CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM SISTEMAS PRODUTIVOS

MAURICIO FERNANDO MUNHOZ

RAEL - *ROADMAP* PARA ADEQUAÇÃO DE EMPRESAS À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

São Paulo
Março/2024

MAURICIO FERNANDO MUNHOZ

RAEL - *ROADMAP* PARA ADEQUAÇÃO DE EMPRESAS À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Dissertação apresentada como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Carlos Hideo Arima.
Área de Concentração: Sistemas Produtivos

São Paulo

Março/2024

FICHA ELABORADA PELA BIBLIOTECA NELSON ALVES VIANA
FATEC-SP / CPS CRB8-10894

Munhoz, Mauricio Fernando

M966r RAEL : *Roadmap* para adequação de empresas à Lei Geral de Proteção de Dados (LGPD) / Mauricio Fernando Munhoz. – São Paulo: CPS, 2024.
161 f.: il.

Orientador: Prof. Dr. Carlos Hideo Arima
Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) - Centro Estadual de Educação Tecnológica Paula Souza, 2024.

1. *Roadmap*. 2. LGPD. 3. Privacidade. 4. Segurança da Informação. 5. Lei Geral de Proteção de Dados. I. Arima, Carlos Hideo. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

MAURICIO FERNANDO MUNHOZ

RAEL - *ROADMAP* PARA ADEQUAÇÃO DE EMPRESAS À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Prof. Dr. Carlos Hideo Arima
Orientador - CEETEPS

Prof. Dr. Fernando Almeida Santos
Examinador Externo - PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO - PUC

Prof. Dr. Napoleão Verardi Galegale
Examinador Interno - CEETEPS

São Paulo, 26 de março de 2024

À minha mãe, Anita, por seu apoio incansável e dedicação interminável, que sempre me incentivaram a persistir e nunca desistir.

AGRADECIMENTOS

Ao meu orientador, professor Doutor Carlos Hideo Arima, por seu apoio e pela orientação ao longo de todo o processo, por todo o aprendizado e paciência na condução deste trabalho.

Agradeço a minha esposa Cintia e minhas filhas, pelo apoio e compreensão pela ausência ao longo destes dois anos de intenso trabalho e dedicação.

À minha mãe Anita e ao meu irmão Mauro, por proverem apoio e suporte nos momentos de dificuldade.

Aos Professores do Curso de Mestrado Profissional do Centro Paula Souza, pelos valiosos ensinamentos, críticas e sugestões, extremamente valiosas para o aprendizado e para o desenvolvimento da pesquisa.

Aos meus queridos professores da Escola Estadual Professor Eurico Figueiredo, com destaque para professor Ivan de Geografia, professora Inês de História, professor Pedro de Matemática e outros tantos, os quais propiciaram uma formação rica e maravilhosa que me trouxe até aqui.

Ao amigo Fábio Remo Colângelo pelo apoio no desenvolvimento do trabalho de pesquisa.

“A diferença entre ganhar e perder é,
muitas vezes, não desistir.”

Walt Disney

RESUMO

MUNHOZ, M.F. ***Roadmap* para adequação de empresas à Lei Geral de Proteção de Dados (LGPD).** 161f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2024.

O presente trabalho apresenta o desenvolvimento do RAEL - *Roadmap* para Adequação de Empresas à Lei Geral de Proteção de Dados (LGPD), visando oferecer suporte às organizações brasileiras no cumprimento da Lei Geral de Proteção de Dados (LGPD), legislação aprovada em 2018 em resposta à crescente coleta e uso de dados pessoais por empresas. O processo de desenvolvimento foi baseado na metodologia *Design Science Research Methodology* (DRSM) que direciona os objetivos específicos, consistindo em identificar o problema por meio de uma revisão da bibliografia e da aplicação de uma pesquisa *survey* sobre o nível de adequação das organizações à LGPD, com participação de 29 empresas, com destaque para 8 empresas de tecnologia, 6 do setor educacional, 4 do financeiro e 4 da indústria, desenhar e desenvolver o RAEL com apoio o *Design Thinking* e *Scrum*, apresentar seu uso em uma empresa de *data center* da grande São Paulo, obter avaliações de especialistas em TIC e SI e comunicar os resultados à comunidade acadêmica. Espera-se que o RAEL facilite o processo de adequação à LGPD, visando garantir a proteção dos dados privados de clientes, colaboradores e parceiros, bem como contribuir para discussões sobre gestão de segurança da informação e privacidade de dados, promovendo um debate sobre o direito à privacidade e à proteção de dados pessoais, sendo uma contribuição para a conformidade das empresas à legislação de privacidade.

Palavras-Chave: *Roadmap.* LGPD. Privacidade. Segurança da Informação. Lei Geral de Proteção de Dados.

ABSTRACT

MUNHOZ, M.F. ***Roadmap* for adequation companies to LGPD.** 161f. Dissertation (Professional Master's in Management and technology in Production Systems). Paula Souza State Center for Technological Education, São Paulo, 2024.

This work presents the development of RAEL - Roadmap for Adequacy of Companies to the General Data Protection Law (LGPD), aiming to offer support to Brazilian organizations in complying with the General Data Protection Law (LGPD), legislation approved in 2018 in response to the increasing collection and use of personal data by companies. The development process was based on the Design Science Research Methodology (DRSM) methodology, which directs specific objectives, consisting of identifying the problem through a review of the bibliography and the application of a survey on the level of adequacy of organizations to LGPD, with participation of 29 companies, with emphasis to 8 technology companies, 6 from education, 4 from finance and 4 from industry, design and develop RAEL with support from Design Thinking and Scrum, present its use in a data center company in greater São Paulo, obtain evaluations from ICT and IS experts and communicate the results to the academic community. RAEL is expected to facilitate the process of adapting to the LGPD, aiming to guarantee the protection of the private data of customers, employees and partners, as well as contributing to discussions on information security management and data privacy, promoting a debate on the right to privacy and protection of personal data, being a contribution to companies' compliance to privacy legislation.

Keywords: Roadmap. LGPD. Privacy. Information Security. General Law on Data Protection.

LISTA DE FIGURAS

Figura 1 – Etapas componentes do *Design Thinking* segundo Brown 30
Figura 2 – Esquema geral de um *Roadmap* Tecnológico.....33
Figura 3 – Caracterização de *roadmaps* por aplicação/propósito e formato 34
Figura 4 – Caracterização de *roadmaps* por aplicação / propósito 35
Figura 5 – Exemplos de formatos de *roadmaps* de tecnologia.....36
Figura 6 – Exemplo de estrutura de um *roadmap* multicamadas 38
Figura 7 – Lógica para construção das classes de problemas 40
Figura 8 – Fluxo de desenvolvimento do *roadmap* com base na DSRM.....42
Figura 9 – Estrutura do Business Capability Model.....52
Figura 10 – Relação entre os principais componentes do modelo relacionados à literatura 52
Figura 11 – Estrutura geral do modelo para capacitação de processos.....53
Figura 12 – Etapas do método LGPD4BP.....55
Figura 13 – Visão geral do Framework.....61
Figura 14 – Cálculo do coeficiente alpha de Cronbach para os 42 respondentes.....65
Figura 15 – Cálculo do coeficiente alpha de Cronbach excluindo 13 estagiários.....66
Figura 16 – Porte das empresas quanto ao número de funcionários 67
Figura 17 – Setor de atuação das empresas.....67
Figura 18 – Tempo de experiência profissional dos participantes 68
Figura 19 – Departamento X nível hierárquico dos participantes 68
Figura 20 – Envolvimento dos participantes no processo de implementação da LGPD 69
Figura 21 – Percepção do nível de adequação da organização à LGPD (Escala de 1 a 10).....70
Figura 22 – Sua empresa tem recursos financeiros suficientes para adequação à LGPD? 71
Figura 23 – A empresa teve facilidade de identificar ferramentas e métodos que apoiassem a implementação da LGPD? 71
Figura 24 – A empresa teve dificuldade de contratar profissionais para a adequação à LGPD? 72
Figura 25 – Sua empresa tem conhecimento suficiente para adequação à LGPD? 72
Figura 26 – As equipes de TI e segurança da informação da sua empresa estão

suficientemente capacitadas para implementar a LGPD?.....73
Figura 27 – Sua empresa tem políticas e procedimentos relativos à quais aspectos da LGPD? 74
Figura 28 – As políticas e procedimentos de sua organização são adequadas e suficientes para assegurar o atendimento aos requisitos da LGPD? 75
Figura 29 – Medidas implementadas pelas organizações para adequação à LGPD 76
Figura 30 – Áreas que recebem treinamento sobre a LGPD nas empresas pesquisadas 77
Figura 31 – Os dados coletados por sua organização são os estritamente necessários para cumprir os objetivos para os quais foram coletados? 78
Figura 32 – Modelo de governança corporativa de TIC 81
Figura 33 – Controles da ABNT NBR ISO/IEC 27002 82
Figura 34 - Visão geral do RAEL 88

LISTA DE QUADROS

Quadro 1 – Comparativo entre o RAEL e propostas anteriores 17
Quadro 2 – Etapas adicionadas ao RAEL comparando com propostas anteriores ...18
Quadro 3 – Critérios de busca sobre metodologias para implementação da LGPD .20
Quadro 4 – Critérios de seleção sobre métodos para implementação da LGPD 21
Quadro 5 – Critérios de busca de artigos sobre pesquisa ou *survey* relacionadas à LGPD 22
Quadro 6 – Critério seleção de artigos: Uso da IA para adequação de empresas à GDPR ou LGPD 22
Quadro 7 – Artigos resultado da revisão da bibliografia que tenham relação com *survey* ou pesquisa relacionada à LGPD 23
Quadro 8 – Visão geral dos principais artigos da LGPD 26
Quadro 9 – Sumário de artigos analisados 50
Quadro 10 – Artigos selecionados para leitura por atenderem aos critérios de seleção 50
Quadro 11 – Critérios e alternativas possíveis 57
Quadro 12 – Processos propostos para implementação da LGPD em agências da APF 59
Quadro 13 – Programas e seus respectivos controles para implementação da LGPD 62
Quadro 14 – Sumário das propostas de cada artigo analisado 63
Quadro 15 – Outras normas referenciadas no *roadmap* 83
Quadro 16 – Etapas do RAEL com justificativa para a sua inclusão no *roadmap* 85
Quadro 17 – Informações de cada etapa do RAEL 87
Quadro 18 – Questões sobre o perfil dos avaliadores do RAEL 90
Quadro 19 – Questões referentes à avaliação do RAEL 90

LISTA DE TABELAS

Tabela 1 – Matriz de Critérios de Priorização e Prioridade.....58

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ANPD – Autoridade Nacional de Proteção de Dados

CEETEPS – Centro Estadual de Educação Tecnológica Paula Souza

DP – Dados Pessoais

DPIA - *Data Protection Impact Assessment*

DPO – *Data Protection Officer*

DSR – *Design Science Research*

DSRM – *Design Science Research Methodology*

GDPR – *General Data Protection Regulation*

ISO – *International Organization for Standardization*

IEC - *International Electrotechnical Commission*

LGPD – Lei Geral de Proteção de Dados

NIST – *National Institute of Standards and Technology*

RIPD – Relatório de Impacto à Proteção de Dados pessoais

SI – Segurança da Informação

TCLE – Termo de Consentimento Livre e Esclarecido

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

EU – *European Union*

SUMÁRIO

1 INTRODUÇÃO 15
1.1 Justificativa 15
1.2 Contribuições do trabalho desenvolvido 16
1.3 Questão da pesquisa 18
1.4 Objetivo geral 19
1.5 Objetivos específicos 19
2 REFERENCIAL TEÓRICO 20
2.1 Pesquisa *survey* 21
2.2 Privacidade de usuários e leis de proteção à privacidade 24
2.3 Lei Geral de Proteção de Dados (LGPD) 26
2.4 Instrumentos de apoio para desenvolvimento do *roadmap* 27
2.4.1 *Design Thinking* 28
2.4.2 *Scrum* 30
2.5 *Roadmap* 32
3 METODOLOGIA 39
3.1 Etapa de identificação do problema e motivação 43
3.2 Etapa de definição dos resultados esperados 44
3.3 Etapa de desenho e desenvolvimento 45
3.4 Etapa de demonstração 46
3.5 Etapa de avaliação 47
3.6 Etapa de comunicação 48
4 RESULTADOS E DISCUSSÃO 49
4.1 Resultado da etapa de identificação do problema e motivação 49
4.1.1 Resultado da pesquisa bibliográfica 49
4.1.2 Resultados da *survey* 64
4.1.2.1 Perfil das empresas e dos participantes da *survey* 66
4.1.2.2 Nível de adequação das organizações à LGPD 69
4.1.2.3 Desafios do processo de adequação à LGPD 70
4.1.2.4 Medidas implementadas pelas empresas participantes 74
4.1.2.5 Considerações finais sobre resultados da *survey* 78
4.2 Resultado da etapa de definição dos resultados esperados 80
4.3 Resultado da etapa de desenho e desenvolvimento 84
4.4 Resultado da etapa de demonstração 89

4.5 Resultado da etapa de avaliação 89
4.6 Resultado da etapa de comunicação 94
5 CONSIDERAÇÕES FINAIS 95
REFERÊNCIAS 98
APÊNDICE A – TCLE APRESENTADO AOS RESPONDENTES DA PESQUISA ..102
APÊNDICE B – QUESTIONÁRIO DA *SURVEY* 103
APÊNDICE C – RESULTADOS DA *SURVEY*: DESAFIOS NA IMPLEMENTAÇÃO DA LGPD NAS ORGANIZAÇÕES 107
APÊNDICE D – ELEMENTOS DA NBR ISO/IEC 27002 BASE PARA ELABORAÇÃO DO ROADMAP 116
APÊNDICE E – VISÃO GERAL DAS ETAPAS DO RAEL 128
APÊNDICE F – DETALHAMENTO DAS ETAPAS DO RAEL 134
APÊNDICE G – FASE 1 - PREPARAÇÃO – RAEL 147
APÊNDICE H – FASE 2 - IMPLEMENTAÇÃO – RAEL 148
APÊNDICE I – FASE 3 - MANUTENÇÃO – RAEL 149
APÊNDICE J – VISÃO GERAL DO RAEL COM TODAS AS FASES 150
APÊNDICE K – AVALIAÇÃO DA ETAPA DE DEMONSTRAÇÃO DO RAEL 151
APÊNDICE L – TCLE APRESENTADO AOS AVALIADORES 159
APÊNDICE M – QUESTIONÁRIO PARA AVALIAÇÃO DO RAEL 160

1 INTRODUÇÃO

O advento das redes sociais como Facebook e Twitter (atualmente renomeada como X) potencializou a coleta e utilização de dados privados de usuários por empresas de tecnologia, inicialmente com propósito de gerar ações de marketing direcionadas e potencializar o retorno destas.

No entanto, tais informações passaram a ser utilizadas para a geração de conteúdo que pode influenciar os usuários em aspectos como posicionamento político, religioso, ideológico e outros, tendo influenciado em eventos como a eleição americana de 2016 e a saída do Reino Unido da União Europeia, conhecida como *Brexit,* o que levou a União Europeia a aprovar em 2016 uma lei visando estabelecer medidas para proteção das informações pessoais de seus cidadãos, denominada *General Data Protection Regulation* (GDPR).

Em agosto de 2018 foi aprovada pelo Congresso Brasileiro a Lei 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD). A lei sofreu grande influência da GDPR, norteada pelos mesmos princípios de proteção à privacidade dos cidadãos e sendo de aplicação obrigatória por toda empresa brasileira ou pessoa natural que realize tratamento de dados pessoais de clientes, funcionários e outros para fins de oferta ou fornecimento de bens ou serviços, independendo do seu porte, faturamento e setor de atuação.

1.1 Justificativa

Estudos realizados sobre os desafios enfrentados na implementação da LGPD e da GDPR apontam a falta de recursos financeiros, em especial em pequenas e médias empresas, a dificuldade de contratação de profissionais qualificados e a falta de conhecimento sobre as ações a serem implementadas como alguns dos principais empecilhos a serem superados pelas empresas.

Layton e Baranes (2017) discutem a transferência de responsabilidade para organizações e destacam a relevância de compreender como as pequenas e médias empresas estão se preparando para essa transição, pois a conformidade com novas legislações pode representar um desafio oneroso.

Da mesma forma, Freitas e Silva (2018), ao analisarem o impacto da GDPR em empresas de menor porte, ressaltam que a escassez de recursos humanos e as

restrições orçamentárias são fatores cruciais que dificultam o atendimento às obrigações legais impostas, sendo crucial encontrar soluções eficientes e efetivas.

Em complemento a estes estudos, Canedo et al (2020) identificaram em suas pesquisas, organizações nas quais profissionais de Tecnologia da Informação e Comunicação não foram devidamente informados sobre a LGPD e as mudanças necessárias em seus sistemas, o que pode gerar lacunas na implementação eficaz das medidas de conformidade.

Além disso, Ferrão et al (2021) constataram a carência de maturidade na maioria das organizações brasileiras em aspectos cruciais como governança, gestão de dados e segurança da informação. Essas lacunas existentes nas organizações podem representar um obstáculo significativo na adaptação às exigências regulatórias e na garantia da proteção adequada dos dados.

Passados 5 anos da sua publicação e 3 anos de sua efetiva entrada em vigor, a Autoridade Nacional de Proteção de Dados, órgão instituído pela LGPD para monitoramento de sua aplicação, iniciou a aplicação de sanções a empresas por descumprimento da lei, acendendo um sinal de alerta para organizações que ainda não tenham se adequado e implantado as medidas necessárias.

Neste cenário, o desenvolvimento e a proposição de ferramentas e métodos que sejam intuitivos e de fácil entendimento, é importante para dar amparo e suporte a organizações de todos os portes, em especial para pequenas e médias organizações, dado as dificuldades apontadas nos estudos mencionados anteriormente.

1.2 Contribuições do trabalho desenvolvido

Do ponto de vista da gestão e da tecnologia em sistemas produtivos, a presente pesquisa pretende contribuir para que as organizações brasileiras tenham conhecimento de como o *roadmap*, representado como artefato, seja útil para colaborar de maneira significativa no processo de adequação de organizações à LGPD, e contribuir para que os gestores destas organizações possam assegurar a proteção dos dados privados de seus clientes, usuários, colaboradores e parceiros.

Sob a perspectiva acadêmica, esta pesquisa pretende contribuir com a discussão da gestão da segurança de informações e da privacidade de dados e sobre como o artefato *roadmap* possa abrir oportunidades de novas pesquisas envolvendo

o contexto da segurança da informação, da privacidade dos dados e da adequação de empresas à legislação relacionada ao tema.

O estudo realizado traz também contribuição por se diferenciar dos estudos anteriores com relação ao produto gerado, às empresas alvo para aplicação do *roadmap* e de outros aspectos, apresentados no quadro 1:

Quadro 1 - Comparativo entre o RAEL e propostas anteriores

TÍTULO	**Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD).**	**Ensuring privacy in the application of the Brazilian general data protection law (LGPD).**	**RAEL**
DESCRIÇÃO	Processo de implementação da LGPD para agências da Administração Pública Federal (APF)	Remodelagem do guia de implementação da LGPD da Fundação Vanzolini	Roadmap para adequação de organizações à LGPD
# ETAPAS / PROCESSOS	14	16	20
FOCO	Implementação da LGPD	Implementação da LGPD	Adequação Serve para empresas que podem ou não ter implementado a LGPD
ABRANGÊNCIA	Agências da Administração Pública Federal	Qualquer organização	Qualquer organização
VALIDAÇÃO	Validação em Agência APF	Pesquisa com praticantes de TIC	Empresa do setor privado da área de TIC
NORMAS ABRANGIDAS	O artigo não faz menção à nenhuma norma	ISO 27001	NBR ISO/IEC 27001 E 38500, NIST CIBERSECURITY FRAMEWORK E NIST PRIVACY FRAMEWORK
FORMATO	FLUXOGRAMA	LIVRO	ROADMAP

Fonte: Resultado da pesquisa

O quadro 2 traz um comparativo dos principais elementos da proposta do RAEL que se diferenciam das propostas anteriores:

Quadro 2 – Etapas adicionadas ao RAEL comparando com propostas anteriores

Etapas Adicionadas	Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)	Ensuring privacy in the application of the Brazilian general data protection law (LGPD)	RAEL
Obtenção de aprovação pelos detentores dos dados	NÃO	SIM	SIM
direito a esquecimento - remoção dos dados	NÃO	SIM	SIM
Auditorias periódicas	NÃO	SIM	SIM
Transferência internacional de dados	NÃO	NÃO	SIM
Cronograma de gestão do projeto	NÃO	NÃO	SIM
Medidas para eliminar os dados ao término do processamento	NÃO	SIM	SIM
Medidas para respostas a incidentes	NÃO	SIM	SIM
Revisão de contratos com parceiros, fornecedores e outros	NÃO	NÃO	SIM
Constituição de um comitê interno para gestão da LGPD	NÃO	NÃO	SIM

Fonte: Resultado da pesquisa

Este estudo pode despertar interesse de diversas áreas do conhecimento, existindo uma lacuna entre a pesquisa e a prática, que pode ser preenchida pela DSRM na área de engenharia de produção, que possa contribuir para ampliar o necessário debate sobre o direito à privacidade e à proteção de dados pessoais no contexto das organizações brasileiras e na adequação destas à legislação de privacidade.

1.3 Questão da pesquisa

Desta forma surge a questão da pesquisa: como estruturar o *roadmap,* um guia que mostra os melhores caminhos para atingir um objetivo e que sirva de apoio a organizações brasileiras no processo de adequação à LGPD?

O *roadmap* é, segundo Farruck, Phaal e Probert (2003), um método prático que

auxilia na exploração de diferentes opções tecnológicas em termos de mercado e recurso, explorando as interações entre recursos tecnológicos, objetivos de negócios e o ambiente, sendo assim uma ferramenta de apoio para organizações que procurem adequar-se à LGPD e para os profissionais envolvidos no processo.

A partir da questão da pesquisa foram definidos os objetivos gerais e específicos, que são apresentados a seguir.

1.4 Objetivo geral

O objetivo geral da pesquisa consiste em desenvolver um *roadmap,* denominado ***R****oadmap* para **A**dequação de **E**mpresas à **L**GPD (RAEL), que sirva como guia de apoio às organizações brasileiras no processo de adequação à LGPD.

1.5 Objetivos específicos

Os objetivos específicos da pesquisa são:

1. Identificar o problema que permita estruturar um artefato de apoio às organizações brasileiras no processo de adequação à LGPD;
2. Definir os resultados esperados para este artefato *roadmap*, com base no problema identificado;
3. Desenhar e desenvolver um *constructo* do *roadmap* que permita às organizações brasileiras adequarem-se à LGPD assegurando a proteção dos dados privados de seus clientes, colaboradores e parceiros;
4. Prover a demonstração do uso do *roadmap* em um cenário real, por meio de visão teórica e prática, como um guia orientador às organizações brasileiras para alcançarem o objetivo de adequação à LGPD;
5. Obter a avaliação do *roadmap* com atores que estejam diretamente envolvidos com o processo de adequação à LGPD;
6. Comunicar o resultado da pesquisa à comunidade acadêmica e demais partes interessadas, por meio da publicação das etapas da pesquisa e do produto.

2 REFERENCIAL TEÓRICO

Neste item são abordados os aspectos teóricos utilizados para o embasamento do desenvolvimento do trabalho, ressaltando os principais aspectos relevantes.

A revisão sistemática da bibliografia tem como objetivo identificar os métodos de apoio à implementação da LGPD que foram desenvolvidos e propostos. Para isso, foi realizado um levantamento de artigos publicados no período entre 2018, data de aprovação da LGPD, e 2022, contendo a palavra-chave "LGPD". A pesquisa foi realizada na base *Scopus,* utilizando a ferramenta *Publish or Perish*, e no *website* da *Web of Science*. Este processo visou compilar e analisar criticamente a literatura existente sobre os métodos disponíveis para auxiliar na implementação da Lei Geral de Proteção de Dados (LGPD).

Em seguida foi realizada revisão dos títulos dos artigos para identificação de outras terminologias aplicadas à LGPD que também pudessem ter sido utilizadas como palavras-chave de artigos, identificando as seguintes terminologias, também adotadas para a LGPD: *“General Data Protection Law”, “General Law on Data Protection”* e “Lei Geral de Proteção de Dados”.

Foi realizada então nova busca nas mesmas bases com os 4 termos e o operador booleano *OR,* resultando na *string* de busca: *"General Data Protection Law*" *OR* "LGPD" *OR "General Law on Data Protection" OR* "Lei Geral de Proteção de Dados", conforme apresentado no quadro 3:

Quadro 3 - Critérios de busca sobre metodologias para implementação da LGPD

Atributo	Critério
Bases de Pesquisa	*Scopus e Web of Science*
Expressão	*"General Data Protection Law" OR "LGPD" OR "General Law on Data Protection" OR "Lei Geral de Proteção de Dados"*
Período	2018 a 2022
Idioma	Inglês ou português
Publicação	Artigos publicados em Periódicos e conferências

Fonte: Resultado da pesquisa

Os artigos obtidos foram submetidos a análise de duplicidades, leitura do título e, quando necessário, do resumo a fim de avaliar a relação dos artigos com o objetivo

da pesquisa, e, finalmente, análise textual dos artigos restantes.

O quadro 4 apresenta os critérios para seleção dos artigos:

Quadro 4 - Critérios de seleção sobre métodos para implementação da LGPD

Tipo de Critério	Critério
Inclusão	Artigos relacionados a métodos de implementação da LGPD
Exclusão	Artigos cujo título indique a falta de relação com o tema da busca Artigos cujo resumo não tenha relação com o tema da busca Artigos não disponíveis para consulta online Capítulos de livros, dissertações de mestrado ou teses de doutorado

Fonte: Resultado da pesquisa

2.1 Pesquisa *survey*

Para identificar as necessidades das organizações, como parte da etapa de identificação do problema, foi utilizada a pesquisa s*urvey* como meio de interagir com profissionais do mercado e entender o contexto em que a LGPD está relacionada com as empresas e seus profissionais.

Segundo Pinsonneault e Kraemer (1993), a pesquisa *survey* é especialmente indicada para responder questões sobre o que, quanto e quantos, e em grande extensão, questões sobre como e por quê. Essas questões devem ter 3 características distintas: produzir descrições quantitativas de alguns aspectos da população de estudo, utilizar questões estruturadas e predefinidas, cujas respostas constituem os dados a serem analisados, e a informação, em geral, coletada em uma fração da população de estudo, mas de forma que permita generalizar os achados.

