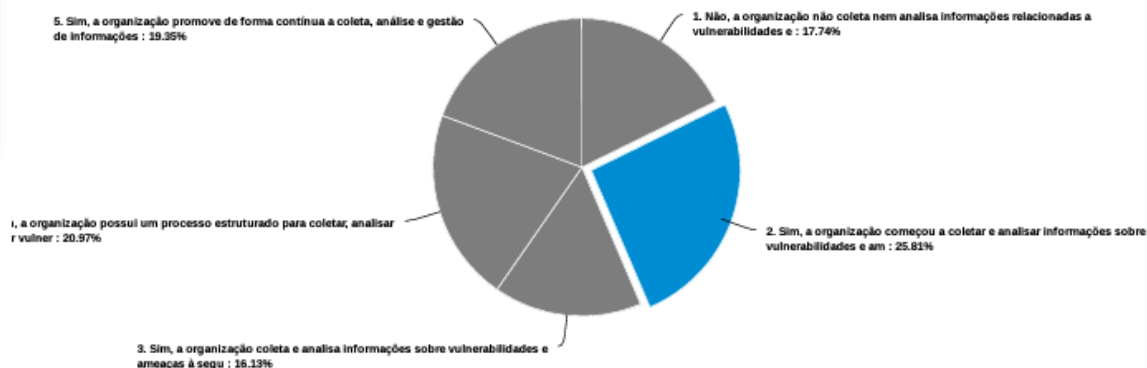
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não utiliza criptografia para proteger os dados pessoais.	14	21.88%					
2. Sim, a organização reconhece a importância da criptografia, mas sua aplicação é limitada ou inconsistente.	13	20.31%					
3. Sim, a organização usa criptografia para proteger alguns dados pessoais, mas não de forma abrangente ou em todas as áreas necessárias.	13	20.31%					
4. Sim, a organização usa criptografia de maneira abrangente para proteger os dados pessoais, mas ainda existem áreas que necessitam de melhorias ou revisões.	15	23.44%					
5. Sim, a organização utiliza criptografia de forma consistente e abrangente para proteger todos os dados pessoais, com monitoramento contínuo e revisões regulares para garantir a segurança.	9	14.06%					
Total	64	n = 64					

18. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui gestão de backup nem trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais.	11	17.19%					
2. Sim, a organização começou a desenvolver um sistema de gestão de backup e trilhas de auditoria, mas de forma limitada ou informal.	10	15.62%					
3. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria, mas ele não cobre todas as áreas necessárias ou não é aplicado de forma consistente.	13	20.31%					
4. Sim, a organização possui gestão de backup e trilhas de auditoria abrangentes, mas ainda há necessidade de melhorias ou maior integração com as práticas de gestão de dados.	20	31.25%					
5. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria robusto e bem implementado, que garante a proteção e integridade dos dados e informações pessoais em todas as fases do ciclo de vida.	10	15.62%					
Total	64	n = 64					

19. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades?



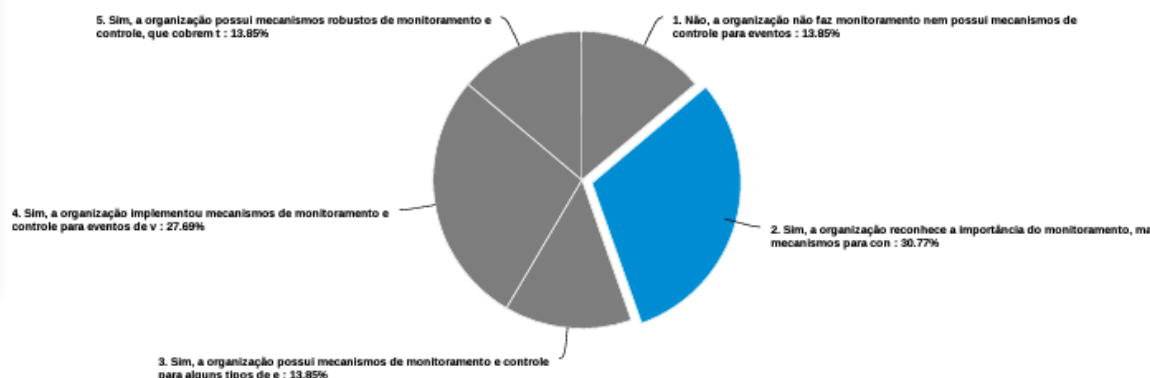
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não coleta nem analisa informações relacionadas a vulnerabilidades e ameaças à segurança da informação.	11	17.74%					
2. Sim, a organização começou a coletar e analisar informações sobre vulnerabilidades e ameaças, mas o processo é informal ou limitado.	16	25.81%					
3. Sim, a organização coleta e analisa informações sobre vulnerabilidades e ameaças à segurança da informação, mas ainda não possui um processo estruturado para gestão de vulnerabilidades.	10	16.13%					
4. Sim, a organização possui um processo estruturado para coletar, analisar e gerir vulnerabilidades e ameaças à segurança da informação, mas precisa de melhorias ou maior abrangência.	13	20.97%					
5. Sim, a organização promove de forma contínua a coleta, análise e gestão de informações sobre vulnerabilidades e ameaças à segurança da informação, com produção de inteligência e ações preventivas robustas.	12	19.35%					
Total	62	n = 62					

20. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes?



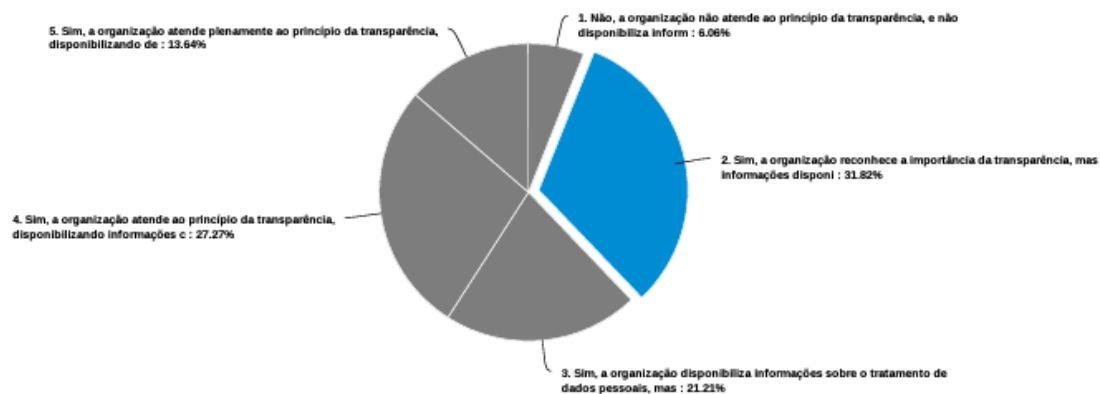
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui controle de acesso nem autenticação segura às informações pessoais.	4	6.25%					
2. Sim, a organização reconhece a necessidade de controle de acesso e autenticação segura, mas a implementação é parcial ou inconsistente.	10	15.62%					
3. Sim, a organização estabeleceu controle de acesso e autenticação segura para algumas áreas, mas ainda existem lacunas ou áreas não cobertas.	16	25%					
4. Sim, a organização possui controle de acesso e autenticação segura para a maioria das áreas, mas ainda precisa monitorar e realizar revisões regulares.	21	32.81%					
5. Sim, a organização estabelece e mantém controle de acesso e autenticação segura em todas as áreas, com conformidade total às legislações e normas vigentes, e realiza revisões e aprimoramentos contínuos.	13	20.31%					
Total	64	n = 64					

21. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais?



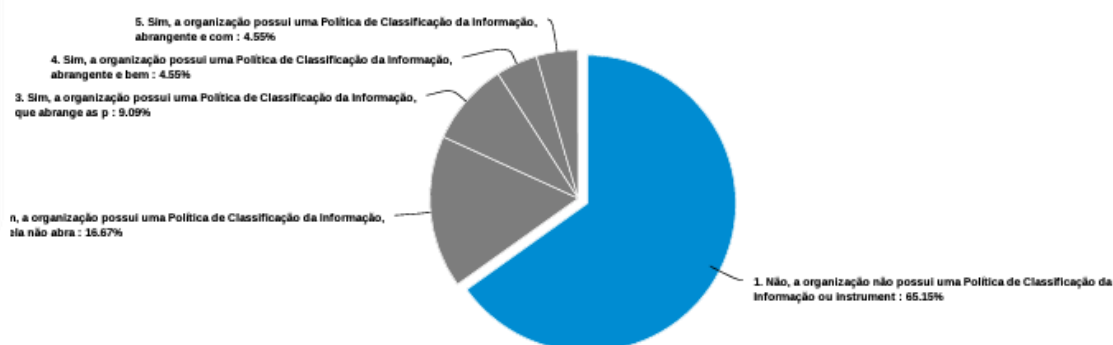
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não faz monitoramento nem possui mecanismos de controle para eventos de violação e vazamento de dados pessoais.	9	13.85%					
2. Sim, a organização reconhece a importância do monitoramento, mas os mecanismos para controle e resposta a eventos de violação e vazamento de dados pessoais são limitados ou não estão formalmente implementados.	20	30.77%					
3. Sim, a organização possui mecanismos de monitoramento e controle para alguns tipos de eventos de violação e vazamento de dados pessoais, mas eles não são abrangentes nem regularmente revisados.	9	13.85%					
4. Sim, a organização implementou mecanismos de monitoramento e controle para eventos de violação e vazamento de dados pessoais, mas ainda existem áreas que precisam de aprimoramento e maior integração com outras práticas de segurança.	18	27.69%					
5. Sim, a organização possui mecanismos robustos de monitoramento e controle, que cobrem todos os eventos de violação e vazamento de dados pessoais, e são revisados e aprimorados regularmente para garantir conformidade com as normas.	9	13.85%					
Total	65	n = 65					