Para elaboração das questões da *survey* foram considerados os estudos realizados por Layton e Baranes (2017), Freitas e Silva (2018), Canedo et al (2020) e Ferrão et al (2021) que enfatizam a dificuldade de adequação de pequenas e médias empresas, a falta de preparação de profissionais de TIC e Segurança da Informação e deficiências em governança e segurança da informação como grandes desafios.

Adicionalmente foi realizada uma revisão da literatura das pesquisas *survey* sobre a LGPD considerando artigos abertos para consulta e publicados no período entre 2016 e 2022 nas línguas portuguesa e inglesa em periódicos e anais de congresso.

As bases selecionadas para a pesquisa foram a *Web of Science* e *Scopus* em

virtude de sua relevância e qualidade dos artigos, com as pesquisas sendo realizadas no período entre 01-04-2023 e 15-04-2023.

A pesquisa teve como foco específico pesquisas ou *surveys* relacionadas à LGPD, sendo assim, os termos para busca foram as palavras-chave “LGPD” e (“PESQUISA” OU “*SURVEY*”).

As ferramentas utilizadas para as buscas foram o *software* “*Publish or Perish*” para a base da *Scopus*, e o *website* da *Web of Science*.

O Quadro 5 apresenta os critérios utilizados na pesquisa.

Quadro 5 - Critérios de busca de artigos sobre pesquisa ou *survey* relacionadas à LGPD

Atributo	**Critério**
Expressão	**("LGPD") AND ("*SURVEY*" OR "PESQUISA")**
Período	2016 a 2022
Idioma	Inglês ou português
Publicação	Artigos publicados em Periódicos e conferências
Base de Pesquisa	*Web of Science* e *Scopus*

Fonte: Resultado da pesquisa

A pesquisa resultou em 16 artigos da base da *Scopus* e 9 artigos na base da *Web of Science*, sendo que 8 dos 9 artigos da *Web of Science* já apareciam nos resultados da base da *Scopus*, sendo considerado apenas 1 novo artigo, o que resultou em um total de 17 artigos.

Foi realizada a leitura de título e, quando necessário, do resumo dos 17 artigos, resultando ao final em 3 artigos que foram utilizados como referencial para a elaboração das questões da *survey.*

O quadro 6 contém os critérios de seleção de artigos resultado deste processo.

Quadro 6 - Critério seleção de artigos: Uso da IA para adequação de empresas à GDPR ou LGPD

Tipo de Critério	**Critério**
Inclusão	Artigos relacionados a pesquisa ou *survey* relacionadas à LGPD
Exclusão	Artigos não disponíveis para consulta online Artigos cujo título indique a falta de relação com o tema da busca Artigos cujo resumo não tenha relação com o tema da busca
Total de artigos Analisados	16 artigos da base *Scopus* + 1 artigo da base *Web of Science*

Fonte: Resultado da pesquisa

O quadro 7 traz os artigos selecionados:

Quadro 7 – Artigos resultado da revisão da bibliografia que tenham relação com *survey* ou pesquisa relacionada à LGPD

Artigo	Autor	Título	Ano
1	*Canedo et al.*	*Perceptions of ICT practitioners regarding software privacy*	**2020**
2	*Ferrão et al.*	*Diagnostic of data processing by brazilian organizations—a low compliance issue*	**2021**
3	*Louzeiro et al*	*General Data Protection Law: Observations and Analysis of the Compliance Level of Organizations*	**2021**

Fonte: Resultado da pesquisa

Os artigos do quadro 7 foram utilizados como base para a elaboração das questões da *survey* juntamente com os artigos de Layton e Baranes (2017) e Freitas e Silva (2018) que apresentam *surveys* relacionadas à adequação das empresas à GDPR.

Com base nos artigos mencionados foram elaboradas 17 questões, as quais em grande parte foram questões de múltipla escolha com uso de escala *Likert*, abordando aspectos sobre perfil das empresas e dos participantes, dificuldades no processo de adequação, nível de adequação das organizações e principais aspectos implementados para assegurar adequação à LGPD.

As questões 1 a 6 têm por objetivo tabular o estrato social dos participantes e de suas organizações. A Q7 tem por objetivo coletar a percepção do participante quanto ao nível de adequação de sua organização à LGPD.

As questões Q8 a Q12 tem por objetivo avaliar os desafios enfrentados pelas organizações em termos de recursos financeiros, dificuldade de obtenção de profissionais e ferramentas e métodos para apoiar a implementação da LGPD e o grau de conhecimento e preparação dos profissionais envolvidos.

As questões Q13 e Q14 objetivam avaliar as políticas e procedimentos implementados e a percepção quanto a estas serem adequadas e suficientes para adequação das organizações dos participantes.

A Q15 tem por objetivo identificar quais as áreas das organizações que receberam treinamento relativo à LGPD.

A Q16 visa identificar quais as medidas implementadas pelas organizações visando adequação, enquanto a Q17 é sobre a percepção dos participantes sobre os dados coletados pelas organizações serem os estritamente necessários.

2.2 Privacidade de usuários e leis de proteção à privacidade

Os dados, na contemporaneidade, são considerados como o precioso recurso da era digital, sendo considerados o "novo petróleo" devido à sua grande importância nas estratégias de mercado (COSTA E OLIVEIRA, 2019). O surgimento das Redes Sociais no início do século XXI representou um marco na área da Tecnologia, com o *Facebook* emergindo como líder desse movimento. Fundado em 2004 com acesso inicialmente restrito aos estudantes de *Harvard*, expandiu rapidamente sua base de usuários para outras universidades, alunos do ensino médio e posteriormente para maiores de 13 anos. Com um crescimento notável e aquisições estratégicas, de *Whastapp* e *Instagram* alcançou a impressionante marca de mais de 2 bilhões de usuários (Hirata, 2014).

Srnicek (2018) descreve o capitalismo contemporâneo como guiado pela *"data-driven economy"* (economia movida a dados), ressaltando a centralidade da exploração econômica dos dados nas empresas transnacionais, tais como *Alibaba, Facebook, Alphabet, Amazon, Tencent* e *Uber*.

O *Facebook,* além de redefinir a interação entre pessoas, iniciou uma estratégia de coleta de dados por meio do botão "curtir", permitindo o mapeamento extensivo do perfil de seus usuários. Cada interação alimentava uma estrutura massiva de coleta de dados, impulsionando o *marketing* digital personalizado e deslocando as receitas publicitárias das mídias tradicionais para suas próprias plataformas (Hirata, 2014).

No entanto, essa crescente acumulação de dados gerou implicações mais amplas, especialmente quando essas informações começaram a ser compartilhadas com parceiras sem o consentimento explícito dos usuários. A utilização desses dados pelas empresas parceiras não se restringiu apenas à publicidade, mas também incluiu a geração de mensagens personalizadas com o objetivo de influenciar as opiniões e comportamentos dos usuários. O poder decorrente dessas práticas transcendeu os limites das receitas publicitárias, impactando diretamente a esfera da privacidade e da manipulação de dados (Hirata, 2014).

Em 2015, a *Cambridge Analytica* teve acesso aos perfis de aproximadamente 20 milhões de usuários do *Facebook,* aproveitando questões de segurança que possibilitaram o acesso a outros 60 milhões de usuários. Essa empresa desempenhou um papel significativo na campanha presidencial dos Estados Unidos em 2016, utilizando as informações coletadas dos perfis do *Facebook* para influenciar

diretamente as escolhas dos eleitores. Suas ações foram apontadas como contribuintes para a vitória de Donald Trump, um candidato considerado improvável até então (Isaak e Hannah, 2018).

A influência da *Cambridge Analytica* não se limitou à eleição presidencial americana, estendendo-se ao referendo sobre a saída do Reino Unido da União Europeia, conhecido como *Brexit.* Contratada pelos defensores do *Brexit,* mesmo quando pesquisas indicavam a tendência oposta, a empresa desempenhou um papel crucial na vitória do movimento de saída do Reino Unido da UE (Isaak e Hannah,2018).

Esses eventos geraram uma onda de preocupação entre legisladores globais, especialmente na União Europeia, que reagiu aprovando a *General Data Protection Regulation* (GDPR) em 2016. Essa regulação foi criada para salvaguardar o direito à privacidade dos cidadãos, estabelecendo requisitos rígidos para a coleta e o tratamento de dados por empresas, juntamente com punições severas em caso de violação das normas. A GDPR também estabeleceu um prazo de dois anos para as organizações se adaptarem às suas exigências, visando proteger os dados de clientes, usuários e colaboradores (Isaak e Hannah, 2018).

Segundo Ooijen e Vrabec (2019), a GDPR estabelece uma necessidade ampliada de controle individual, demandando uma abordagem mais explícita e cautelosa em comparação com legislações anteriores sobre privacidade de dados.

Layton e Baranes (2017) observam que a responsabilidade sobre a proteção dos dados nas organizações suscita dúvidas acerca da preparação das pequenas e médias empresas para atender a esses requisitos. Há uma urgência por encontrar meios menos dispendiosos para cumprir com os parâmetros legais, especialmente em organizações com recursos humanos e orçamentários limitados, pois a conformidade com a GDPR pode demandar investimentos substanciais.

Na análise da aplicação da GDPR em empresas de menor porte, Freitas e Silva (2018) destacam a insuficiência de recursos humanos para atender às obrigações legais, juntamente com consideráveis restrições de orçamento. Eles também ressaltam a importância de encontrar soluções eficazes e viáveis para se adequar às exigências da legislação.

Além disso, Doneda (2017) identificou a existência de leis gerais de proteção de dados em 109 países, o que evidencia a crescente relevância do tema em âmbito global e o impulso na adoção de regulamentações específicas para a proteção de dados.

2.3 Lei Geral de Proteção de Dados (LGPD)

Em 2018 o Congresso Brasileiro aprovou uma legislação nos mesmos moldes da GDPR, denominada Lei Geral de Proteção de Dados brasileira, ou LGPD, que herdou grande parte de suas características de sua irmã mais velha. Da mesma forma que sua similar europeia, a lei estabeleceu um prazo de dois anos para que as empresas pudessem se adequar, implementando medidas para assegurar a proteção e a privacidade dos dados pessoais de seus usuários, clientes e colaboradores.

O Quadro 8 apresenta uma visão geral dos principais artigos da lei:

Quadro 8 - Visão geral dos principais artigos da LGPD

ARTIGO	TEOR
3	Trata da aplicabilidade da lei, a qual se aplica a qualquer operação de tratamento realizada por pessoa natural ou pessoa jurídica de direito público ou privado, desde que atendidas certas condições.
5	Define os conceitos de dado pessoal, dado pessoal sensível, titular, controlador, operador, agente de tratamento, tratamento, anonimização, consentimento e outros que serão objeto da lei.
6	Define os princípios que devem nortear as atividades de tratamento, tais como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, dentre outros.
7	Define as hipóteses nas quais o tratamento de dados poderá ser realizado.
9	Define o direito às informações sobre o tratamento de dados por parte do titular.
11	Define as hipóteses nas quais o tratamento de dados sensíveis poderá ser realizado.
15	Dispõe sobre as condições para o término do tratamento de dados.
16	Dispõe sobre a eliminação dos dados pessoais e quais as exceções que autorizam sua conservação por parte do controlador.
18	Estabelece o direito do titular de obter informações sobre o tratamento de seus dados pessoais, incluindo a confirmação da existência do tratamento, acesso aos dados, correção, portabilidade e eliminação dos dados, dentre outros direitos do titular.
20	Dispõe sobre o direito a explicação sobre os tratamentos de dados automatizados e decisões tomadas com base nestes tratamentos.
33	Estabelece as condições nas quais a transferência internacional de dados pessoais é permitida.
37	Define a exigência de registro das operações de tratamento de dados pessoais realizadas pelo controlador ou operadores por ele nomeados.
48	Define obrigação do controlador em comunicar ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.
52	Define as sanções aplicáveis em razão das infrações cometidas às normas previstas na lei.
55-A **55-J**	Cria a Autoridade Nacional de Proteção de Dados, sua composição, estrutura, competência, dentre outros aspectos.
58-A **58-B**	Cria o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e define suas competências.

Fonte: Resultado da pesquisa

Farias e Rached (2019) ressaltam que a gestão de dados dentro das empresas implica em uma significativa mudança cultural, pois muitas organizações não possuem pleno conhecimento dos dados que detêm, nem sabem onde e como esses dados são armazenados e tampouco quem tem acesso a eles. Canedo et al (2020) identificaram em suas pesquisas organizações em que os profissionais de Tecnologia da Informação e Comunicação não estão familiarizados com a nova legislação, desconhecendo tanto sua implementação quanto as mudanças necessárias para a adequação à LGPD.

Além disso, Ferrão et al (2021) identificaram uma falta de maturidade em governança, gestão de dados, privacidade e segurança da informação em muitas organizações brasileiras, o que pode representar um obstáculo significativo na implementação efetiva da lei. Louzeiro et al (2021) também constataram a existência de várias empresas que ainda não estavam em conformidade com a LGPD, destacando que essas empresas têm maior probabilidade de lidar com informações de forma inadequada e, consequentemente, de enfrentar incidentes de vazamento de dados.

Adicionalmente, Ferreira et al (2022) apontam a falta de conhecimento sobre o tema, a escassez de recursos financeiros e humanos, bem como a ausência de apoio da alta administração como alguns dos desafios cruciais para a implementação efetiva da LGPD. Esses aspectos refletem não apenas a complexidade da conformidade com a legislação, mas também a necessidade de um esforço conjunto e uma abordagem holística para garantir a conformidade e a proteção adequada dos dados nas organizações.

2.4 Instrumentos de apoio para desenvolvimento do *roadmap*

O *Design Thinking e Scrum* são utilizados no desenvolvimento do *Roadmap* por meio da interação com o público-alvo (etapa da empatia do *Design Thinking*), elaboração do modelo e na geração das versões incrementais do *Roadmap* (ideação e prototipagem do *Design Thinking*), proporcionando protótipos que possam ser validados e melhorados de forma incremental em ciclos de desenvolvimento, como nos *Sprints* do *Scrum*, até sua demonstração e validação (etapa de teste do *Design Thinking*).

2.4.1 *Design Thinking*

São utilizadas como métodos de apoio ao desenvolvimento do *roadmap* o *Design Thinking* e o *Scrum* por serem métodos que apresentam características adequadas para o *design* incremental de protótipos de produtos ou processos em que as versões iniciais do produto são ajustadas e melhoradas com adição de melhorias ou novas funcionalidades ao longo das etapas de desenvolvimento.

Brown (2008) define o *design thinking* como uma abordagem que se concentra na compreensão profunda das necessidades e desejos dos usuários, visando criar soluções inovadoras e eficazes. Esse processo criativo e colaborativo fundamenta-se na sensibilidade em relação às pessoas, na geração de ideias criativas e na experimentação prática.

O autor enfatiza que o *design thinking* valoriza a colaboração, a criatividade e a resolução de problemas centrados no ser humano. Ele destaca a importância de compreender profundamente as pessoas para desenvolver soluções que atendam às suas necessidades e desejos (Brown, 2008).

Kolko (2015) descreve o *design thinking* como um conjunto de princípios que envolvem empatia com os usuários, disciplina de prototipação, tolerância ao erro e outros aspectos relevantes. Segundo o autor, essa abordagem é a melhor ferramenta para criar interações e estabelecer uma cultura organizacional responsiva e flexível, transcendendo o *design* como um papel específico e estabelecendo princípios para todos que participam da materialização de ideias.

Segundo Corrales-Estrada (2020), para solucionar um problema importante ou atender uma necessidade de um cliente, o primeiro passo é encontrar uma metodologia forte focando nas necessidades organizacionais e nas necessidades não atendidas dos clientes, a qual, baseada na literatura e histórias de sucesso de empresas como *Apple*, IKEA ou Google, é o *design thinking*.

Ela realizou uma revisão dos perfis de *designers* e de suas abordagens de *design thinking* na qual conclui que *o design thinking* não é mais sobre identificar a resposta certa para um problema de *design,* mas sim um processo interativo com potencial geral para transformar problemas em oportunidades, sendo uma atividade centrada no ser humano e preocupada em entender e interpretar as perspectivas de usuários finais e os problemas que enfrentam.

Liedtka (2018) afirma que a estrutura do *design thinking* cria um fluxo natural da pesquisa até o lançamento do produto, onde a imersão na experiência do cliente

produz dados, os quais são transformados em *insights* que ajudam as equipes a definir critérios de *design* usado para avaliar soluções. Essas soluções são examinadas e testadas por meio de protótipos para validar a melhor alternativa.

Bason e Austin (2019) mencionam que o *design thinking* descreve processos, métodos e ferramentas para criar produtos e soluções centrados no ser humano. Essa abordagem busca estabelecer uma conexão pessoal com as pessoas para as quais a solução é direcionada, garantindo que os *designers* compreendam as condições, situações e necessidades sob a perspectiva do usuário.

Adicionalmente, o *design thinking* incentiva os funcionários a experimentarem a falha repetidamente e a identificarem oportunidades para redesenhar e melhorar os processos, contando com o apoio da gestão ao longo desse processo (Bason e Austin, 2019).

Brown (2015) destaca que o *design thinking* constitui um conjunto de ferramentas que, quando dominadas pelas organizações, podem gerar vantagem competitiva sustentável e amadurecer sua atuação no mercado.

De acordo com Brown (2008), os principais componentes do *design thinking,* são:

1. **Empatia**: O primeiro passo é a empatia, que envolve a compreensão profunda das necessidades, motivações e desejos dos usuários. Isso é feito por meio de pesquisa e interação direta com as pessoas para entender o contexto em que vivem e trabalham;
2. **Definição do problema**: Após a empatia, é importante definir o problema de forma clara e específica. Isso ajuda a direcionar o foco da equipe de *design* para um problema que realmente importa e pode ser resolvido de maneira significativa;
3. **Ideação**: A próxima etapa envolve a geração de ideias criativas para abordar o problema definido. A ênfase aqui é na geração de uma ampla variedade de ideias, sem julgamento, para explorar todas as possibilidades;
4. **Prototipagem**: Após a geração de ideias, a equipe cria protótipos rápidos e de baixo custo das soluções mais promissoras. Esses protótipos ajudam a testar e refinar as ideias antes de investir recursos significativos;
5. **Teste**: Os protótipos são testados com os usuários reais para obter *feedback* valioso. Com base no *feedback*, as soluções são iteradas e refinadas até que uma solução final seja desenvolvida;

6. **Implementação**: A fase final envolve a implementação da solução escolhida, levando-a ao mercado ou à implementação prática.

Figura 1 – Etapas Componentes do *Design Thinking* segundo Brown

Fonte: Adaptado de Brown (2008).

2.4.2 *Scrum*

Sutherland e Schwaber (2020) definem *Scrum* como um *framework* leve que visa auxiliar pessoas, equipes e organizações na geração de valor por meio de soluções adaptáveis para problemas complexos, com base no empirismo, que enfatiza que o conhecimento vem da experiência e da tomada de decisões baseadas em observação, e no pensamento enxuto (*lean thinking*), reduzindo o desperdício e concentrando-se na essência. *Scrum* aplica métodos interativos para otimizar e controlar riscos previsíveis, envolvendo grupos com habilidades e experiência coletivas para realizar o trabalho, compartilhando e adquirindo competências conforme necessário.

Sutherland (2014) atribui a origem do *Scrum* ao trabalho de Hirotaka Takeuchi e Ikujiro Nonaka. Esses estudiosos, ao pesquisarem empresas altamente produtivas e inovadoras, como *Honda, Fuji-Xerox, 3M e Hewlett-Packard*, destacaram que as equipes mais eficazes eram multifuncionais, detinham autonomia e autoridade para tomar decisões e tinham objetivos transcendentes. Nesses ambientes, a gestão não impunha ordens, e os executivos atuavam como líderes que serviam aos funcionários, sendo facilitadores focados em remover obstáculos para as equipes, analogamente a um time de rúgbi.

Imai et al (1984) identificaram duas dimensões cruciais no desenvolvimento de novos produtos: a velocidade de desenvolvimento e a flexibilidade das empresas em

adaptar seus processos de desenvolvimento às mudanças no ambiente externo. A combinação dessas dimensões resulta em vantagens competitivas, como aumento de produtividade, melhoria da qualidade e redução de custos.

Imai et al (2008) identificaram 6 fatores internos que contribuem para acelerar e flexibilizar o processo de desenvolvimento:

1. Alta gestão como catalizadora;
2. Times de projeto auto-organizáveis;
3. Fases de desenvolvimento sobrepostas;
4. Aprendizagem múltipla;
5. Controle súbito;
6. Transferência de aprendizado organizacional.

Este processo de desenvolvimento proposto por Imai, Takeuchi e Nonata serviu de base para o desenvolvimento do *Scrum*.

Sutherland e Schwaber (2020) definem o *Scrum* como um método baseado em quatro etapas formais para inspeção e adaptação de um evento específico denominado *Sprint,* que implementa os pilares da transparência, inspeção e adaptação.

Eles argumentam que a transparência é fundamental para dar visibilidade a todos os envolvidos no trabalho, já que artefatos com baixa transparência tendem a levar a decisões que diminuem o valor e aumentam o risco. Essa transparência permite a inspeção, que deve ser realizada de forma frequente e diligente para identificar variações indesejáveis ou problemas nos artefatos. Por sua vez, a inspeção viabiliza a adaptação, pois se algum aspecto do processo se desviar de limites aceitáveis ou se o produto resultante não for satisfatório, o processo aplicado ou os materiais produzidos devem ser ajustados o quanto antes para minimizar o desvio (Sutherland e Schwaber, 2020).

Os autores ressaltam que o ponto central do *Scrum* são os *Sprints*, eventos de duração fixa de um mês ou menos que visam criar consistência e iniciam imediatamente após a conclusão do *Sprint* anterior. Durante esse período, todo o trabalho para alcançar o objetivo do produto ocorre, dividindo-se nas etapas de planejamento do *Sprint*, *Scrums* diários, revisão do *Sprint* e retrospectiva do *Sprint.* Durante o *Sprint*, não são realizadas mudanças que comprometam o objetivo, a qualidade não deve diminuir, a lista de pendências do produto é refinada, se necessário, e o escopo deve ser esclarecido e renegociado à medida que se adquire

conhecimento (Sutherland e Schwaber, 2020).

Sutherland (2014) afirma que as equipes *Scrum* que operam bem conseguem alcançar o que é chamado de "hiper produtividade", com uma melhoria entre 300% e 400% na produtividade de grupos que implementam eficientemente o *Scrum*. Além disso, a melhoria não se restringe apenas à produtividade, já que essas equipes também dobram a qualidade do trabalho realizado.

2.5 *Roadmap*

Kostoff e Schaeller (2001) fornecem uma definição abrangente de "*road map"* como um esquema de caminhos ou rotas dentro de um espaço geográfico, comumente utilizado por viajantes para escolher entre diferentes rotas em direção a um destino específico. Esse conceito oferece uma ferramenta que proporciona compreensão, orientação, direção e um certo grau de certeza em relação ao plano de viagem.

Na esfera da ciência e tecnologia, o termo *roadmap* é empregado de maneira similar ao conceito tradicional de *"road map"* para o planejamento de recursos nesses campos (Kostoff e Schaeller, 2001). De acordo com esses autores, os *roadmaps* oferecem uma visão das diversas alternativas possíveis, oferecendo uma maneira de identificar, avaliar e selecionar as opções viáveis para alcançar um determinado objetivo.

Adicionalmente, os *roadmaps* comunicam visões, estimulam a investigação e monitoram o progresso, servindo como um inventário das possibilidades para um domínio específico (Galvin, 1998). Ainda de acordo com Kerr e Phaal (2015), os criadores de *roadmaps* devem atentar-se para um balanço entre a funcionalidade do *roadmap* (o quê e para quem é dirigida a comunicação) e sua estética.

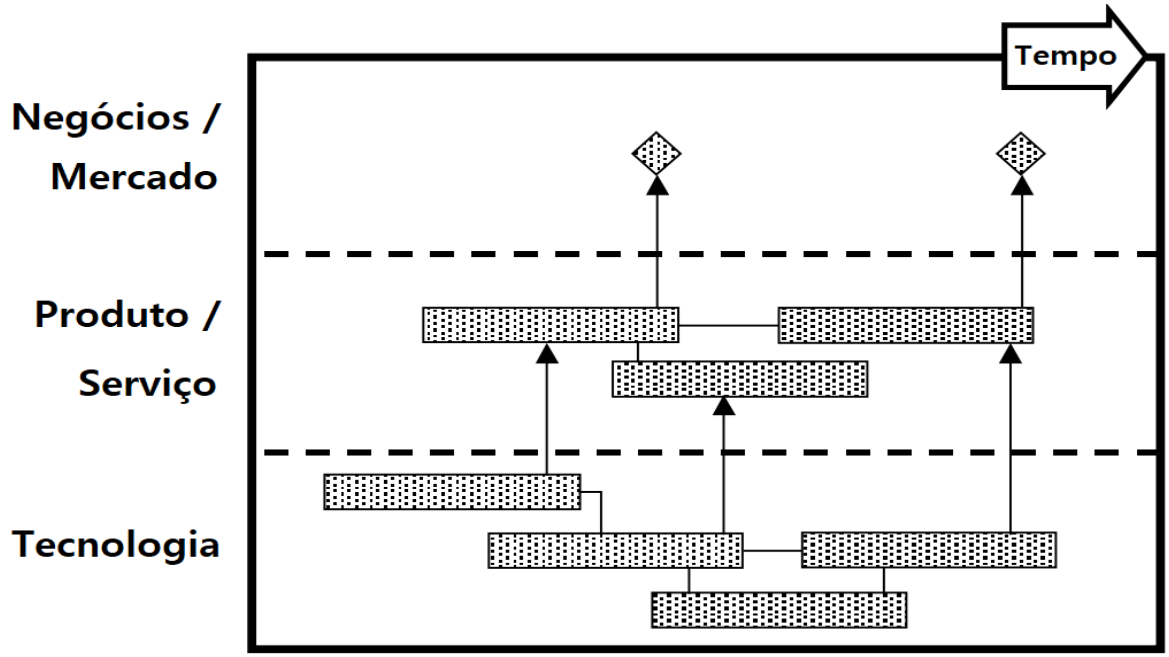
Segundo Münch, Lang e Trieflinger (2019), um *roadmap* pode ser visto como um elemento chave de uma organização, que descreve como um produto atingirá um conjunto de objetivos de negócio e o esforço necessário para chegar lá.

Farruck, Phaal e Probert (2003) definem *roadmapping* como o método prático que auxilia na exploração de diferentes opções tecnológicas em termos de mercado e recursos. Essa técnica é usada principalmente para conectar oportunidades de mercado a produtos, ao desenvolvimento de processos tecnológicos e a atividades de prospecção dentro de um processo. Essas definições fornecem uma compreensão ampla e abrangente do conceito de *roadmapping*, destacando sua utilidade tanto no

planejamento estratégico quanto no desenvolvimento tecnológico e de mercado.

O produto gerado por este método, um *roadmap* tecnológico, compreende várias camadas em um gráfico baseado em tempo, como ilustrado na figura 2.

Figura 2 – Esquema geral de um *Roadmap* tecnológico



Fonte: Adaptado de Farruck, Phaal e Probert (2003)

Segundo Phaal, Farrukh e Probert (2003), o processo de *Roadmapping* Tecnológico é uma técnica poderosa que apoia a gestão e o planejamento, explorando as interações entre recursos tecnológicos, objetivos de negócios e o ambiente. Esse processo é adaptável às necessidades diversas das organizações, referindo-se a várias técnicas e abordagens.

Rinne (2004) destaca as principais funções dos *roadmaps* de tecnologia, enfatizando sua utilidade na representação, comunicação, planejamento e coordenação. Esses *roadmaps* oferecem uma representação ao longo do tempo do relacionamento entre tecnologias e produtos, fundamentais para o planejamento estratégico.

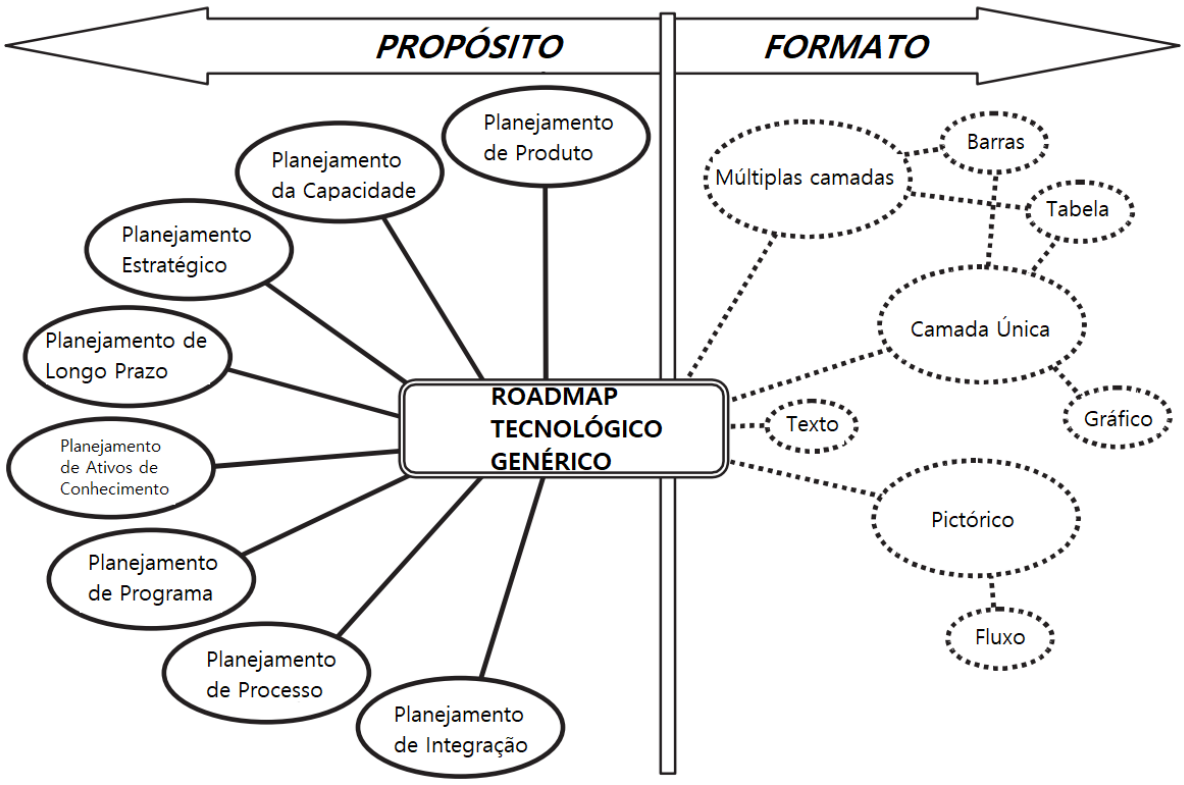
De acordo com Phaal, Farrukh e Probert (2003), os *roadmaps* tecnológicos possuem um grande potencial para apoiar o desenvolvimento e a integração de planos de negócios, produtos e tecnologias. Eles proporcionam às organizações as informações, processos e ferramentas necessárias para a sua implementação.

Garcia e Bray (1997) ressaltam que os *roadmaps* tecnológicos devem ser

orientados por necessidades e não por soluções. Dessa forma, eles devem começar com a identificação das necessidades em vez de começar diretamente com a solução. Esses *roadmaps* são considerados uma estratégia de nível superior para o desenvolvimento de tecnologias, exigindo um plano mais detalhado para especificar o projeto e as atividades a serem executadas.

Segundo Phaal, Farrukh e Probert (2003), os *roadmaps* podem ser categorizados por aplicação / propósito ou por formato em grande variedade. Esta grande variedade em parte é atribuída à falta de padrões ou protocolos para sua construção, mas também ocorre devido à necessidade de adaptar a abordagem à diferentes situações. A figura 3 ilustra os diferentes tipos de *roadmap* classificados por aplicação/propósito e formato.

Figura 3 – Caracterização de *roadmaps* por aplicação/propósito e formato



Fonte: Adaptado de Phaal, Farrukh e Probert (2003).

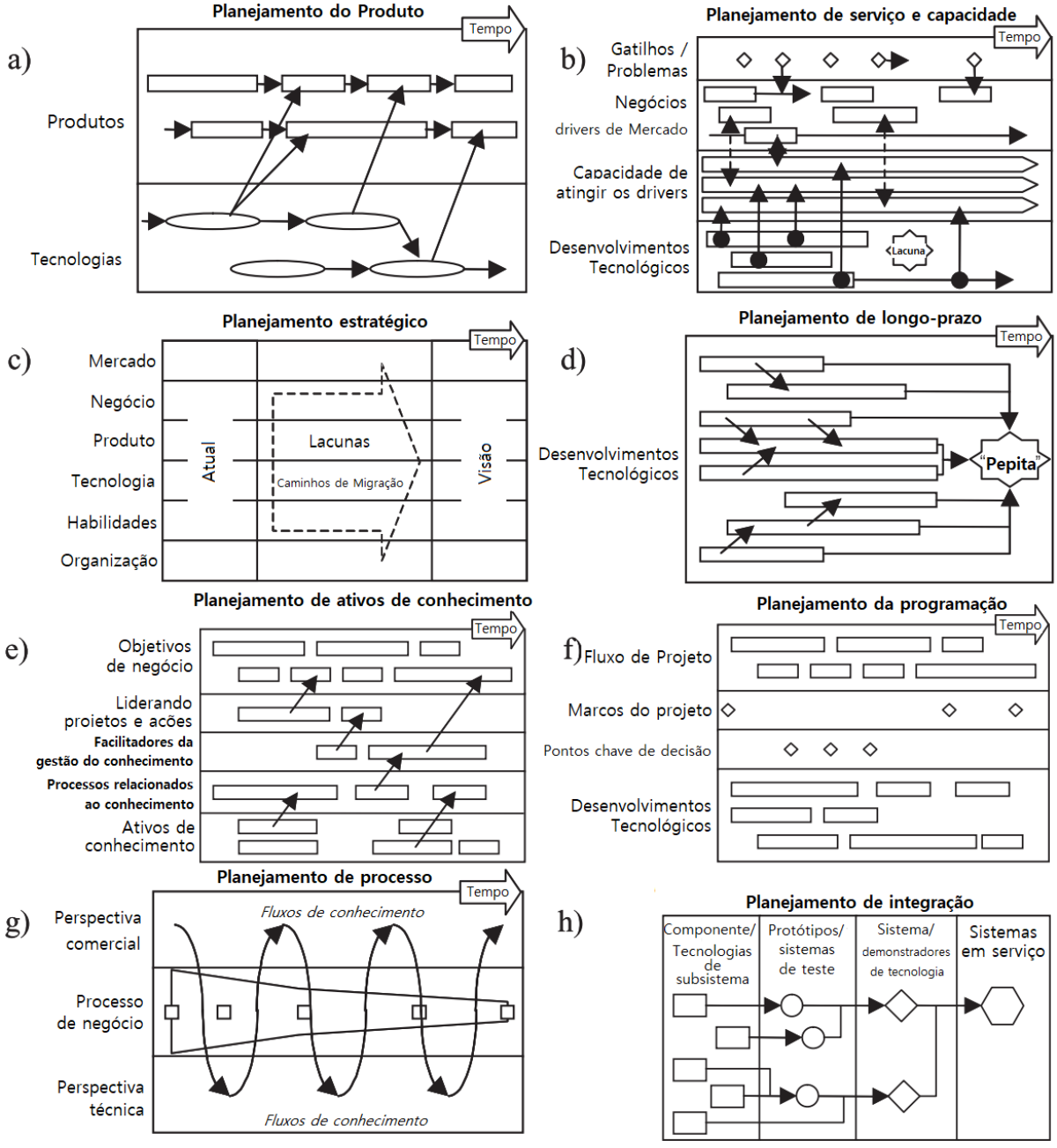
Phaal, Farrukh e Probert (2003) identificaram 8 tipos de *roadmaps* tecnológicos, em termos de aplicação e/ou propósito:

a) Planejamento de produto;
b) Planejamento de serviços / capacidade;
c) Planejamento estratégico;

d) Planejamento de longo prazo;
e) Planejamento de ativos de conhecimento;
f) Planejamento de programação;
g) Planejamento de processos;
h) Planejamento integrado.

A figura 4 traz exemplos dos diferentes *roadmaps* por aplicação/propósito:

Figura 4 – Caracterização de *roadmaps* por aplicação / propósito

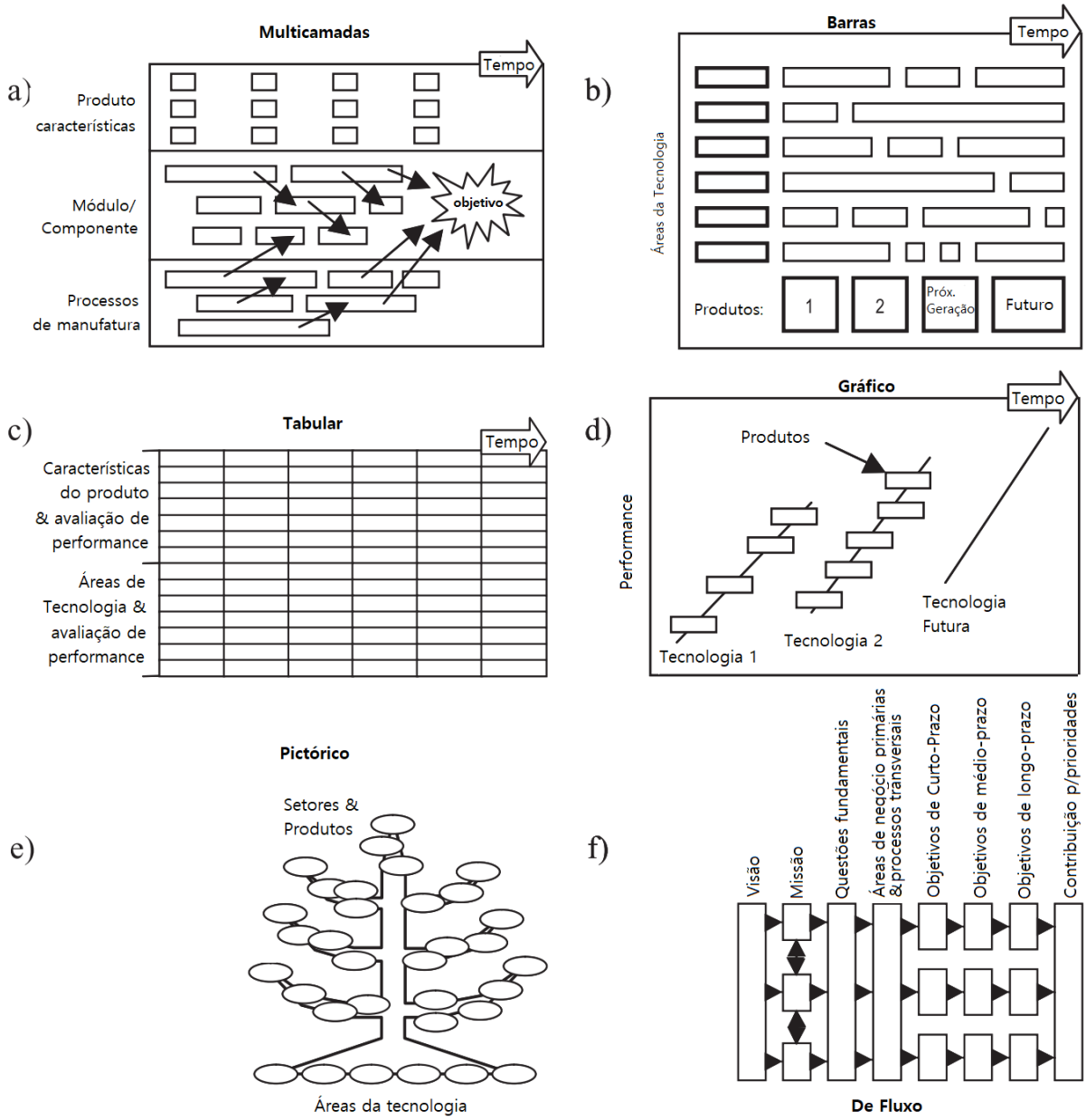


Fonte: Adaptado de Phaal, Farrukh e Probert (2003).

Com relação ao formato, Phaal, Farrukh e Probert (2003) classificam os *roadmaps* tecnológicos como sendo (figura 5):

a) Multicamadas;
b) Barras;
c) Tabular;
d) Gráfico;
e) Pictórico;
f) De fluxo.

Figura 5 – Exemplos de formatos de *roadmaps* de tecnologia



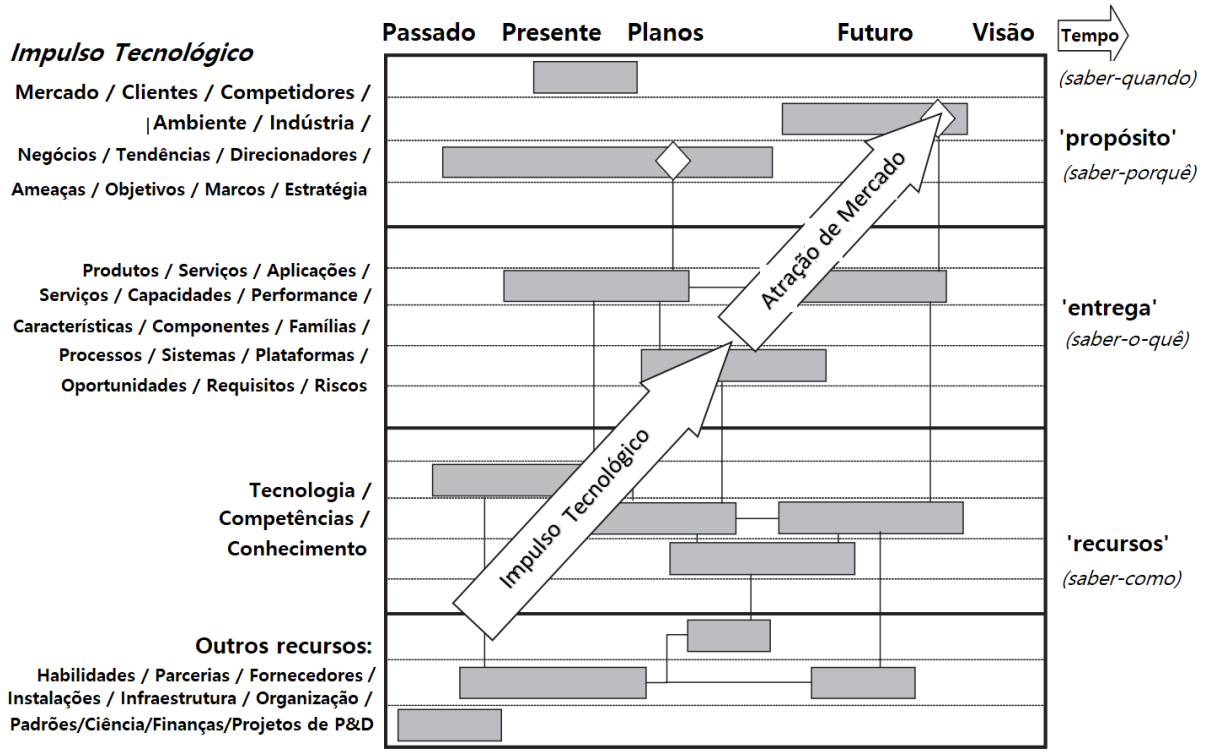
Fonte: Adaptado de Phaal, Farrukh e Probert (2003).

De acordo com Farruck, Phaal e Probert (2003), o formato de *roadmap* mais comum é o de *roadmap* multicamadas, sendo também o mais flexível em aplicação e tendo as seguintes dimensões:

a) **Tempo:** que pode ser adaptada a cada situação em termos de horizonte de tempo, adotando escalas de tempo proporcionais à duração do projeto (Farruck, Phaal e Probert, 2003);
b) **Camadas:** O eixo vertical do *roadmap* deve atender às necessidades da organização e do problema a ser endereçado. Grande parte do trabalho inicial será dedicado à definição das camadas (Farruck, Phaal e Probert, 2003);
c) **Anotações:** Além da informação contida nas camadas, outras informações tais como o relacionamento entre camadas e subcamadas, estratégias, elementos e pessoas chaves e outros elementos gráficos tais como sistemas de cores e notas podem ser utilizados para indicar caminhos críticos, oportunidades e ameaças (Farruck, Phaal e Probert, 2003);
d) **Processo:** Os passos a serem seguidos para cumprir o *roadmap*, os quais serão diferentes de acordo com cada organização, projeto e objetivo. Os processos em geral dependerão de diversos fatores, incluindo os recursos disponíveis, outros processos e métodos de gestão empregados (Farruck, Phaal e Probert, 2003).

A figura 6 refere-se a um exemplo de estrutura de *roadmap* multicamadas com as suas diferentes dimensões.

Figura 6 – Exemplo de estrutura de um *roadmap* multicamadas



Fonte: Adaptado de Farruck, Phaal e Probert (2003).

Kerr e Phaal (2015) propõe uma abordagem voltada ao *design* para o desenvolvimento de *roadmaps*, composta de 4 passos:

1. Definição da estrutura para o *roadmap*;
2. Estabelecer a estrutura do layout para o *roadmap*;
3. Descrever o relacionamento que conecta vários elementos do *roadmap*;
4. Articular uma direção para a narrativa capturada pelo *roadmap.*

Esta abordagem envolve gerar conceitos visuais e refiná-los para produzir representações customizadas que se tornam *templates* nos quais o conteúdo relevante é inserido e a apresentação estética é então finalizada (Kerr e Phaal, 2015).

A fase de planejamento é a mais importante para customização do *roadmap*, para permitir uma articulação entre os objetivos de negócio e do processo, e para identificar como o processo de *roadmapping* pode auxiliar a atingir este objetivo (Farruck, Phaal e Probert, 2003).

3 METODOLOGIA

A metodologia empregada no desenvolvimento do *roadmap* é a *Design Science Research Methodology* (DSRM), a qual, segundo Peffers et al. (2007) é a proposta de um *framework* comum para a ciência do *design* e para sistemas de informação, assim como um *template* para leitores e revisores, a fim de reconhecer e avaliar os resultados de tais pesquisas.

De acordo com Lacerda et al. (2013), a *Design Science* é responsável por conceber e validar sistemas que ainda não existem, envolvendo a criação, recombinação ou alteração de métodos, produtos e processos para melhorar situações existentes.

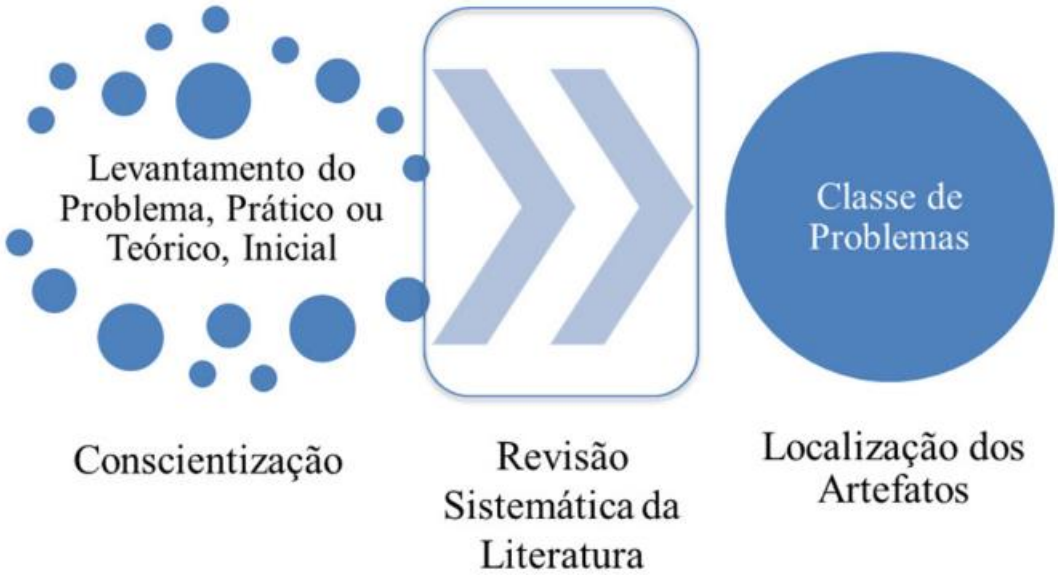
Além disso, Lacerda et al. (2013) ressaltam que os artefatos e suas soluções podem ser não apenas a resolução de um problema específico, mas também permitir a generalização da solução, compartilhando características comuns que possibilitam a organização do conhecimento de uma *Design Science* em "classes de problemas", permitindo, assim, a generalização e o avanço do conhecimento na área.

O propósito da *Design Science* é produzir sistemas inexistentes ou modificar sistemas e situações organizacionais para alcançar melhores resultados, com uma visão pragmática do conhecimento a serviço da ação e inspirada em propostas e soluções ideais, baseadas no pensamento sistêmico (Lacerda et al., 2013).

Ainda segundo Lacerda et al (2013), a partir de um problema identificado, é necessário identificar as repercussões para a organização, bem como os objetivos a serem alcançados para que o problema seja satisfatoriamente solucionado, sendo esta etapa denominada da “conscientização”, a partir da qual é necessário realizar uma revisão sistemática para estabelecer o quadro de soluções empíricas, identificando as soluções que procuram resolver o problema, para, em seguida, caracterizar os artefatos associados.

A figura 7 apresenta o fluxo desta proposição de lógica para a construção das classes de problemas.

Figura 7 – Lógica para construção das classes de problemas



Fonte: Lacerda et al (2013).

Lacerda et al (2013) estabelecem que, a partir da definição da classe de problemas, é necessário caracterizar os artefatos associados nas seguintes categorias:

• **Constructos:** conceituações usadas para descrever os problemas dentro do domínio e especificar soluções (Lacerda et al 2013 apud March e Smith, 1995);

• **Modelos:** conjuntos de proposições ou declarações que expressam relações entre constructos, e, no *design,* representam situações como problema e solução (Lacerda et al 2013 apud March e Smith, 1995);

• **Métodos**: conjuntos de passos para execução de uma tarefa, baseados em constructos subjacentes e modelos em um espaço de solução (Lacerda et al 2013 apud March e Smith, 1995);

• **Instanciações:** Uma instanciação é a concretização de um artefato em seu ambiente, operacionalizando constructos, modelos e métodos, mas pode preceder a articulação completa destes (Lacerda et al 2013 apud March e Smith, 1995).

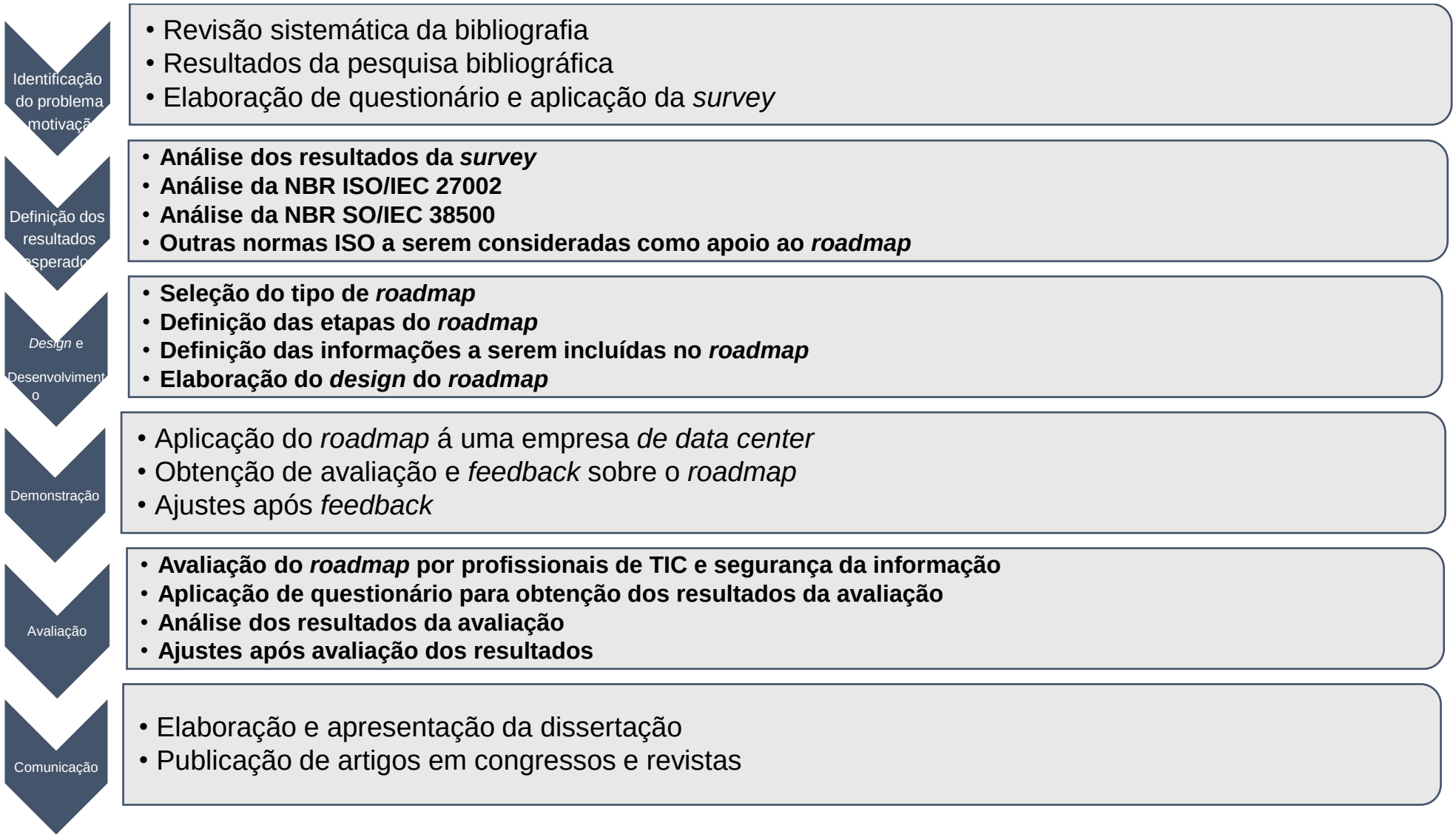
Peffers et al (2007) sintetizaram as proposições de diversos pesquisadores sobre as etapas para o desenvolvimento de pesquisas sobre um determinado problema, consolidando os mesmos no processo *denominado Design Science Research Method* (DSRM), composto por seis etapas distintas, dispostas em uma ordem sequencial, embora, não haja necessidade de que o pesquisador sempre cumpra as seis etapas em sequência:

1. **Identificação do problema e motivação:** Nesta etapa, busca-se definir o problema de pesquisa específico e justificar o valor de uma solução. A definição do problema será usada para desenvolver um artefato que possa oferecer uma solução eficaz, dividindo-se o problema em partes conceituais com base em sua complexidade;
2. **Definição dos resultados esperados**: Inferir os objetivos de uma solução para o problema definido e conhecer o que é possível e tangível. O pesquisador deve conhecer o estado atual do problema e das soluções atuais, quando houver, e qual a eficácia delas;
3. **Desenho e desenvolvimento:** Criar o artefato, que pode ser um constructo, modelo, método ou instanciação. Esta atividade deve incluir a definição das funcionalidades desejadas, sua arquitetura e a criação do próprio artefato;
4. **Demonstração:** Demonstrar o uso do artefato para solucionar uma ou mais instâncias do problema, o que pode envolver experimentação, simulação, estudo de caso, prova de conceito ou outras atividades;
5. **Avaliação:** Observar e medir o quanto o artefato auxilia na solução do problema, comparando os objetivos da solução com os resultados efetivamente obtidos durante a demonstração;
6. **Comunicação:** Comunicar o problema e sua importância, o artefato, sua utilidade e inovação, o rigor de seu *design* e sua efetividade para *stakeholders*.