22. A organização atende ao princípio da transparência?



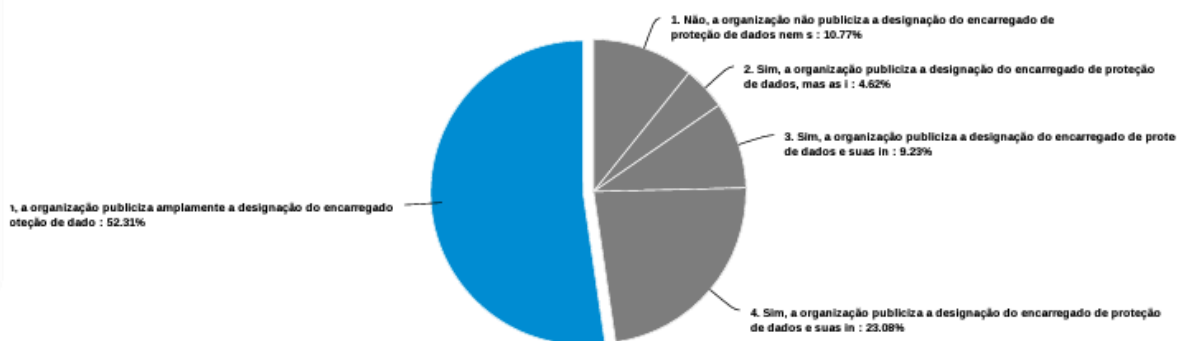
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não atende ao princípio da transparência, e não disponibiliza informações claras e acessíveis sobre o tratamento de dados pessoais.	4	6.06%					
2. Sim, a organização reconhece a importância da transparência, mas as informações disponibilizadas sobre o tratamento de dados pessoais são limitadas ou não estão acessíveis de maneira clara para todos os interessados.	21	31.82%					
3. Sim, a organização disponibiliza informações sobre o tratamento de dados pessoais, mas estas não cobrem todas as exigências legais ou carecem de clareza e acessibilidade.	14	21.21%					
4. Sim, a organização atende ao princípio da transparência, disponibilizando informações claras, acessíveis e abrangentes sobre o tratamento de dados pessoais, mas ainda existem áreas que podem ser aprimoradas, e o monitoramento dessas práticas não é realizado de forma contínua.	18	27.27%					
5. Sim, a organização atende plenamente ao princípio da transparência, disponibilizando de forma clara, acessível e completa todas as informações necessárias sobre o tratamento de dados pessoais, com monitoramento e controle contínuos para garantir conformidade com as regulamentações aplicáveis.	9	13.64%					
Total	66	n = 66					

23. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes?



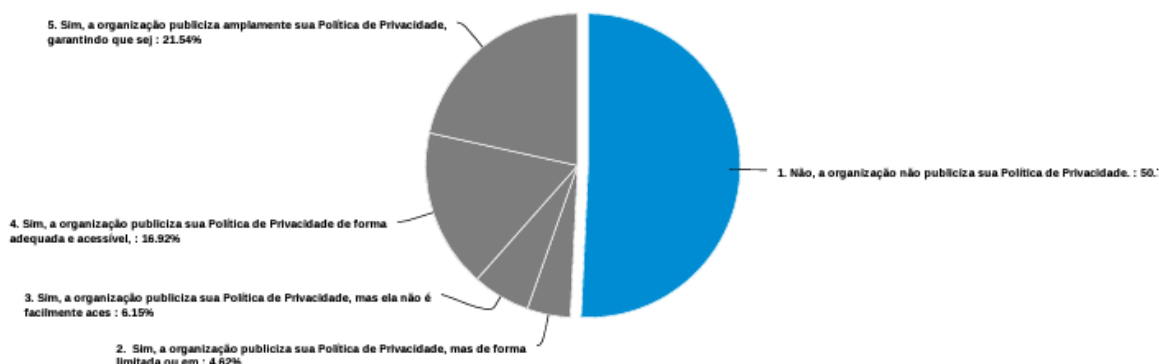
Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não possui uma Política de Classificação da Informação ou instrumento similar.	43	65.15%					
2. Sim, a organização possui uma Política de Classificação da Informação, mas ela não abrange todas as categorias de dados, especialmente os dados sensíveis e os relacionados a crianças e adolescentes.	11	16.67%					
3. Sim, a organização possui uma Política de Classificação da Informação, que abrange as principais categorias de dados, mas ainda há lacunas ou áreas que necessitam de revisão.	6	9.09%					
4. Sim, a organização possui uma Política de Classificação da Informação, abrangente e bem estruturada, mas que ainda necessita de aprimoramentos ou de monitoramento contínuo.	3	4.55%					
5. Sim, a organização possui uma Política de Classificação da Informação, abrangente e completamente implementada, cobrindo todas as categorias de dados, incluindo dados pessoais sensíveis e os relacionados a crianças e adolescentes, com revisões regulares para assegurar conformidade.	3	4.55%					
Total	66	n = 66					

24. A designação do encarregado e suas informações de contato foram publicizadas em algum meio de comunicação oficial?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não publiciza a designação do encarregado de proteção de dados nem suas informações de contato.	7	10.77%					
2. Sim, a organização publiciza a designação do encarregado de proteção de dados, mas as informações de contato não estão facilmente acessíveis ou são limitadas.	3	4.62%					
3. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato, mas a divulgação não é ampla ou acessível a todos os interessados.	6	9.23%					
4. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato de forma adequada, mas não há monitoramento da acessibilidade para garantir que as informações estejam disponíveis e acessíveis a todos.	15	23.08%					
5. Sim, a organização publiciza amplamente a designação do encarregado de proteção de dados e suas informações de contato, garantindo fácil acesso e disponibilidade contínua para todos os interessados, com monitoramento regular dessa acessibilidade.	34	52.31%					
Total	65	n = 65					