A DSRM propõe a elaboração de uma solução para um problema real, gerando um produto. A metodologia de pesquisa aplicada no presente estudo é baseada na DSRM, que tem fundamentação no processo de *Design Science* e na condução das etapas para a produção de um artefato para abordagem de um problema, neste caso, a elaboração de um *roadmap* para adequação de empresas à LGPD, com base nas etapas definidas por Peffers et al (2007) como a abordagem para a elaboração de um modelo para solução de um determinado problema.

A figura 8 apresenta o fluxo de desenvolvimento do *roadmap* com base nas 6 etapas da DSRM, incluindo também os elementos que compõe as subetapas que subsidiaram o desenvolvimento do *roadmap*:

Figura 8 – Fluxo de desenvolvimento do *roadmap* com base na DSRM



Fonte: Resultado da Pesquisa.

3.1 Etapa de identificação do problema e motivação

Peffers et al (2007) estabelecem como diretrizes para esta etapa a definição do problema, a qual motiva o pesquisador a buscar a solução. Esta definição será utilizada para o desenvolvimento de um artefato que possa efetivamente prover uma solução. Além disso, o pesquisador deve justificar o valor da solução, o que o motiva a buscar a solução. Os recursos necessários para esta atividade incluem o conhecimento do estado do problema e a importância de sua solução.

A pesquisa teve por objetivo o desenvolvimento de um *roadmap* para adequação de empresas à LGPD cujo problema e motivação estão embasados nos desafios mencionados em 2.4, os quais remetem à questão de pesquisa: como estruturar um *roadmap* que sirva de apoio a organizações brasileiras no processo de adequação à LGPD.

Para identificação das questões relativas ao processo de adequação de organizações brasileiras à LGPD foi realizada a revisão sistemática da bibliografia, conforme relatado no item 2.1, e os resultados da pesquisa apontaram as ferramentas e métodos propostos como apoio à adequação de empresas à LGPD e confirmaram a inexistência de uma ferramenta de *roadmap* voltada a este objetivo. Os resultados da revisão da bibliografia também serviram de subsídio para a elaboração da pesquisa *survey,* detalhada no item 2.2, a qual complementa as informações da revisão bibliográfica com as percepções dos participantes sobre a situação de suas organizações no que concerne à adequação à LGPD.

A abordagem do *Design Thinking* for utilizada como apoio nesta etapa, primeiramente na definição do problema, que foi direcionada pela questão de pesquisa, pela revisão bibliográfica e por meio da realização da pesquisa *survey*, que conforme definido na etapa da empatia do *Design Thinking* permitiu identificar as necessidades do usuário.

As questões foram inseridas em um formulário da ferramenta *Forms* da *Microsoft*, e o *link* da pesquisa foi disponibilizado por meio de mensagens enviadas por *e-mail* e pela rede social *LinkedIn* para profissionais dos setores público e privado nos mais diversos segmentos, ficando disponível para resposta por cerca de 50 dias.

A fim de preservar a privacidade dos participantes não foi coletado nenhum tipo de dado pessoal ou que permita a identificação das organizações às quais eles pertenciam. Além disso, antes do início da pesquisa, os respondentes tinham acesso

à um Termo de Consentimento Livre e Esclarecido (TCLE) que dava ciência aos participantes sobre as condições gerais da pesquisa e sobre a confidencialidade dos dados e mencionando que o preenchimento da pesquisa implicava na concordância com as condições apresentadas no TCLE, conforme apêndice A.

Ao término do período de coleta foram obtidas 43 respostas à *survey*. No entanto, um dos respondentes não preencheu a quase totalidade das respostas, tendo sido removido da análise.

O apêndice A apresenta o termo de consentimento livre elaborado e apresentado aos respondentes antes do início da *survey* e o apêndice B apresenta as questões elaboradas para a *survey*, com a indicação do autor que foi base para a elaboração da questão, enquanto o apêndice C apresenta os resultados gerais da survey.

3.2 Etapa de definição dos resultados esperados

Peffers et al. (2007) definem que nesta etapa deve-se inferir os objetivos de uma solução a partir da definição do problema e do conhecimento do que é possível e viável, podendo ser objetivos quantitativos, ou seja, quais os termos em que uma solução seria melhor do que as atuais ou qualitativos, por exemplo, uma descrição de como o novo artefato apoiará soluções para problemas não abordados até o momento.

O problema que se procura endereçar é aquele proposto na questão de pesquisa: Como estruturar um *roadmap* que sirva de apoio a organizações brasileiras no processo de adequação à LGPD?

Tendo em vista que a solução que se procura tem por objetivo atender ao cumprimento de uma lei específica, no caso a LGPD, esta deve servir como base para a construção do conjunto de etapas a serem definidas para o *roadmap.* Uma visão geral dos principais componentes da lei que são considerados na elaboração do *roadmap* estão descritos no quadro 8 do item 2.3.

Além disso, os resultados da pesquisa bibliográfica (item 4.1.1) e da pesquisa *survey* (item 4.1.2) fornecem subsídios para a elaboração do *roadmap* a partir da constatação da falta de implementação de elementos que são base para a adequação à lei, tais como a elaboração e implementação de políticas, procedimentos, termos de responsabilidade, cláusulas contratuais e outros mecanismos que a pesquisa indicou não serem de ampla adoção pelas organizações no seu processo de adequação à

LGPD.

Como complemento, as normas ISO/NBR e os frameworks de segurança *NIST Cibersecurity Framework* e *NIST Privacy Framework* foram também considerados como referência para a definição dos resultados do RAEL.

3.3 Etapa de desenho e desenvolvimento

De acordo com Peffers et al. (2007) a atividade de desenho e desenvolvimento tem por objetivo a criação do artefato, o qual pode ser um constructo, modelo, método ou instanciação. Conforme mencionado, o artefato a ser desenvolvido é um *roadmap* intitulado ***Roadmap* para Adequação de Empresas à LGPD - RAEL** que será um *roadmap* multicamadas, por ser, segundo Farruck, Phaal e Probert (2003) o mais comum e o mais flexível em aplicação, tendo em geral 4 dimensões: tempo, camadas, anotações e processo, as quais foram explicadas no item 2.6.

Quanto ao modelo do **RAEL** no que tange ao propósito, ele se assemelha a um *roadmap* de planejamento estratégico, tendo em vista as características do **RAEL** serem voltadas à adequação a uma lei, que é estratégica para a adequação da empresa à legislação.

Quanto ao formato, o *roadmap* multicamadas será no formato de tabela e/ou de fluxo, por conter um grande volume de informações, organizadas em categorias e com etapas que se sucedem.

O processo de elaboração do *roadmap* consistiu na elaboração de um *design* inicial pelo pesquisador a partir das definição do modelo conforme mencionado e com base nos estudos realizados, o qual foi posteriormente refinado por meio da metodologia *Scrum,* aplicando sucessivos *Sprints* em interações, realizadas inicialmente com o orientador e, posteriormente, com o proprietário da empresa de *data center* responsável pela aplicação e demonstração do *roadmap,* revisando as anotações deste sobre cada etapa do *roadmap,* bem como por meio de uma entrevista semiestruturada, agregando assim a experiência deste profissional como DPO da empresa e de diversos de seus clientes na adequação à LGPD ao processo de refinamento do artefato.

A fim de tornar mais fácil a visualização e navegação no *roadmap*, ele foi adaptado ao final do processo para um formato gráfico e gerado no formato de arquivo PDF, o qual permite sua visualização em diferentes dispositivos sem que seja necessário o uso do *Microsoft Excel*, software originalmente utilizado no seu

desenvolvimento. Além disso, o formato PDF também permite a ampliação e visualização detalhada do conteúdo conforme necessário, facilitando a visão geral quando for requerida, e ao mesmo tempo permitindo a visualização detalhada do conteúdo de cada etapa.

3.4 Etapa de demonstração

Peffers et al. (2012) ressalta que a demonstração do uso do artefato pode envolver, além da pesquisa teórica, a experimentação, simulação, estudo de caso, prova, *benchmarking* ou outro mecanismo apropriado, utilizando recursos necessários para resolver o problema com base no conhecimento efetivo de como usar o artefato e como ele pode funcionar de forma viável.

Para demonstração do artefato foi utilizada uma empresa de *data center* localizada na região da grande São Paulo, a qual denominaremos como empresa XYZ, a qual concordou em aplicar o RAEL na avaliação do seu nível de adequação à LGPD.

O responsável pela avaliação foi o proprietário da empresa, que exerce o papel de DPO, também conhecido na terminologia da LGPD como Encarregado pelo Tratamento de Dados Pessoais, não apenas da empresa, como também de diversos clientes que mantém serviço de hospedagem de servidores na mesma.

O proprietário da XYZ atua há mais de 20 anos na área de gestão de tecnologia da informação exercendo diversas atividades, como proprietário de empresa, gestor de Infraestrutura de TI e auditor de sistemas, tendo ampla experiência na aplicação de metodologias/*frameworks* de implementação de segurança da informação como COBIT e ITIL, além de formação como DPO.

A XYZ concordou em aplicar o RAEL na avaliação da adequação de sua empresa à LGPD mediante a condição de sigilo do nome, em função de que alguma das informações compartilhadas poderiam estar sob proteção contratual, além do fato de que os resultados da avaliação poderiam eventualmente indicar o descumprimento da legislação por parte da empresa, gerando impactos legais e contratuais para ela e para seus clientes.

Para a demonstração a XYZ recebeu uma planilha em formato *Microsoft Excel* contendo as etapas do RAEL. Durante a aplicação do RAEL na avaliação da adequação da XYZ à LGPD foram sendo efetuadas observações na planilha com comentários sobre dúvidas, críticas e sugestões de melhoria ao RAEL.

Ao final da avaliação foi realizada uma entrevista não estruturada para obtenção do *feedback* sobre o *roadmap* e para comentário sobre os pontos identificados durante a demonstração.

3.5 Etapa de avaliação

Peffers et al. (2012) definem que a etapa de avaliação consiste em observar e medir quão bem o artefato suporta a solução do problema. Dependendo da natureza do problema e do artefato, a avaliação pode assumir diversos formatos, podendo incluir pesquisas de satisfação ou *feedback* dentre outras opções. Ao final desta etapa os pesquisadores podem decidir retornar para a etapa de desenho e desenvolvimento ou avançar para a etapa da comunicação, deixando melhorias adicionais para projetos posteriores.

Para a avaliação do RAEL foram convidados 4 profissionais com experiência na área de tecnologia da informação com foco em segurança da informação e vivência profissional de mais de 10 anos de atuação que pudessem avaliar o RAEL, a fim de identificar sua consistência no atingimento do objetivo para o qual o *roadmap* foi desenvolvido, que é prover apoio a empresas no processo de adequação à LGPD.

Estes profissionais foram selecionados por meio de indicação ou contato profissional do pesquisador mantido por meio da rede LinkedIn com eles.

Para a realização da avaliação foi desenvolvido um questionário com questões elaboradas em escala *Likert* divididas em 2 blocos:

Bloco 1: Questões 1 a 3 – Obtenção do perfil dos avaliadores;

Bloco 2: Questões 4 a 20 – Questões elaboradas com objetivo de coletar as impressões dos avaliadores com relação ao *roadmap* e sua aplicação como guia de apoio às organizações brasileiras no processo de adequação à LGPD.

No bloco 2, após cada questão, os avaliadores poderiam tecer seus comentários quanto à avaliação realizadas para a questão, caso assim o desejassem.

Para fins da avaliação o RAEL foi compartilhado com estes profissionais e foi compartilhado um link para o questionário geral de avaliação via *Microsoft Forms*, onde os avaliadores responderam às questões e teceram seus comentários de forma anônima e sem que um avaliador tivesse conhecimento dos resultados dos demais.

Antes de iniciar o preenchimento do formulário, foi exibido aos avaliadores um TCLE esclarecendo que a coleta dos dados ocorre de livre e espontânea vontade e

que poderia ser interrompida a qualquer momento, e que não haveria coleta de nenhum dado que permitisse a identificação dos respondentes, tais como e-mail, nome, telefone ou qualquer outro dado pessoal.

O apêndice L contém o TCLE apresentado aos avaliadores antes do início do preenchimento do formulário de avaliação, e o apêndice M apresenta as questões elaboradas para a avaliação do RAEL.

3.6 Etapa de comunicação

Peffers et al. (2007) definem a etapa de comunicação como sendo aquela na qual são comunicados o problema e sua relevância, o artefato, sua utilidade e novidade, os critérios e o rigor do *design* e sua efetividade para pesquisadores e outras audiências relevantes, tais como profissionais da área, quando apropriado. A comunicação pode ocorrer por meio da publicação de artigos, teses e dissertações, participação em seminários ou outros meios que permitam tornar públicos os resultados do desenvolvimento da pesquisa.

4 RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados os resultados de cada uma das seis etapas do trabalho de pesquisa realizadas com base na DSRM.

4.1 Resultado da etapa de identificação do problema e motivação

Os resultados da etapa de identificação do problema e motivação foram endereçados por meio da revisão sistemática da bibliografia, bem como por meio da pesquisa *survey*, abordada no item 2.1. A seguir são comentados os resultados de cada um destes instrumentos de desenvolvimento do trabalho.

4.1.1 Resultado da pesquisa bibliográfica

Como resultado das pesquisas realizadas na ferramenta *"Publish or Perish*", foram identificados 85 artigos na base *Scopus* e 56 artigos na *Web of Science*, totalizando 141 artigos, os quais foram exportados para uma planilha para análise.

Posteriormente, foi conduzida uma análise para identificar e eliminar possíveis duplicidades entre as duas bases, resultando na exclusão de 34 artigos da base *Web of Science*. Isso resultou em um total de 107 artigos restantes para revisão.

Em seguida, procedeu-se à leitura dos títulos e, quando necessário, dos resumos, a fim de descartar os artigos que não estivessem relacionados ao objetivo da pesquisa. Também foram excluídos os resultados referentes a livros, dissertações de mestrado, teses de doutorado ou artigos indisponíveis para consulta.

Dentre os 107 artigos após a remoção de duplicatas, 72 foram descartados após a análise dos títulos e outros 27 foram excluídos após a avaliação dos resumos, por não abordarem métodos para a implementação da LGPD. Além disso, um artigo não estava disponível para acesso online.

O quadro 9 apresenta o sumário do total de artigos analisados e descartes efetuados durante o processo de análise:

Quadro 9 - Sumário de artigos analisados

SUMÁRIO DE ARTIGOS ANALISADOS		
+	**ARTIGOS *SCOPUS***	**85**
	ARTIGOS *WEB OF SCIENCE*	**56**
TOTAL DE ARTIGOS PESQUISADOS		**141**
-	**ARTIGOS DUPLICADOS**	**34**
TOTAL APÓS REMOÇÃO DUPLICADOS		**107**
-	**DESCARTADOS APÓS LEITURA DO TÍTULO**	**72**
-	**DESCARTADOS APÓS LEITURA DO RESUMO**	**27**
-	**INDISPONÍVEL PARA ACESSO ONLINE**	**1**
TOTAL PARA LEITURA TEXTUAL		**7**

Fonte: Resultado da pesquisa

Após a aplicação dos critérios de seleção restaram 7 artigos, para os quais foram efetuadas a leitura e análise textual. O quadro 10 apresenta os artigos selecionados:

Quadro 10 - Artigos selecionados para leitura por atenderem aos critérios de seleção

Artigo	Título do Artigo	Autor	Publicação	Categoria
1	*Components of the preliminary conceptual model for process capability in LGPD (Brazilian data protection regulation) context.* Componentes do modelo conceitual preliminar para capacitação de processos no contexto da LGPD.	Muncinelli et al.	2020	Ferramenta de apoio à implementação da LGPD
2	*Developing a conceptual model for process capability in the Brazilian data protection regulation context.* Desenvolvendo um modelo conceitual para capacitação de processos no contexto da lei brasileira de proteção de dados.	Muncinelli et al.	2021	Ferramenta de apoio à implementação da LGPD
3	*Are My Business Process Models Compliant with LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes.* Estão meus modelos de processo de negócio em conformidade com a LGPD? O método LGPD4BP para avaliação e modelagem consciente dos processos de negócio.	Araújo et al.	2021	Ferramenta de apoio à implementação da LGPD

4	*Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security.* Utilizando o MCDA para critério de seleção de segurança de dados pessoais em conformidade com a LGPD.	Ribeiro e Canedo	2020	Ferramenta de apoio à implementação da LGPD
5	*Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD).* Proposta de um processo de implementação para a Lei Geral de Proteção de Dados Brasileira (LGPD).	Canedo et al.	2021	Processo de implementação da LGPD
6	*Framework for the development of computational solutions for the support of requirements engineering with a focus on data protection. Framework* para o desenvolvimento de soluções computacionais para o suporte de engenharia de requisitos com foco na proteção de dados.	Silva et al.	2022	*Framework* para desenvolvimento de sistemas aderentes à LGPD
7	*Ensuring privacy in the application of the Brazilian general data protection law (LGPD).* Assegurando privacidade na aplicação da Lei Geral de Proteção de Dados Brasileira (LGPD).	Castro et al.	2022	Guia para implementação da LGPD

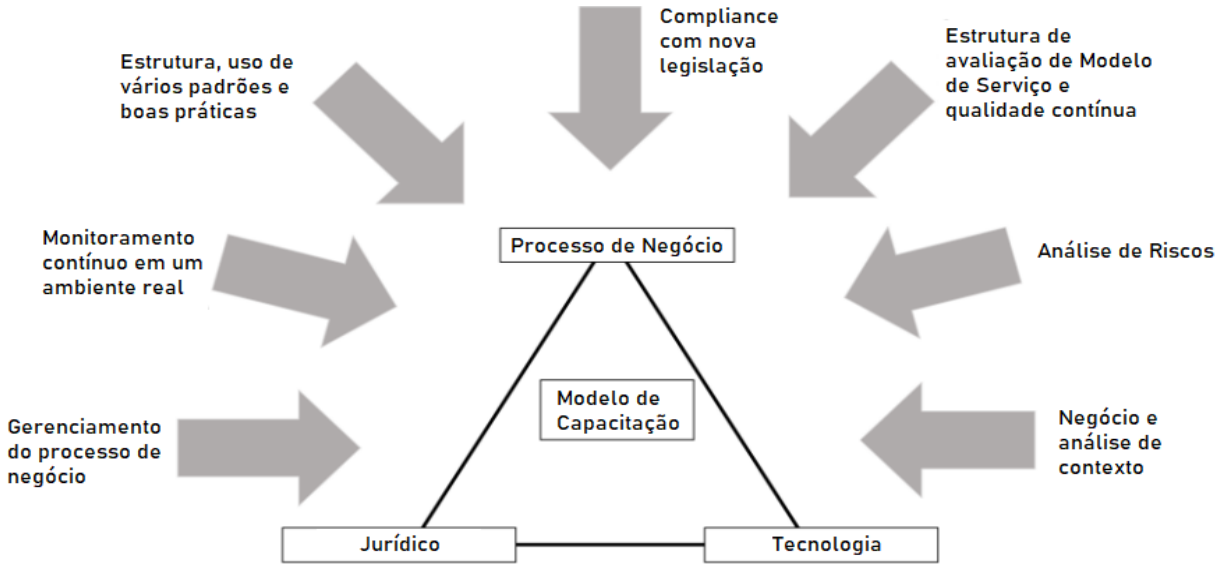
Fonte: Resultado da pesquisa

Apresenta-se na sequência, uma visão geral dos artigos selecionados:

O artigo 1, intitulado *"Components of the preliminary conceptual model for process capability in LGPD (Brazilian data protection regulation) contexto"* (Muncinelli et al, 2020) relata uma pesquisa sobre as principais áreas de contribuição para lidar com a transformação digital, com foco em cibersegurança, no contexto da legislação de proteção de dados pessoais (LGPD). Este estudo analisou 30 artigos dentre um total de 56 publicados entre os anos de 2010 e 2019, consolidando os resultados para identificar os sete principais conceitos a serem utilizados como componentes na construção de um modelo de capacidade de negócios (*business capability model)*.

A figura 9 apresenta a imagem do modelo proposto, exibindo sua estrutura em termos de áreas de atuação e etapas, conforme detalhado no referido artigo.

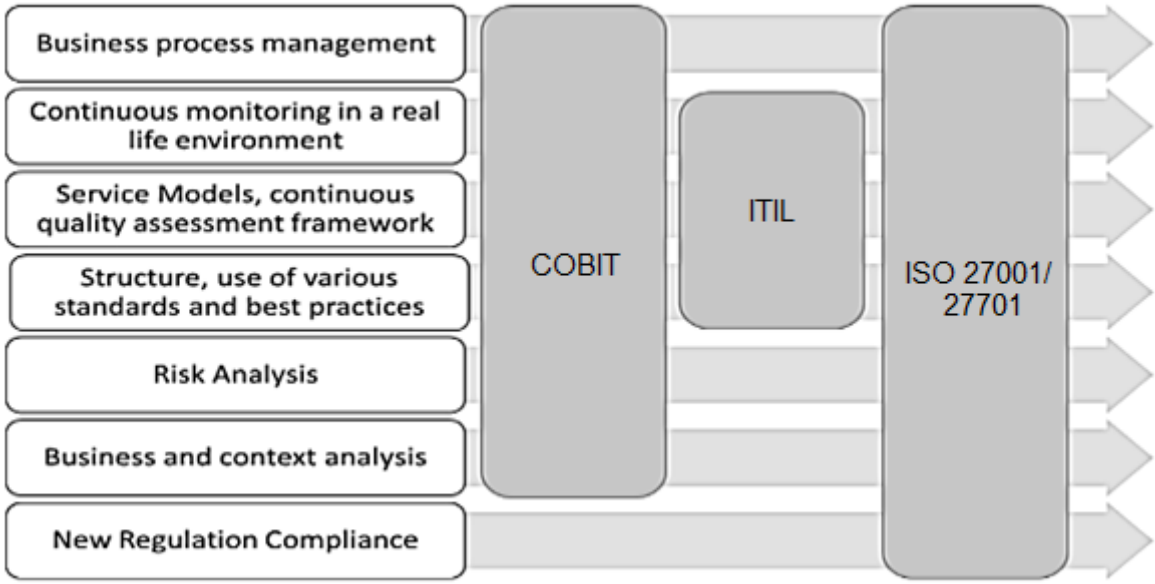
Figura 9 – Estrutura do *Business Capability Model*



Fonte: adaptado de Muncinelli et al, 2020.

O artigo finaliza com uma análise da relação dos *frameworks* COBIT, ITIL e ISO 27001 / 27701 com relação aos 7 conceitos, em termos de correlação, conforme apresentado na figura 10.

Figura 10 – Relação entre os principais componentes do modelo relacionados à literatura

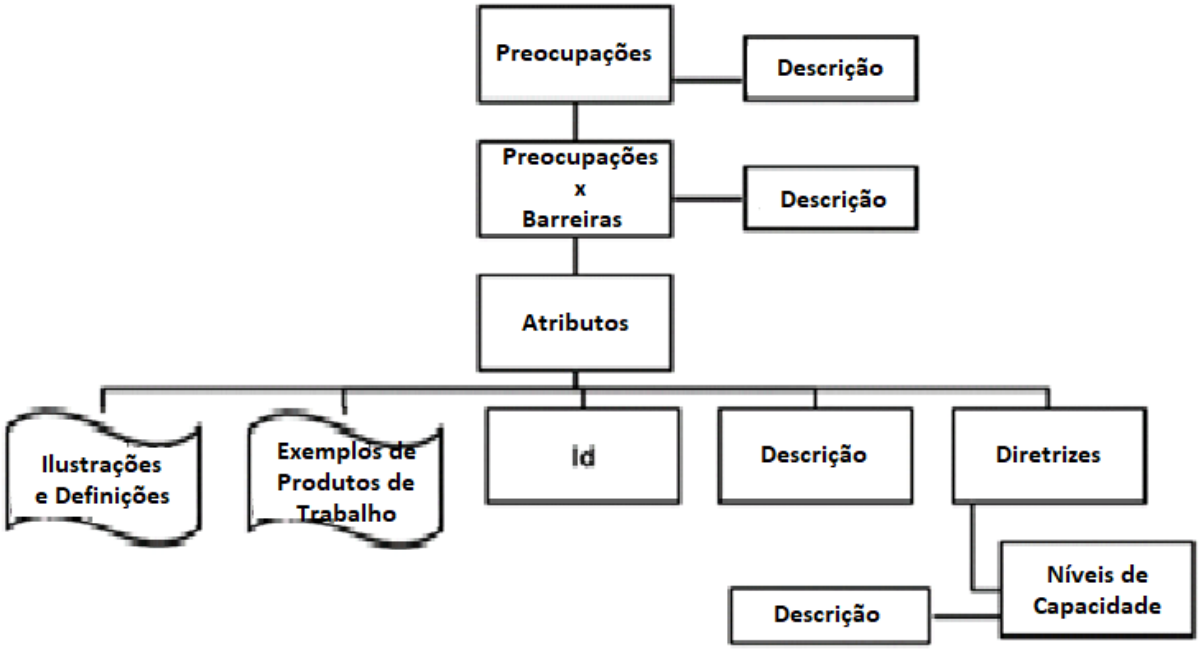


Fonte: Muncinelli et al, 2020.