25. A Política de Privacidade da organização está publicizada?



Resposta	Contagem	Porcentagem	20%	40%	60%	80%	100%
1. Não, a organização não publiciza sua Política de Privacidade.	33	50.77%					
2. Sim, a organização publiciza sua Política de Privacidade, mas de forma limitada ou em meios de comunicação de difícil acesso.	3	4.62%					
3. Sim, a organização publiciza sua Política de Privacidade, mas ela não é facilmente acessível e compreensível para todos os interessados.	4	6.15%					
4. Sim, a organização publiciza sua Política de Privacidade de forma adequada e acessível, mas ainda há necessidade de melhorias na comunicação ou atualização regular.	11	16.92%					
5. Sim, a organização publiciza amplamente sua Política de Privacidade, garantindo que seja facilmente acessível, compreensível e regularmente revisada para garantir conformidade com as regulamentações aplicáveis.	14	21.54%					
Total	65	n = 65					

APÊNDICE O – Instrumento de medição ajustado após o teste piloto

TRATAMENTO DE DADOS E INFORMAÇÕES PESSOAIS NA INSTITUIÇÃO

Considerando a Constituição Federal de 1988;

Considerando a Lei nº 7.232/1984 (Política Nacional de Informática); a Lei nº 8.159/1991 (Lei de Arquivos); a Lei nº 10.741/2003 (Estatuto do Idoso); a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados);

Considerando o Decreto nº 7.724/2012, o Decreto nº 9.637/2018, o Decreto nº 10.046/2019 e o Decreto-Lei nº 2.848/1940 (Código Civil);

Considerando a Norma ABNT NBR ISO/IEC 27701:2019, a Norma ABNT NBR ISO/IEC 27014:2021, a Norma ABNT NBR ISO/IEC 27002:2022, a Norma ABNT NBR ISO/IEC 27005:2023, a Norma ABNT NBR ISO/IEC 27035:2023 e a Norma ABNT NBR ISO/IEC 29134:2023;

Considerando a Instrução Normativa GSI/PR 1/2020 e a Instrução Normativa SGD/ME nº 117/2020;

Considerando a Resolução CONARQ nº 54/2023;

Solicito, de forma objetiva, a esta instituição o fornecimento das informações pertinentes ao questionário abaixo, conforme as normativas mencionadas.

Nome da Universidade

1. A organização elaborou um programa de governança, plano de governança ou documento equivalente para conduzir iniciativas na identificação, planejamento ou implementação das medidas necessárias para garantir a conformidade no que diz respeito ao tratamento de dados pessoais?

- ☐ 1. Não, a organização ainda não elaborou um programa, plano de governança ou documento com esse direcionamento.
- ☐ 2. Sim, a organização está em fase inicial de elaboração do programa, plano de governança ou documento equivalente com esse direcionamento.

- ☐ 3. Sim, a organização já elaborou um programa, plano de governança ou documento equivalente com esse direcionamento, mas este ainda não foi totalmente implementado.
- ☐ 4. Sim, a organização elaborou e implementou o programa, plano de governança ou documento equivalente com esse direcionamento, mas este documento não é monitorado regularmente.
- ☐ 5. Sim, a organização elaborou e implementou completamente o programa, plano de governança ou documento equivalente com esse direcionamento, e está monitorando regularmente para garantir a conformidade contínua com as regulamentações sobre tratamento e proteção de dados pessoais.

2. A organização designou formalmente o Encarregado de Proteção de Dados (EPD) ou Data Protection Officer (DPO)?

- ☐ 1. Não, a organização não designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO.
- ☐ 2. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas suas funções não estão claramente definidas.
- ☐ 3. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, mas sua atuação é limitada e/ou não é amplamente reconhecida internamente.
- ☐ 4. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, com papel reconhecido, mas ainda há lacunas na sua atuação ou na integração com outras áreas.
- ☐ 5. Sim, a organização designou formalmente um Encarregado de Proteção de Dados (EPD) ou DPO, que atua de forma efetiva, integrada às áreas, e com reconhecimento e suporte da alta administração.

3. A organização estabeleceu comitê interno ou equivalente para acompanhar e lidar com questões relacionadas ao tratamento de dados pessoais na instituição, assegurando compliance com todas as leis e regulamentações aplicáveis?

- ☐ 1. Não, a organização não possui um comitê ou equivalente.
- ☐ 2. Sim, a organização possui um comitê, mas não está ativo ou não tem funções definidas.
- ☐ 3. Sim, a organização possui um comitê ativo, mas ele se concentra apenas em tarefas pontuais ou de suporte, sem uma atuação estratégica.

- ☐ 4. Sim, a organização possui um comitê ativo com funções bem definidas, e está desenvolvendo sua capacidade de atuação estratégica e integração com todas as áreas relevantes.
- ☐ 5. Sim, a organização possui um comitê ativo, com funções bem definidas, que cobre todas as áreas necessárias e está em plena operação.

4. A organização possui Política de Privacidade ou documento equivalente que determine e forneça informações sobre o tratamento dos dados pessoais fornecidos pelos titulares?