O artigo 2, denominado "*Developing a conceptual model for process capability in the Brazilian data protection regulation context"* (Muncinelli et al, 2020), dos mesmos autores do artigo 1, dá continuidade ao teor do artigo anterior com foco no relato do desenvolvimento do modelo baseado no processo de pesquisa descrito no primeiro

artigo, propondo a estrutura geral do modelo, conforme apresentada na figura 11.

Figura 11 – Estrutura geral do modelo para capacitação de processos



Fonte: Adaptado de Muncinelli et al, 2021.

Além disso, o artigo propõe 4 níveis de maturidade para o modelo em desenvolvimento: Nível 1 – Incompleto, Nível 2 – Definido, Nível 3 – Gerenciado, Nível 4 – Institucionalizado, bem como apresenta os critérios para avaliação de adequação a cada nível.

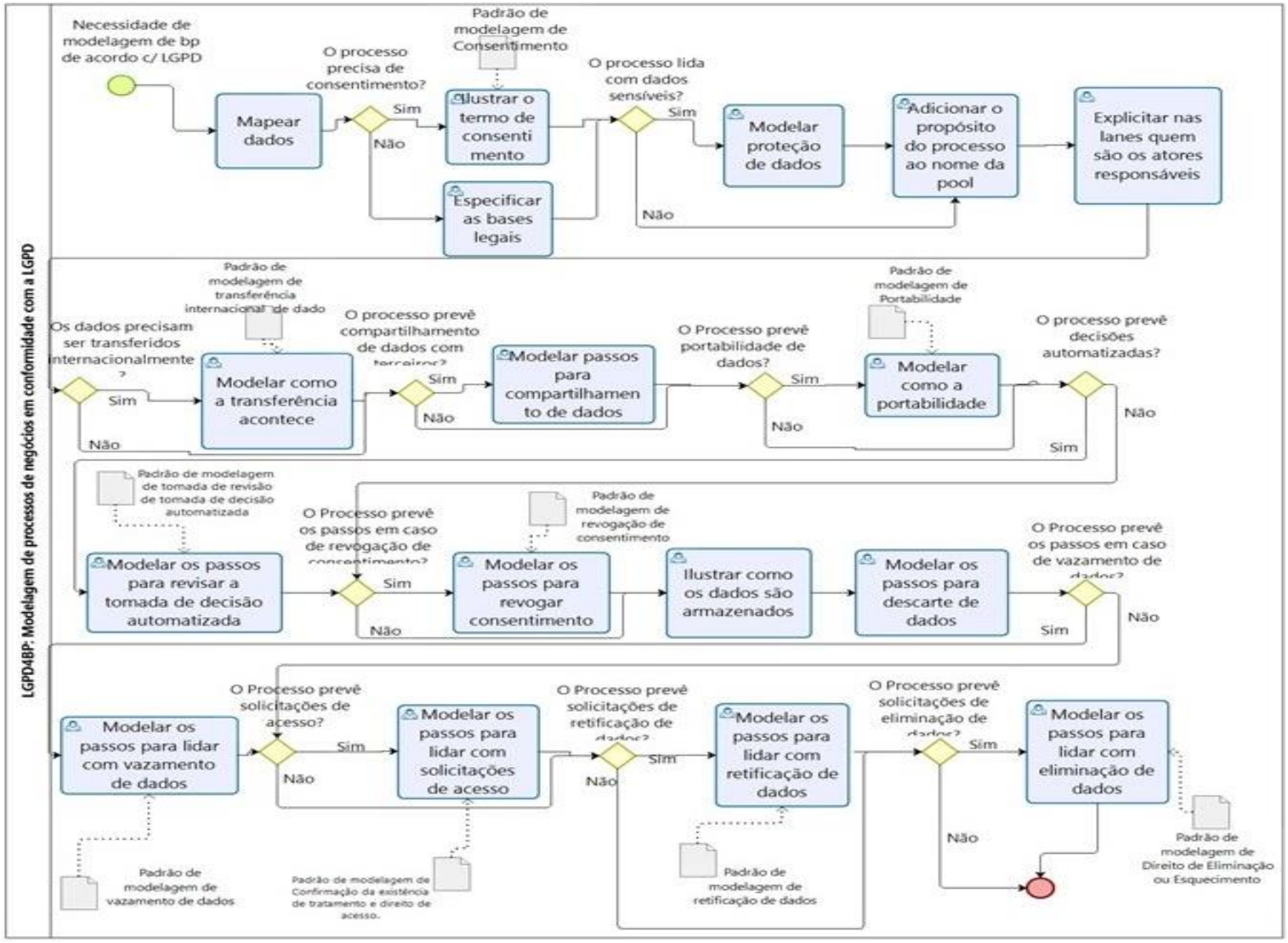
Como os dois artigos são parte do desenvolvimento de uma tese de doutorado ainda em desenvolvimento durante a publicação deles, não foi apresentado o resultado final.

O artigo 3, intitulado "*Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes*" (Araújo et al, 2021), aborda as questões de pesquisa relacionadas à avaliação da conformidade de um processo em relação à LGPD e como modelar um processo de negócio alinhado com os requisitos estabelecidos por essa legislação.

O Método proposto, LGPD4BP, é composto por um questionário de avaliação da conformidade dos processos à LGPD com 18 questões, um catálogo com 9 padrões de modelagem: Consentimento, Confirmação da existência de tratamento e direito de acesso, Portabilidade, Vazamento de dados, Revisão de tomada de decisão

automatizada, Revogação de consentimento, Retificação de dados, Direito de esquecimento ou eliminação de dados pessoais, Transferência internacional de dados, que estão relacionadas às 18 questões e um método de modelagem de processos em conformidade com a LGPD, apresentado na figura 12.

Figura 12 – Etapas do método LGPD4BP



Fonte: Araújo et al., 2021.

O artigo finaliza com o relato dos resultados da aplicação do método em um estudo de caso no Colégio de Aplicação da Universidade Federal de Pernambuco (UFPE), avaliado por meio da aplicação de um questionário sobre a utilidade e facilidade de cada uma das 3 tarefas do método. Importante salientar que o questionário não foi aplicado aos usuários do método, e sim a 18 alunos da pós-graduação em sistemas da UFPE que assistiram um vídeo de treinamento do método e foram convidados a aplicá-lo no contexto do Colégio de Aplicação, o que não representa um uso efetivo do método, mas um exercício de uso dele.

O artigo 4, "*Using MCDA for selecting criteria of LGPD compliant personal data security*" (Ribeiro e Canedo, 2020) tem como proposta a aplicação do processo MCDA – *Multiple Criteria Decision Analysis*, ou Tomada de Decisão de Múltiplos Critérios, juntamente com o método PROMETHEE II – *Preference Ranking Organization Method for Enriched Evaluation*, ou *Ranking* de Preferência de Métodos Organizacionais para Avaliação Enriquecida e com o método AHP – *Analytic Hierarchy Process*, ou Processo de Hierarquia Analítica para a identificação de critérios de segurança de dados pessoais e priorização dos mesmos para permitir a adequação da Universidade de Brasília (UnB) à LGPD, além de apresentar o estudo de caso da aplicação destes conceitos na instituição.

É feita uma breve explanação de cada método e da estrutura geral de sistemas da UnB, composta de 34 sistemas desenvolvidos internamente e um sistema com 3 módulos adquirido junto à Universidade Federal do Rio Grande do Norte (UFRN), os quais devem ser adequados à LGPD.

Para identificação dos critérios chave de segurança foi realizada a leitura da LGPD, bem como da GDPR e norma ISO 27701, e os critérios selecionados foram: Nível de Proteção de Dados, Risco de Segurança, Severidade de Incidentes e Risco de Privacidade de Dados.

Foi aplicado o método AHP para definição de quais princípios-chave da LGPD são relevantes para implementação da segurança de dados pessoais, resultando na priorização da Segurança, Necessidades e Prevenção como sendo os princípios mais importantes.

Foi elaborado um quadro associando cada um dos 4 critérios-chave com as alternativas disponíveis para melhor implementação de segurança de dados pessoais na UnB, conforme definido no Quadro 11.

Quadro 11 – Critérios e alternativas possíveis

Critério	Definição	Alternativas
Nível de Proteção de Dados	LPGD assume que o Brasil só será capaz de transferir dados para países que forneçam à LGPD um nível de proteção de dados pessoais adequado. A LGPD determina que a autoridade nacional deve ter padrões e técnicas estabelecidos para assegurar proteção de dados.	1. Limitar acesso apenas ao mantenedor dos dados 2. Anonimização de dados pessoais 3. Hashing de dados sensíveis 4. Apagando dados pessoais 5. Mantendo dados pessoais armazenados 6. Classificando importância de dados pessoais
Riscos de Segurança	A LGPD menciona que agências do governo federal e empresas privadas devem identificar os riscos relacionados à dados pessoais, bem como quais ações devem ser tomadas para mitigar estes riscos.	1. Definir Security Officer 2. Definir uma Política de Segurança de Dados Pessoais 3. Utilizar sistema de criptografia 4. Utilização de certificado para acesso à dados pessoais 5. Criação de Grupos de Usuários 6. Utilização de Firewall
Severidade de Incidentes	Dependendo da severidade do incidente, a LGPD determina que medidas devem ser tomadas para informar os sujeitos dos dados sobre os danos causados e medidas devem ser tomadas para reverter ou mitigar os efeitos do incidente.	1. Mapear potenciais incidentes 2. Desenvolver um Plano de Resposta a Incidentes 3. Avaliar as Melhores Soluções Técnicas para resolver o incidente 4. Definir medidas de mitigação do incidente
Riscos de Privacidade de Dados	LGPD recomenda que riscos de privacidade de dados devem ser registrados e medidas apropriadas devem ser tomadas para mitigar estes riscos.	1. Verificar privacidade de serviços Web 2. Criar Grupos de Acesso a Dados Pessoais restritos 3. Verificar Dados Pessoais armazenados por cada um dos serviços

Fonte: Ribeiro e Canedo, 2020.

Para definição do critério de seleção da melhor alternativa foi utilizado o método PROMETHEE II, definindo pesos numa escala 1-3-5-7-9 para cada um dos critérios, onde o valor 1 da escala significa que o critério tem importância equivalente a outro critério, enquanto o valor 9 significa que o critério é muito mais significativo com relação a outro.

A tabela 1 apresenta os critérios de priorização.

Tabela 1 – Matriz de Critérios de Priorização e Prioridade.

Critério	Nível de Proteção de Dados	Riscos de segurança	Severidade do Incidente	Riscos de Privacidade de Dados	Critério de Prioridade
Nivel de proteção de Dados	1	0,33	5	0,2	0,14
Riscos de Segurança	3	1	7	0,33	0,27
Severidade do Incidente	0,2	0,14	1	0,14	0,05
Riscos de Privacidade de Dados	5	3	7	1	0,54
Soma	9,2	4,48	20	1,68	

Fonte: Ribeiro e Canedo, 2020.

Como resultado os Riscos de Privacidade de Dados são os que apresentam o mais alto critério a ser implementado na UnB, e que os métodos MCDA, PROMETHEE II e AHP auxiliaram no processo de priorização, definindo iniciativas a serem priorizadas pela UnB.

Como trabalho futuro os autores pretendem monitorar o comportamento dos sistemas da UnB com relação à privacidade dos dados dos usuários, identificando novos critérios e alternativas para assegurar conformidade com a lei.

O artigo 5, denominado "*Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)"* (Canedo et al., 2021), apresenta proposta de um processo de implementação da LGPD para agências da Administração Pública Federal (APF), consistindo em 14 processos a serem conduzidos para a implementação da LGPD.

O quadro 12 contém cada um dos processos e uma breve explanação:

Quadro 12 – Processos propostos para implementação da LGPD em agências da APF

1 – Estudo da LGPD e outras leis relacionadas que guiam o negócio	Inicia com o estudo da Política de Segurança da Informação e Comunicação e leis e regulamentos relacionados, aplicáveis no contexto das agências da APF.
2 – Aplicação do questionário	Visa diagnosticar o estágio da agência APF com relação à LGPD.
3 – Designação do Oficial de Proteção de Dados / *Data Protection Officer* (DPO)	O DPO age como canal de comunicação entre o controlador, proprietários dos dados e a Autoridade Nacional de Proteção de Dados.
4 – Mapeamento do Fluxo de Dados e Processamento	Visa estruturar todos os dados pessoais, o propósito e as bases legais que legitimam o tratamento e as formas de assegurar conformidade e direitos dos proprietários dos dados.
5 – Analisar / Melhorar Políticas de Segurança Interna e Externa	Pesquisar normas, padrões, procedimentos, regras que possam amparar a implementação da LGPD.
6 – Mapear os riscos	Identificar ameaças que possam afetar dados pessoais processados no contexto da agência.
7 – Formular / Corrigir Avaliação do Impacto da Proteção de Dados (AIPD)	Identificar as obrigações de proteção de dados da agência e prover o *framework* para qualquer estratégia de proteção de dados.
8 – Aprovar a Avaliação do Impacto da Proteção de Dados (AIPD)	O controlador dos dados deve checar as informações submetidas no relatório e auditar a política no contexto dos dados pessoais.
9 – Formular / Corrigir a Política de Proteção de Dados	Criar ou refazer a política de proteção de dados atendendo os principais aspectos da LGPD.
10 – Implementar / Reimplementar Política de Proteção de Dados	O objetivo é criar uma política que mensura processamento de dados pessoais coletados pela agência
11 – Análise Pós-Implementação do Impacto da Política de Proteção de Dados	O objetivo é a implementação de vários controles, junto com a análise detalhada do ambiente computacional e organizacional.
12 – Treinamentos	Prover ao mesmo tempo uma comunicação atrativa e objetiva dos conceitos de segurança de dados e boas práticas para garantir a privacidade dos dados.
13 – Concepção de Novos Dados	O objetivo é identificar situações de invasão da privacidade em qualquer proposta para novos sistemas ou mudanças nos sistemas atuais da agência.
14 – Tecnologia da Informação e Comunicação Direcionada à Governança da Proteção de Dados	O objetivo é conduzir um conjunto de políticas, regras e processos para condução da proteção dos dados pessoais da agência.

Fonte: Adaptado de Canedo et al, 2021.

Os autores afirmam que o processo é genérico, podendo ser implementado em qualquer agência da APF, mas creem que possa ser aplicado a qualquer organização privada, tendo como planejamento de estudos futuros a aplicação do modelo a agências em diferentes contextos.

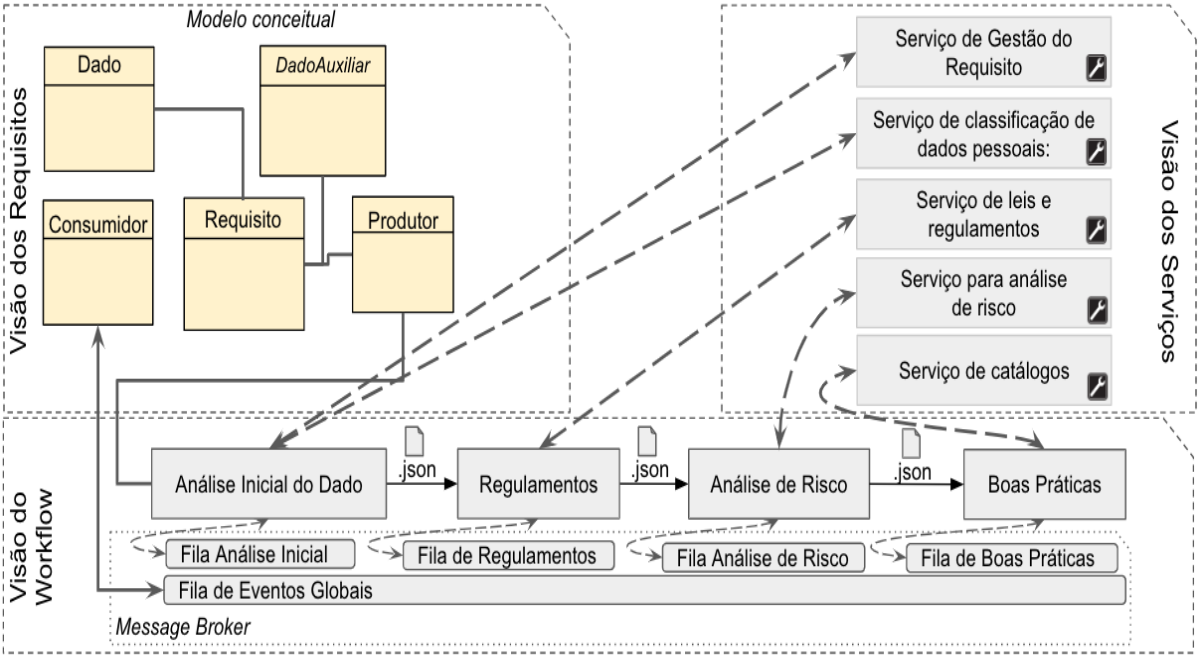
O artigo 6, intitulado "*Framework for the development of computational solutions for the support of requirements engineering with a focus on data Protection"* (DA SILVA et al, 2022) apresenta um *framework* voltado à construção de requisitos de software tendo como base regulamentos de proteção de dados.

O *framework* utiliza três visões para atingir este objetivo:

1. **Visão dos Requisitos:** propõe um modelo conceitual com definições de comunicação e *template* a serem implementados por ferramentas que desejam aderir ao *framework;*
2. **Visão do *Workflow*:** processa o requisito de *software* recebido, orquestrando etapas que consideram as peculiaridades de cada requisito. Esta visão é dividida em 4 etapas: Análise Inicial do Dado, Regulamentos, Análise dos Riscos e Boas práticas;
3. **Visão dos Serviços:** composta por um conjunto de serviços com objetivos específicos relacionados à proteção de dados pessoais e tendem a se manter iguais indiferente do segmento da empresa. Esta visão é dividida em 5 serviços: Serviço de Gestão de Requisitos, Serviço de Classificação de Dados Pessoais, Serviço de Leis e Regulamentos, Serviço de Análise de Risco e Serviço de Catálogos.

A figura 13 exibe uma visão geral do *framework*:

Figura 13 – Visão geral do *Framework*



Fonte: Da Silva et al, 2022.

O artigo apresenta um exemplo prático da aplicação do *framework* em uma empresa hipotética para desenvolvimento de um *software* de gestão educacional. Tendo em vista que o trabalho estava em desenvolvimento o exemplo é apresenta apenas as etapas iniciais da Visão do *Workflow*, que estabelece a Análise Inicial do Dado e Regulamentos.

Os autores concluem apontando a necessidade de seguir com o desenvolvimento das etapas da Visão do *Workflow* e que é preciso expor a solução a um estudo de caso que considere a dinamicidade de um ambiente de desenvolvimento real.

O artigo 7, de título "*Ensuring privacy in the application of the Brazilian general data protection law (LGPD)"* (Castro et al, 2022) propõe uma revisão do Guia de Implementação da LGPD elaborado pela Fundação Vanzolini, que garante a implementação da LPGD por meio de 4 programas, divididos em controles, conforme quadro 13:

Quadro 13 – Programas e seus respectivos controles para implementação da LGPD

Programa	Controles
1 - Cybersecurity and Information Security Management System (CISMS)	1.1. Estruturando o CISMS 1.2. Implementação do CISMS 1.3. Manutenção do CISMS 1.4. Execução do CISMS
2 - Proteção da Informação	2.1. Gerenciar requerimentos 2.2. Captura da informação 2.3. Avaliação da informação 2.4. Acesso à informação 2.5. Remoção da informação 2.6. Tratamento ético 2.7. Acesso à mídia de armazenamento 2.8. Auditoria de segurança e privacidade 2.9. Atendimento de solicitações 2.10. Reporte de Incidentes
3 – Continuidade dos Negócios	3.1 *Backup* de Dados
4 – Atitudes Seguras	4.1. Treinamento

Fonte: Adaptado de Castro et al. 2022

O *framework* proposto é uma evolução do processo acima, consistindo na adição de um controle ao processo 2 visando conformidade com a norma ISO/IEC 27001:2013 em virtude de a norma apresentar diversas similaridades com os requerimentos da LGPD, tais como controle de acesso às informações, atribuição de responsabilidades para proteção de ativos e exigindo de fornecedores o atendimento de padrões de segurança definidos pela organização. Os autores ressaltam que a norma não atende a todos os requisitos da LGPD, e propõe a adição de um novo programa aos 4 originais, logo após o segundo. Desta forma, o programa 3 passa a ser o novo programa proposto, denominado Melhorando a Privacidade, com o programa 3 original passando a ser o programa 4, e o programa original 4 passando a ser o programa 5.

O programa proposto, “Melhorando a Privacidade”, é uma adoção da abordagem *Privacy By Design* que consiste em 7 princípios: Proativo não Reativo / Preventivo não Remediador, Privacidade como Padrão, Privacidade Incorporada ao *Design*, Total Funcionalidade, Segurança de Ponta-a-Ponta, Transparência e Visibilidade e Respeito à Privacidade do Usuário*,* os quais são relacionados pelos autores a alguns artigos da LGPD.

O artigo apresenta os resultados de uma pesquisa com praticantes de TIC para verificação do atual estágio de prática do *framework* proposto e aponta como fator limitante do *framework* a necessidade de funcionários experientes, dado o

envolvimento de muitos conceitos específicos e complexos para a correta integração dos controles do *framework* e conclui apontando a existência de vários conceitos e procedimentos envolvidos para a correta integração e conformidade com os requisitos da LGPD, que se negligenciados trarão às organizações dificuldades para legitimação de seus serviços.

O quadro 14 traz um sumário das propostas dos artigos analisados:

Quadro 14 – Sumário das propostas de cada artigo analisado

Artigo	Proposta
1	Proposta de um *business capability model* para adequação de organizações à LGPD
2	Elaboração da estrutura geral do *business capability model* proposto no artigo 1
3	Proposição de um método para avaliação da conformidade dos processos de uma organização à LGPD e um catálogo com 9 padrões de modelagem de processos de negócio para adequação à LGPD.
4	Ferramenta que propõe uso dos métodos MCDA, PROMETHEE II e AHP para identificação e priorização de critérios de segurança de dados pessoais.
5	Propõe um processo de implementação da LGPD para agências da Administração Pública Federal (APF), consistindo em 14 processos a serem conduzidos para a implementação da LGPD.
6	Propõe um *framework* voltado à construção de requisitos de *software* tendo como base regulamentos de proteção de dados.
7	Propõe a remodelagem do Guia de Implementação da LGPD da Fundação Vanzolini com adição de elementos da norma ISO/IEC 27001:2013 e da abordagem *Privacy By Design.*

Fonte: Resultado da pesquisa

A revisão da literatura realizada teve como objetivo, responder à questão de pesquisa sobre os métodos de desenvolvimento e implantação de processos para auxiliar na implementação da LGPD.

A pesquisa realizada identificou 85 artigos na base *Scopus* e 56 na *Web of Science*, totalizando 141 artigos. Após a remoção de duplicatas e a aplicação de critérios de seleção, restaram 7 artigos para análise detalhada.

Os sete artigos selecionados abordam ferramentas e métodos para a implementação da LGPD no contexto brasileiro, oferecendo contribuições específicas para lidar com os desafios da transformação digital, cibersegurança e conformidade com a legislação. Eles apresentam abordagens distintas, desde propostas de modelos

conceituais para capacitação de processos até *frameworks* e métodos práticos para avaliar a conformidade de processos de negócio com a LGPD.

A pesquisa não identificou métodos que apoiem a implementação geral da LGPD, mas sim métodos com abordagem específica para determinadas etapas ou processos da adequação das organizações à LGPD.

Destacam-se contribuições como o desenvolvimento de modelos conceituais para capacitação de processos, métodos de avaliação de conformidade e modelagem de processos alinhados com a LGPD. Além disso, há a aplicação de métodos de análise e decisão múltipla para selecionar critérios de segurança de dados pessoais e propostas de processos de implementação da LGPD em agências governamentais, evidenciando uma diversidade de abordagens para enfrentar os desafios impostos pela legislação.

Contudo, alguns artigos ainda estão em desenvolvimento ou em estágios preliminares, como parte de teses de doutorado, apresentando resultados parciais ou análises iniciais. Isso sugere a necessidade de futuras pesquisas para validar e aprimorar as abordagens propostas, aplicando-as em contextos reais e avaliando sua eficácia e aplicabilidade prática.

4.1.2 Resultados da *survey*

A *survey* teve um total de 42 respondentes de empresas de diversos segmentos econômicos, com participantes de diversas áreas de atuação, tempo de experiência e cargos, e o resultado geral da pesquisa é apresentado no apêndice C.

No entanto, 13 participantes, ou 31% do total, são estagiários. Embora possam eventualmente estar envolvidos no processo e até mesmo participar ativamente do mesmo, em geral este público não tem ainda um nível de conhecimento da dinâmica organizacional que assegure que as informações por eles fornecida seja relevante para o estudo.

A fim de confirmar esta hipótese, foi realizado o cálculo do coeficiente *Alfa* de *Cronbach* (α), uma medida frequentemente empregada de confiabilidade, que avalia a consistência interna de questionários compostos por dois ou mais indicadores de construto (Bland; Altman, 1997).

O coeficiente *alfa* varia de 0 a 1. Quanto mais próximo de 1, maior é a consistência interna do conjunto de itens, indicando que as perguntas estão fortemente correlacionadas e medem o mesmo construto. Valores acima de 0,70 a 0,80 geralmente são considerados aceitáveis para indicar uma boa consistência interna (Bland; Altman, 1997).

Para realização do cálculo do coeficiente, os dados da *survey* foram convertidos da escala *Likert* para valores numéricos.

Por meio da atribuição de valores, as percepções dos entrevistados, geralmente expressas em respostas de uma escala nominal, são convertidas para uma escala numérica (Hora et al., 2010), seguindo a correspondência do exemplo abaixo:

- Resposta 1 - Discordo totalmente é designada ao valor 1;
- Resposta 2 - Discordo parcialmente é atribuída ao valor 2;
- Resposta 3 - Nem discordo e nem concordo é associada ao valor 3;
- Resposta 4 - Concordo parcialmente é indicada pelo valor 4;
- Resposta 5 - Concordo totalmente é atribuída ao valor 5.

Para realização do cálculo foi realizada a conversão de todas as respostas, e gerada uma matriz de valores de cada respondente, e utilizada a biblioteca *Numpy* em *Python* para o cálculo.

O cálculo foi realizado com a matriz contendo todas as 42 respostas, e o coeficiente alfa obtido foi de 0,7145, conforme apresentado na figura 14:

Figura 14 - Cálculo do coeficiente alpha de Cronbach para os 42 respondentes

```
# Converter os dados para um array do NumPy para facilitar os cálculos
dados_array = np.array(dados)

# Calcular a variância de cada questão
variancia_por_questao = np.var(dados_array, axis=0, ddof=1)

# Calcular a variância total dos escores das questões
variancia_total = np.var(dados_array.sum(axis=1), ddof=1)

# Número de questões
num_questoes = len(variancia_por_questao)

# Calcular o coeficiente alfa de Cronbach
alfa_cronbach = (num_questoes / (num_questoes - 1)) * (1 - np.sum(variancia_por_questao) / variancia_total)

print(f"Coeficiente Alfa de Cronbach: {alfa_cronbach:.4f}")
```

```
Coeficiente Alfa de Cronbach: 0.7145
```

Fonte: Resultado da pesquisa

Em seguida foram removidas da matriz as respostas do grupo de estagiários, e realizado novo cálculo do coeficiente, conforme apresentado na figura 15:

Figura 15 - Cálculo do coeficiente alpha de Cronbach excluindo 13 estagiários

```
# Converter os dados para um array do NumPy para facilitar os cálculos
dados_array = np.array(dados)

# Calcular a variância de cada questão
variancia_por_questao = np.var(dados_array, axis=0, ddof=1)

# Calcular a variância total dos escores das questões
variancia_total = np.var(dados_array.sum(axis=1), ddof=1)

# Número de questões
num_questoes = len(variancia_por_questao)

# Calcular o coeficiente alfa de Cronbach
alfa_cronbach = (num_questoes / (num_questoes - 1)) * (1 - np.sum(variancia_por_questao) / variancia_total)

print(f"Coeficiente Alfa de Cronbach: {alfa_cronbach:.4f}")
```

```
Coeficiente Alfa de Cronbach: 0.7726
```

Fonte: Resultado da pesquisa

Embora os dois valores estejam acima de 0,70, em uma escala desejável de resultados, o coeficiente obtido com a exclusão das respostas dos estagiários é mais próximo do ideal, e, por esta razão, as respostas relativas a este público não serão consideradas na análise, restando assim 29 registros.

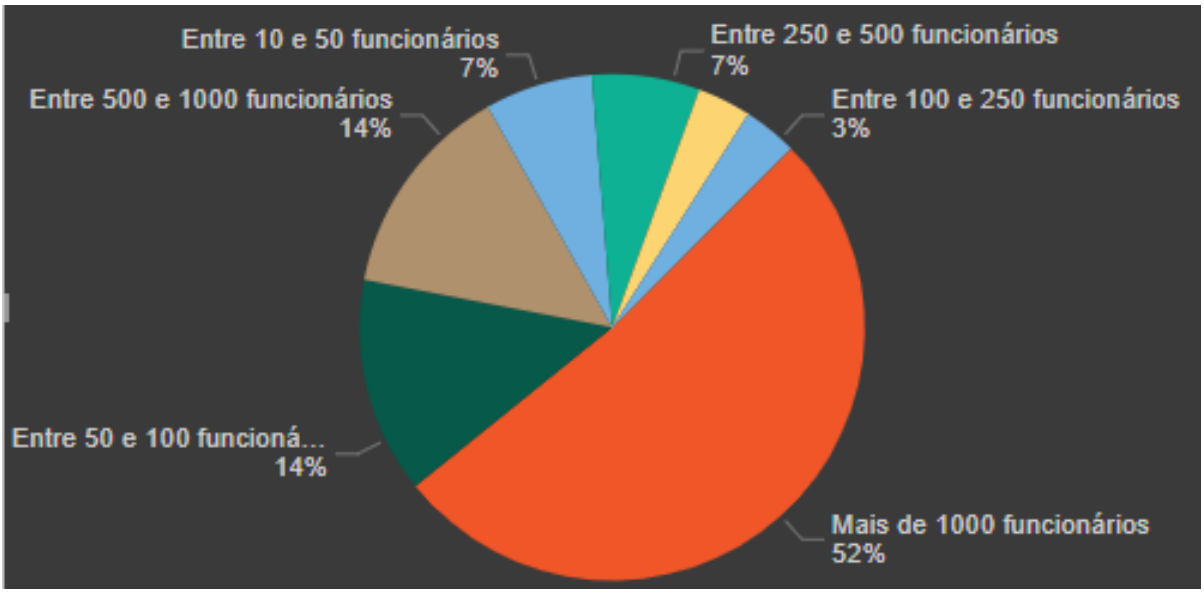
Foi analisada a possibilidade de exclusão das respostas de participantes que não tivessem nenhum nível de envolvimento com a LGPD, no entanto, embora estes profissionais não tenham envolvimento sua percepção é importante uma vez que a LGPD afeta toda a organização, e mesmo os não envolvidos no processo deveriam ter algum tipo de noção ou receber treinamento sobre a lei e seus impactos dentro da empresa.

Sendo assim, os resultados são apresentados levando em consideração as respostas de 29 do total de 42 participantes, excluindo-se as respostas dos estagiários, pela maior confiabilidade apresentada com este recorte.

4.1.2.1 Perfil das empresas e dos participantes da *survey*

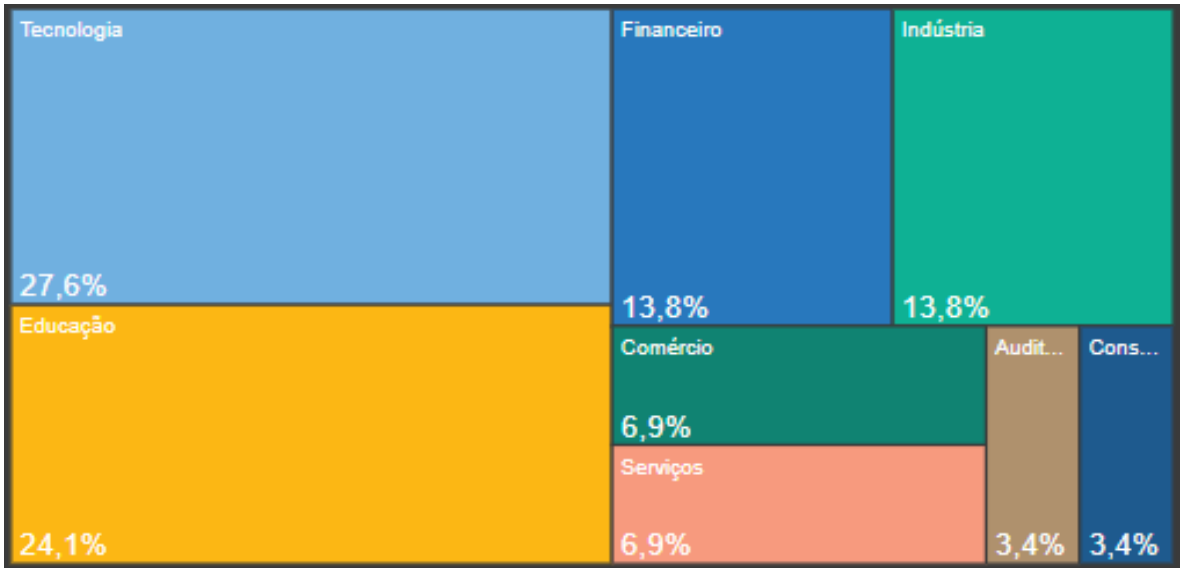
As Figuras 16 e 17 apresentam o perfil das empresas participantes da *survey*.

Figura 16 - Porte das empresas quanto ao número de funcionários



Fonte: Resultado da pesquisa

Figura 17 - Setor de atuação das empresas

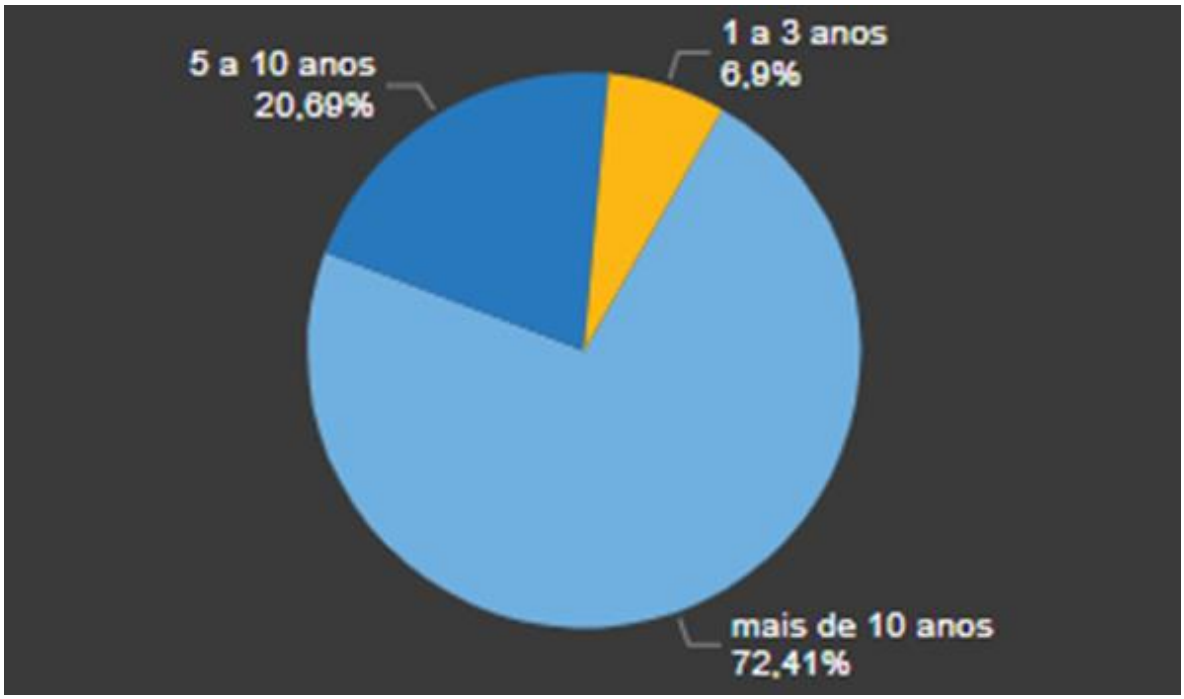


Fonte: Resultado da pesquisa

Os dados coletados são majoritariamente de empresas com mais de 100 funcionários (76% dos respondentes). O setor com maior número de empresas foi o de tecnologia, correspondendo a 27%, seguido do setor educacional com 24%.

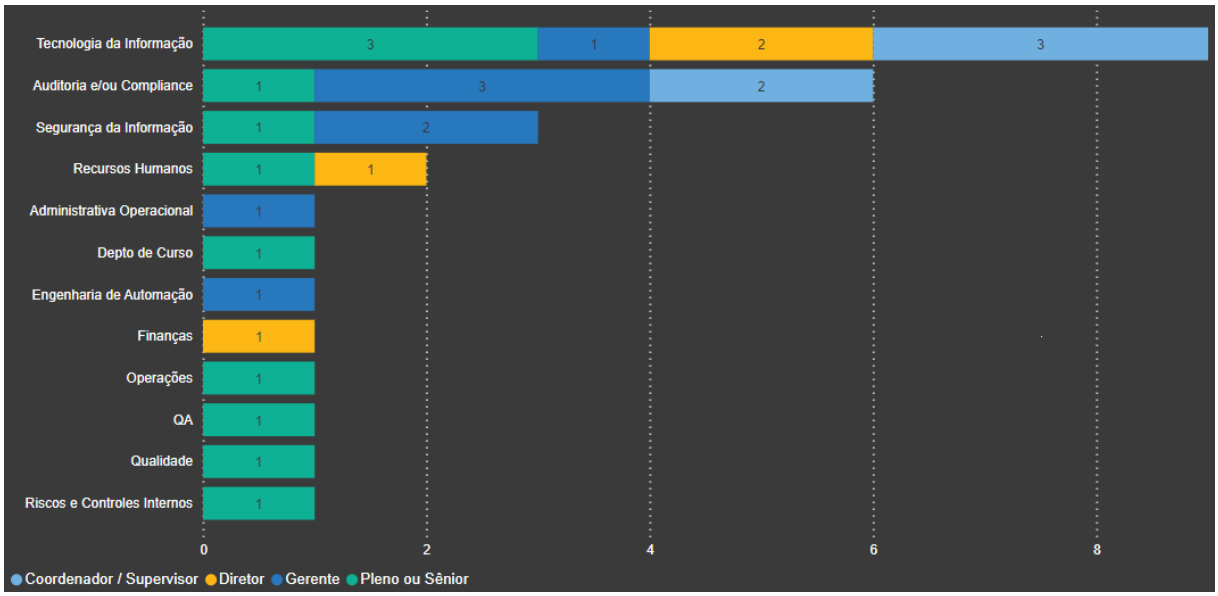
As Figuras 18 a 20 apresentam o perfil dos participantes da *survey*.

Figura 18 - Tempo de experiência profissional dos participantes



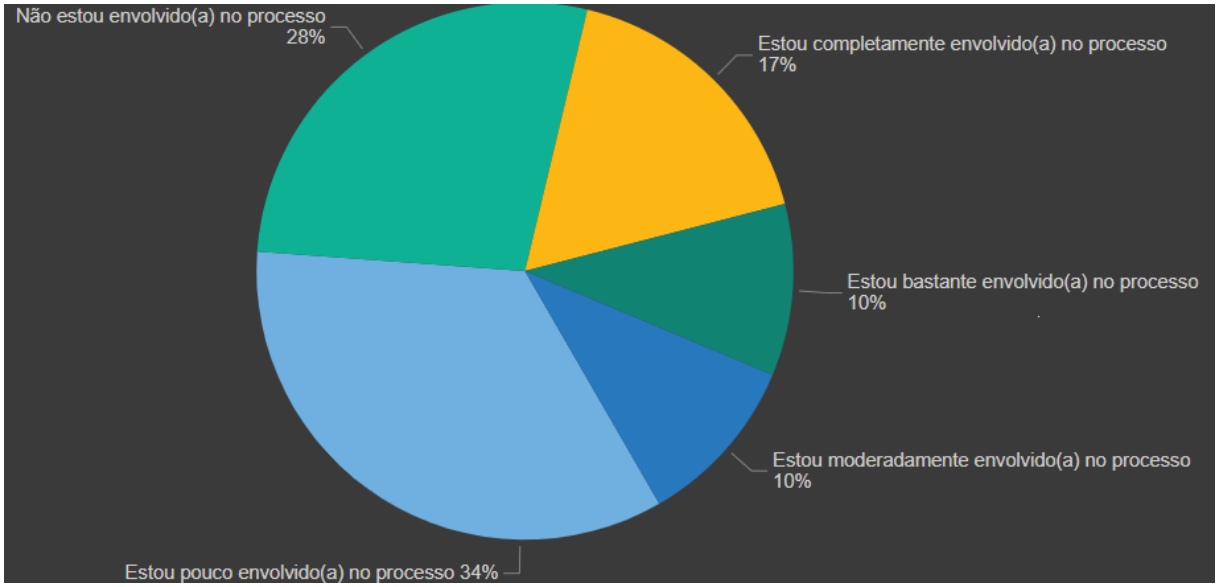
Fonte: Resultado da pesquisa

Figura 19 - Departamento X Nível Hierárquico dos participantes



Fonte: Resultado da pesquisa

Figura 20 - Envolvimento dos participantes no processo de implementação da LGPD



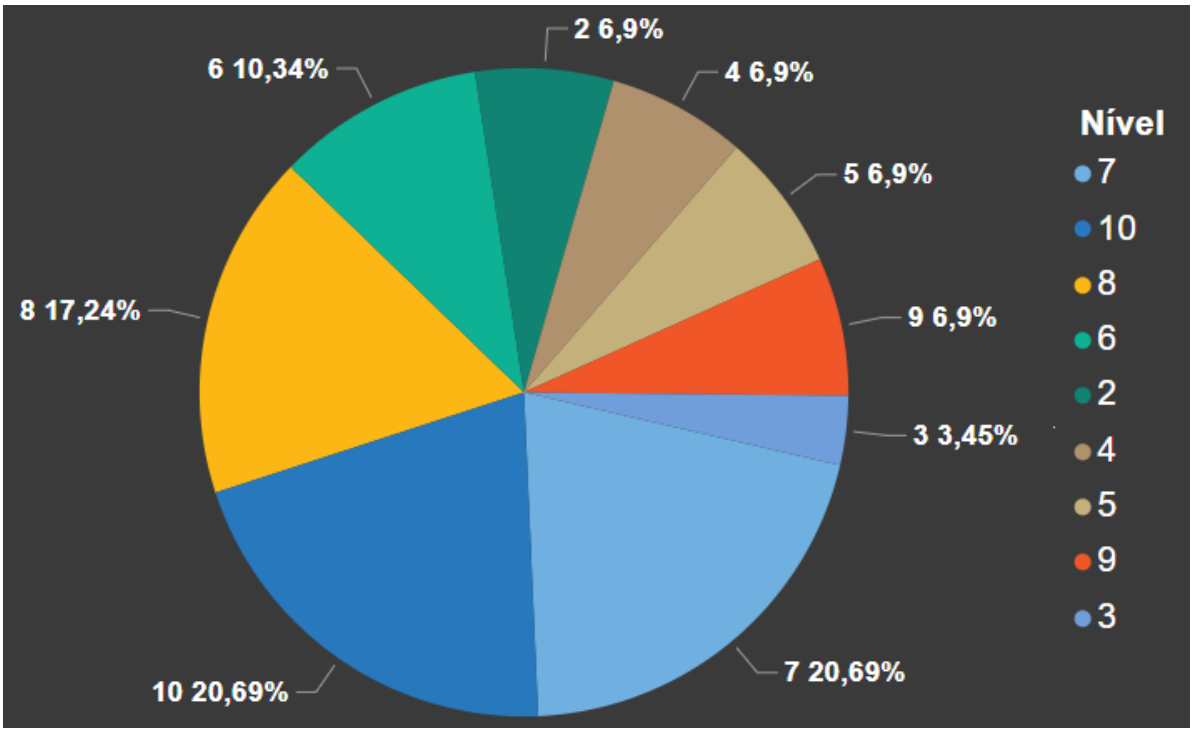
Fonte: Resultado da pesquisa

No perfil dos respondentes destaca-se que mais de 70% dos participantes têm mais de 10 anos de experiência, com a maioria dos participantes pertencendo ao departamento de Tecnologia da Informação. Com relação aos cargos há uma distribuição uniforme de respondentes. Com relação ao envolvimento no processo, a predominância é de respondentes com pouco envolvimento no processo de adequação à LGPD.

4.1.2.2 Nível de adequação das organizações à LGPD

A figura 21 apresenta a percepção dos respondentes quanto ao nível de adequação de suas organizações à LGPD em uma escala entre 1 e 10, sendo 1 totalmente não adequado e 10 totalmente adequado.

Figura 21 – Percepção do nível de adequação da organização à LGPD (Escala de 1 a 10)



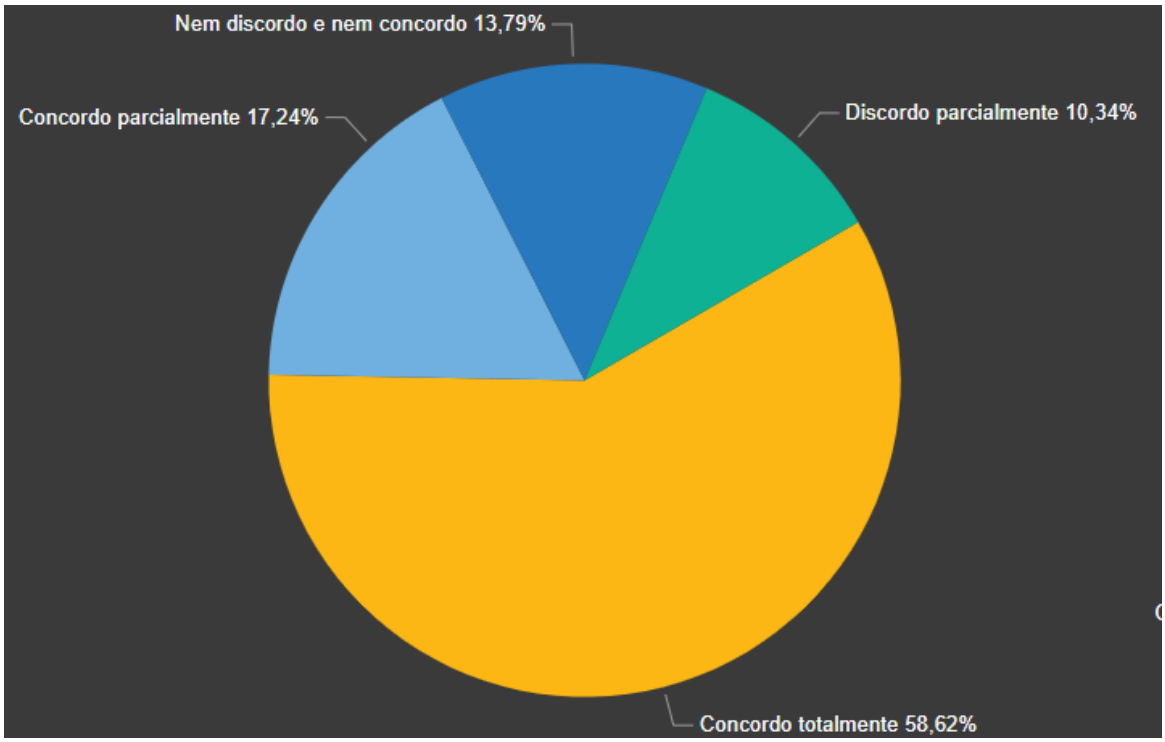
Fonte: Resultado da pesquisa

21% consideram suas organizações totalmente adequadas, e os participantes que avaliaram o nível de adequação de suas organizações entre 7 e 9 foram 45% dos respondentes, perfazendo 66% de participantes com notas entre 7 e 10 para a adequação à LGPD.

4.1.2.3 Desafios do processo de adequação à LGPD

As figuras 22 a 26 apresentam os resultados do levantamento dos desafios identificados pelos respondentes da *survey*.

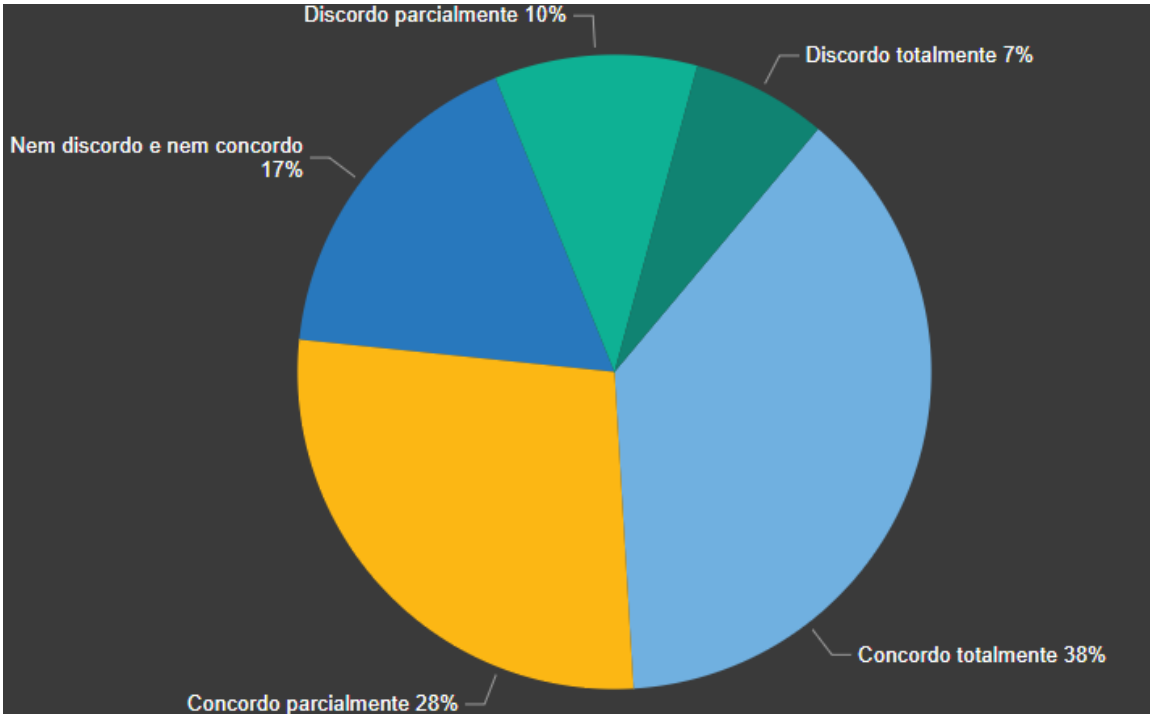
Figura 22 - Sua empresa tem recursos financeiros suficientes para adequação à LGPD?



Fonte: Resultado da pesquisa

No geral não há um entendimento de que as empresas tenham encontrado dificuldade de recursos financeiros para adequar-se à lei.