- ☐ 1. Não, a organização ainda não possui uma Política de Privacidade.
- ☐ 2. Sim, a instituição está desenvolvendo uma Política de Privacidade, mas ela ainda está em fase de elaboração.
- ☐ 3. Sim, a instituição possui uma Política de Privacidade, mas não é aplicada de maneira consistente.
- ☐ 4. Sim, a instituição possui uma Política de Privacidade, que é aplicada e divulgada, mas ainda precisa de melhorias.
- ☐ 5. Sim, a instituição possui uma Política de Privacidade, que é divulgada, aplicada de forma consistente e regularmente revisada.

5. A organização identificou se existe compartilhamento ou transferência de dados pessoais na instituição?

- ☐ 1. Não, a organização não identificou o compartilhamento ou transferência de dados pessoais.
- ☐ 2. Sim, a organização começou a mapear o compartilhamento ou transferência de dados pessoais, mas o processo é incompleto ou informal.
- ☐ 3. Sim, a organização identificou as principais áreas onde ocorre compartilhamento ou transferência de dados pessoais, mas ainda não há uma visão abrangente ou documentada.
- ☐ 4. Sim, a organização identificou e documentou o compartilhamento e a transferência de dados pessoais, mas faltam procedimentos formais para monitoramento ou controle.
- ☐ 5. Sim, a organização identificou, documentou e implantou procedimentos formais para monitorar e controlar o compartilhamento e a transferência de dados pessoais, com revisões regulares para garantir conformidade.

6. A organização segue o princípio da segregação das funções, evitando que o Encarregado de Proteção de Dados (EPD) assuma outras funções que possam gerar conflitos de interesse?

- ☐ 1. Não, a organização não segue o princípio da segregação das funções, e o Encarregado de Proteção de Dados (EPD) acumula funções que claramente geram conflitos de interesse. Caso a organização não tenha designado o EPD, essa alternativa será considerada 'não aplicável' e equiparada à alternativa de resposta 'não implementado', visto que descumpre um requisito legal.
- ☐ 2. Sim, a organização reconhece a importância da segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda acumula outras funções que podem resultar em conflitos de interesse.
- ☐ 3. Sim, a organização implementa a segregação das funções, mas o Encarregado de Proteção de Dados (EPD) ainda desempenha algumas atividades que podem potencialmente criar conflitos de interesse.
- ☐ 4. Sim, a organização implementou a segregação das funções, garantindo que o Encarregado de Proteção de Dados (EPD) tenha autonomia na função. Entretanto, interferências de órgãos superiores comprometem parcialmente essa autonomia.
- ☐ 5. Sim, a organização assegura que o Encarregado de Proteção de Dados (EPD) tenha total autonomia e dedicação exclusiva à sua função, sem acumular outras atividades que possam comprometer sua independência ou gerar conflitos de interesse, e sem interferências de órgãos superiores na tomada de decisões.

7. A organização realizou a identificação das categorias de dados pessoais e dos titulares de dados pessoais com os quais a instituição mantém relação?

- ☐ 1. Não, a organização não realizou a identificação das categorias de dados pessoais nem dos titulares.
- ☐ 2. Sim, a organização identificou algumas categorias de dados pessoais e titulares, mas de forma limitada e incompleta.
- ☐ 3. Sim, a organização identificou as principais categorias de dados pessoais e titulares, mas ainda há lacunas ou falta de documentação completa.
- ☐ 4. Sim, a organização identificou e documentou as categorias de dados pessoais e titulares, mas há necessidade de revisões, monitoramento ou melhorias no processo.
- ☐ 5. Sim, a organização identificou, documentou e mantém um controle contínuo e atualizado das categorias de dados pessoais e dos titulares com os quais mantém relação.

8. A organização realizou a identificação dos agentes (controladores e operadores) de tratamento de dados pessoais da instituição?

- ☐ 1. Não, a organização não identificou os agentes (controladores e operadores) de tratamento de dados pessoais.
- ☐ 2. Sim, a organização iniciou a identificação dos agentes de tratamento de dados pessoais, mas o processo é incompleto ou informal.
- ☐ 3. Sim, a organização identificou os principais agentes de tratamento de dados pessoais, mas ainda há áreas sem identificação clara ou documentação adequada.
- ☐ 4. Sim, a organização identificou e documentou os agentes de tratamento de dados pessoais, mas o processo de monitoramento ou revisão ainda precisa ser aprimorado.
- ☐ 5. Sim, a organização identificou, documentou e mantém um processo formal e contínuo para monitorar e revisar os agentes de tratamento de dados pessoais, garantindo conformidade com as normas.

9. A organização realizou a identificação dos processos e atividades operacionais que lidam com dados pessoais?

- ☐ 1. Não, a organização não identificou os processos e atividades operacionais que lidam com dados pessoais.
- ☐ 2. Sim, a organização começou a identificar os processos e atividades operacionais que lidam com dados pessoais, mas o mapeamento é parcial ou informal.
- ☐ 3. Sim, a organização identificou os principais processos e atividades que lidam com dados pessoais, mas ainda faltam detalhes ou documentação completa.
- ☐ 4. Sim, a organização identificou e documentou os processos e atividades operacionais que lidam com dados pessoais, mas existem áreas que requerem revisões ou melhorias.
- ☐ 5. Sim, a organização identificou, documentou e mantém um processo contínuo para monitorar, revisar e melhorar os processos e atividades operacionais que lidam com dados pessoais.