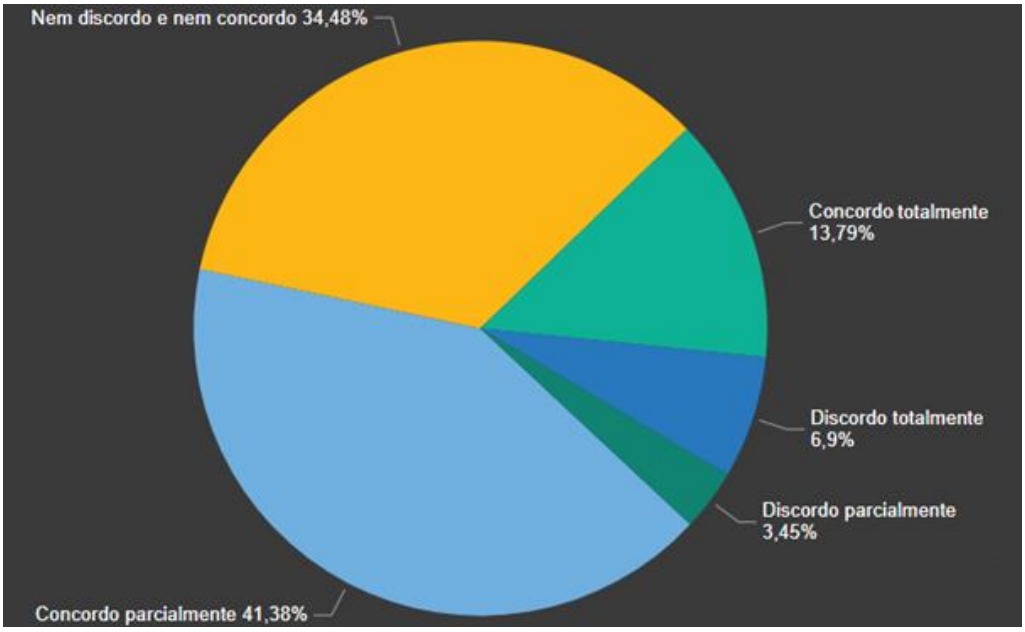
Figura 23 - A empresa teve facilidade de identificar ferramentas e métodos que apoiassem a implementação da LGPD?



Fonte: Resultado da pesquisa

No geral as empresas tiveram facilidade em identificar ferramentas e métodos que apoiassem a implementação da LGPD, com 38% dos respondentes concordando totalmente, e 28% concordando parcialmente.

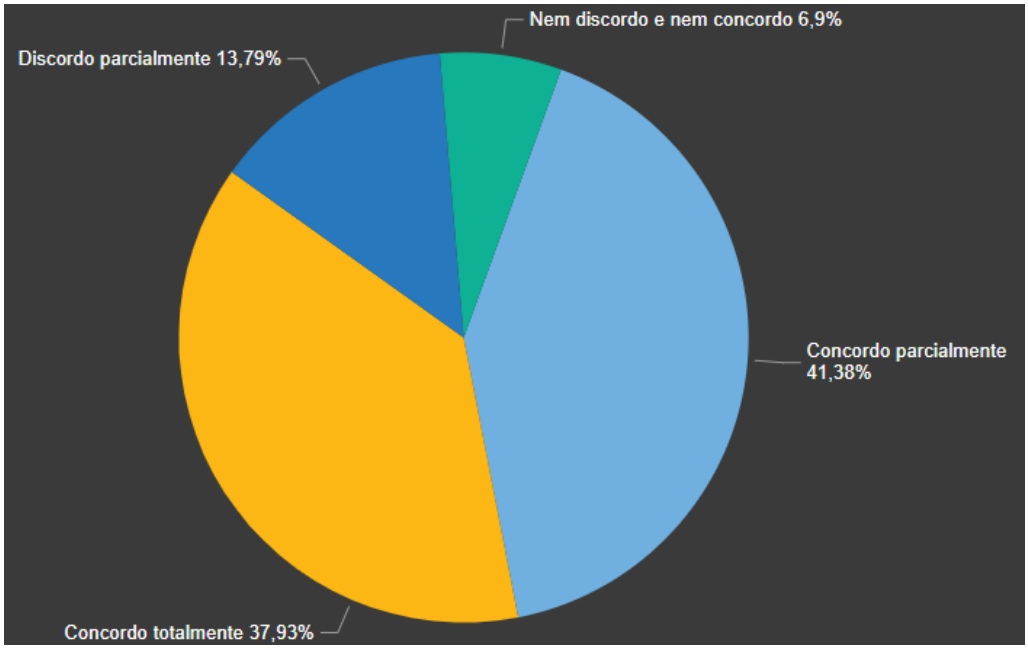
Figura 24 - A empresa teve dificuldade de contratar profissionais para a adequação à LGPD?



Fonte: Resultado da pesquisa

No geral há um entendimento de que as empresas tenham encontrado alguma dificuldade para contratar profissionais (41%).

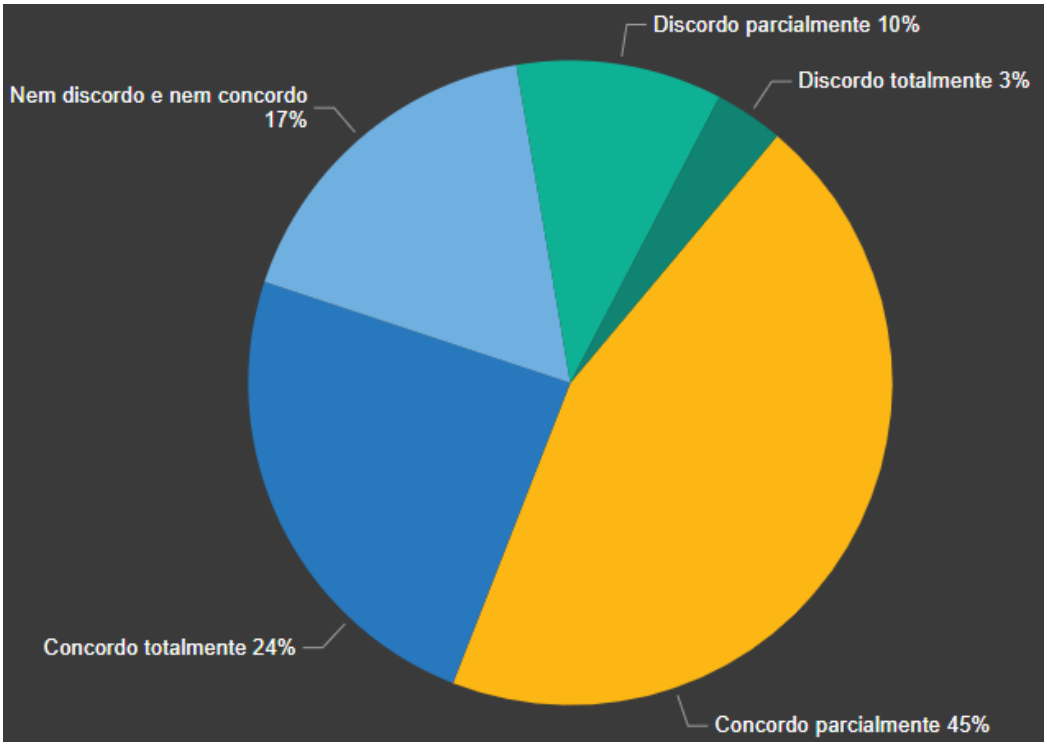
Figura 25 - Sua empresa tem conhecimento suficiente para adequação à LGPD?



Fonte: Resultado da pesquisa

Há um equilíbrio entre os que concordam totalmente e parcialmente que suas organizações têm conhecimento suficiente para adequação à LGPD, com ligeira vantagem para a concordância parcial, que tem 41% contra 38% dos que concordam totalmente.

Figura 26 - As equipes de TI e segurança da informação da sua empresa estão suficientemente capacitadas para implementar a LGPD?



Fonte: Resultado da pesquisa

Há uma predominância dos que concordam parcialmente que suas equipes de TI e Segurança da Informação estão capacitadas correspondendo a 45% do total, enquanto aqueles que concordam totalmente perfazem 24% do total.

Em suma, a avaliação geral das dificuldades enfrentadas apontou a contratação de profissionais como o maior desafio identificado, com 55% dos participantes concordando em algum nível que suas organizações tiveram dificuldade de contratar profissionais.

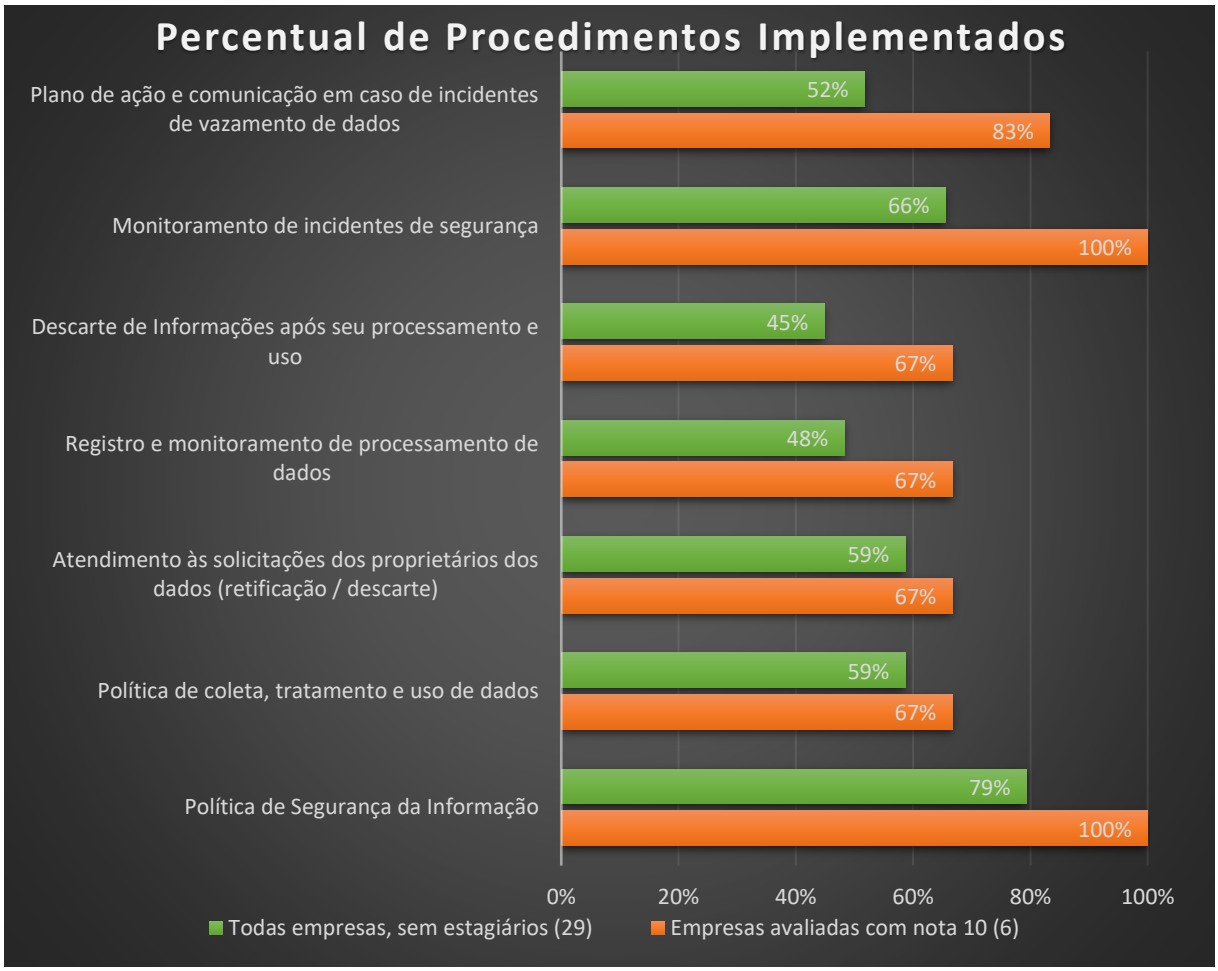
No geral, a análise das respostas às questões deste bloco contradiz as constatações apontadas em estudos anteriores relativos à LGPD e GDPR que apontavam a falta de recursos, falta de ferramentas e de conhecimento do tema por profissionais de TI e de Segurança da Informação como sendo alguns dos principais desafios enfrentados pelas organizações.

4.1.2.4 Medidas implementadas pelas empresas participantes

Na análise das medidas adotadas pelas organizações para adequação à LGPD foi feita uma análise adicional relativa às empresas que foram avaliadas pelos entrevistados com nota 10 no nível de adequação à LGPD, com o propósito de identificar se as empresas que, na avaliação de seus colaboradores, atendem aos requisitos da LGPD, implementaram as medidas e procedimentos que são requeridos pela lei.

A figura 27 lista as políticas e procedimentos implementados para atender à LGPD.

Figura 27 - Sua empresa tem políticas e procedimentos relativos à quais aspectos da LGPD?



Fonte: Resultado da pesquisa

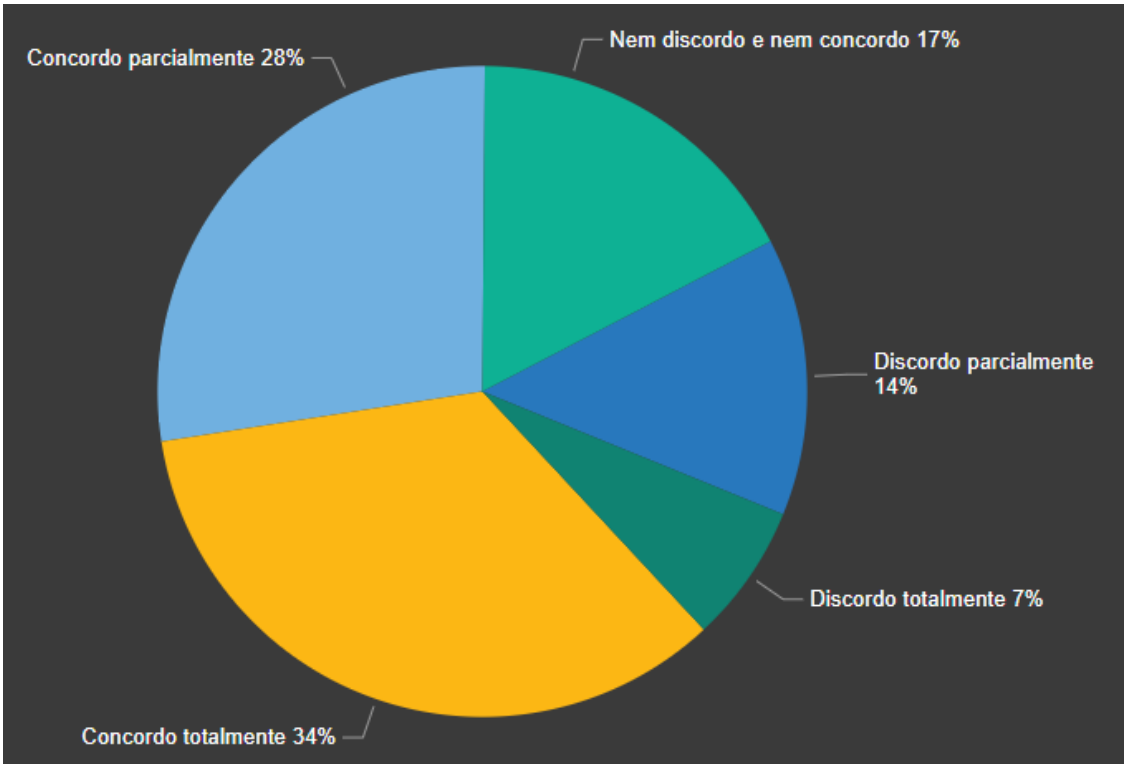
No geral, nenhuma das políticas foi implementada na totalidade das organizações pesquisada. Até mesmo nas empresas avaliadas como nota 10, somente 2 instrumentos foram implementados em todas as 6 empresas: A política de

segurança da informação e procedimentos de monitoramento de incidentes.

É importante ressaltar que estes mecanismos são apontados na lei como sendo instrumentos requeridos por empresas que realizam tratamento de dados pessoais de clientes, usuários e/ou colaboradores.

A figura 28 apresenta a avaliação dos participantes quanto às políticas e procedimentos implementados por suas organizações serem adequadas e suficientes para assegurar o atendimento aos requisitos da LGPD.

Figura 28 - As políticas e procedimentos de sua organização são adequadas e suficientes para assegurar o atendimento aos requisitos da LGPD?



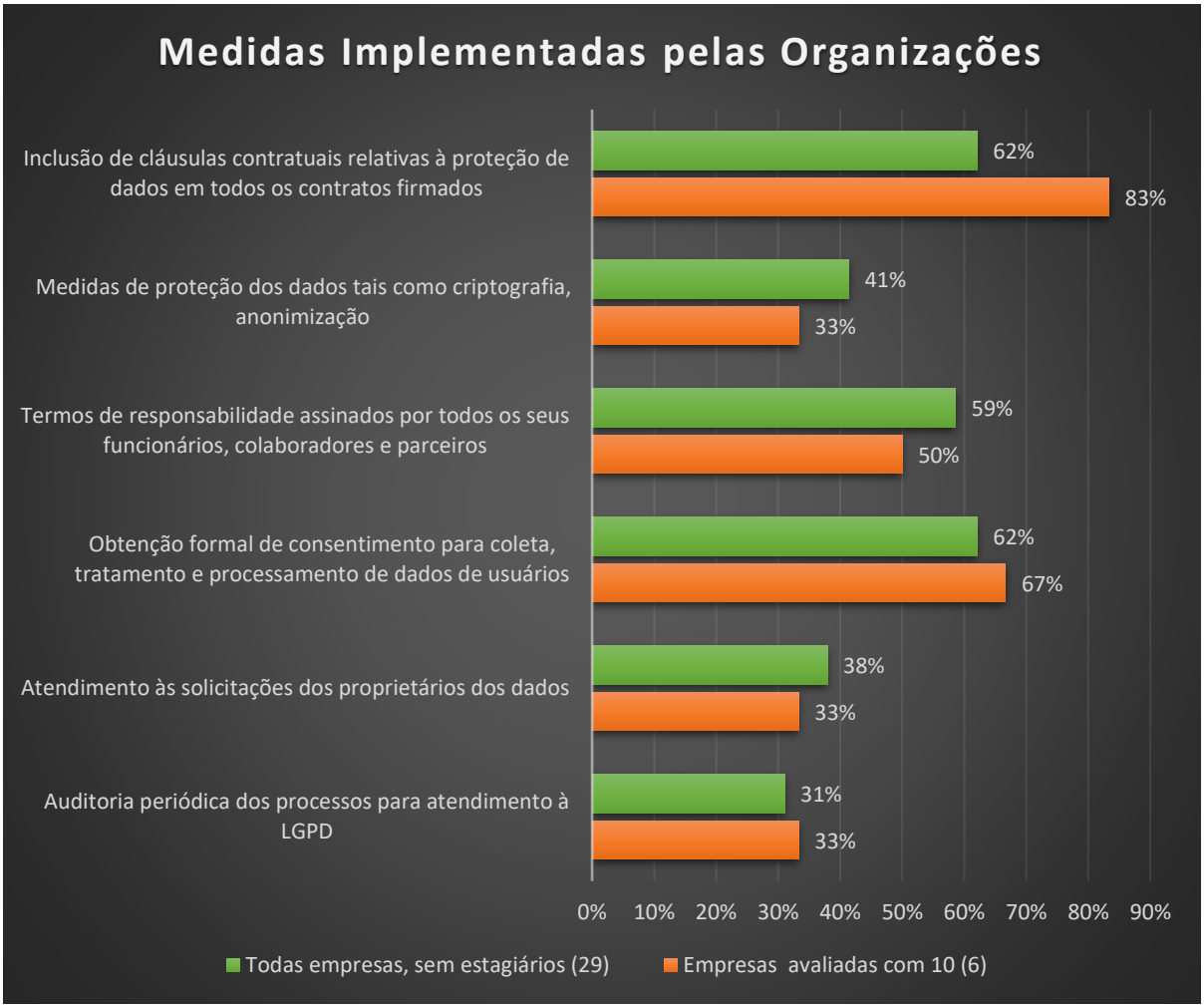
Fonte: Resultado da pesquisa

Na avaliação geral não há um consenso sobre as políticas e procedimentos implementados serem suficientes. Já nas empresas avaliadas como nota 10 a totalidade dos respondentes concordam totalmente que suas empresas implementaram políticas e procedimentos adequadas e suficientes para atender aos requisitos da lei, o que se contrapõe aos resultados apresentados na figura 19, onde não houve, mesmo nestas empresas, implementação da totalidade das políticas e procedimentos requeridos pela lei.

A figura 29 é relativa à quais medidas foram implementadas pelas organizações

para atendimento à LGPD.

Figura 29 – Medidas implementadas pelas organizações para adequação à LGPD



Fonte: Resultado da pesquisa

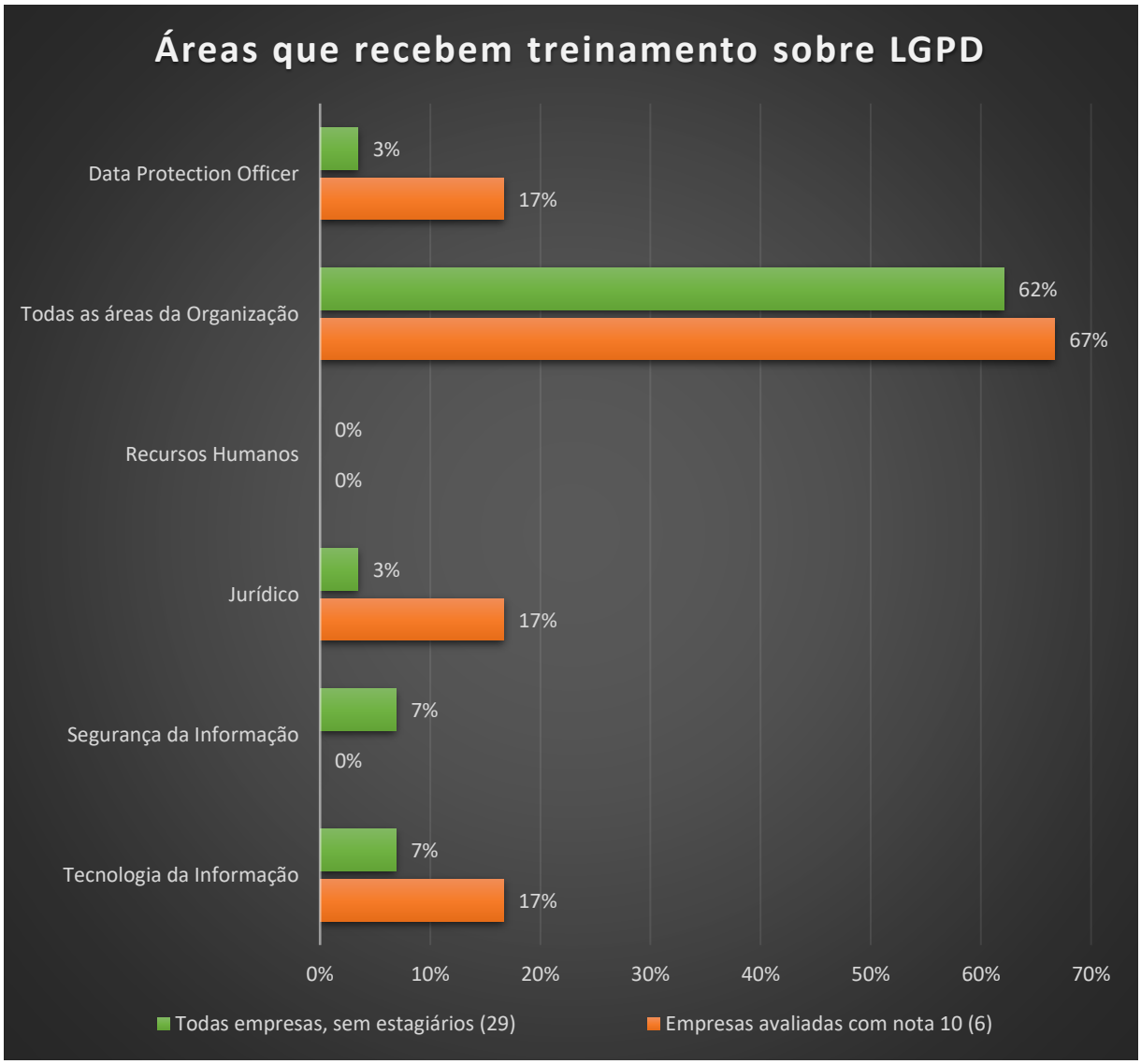
Nas medidas apontadas, ao menos a “Obtenção formal de consentimento”, o “Termo de responsabilidade” e o “Atendimento às solicitações dos proprietários dos dados” são medidas exigidas pela lei, e mesmo estas medidas não foram implementadas por todas as empresas em nenhum dos recortes apresentados, quer seja na avaliação geral ou mesmo nas empresas avaliadas como nota 10.

De fato, 3 das 6 medidas foram implementadas por menos de 50% dos respondentes em qualquer um dos recortes realizados (geral ou empresas nota 10).

Salvo na situação em que as empresas não realizem tratamento de informações, a grande maioria, senão a totalidade destas medidas deveriam, em princípio, ser implementadas por toda e qualquer empresa para que ela esteja em conformidade com a lei.

A figura 30 apresenta quais grupos recebem treinamento periódico para conscientização sobre a LGPD.

Figura 30 – Áreas que recebem treinamento sobre a LGPD nas empresas pesquisadas



Fonte: Resultado da pesquisa

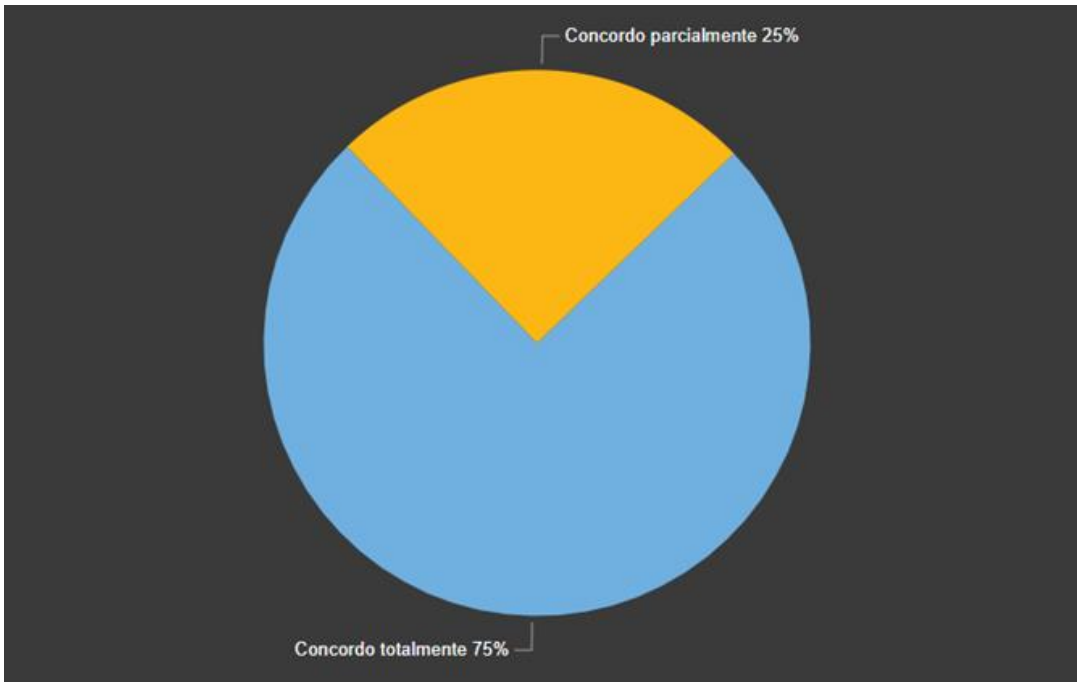
Na avaliação destes resultados destaca-se um índice significativo de empresas que aplicam treinamento para todas as áreas da organização, com 62% das empresas no geral e 67% nas empresas avaliadas com nota 10.