10. Existem mecanismos formais na organização que garantam os direitos dos titulares de dados pessoais?

- ☐ 1. Não, a organização não possui mecanismos formais para garantir os direitos dos titulares de dados pessoais.
- ☐ 2. Sim, a organização começou a desenvolver mecanismos para garantir os direitos dos titulares, mas estes ainda são limitados ou informais.
- ☐ 3. Sim, a organização possui mecanismos formais para garantir os direitos dos titulares, mas eles não são abrangentes ou totalmente implementados.
- ☐ 4. Sim, a organização possui mecanismos formais que garantem os direitos dos titulares, mas esses mecanismos existentes não são revisados ou monitorados regularmente.
- ☐ 5. Sim, a organização possui mecanismos formais, abrangentes e bem implementados que garantem os direitos dos titulares de dados pessoais, com revisões e melhorias contínuas.

11. A organização estabelece regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de dados, quando necessário?

- ☐ 1. Não, a organização não possui regras operacionais para esconder dados pessoais sensíveis, nem utiliza técnicas como mascaramento, pseudonimização ou anonimização.
- ☐ 2. Sim, a organização reconhece a importância de proteger dados sensíveis, mas as regras operacionais e técnicas de mascaramento, pseudonimização ou anonimização não são implementadas ou são aplicadas de forma inconsistente.
- ☐ 3. Sim, a organização desenvolveu regras operacionais e começou a aplicar técnicas de mascaramento, pseudonimização ou anonimização, mas a aplicação é parcial ou não abrange todos os dados sensíveis.
- ☐ 4. Sim, a organização possui regras operacionais bem estabelecidas para esconder dados pessoais sensíveis, utilizando técnicas adequadas, mas há áreas que necessitam de aprimoramento e monitoramento.
- ☐ 5. Sim, a organização estabelece e aplica rigorosamente regras operacionais para esconder dados pessoais sensíveis, utilizando técnicas como mascaramento, pseudonimização ou anonimização de forma consistente, abrangente e monitorada regularmente.

12. A organização possui programas ou planos de capacitação que abranjam treinamento e conscientização sobre questões relacionadas ao tratamento e proteção de dados e informações pessoais?

- ☐ 1. Não, a organização não possui programas ou planos de capacitação sobre tratamento e proteção de dados e informações pessoais.
- ☐ 2. Sim, a organização possui programas ou planos de capacitação, mas estes atendem aspectos pontuais relacionados ao tratamento e proteção de dados e informações pessoais.
- ☐ 3. Sim, a organização tem programas ou planos de capacitação que cobrem questões essenciais sobre o tratamento e a proteção de dados e informações pessoais, mas algumas áreas ainda precisam ser aprimoradas para garantir a efetividade do treinamento.
- ☐ 4. Sim, a organização possui programas de capacitação bem estruturados, que abrangem as questões relevantes sobre o tratamento e a proteção de dados e informações pessoais, mas os programas não são atualizados nem monitorados regularmente.
- ☐ 5. Sim, a organização possui programas ou planos de capacitação completos e regulares, cobrindo o tratamento e a proteção de dados e informações pessoais, com revisão e atualização contínuas para garantir a eficácia.

13. A organização conscientiza os seus agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades?

- ☐ 1. Não, a organização não realiza conscientização dos agentes de tratamento de dados pessoais sobre seus papéis e responsabilidades.
- ☐ 2. Sim, a organização começou a conscientizar seus agentes de tratamento de dados pessoais, mas as atividades são pontuais e não cobrem todas as responsabilidades.
- ☐ 3. Sim, a organização realiza atividades de conscientização sobre papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas ainda há lacunas na abrangência ou na frequência dessas atividades.
- ☐ 4. Sim, a organização possui programas de conscientização estabelecidos, que cobrem os papéis e responsabilidades dos agentes de tratamento de dados pessoais, mas a aplicação não é monitorada regularmente.
- ☐ 5. Sim, a organização conscientiza plenamente seus agentes de tratamento de dados pessoais sobre todos os seus papéis e responsabilidades, com programas contínuos e abrangentes de capacitação.

14. Os colaboradores (terceirizados e parceiros) da organização que exercem atividades atreladas ao tratamento de dados pessoais recebem treinamentos e capacitações específicas

sobre o tema?

- ☐ 1. Não, os colaboradores, terceirizados e parceiros não recebem treinamentos ou capacitações sobre tratamento e proteção de dados pessoais.
- ☐ 2. Sim, alguns colaboradores, terceirizados ou parceiros recebem treinamentos sobre tratamento de dados pessoais, mas de forma pontual e não abrange todos os envolvidos.
- ☐ 3. Sim, a organização começou a oferecer treinamentos específicos para colaboradores, terceirizados e parceiros sobre tratamento de dados pessoais, mas ainda não são abrangentes ou regulares.
- ☐ 4. Sim, a organização possui programas de treinamento específicos para colaboradores, terceirizados e parceiros, cobrindo assuntos relacionados ao tratamento e proteção de dados pessoais, mas ainda há melhorias necessárias nesse programa.
- ☐ 5. Sim, a organização oferece treinamentos e capacitações regulares e específicos para todos os colaboradores, terceirizados e parceiros, garantindo que todos estejam capacitados para tratar dados e informações pessoais de forma segura e conforme as regulamentações.

15. A organização conscientiza regularmente quanto aos riscos associados ao tratamento inadequado de dados pessoais?

- ☐ 1. Não, a organização não realiza conscientização sobre esses riscos.
- ☐ 2. Sim, a organização começou a conscientizar sobre os riscos, mas as atividades são esporádicas e não cobrem todos os aspectos críticos.
- ☐ 3. Sim, a organização realiza conscientização sobre os riscos de forma regular, mas ainda há lacunas na cobertura de todos os riscos ou áreas específicas de tratamento de dados pessoais.
- ☐ 4. Sim, a organização possui um programa regular de conscientização sobre os riscos associados ao tratamento inadequado de dados pessoais, mas com necessidade de melhorias em algumas áreas.
- ☐ 5. Sim, a organização realiza conscientização contínua e abrangente sobre todos os riscos associados ao tratamento inadequado de dados pessoais.

16. A organização definiu e elaborou a Política de Segurança da Informação ou instrumento similar?

- ☐ 1. Não, a organização não definiu nem elaborou uma Política de Segurança da Informação ou documento similar.
- ☐ 2. Sim, a organização começou a elaborar uma Política de Segurança da Informação ou instrumento similar, mas ainda está em fase de elaboração.
- ☐ 3. Sim, a organização elaborou uma Política de Segurança da Informação ou instrumento similar, mas sua implementação é parcial ou não foi formalmente adotada.
- ☐ 4. Sim, a organização elaborou e implementou uma Política de Segurança da Informação ou instrumento similar, mas ainda não realiza monitoramento ou revisões regulares.
- ☐ 5. Sim, a organização elaborou, implementou e monitora regularmente a Política de Segurança da Informação ou instrumento similar, assegurando conformidade contínua com as normas e regulamentações aplicáveis.

17. A organização usa criptografia para proteger os dados pessoais?

- ☐ 1. Não, a organização não utiliza criptografia para proteger os dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância da criptografia, mas sua aplicação é limitada ou inconsistente.
- ☐ 3. Sim, a organização usa criptografia para proteger alguns dados pessoais, mas não de forma abrangente ou em todas as áreas necessárias.
- ☐ 4. Sim, a organização usa criptografia de maneira abrangente para proteger os dados pessoais, mas ainda existem áreas que necessitam de melhorias ou revisões.
- ☐ 5. Sim, a organização utiliza criptografia de forma consistente e abrangente para proteger todos os dados pessoais, com monitoramento contínuo e revisões regulares para garantir a segurança.

18. A organização possui gestão de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais?

- ☐ 1. Não, a organização não possui gestão de backup nem trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais.
- ☐ 2. Sim, a organização começou a desenvolver um sistema de gestão de backup e trilhas de auditoria, mas de forma limitada ou informal.

- ☐ 3. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria, mas ele não cobre todas as áreas necessárias ou não é aplicado de forma consistente.
- ☐ 4. Sim, a organização possui gestão de backup e trilhas de auditoria abrangentes, mas ainda há necessidade de melhorias ou maior integração com as práticas de gestão de dados.
- ☐ 5. Sim, a organização possui um sistema de gestão de backup e trilhas de auditoria robusto e bem implementado, que garante a proteção e integridade dos dados e informações pessoais em todas as fases do ciclo de vida.

19. A organização promove formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades?

- ☐ 1. Não, a organização não coleta nem analisa informações relacionadas a vulnerabilidades e ameaças à segurança da informação.
- ☐ 2. Sim, a organização começou a coletar e analisar informações sobre vulnerabilidades e ameaças, mas o processo é informal ou limitado.
- ☐ 3. Sim, a organização coleta e analisa informações sobre vulnerabilidades e ameaças à segurança da informação, mas ainda não possui um processo estruturado para gestão de vulnerabilidades.
- ☐ 4. Sim, a organização possui um processo estruturado para coletar, analisar e gerir vulnerabilidades e ameaças à segurança da informação, mas precisa de melhorias ou maior abrangência.
- ☐ 5. Sim, a organização promove de forma contínua a coleta, análise e gestão de informações sobre vulnerabilidades e ameaças à segurança da informação, com produção de inteligência e ações preventivas robustas.

20. A organização estabelece controle de acesso e autenticação segura às informações pessoais conforme às legislações e normas vigentes?

- ☐ 1. Não, a organização não possui controle de acesso nem autenticação segura às informações pessoais.
- ☐ 2. Sim, a organização reconhece a necessidade de controle de acesso e autenticação segura, mas a implementação é parcial ou inconsistente.

- ☐ 3. Sim, a organização estabeleceu controle de acesso e autenticação segura para algumas áreas, mas ainda existem lacunas ou áreas não cobertas.
- ☐ 4. Sim, a organização possui controle de acesso e autenticação segura para a maioria das áreas, mas ainda precisa monitorar e realizar revisões regulares.
- ☐ 5. Sim, a organização estabelece e mantém controle de acesso e autenticação segura em todas as áreas, com conformidade total às legislações e normas vigentes, e realiza revisões e aprimoramentos contínuos.

21. A organização faz monitoramento e controle dos eventos associados à violação e vazamento de dados pessoais?

- ☐ 1. Não, a organização não faz monitoramento nem possui mecanismos de controle para eventos de violação e vazamento de dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância do monitoramento, mas os mecanismos para controle e resposta a eventos de violação e vazamento de dados pessoais são limitados ou não estão formalmente implementados.
- ☐ 3. Sim, a organização possui mecanismos de monitoramento e controle para alguns tipos de eventos de violação e vazamento de dados pessoais, mas eles não são abrangentes nem regularmente revisados.
- ☐ 4. Sim, a organização implementou mecanismos de monitoramento e controle para eventos de violação e vazamento de dados pessoais, mas ainda existem áreas que precisam de aprimoramento e maior integração com outras práticas de segurança.
- ☐ 5. Sim, a organização possui mecanismos robustos de monitoramento e controle, que cobrem todos os eventos de violação e vazamento de dados pessoais, e são revisados e aprimorados regularmente para garantir conformidade com as normas.

22. A organização atende ao princípio da transparência?

- ☐ 1. Não, a organização não atende ao princípio da transparência, e não disponibiliza informações claras e acessíveis sobre o tratamento de dados pessoais.
- ☐ 2. Sim, a organização reconhece a importância da transparência, mas as informações disponibilizadas sobre o tratamento de dados pessoais são limitadas ou não estão acessíveis de maneira clara para todos os interessados.

- ☐ 3. Sim, a organização disponibiliza informações sobre o tratamento de dados pessoais, mas estas não cobrem todas as exigências legais ou carecem de clareza e acessibilidade.
- ☐ 4. Sim, a organização atende ao princípio da transparência, disponibilizando informações claras, acessíveis e abrangentes sobre o tratamento de dados pessoais, mas ainda existem áreas que podem ser aprimoradas, e o monitoramento dessas práticas não é realizado de forma contínua.
- ☐ 5. Sim, a organização atende plenamente ao princípio da transparência, disponibilizando de forma clara, acessível e completa todas as informações necessárias sobre o tratamento de dados pessoais, com monitoramento e controle contínuos para garantir conformidade com as regulamentações aplicáveis.

23. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo a classificação de dados pessoais, dados pessoais sensíveis e os dados relacionados a crianças e adolescentes?

- ☐ 1. Não, a organização não possui uma Política de Classificação da Informação ou instrumento similar.
- ☐ 2. Sim, a organização possui uma Política de Classificação da Informação, mas ela não abrange todas as categorias de dados, especialmente os dados sensíveis e os relacionados a crianças e adolescentes.
- ☐ 3. Sim, a organização possui uma Política de Classificação da Informação, que abrange as principais categorias de dados, mas ainda há lacunas ou áreas que necessitam de revisão.
- ☐ 4. Sim, a organização possui uma Política de Classificação da Informação, abrangente e bem estruturada, mas que ainda necessita de aprimoramentos ou de monitoramento contínuo.
- ☐ 5. Sim, a organização possui uma Política de Classificação da Informação, abrangente e completamente implementada, cobrindo todas as categorias de dados, incluindo dados pessoais sensíveis e os relacionados a crianças e adolescentes, com revisões regulares para assegurar conformidade.

24. A designação do encarregado e suas informações de contato foram publicizadas em algum meio de comunicação oficial?

- ☐ 1. Não, a organização não publiciza a designação do encarregado de proteção de dados nem suas informações de contato. Caso não exista a designação do EPD, essa questão, embora classificada como 'não aplicável', será tratada como equivalente a 'não implementado', indicando o descumprimento do artigo 41, § 1º da LGPD.

- ☐ 2. Sim, a organização publiciza a designação do encarregado de proteção de dados, mas as informações de contato não estão facilmente acessíveis ou são limitadas.
- ☐ 3. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato, mas a divulgação não é ampla ou acessível a todos os interessados.
- ☐ 4. Sim, a organização publiciza a designação do encarregado de proteção de dados e suas informações de contato de forma adequada, mas não há monitoramento da acessibilidade para garantir que as informações estejam disponíveis e acessíveis a todos.
- ☐ 5. Sim, a organização publiciza amplamente a designação do encarregado de proteção de dados e suas informações de contato, garantindo fácil acesso e disponibilidade contínua para todos os interessados, com monitoramento regular dessa acessibilidade.

25. A Política de Privacidade da organização está publicizada?

- ☐ 1. Não, a organização não publiciza sua Política de Privacidade. Caso a organização não tenha formalizado ou elaborado uma Política de Privacidade, essa alternativa será considerada 'não aplicável', sendo tratada como equivalente à alternativa 'não implementada', indicando a ausência dessa prática fundamental.
- ☐ 2. Sim, a organização publiciza sua Política de Privacidade, mas de forma limitada ou em meios de comunicação de difícil acesso.
- ☐ 3. Sim, a organização publiciza sua Política de Privacidade, mas ela não é facilmente acessível e compreensível para todos os interessados.
- ☐ 4. Sim, a organização publiciza sua Política de Privacidade de forma adequada e acessível, mas ainda há necessidade de melhorias na comunicação ou atualização regular.
- ☐ 5. Sim, a organização publiciza amplamente sua Política de Privacidade, garantindo que seja facilmente acessível, compreensível e regularmente revisada para garantir conformidade com as regulamentações aplicáveis.