Embora cada empresa tenha modelos de negócio e de processamento de dados de clientes diferentes, medidas como obtenção formal de consentimento para tratamento de dados dos usuários e atendimento às solicitações dos proprietários dos dados são requisitos essenciais da LGPD, que, em princípio, deveriam ser

implementadas por todas as empresas, principalmente para que sejam consideradas totalmente aderentes à lei.

A figura 31 apresenta o resultado da opinião dos participantes sobre os dados coletados por suas organizações serem os estritamente necessários para cumprir os objetivos para os quais foram coletados.

Figura 31 - Os dados coletados por sua organização são os estritamente necessários para cumprir os objetivos para os quais foram coletados?



Fonte: Resultado da pesquisa

Na avaliação geral há uma grande predominância da opinião de que os dados coletados são aqueles estritamente necessários, sendo que nas empresas avaliadas como nota 10 o índice é de 100% de participantes que concordam.

4.1.2.5 Considerações finais sobre resultados da *survey*

Em linhas gerais, a análise dos resultados da *survey* indicam um número considerável de empresas com algum nível de adequação à LGPD, no entanto, trata-se de uma lei obrigatória para praticamente toda organização, independentemente de seu porte e área de atuação.

Sendo assim, a existência de empresas que ainda não estejam em conformidade com a lei é um fato preocupante, não apenas para as próprias

organizações, bem como para seus clientes e colaboradores, que não tem garantia de que seus direitos com relação à privacidade de seus dados pessoais estejam sendo respeitados.

Recentemente a Autoridade Nacional de Proteção de Dados aplicou as primeiras sanções relacionadas à falta de adequação de empresas à LGPD. O Despacho que detalha o teor das sanções aplicadas menciona a infração ao artigo 7º da LGPD, que estabelece os requisitos para o tratamento de dados pessoais, bem como ao artigo 41 da LGPD, que estabelece que o controlador deverá indicar o encarregado pelo tratamento de dados pessoais.

A análise do resultado da *survey* quanto ao levantamento das medidas, políticas e procedimentos necessários para a adequação aos requisitos da LGPD realizado por meio das questões Q13 a Q16 aponta que nem todas as organizações implementaram a totalidade das ações necessárias para adequação à legislação, estando, portanto, sujeitas à aplicação de sanções por parte da ANPD.

Avaliando-se a opinião dos participantes quanto às políticas e procedimentos implementados, a grande maioria concorda totalmente ou parcialmente que suas organizações têm políticas e procedimentos suficientes.

No entanto, constata-se que mecanismos e procedimentos importantes não foram apontados por muitos respondentes da *survey* como tendo sido implementados em suas organizações e nenhuma das políticas e procedimentos foi implementada na totalidade das organizações, mesmo naquelas avaliadas com nota 10 pelos respondentes.

Os participantes apontaram como principal desafio a dificuldade de contratação de profissionais qualificados. Fatores como a falta de recursos financeiros, de ferramentas e métodos e de preparação de suas áreas de Tecnologia e de Segurança da Informação, que foram apontados em estudos anteriores como desafios do processo de adequação à LGPD não foram confirmados pelas respostas obtidas na *survey.*

Apesar de 65% das avaliações do nível de adequação terem sido entre 7 e 10, as medidas, políticas e procedimentos implementados pelas organizações não são coerentes com esta avaliação, uma vez que, mesmo em empresas com nota 10 medidas importantes, senão obrigatórias, não foram implementadas.

Os resultados da *survey* permitiram identificar diversos aspectos relativos à percepção dos participantes quanto ao nível de adequação de suas empresas à

LGPD, bem como sobre os mecanismos implementados no processo de adequação.

Estas informações são importantes para a o desenvolvimento do *roadmap,* de suas etapas e dos entregáveis que devem ser resultado das mesmas.

4.2 Resultado da etapa de definição dos resultados esperados

A análise da lei e de seus artigos foi o principal norteador para a definição dos resultados esperados, juntamente com a revisão sistemática da bibliografia e da pesquisa *survey*.

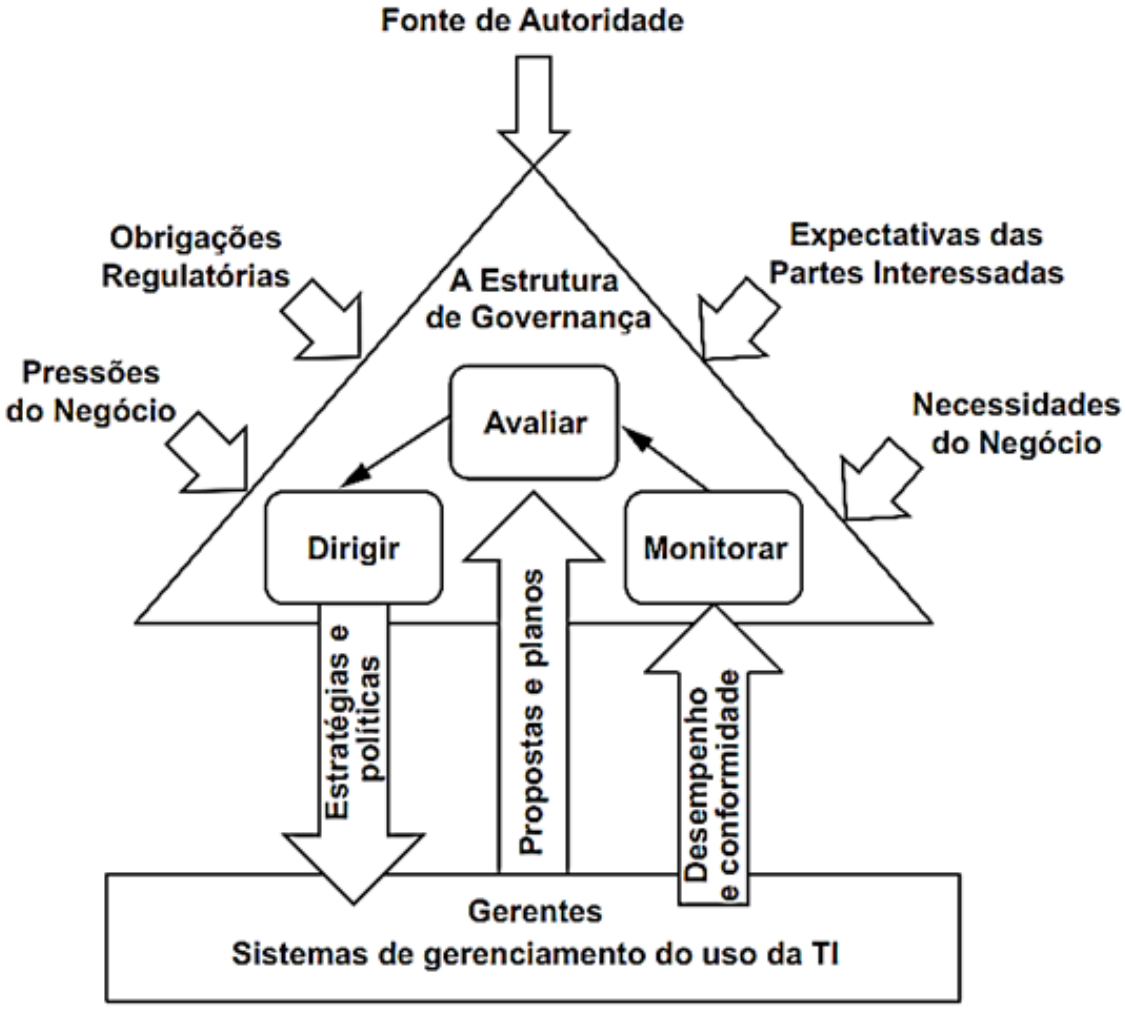
Adicionalmente, foram utilizadas as normas NBR ISO/IEC por serem de ampla divulgação e reconhecimento, além dos *frameworks NIST Cibersecurity Framework* e *NIST Privacy Framework,* por serem abrangentes e abordarem o tema diretamente.

Estes elementos foram a base para a definição das etapas do *roadmap,* que foram ordenadas seguindo um encadeamento lógico e baseado nas dependências e condicionais para realização de cada etapa. Por exemplo, não faz sentido a definição de políticas e procedimentos para adequação à LGPD sem que tenha sido nomeado o responsável pela coordenação de todo o processo, no caso o encarregado de proteção de dados (DPO) e sem que tenham sido mapeados os dados pessoais, bem como a realização de uma análise dos riscos.

Além disso, foram considerados no processo dos resultados esperados quais os elementos que servirão de apoio às organizações para a execução das etapas.

A norma NBR ISO/IEC 38500 propõe um modelo de Governança Corporativa de TIC, que serve como referência para a elaboração dos aspectos de gestão do processo de adequação da TIC à LGPD dentro do *roadmap* (Associação Brasileira de Normas Técnicas, 2009, p. 7), conforme apresentado na figura 32:

Figura 32 - Modelo de Governança Corporativa de TIC



Fonte: Adaptado de Associação Brasileira de Normas e Técnicas. NBR ISO/IEC 38500 2ª. e, (2018).

Segundo a norma NBR ISO/IEC 27002, a segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais, e funções de *software* e *hardware*. Reforça ainda que estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e atendidos e que a identificação de controles a serem implantados requer um planejamento cuidadoso e atenção aos detalhes (Associação Brasileira De Normas Técnicas, 2022, p. 10).

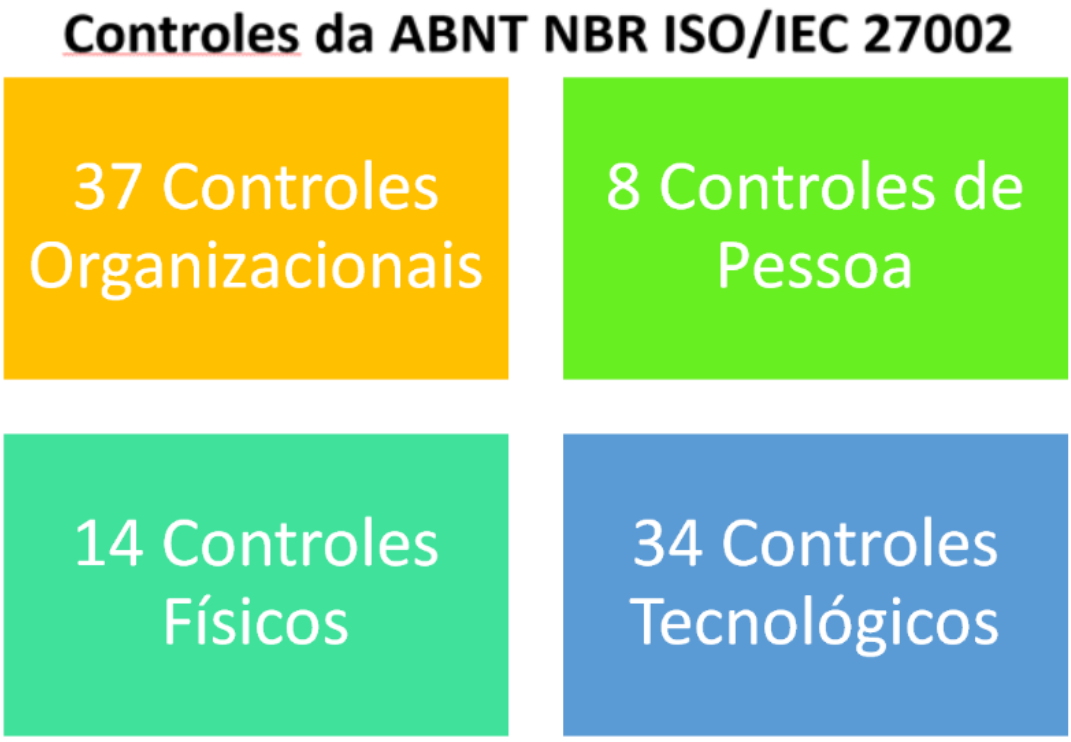
A NBR ISO/IEC 27002 recomenda que requisitos de segurança da informação sejam definidos a partir de 3 fontes:

1. avaliação de riscos, considerando estratégia e objetivos da organização;

2. requisitos legais, estatutários, regulamentares e contratuais que a organização e partes interessadas (parceiros, prestadores de serviços etc.) têm que cumprir;
3. princípios, objetivos e requisitos de negócios das etapas do ciclo de vida da informação que a organização desenvolve para apoiar suas operações.

A norma inclui 93 controles, divididos em 4 seções, conforme a figura 33:

Figura 33 - Controles da ABNT NBR ISO/IEC 27002



Fonte: Adaptado da Norma ISO/IEC 27002

Cada controle é composto por título, atributos, descrição, propósito, orientação e outras informações que apoiam as organizações na identificação dos controles e suas aplicações (Associação Brasileira de Normas Técnicas, 2022, p. 10).

A norma NBR ISO/IEC 27002 inclui aspectos da gestão da TIC que são relevantes para a segurança da informação e, consequentemente, para a adequação de organizações aos aspectos de proteção de dados privados requeridos para adequação à LGPD, e, portanto, a norma foi empregada como a principal referência de apoio às organizações para implementação das etapas do *roadmap,* por ser uma norma de ampla aceitação, de fácil acesso, enquanto outras normas, embora tão

importantes ou relevantes quanto a ISO, não são de amplo conhecimento, sendo mais conhecidas apenas na comunidade técnica de segurança da informação.

O apêndice D contém a lista dos itens da NBR ISO/IEC 27002 que serviram de base para a elaboração do *roadmap*.

Outras normas ISO/IEC foram utilizadas como referência de consulta para os usuários do *roadmap*, juntamente com dois *frameworks* de segurança do NIST, conforme o quadro 15:

Quadro 15 – Outras normas referenciadas no *roadmap*

Norma ISO/IEC	Aplicação
ISO/IEC 27001	Segurança da informação, cibersegurança e proteção da privacidade - Sistemas de gestão de segurança da informação
ISO/IEC 27004	Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Monitoramento, medição, análise e avaliação
ISO/IEC 27005	Segurança da informação, cibersegurança e proteção da privacidade - Orientação sobre gerenciamento de riscos de segurança da informação
ISO/IEC 27017	Código de prática para controles de segurança da informação
ISO/IEC 27018	Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas atuando como processadores de PII
ISO/IEC 27032	Cibersegurança - Diretrizes para segurança na Internet
ISO/IEC 27033	Tecnologia da Informação - Técnicas de segurança - Segurança de rede
ISO/IEC 27034	Tecnologia da Informação - Segurança de aplicativos
ISO/IEC 27036	Cibersegurança – Relacionamentos com fornecedores
ISO/IEC 27701	Técnicas de segurança - Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gerenciamento de informações de privacidade
NIST Privacy *Framework*	*Framework* com foco em privacidade
NIST Cibersecurity *Framework*	*Framework* voltado para a segurança digital e para as organizações do setor privado

Fonte: Resultado da pesquisa

Estes elementos foram base para o desenvolvimento do *roadmap,* sendo acrescidos ao longo as diversas interações ou *sprints* realizados ao longo da etapa de desenvolvimento e que culminaram na elaboração de diferentes versões do *roadmap,* as quais inicialmente foram validadas e criticadas pelo orientador e, antes de sua demonstração e validação por profissionais, a serem relatadas nas etapas seguintes.

4.3 Resultado da etapa de desenho e desenvolvimento

Para o desenho do *roadmap* foram considerados os aspectos relativos à LGPD em termos de requisitos para o cumprimento da lei, bem como elementos identificados durante a revisão bibliográfica e pesquisa *survey* como sendo pontos de atenção que devem ser considerados pelas organizações em sua adequação à lei. A etapa de demonstração também forneceu elementos que influenciaram no desenho do RAEL, assim como a própria etapa de avaliação, na qual ocorreram sugestões dos avaliadores que foram incorporadas ao *roadmap* quando pertinentes.

Ao final deste processo de compilação das etapas, o *roadmap* foi dividido em 3 fases, nas quais as etapas foram agrupadas por similaridade:

1. **Preparação**: Consiste das etapas necessárias para preparação do ambiente da organização para o processo de implementação da LGPD.
2. **Implementação:** Para esta fase foram consideradas todas as etapas essenciais para adequação das empresas à LGPD.
3. **Manutenção:** Nesta fase são consideradas as etapas necessárias para garantir que a adequação das empresas à lei seja mantida ao longo do tempo, contemplando as mudanças que venham a ocorrer no cenário de negócios e que demandem ajustes nos processos implementados para que a empresa continue cumprindo a lei.

O **RAEL** consiste em 20 etapas, as quais foram divididas em 3 grandes fases por similaridade: Preparação, Implementação e Manutenção.

O quadro 16 apresenta as fases do RAEL com suas respectivas etapas do RAEL e qual a base utilizada para a inclusão desta etapa.

Quadro 16 – Etapas do RAEL com justificativa para a sua inclusão no *roadmap*

Fase	# Etapa	Etapa	Origem / Justificativa da Etapa
Preparação	1	Avaliar necessidade de adequação à LGPD	Artigos 3 a 7 da LGPD
Preparação	2	Constituir um comitê Interno para Acompanhamento da LGPD	Sugestão gerada na etapa de demonstração do RAEL - A função de coordenação pode ser realizada por um agente externo, sendo necessário identificar as pessoas internas na organização que farão o acompanhamento do processo e serão acionadas quando necessário.
Preparação	3	Nomear o encarregado de Proteção de Dados (DPO)	Artigo 41 da LGPD
Preparação	4	Mapear / Identificar os dados pessoais / sensíveis tratados pela empresa e seu fluxo dentro da organização desde a coleta até o descarte	Artigo 38 da LGPD
Preparação	5	Analisar a base legal para o tratamento de dados	Artigos 4, 6 e 7 da LGPD
Preparação	6	Análise de riscos	Artigo 50 da LGPD
Preparação	7	Elaborar cronograma geral do projeto	Sugestão gerada na etapa de avaliação do RAEL, a fim de assegurar que as organizações estabeleçam um cronograma que permita o atingimento dos objetivos em tempo hábil de acordo com sua situação geral
Implementação	8	Elaborar ou revisar as Políticas e procedimentos de Segurança da Informação, Proteção, Privacidade e Tratamento de Dados	Artigo 50 § 1º da LGPD Q13, Q14 e Q16 da *survey*

Implementação	9	Revisar contratos com parceiros, fornecedores e demais envolvidos	Artigo 39 da LGPD e outros
Implementação	10	Obter o consentimento dos titulares dos dados	Artigo 7 da LGPD
Implementação	11	Preparação dos profissionais envolvidos	Q10, Q11, Q12 e Q15 da *survey*
Implementação	12	Implementar medidas técnicas para garantir a segurança dos dados	Artigos 46 e 47 da LGPD
Implementação	13	Avaliar e implementar medidas para transferência internacional	Artigo 33 da LGPD
Implementação	14	Estabelecer um processo de gerenciamento e resposta a incidentes de segurança	Artigo 48 da LGPD
Implementação	15	Implementar medidas para eliminação dos dados ao término do tratamento	Artigo 16 da LGPD
Manutenção	16	Manter registros das atividades de tratamento de dados	Artigo 37 da LGPD
Manutenção	17	Atendimento aos direitos dos titulares	Artigo 9 da LGPD
Manutenção	18	Treinamento, Conscientização e Capacitação - demais profissionais da organização	Q10, Q11, Q12 e Q15 da *survey*
Manutenção	19	Implementar um processo de monitoramento que assegure a revisão e atualização periódica dos processos, políticas e procedimentos relacionados à LGPD	Artigo 50 - Item I - letra h.
Manutenção	20	Realizar auditorias regulares	Artigo 50 - item II

Fonte: Resultado da pesquisa

Cada etapa contém as seguintes informações: título, objetivo, referência à ISO 27002, entradas, saídas/entregas, etapa antecessora requerida, etapas das quais depende, áreas / funções envolvidas, artigo LGPD base para a execução da atividade.

O quadro 17 apresenta as informações de cada etapa e seu propósito.

Quadro 17 – Informações de cada etapa do RAEL

INFORMAÇÃO	PROPÓSITO
ETAPA (TÍTULO)	Identificar a etapa
OBJETIVO	Descrever o propósito para o qual a etapa deve ser desenvolvida
REFERÊNCIA À ISO 27002	Listar os itens da ISO 27002 que provêm orientação e subsídio inicial para desenvolvimento dos objetivos da etapa.
ENTRADAS	Documentos, políticas, procedimentos, leis, normas e padrões técnicos que possam subsidiar o desenvolvimento da etapa.
SAÍDAS / ENTREGAS	Possíveis documentos, políticas, procedimentos, padrões, produtos, processos elaborados como resultado da execução da etapa.
ETAPA ANTECESSORA (REQUERIDA)	A etapa imediatamente anterior (se houver) que é requisito para que esta etapa possa ser desenvolvida (pré-requisito imediato da etapa).
ÁREAS / FUNÇÕES ENVOLVIDAS	Listagem de todas as áreas / departamentos ou funções que devem ser envolvidas em algum nível no desenvolvimento da etapa.
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	Listagem dos artigos da LGPD que subsidiam a necessidade de cumprimento / implementação daquela etapa, embora nem todas as empresas tenham que cumprir todas as etapas por conta das diferenças de porte, setor de atuação e características de cada negócio.

Fonte: Resultado da pesquisa

A dimensão Tempo / Duração das etapas não foi incluída tendo em vista que o RAEL tem como foco a adequação de empresas independentemente de seu porte, e sendo assim, cada organização possui uma complexidade de processos, necessidades e recursos financeiros e humanos diferente, podendo levar a abordagens de cronograma diferentes. Para suprir esta questão foi incluída uma etapa específica (etapa 7) no RAEL na fase de preparação visando a elaboração do cronograma do projeto, onde cada empresa deverá definir sua abordagem para este aspecto de forma particular.

As etapas foram enumeradas de 1 a 20, para facilitar sua referenciação em outras etapas, evitando o uso do nome completo da fase a cada referência à mesma.

O apêndice E apresenta uma visão geral das etapas do RAEL.

A figura 34 apresenta uma versão gráfica do RAEL com uma visão geral do *roadmap,* suas fases e etapas, com objetivo de proporcionar uma visão intuitiva do processo a ser percorrido para adequação à LGPD.

Figura 34 - Visão geral do RAEL

Fonte: Resultado da pesquisa

O apêndice F apresenta um quadro com o texto de cada uma das etapas do RAEL em detalhe, a fim de facilitar a leitura de seu conteúdo.

A fim de facilitar a visualização e entendimento do RAEL, os apêndices G a H apresentam recortes das etapas do RAEL. O apêndice G apresenta a fase 1 do RAEL – Preparação, o apêndice H apresenta a fase 2 – Implementação e o apêndice I a fase 3 – Manutenção.

O apêndice J apresenta a visão geral gráfica e detalhada do RAEL, com cada uma de suas etapas.

4.4 Resultado da etapa de demonstração

Como resultado da etapa de demonstração, o representante da empresa XYZ teceu diversos comentários ao RAEL com críticas, sugestões e melhorias, as quais foram incluídas diretamente no *design* do RAEL. Além disso, foi realizada uma entrevista *on-line* com o responsável, a fim de permitir a revisão dos comentários elaborados, esclarecendo dúvidas e obtendo impressões que contribuíram para aprimoração do modelo do *roadmap*.

O apêndice K contém os comentários realizados pelo responsável da empresa XYZ, apontando qual a etapa do RAEL objeto do comentário / crítica / sugestão, a origem do comentário, se inserido como observação na planilha durante o andamento da demonstração ou coletado durante a entrevista, a réplica do pesquisador quanto ao comentário e a ação resultante, quando houver, está indicada na coluna **AÇÃO** do quadro apresentado no apêndice K.

4.5 Resultado da etapa de avaliação

Após a conclusão das respostas ao formulário de avaliação já mencionado no item 3.5 e apresentado no apêndice M, as respostas foram coletadas e exportadas para uma planilha Microsoft Excel, para compilação e análise.

O quadro 18 apresenta as respostas do bloco 1, com as questões de 1 a 3, referentes ao perfil dos avaliadores:

Quadro 18 – Questões sobre o perfil dos avaliadores do RAEL

QUESTÃO	AVALIADOR 1	AVALIADOR 2	AVALIADOR 3	AVALIADOR 4
Q1 - Qual seu tempo de experiência profissional?	Mais de 10 anos	Mais de 10 anos	Mais de 10 anos	Mais de 10 anos
Q2 - Qual seu departamento dentro de sua organização?	Segurança da Informação	Segurança da Informação	Auditoria de Sistemas	Segurança da Informação
Q3 - Qual seu nível hierárquico dentro de sua organização?	Coordenador	Gerente	Pleno ou Sênior	Gerente

Fonte: Resultado da pesquisa

O quadro 19 detalha os resultados das questões do bloco 2, referentes à avaliação do RAEL:

Quadro 19 – Questões referentes à avaliação do RAEL

QUESTÃO	AVALIADOR 1	AVALIADOR 2	AVALIADOR 3	AVALIADOR 4
Q4 - As etapas do *roadmap* são relevantes para a adequação de empresas à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q5 - Caso deseje, insira seus comentários sobre a resposta ao item 4 do questionário:	-	-	-	Todas as etapas são relevantes e necessárias para a aplicação dessa jornada por qualquer empresa, muito bem embasadas pelas referências, responsabilidades e explicações documentadas.
Q6 - As etapas do *roadmap* são suficientes para a adequação de empresas à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q7 - Caso deseje, insira seus comentários sobre a resposta ao item 6 do questionário:	-	-	-	Entendo que o *roadmap* está muito bem documentado e cobre a jornada completa para uma empresa iniciar e concluir sua conformidade à LGPD, assim como também

				manter um ciclo de melhoria contínua.
Q8 - As etapas do *roadmap* estão em uma ordem adequada para o desenvolvimento do processo de adequação à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q9 - Caso deseje, insira seus comentários sobre a resposta ao item 8 do questionário:	-	-	-	-
Q10 - As informações que constam de cada etapa do *roadmap* são suficientes para prover orientação para a adequação à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q11 - Caso deseje, insira seus comentários sobre a resposta ao item 10 do questionário:	-	-	-	-
Q12 - O *roadmap* é relevante para a identificação de processos a serem implementados para a adequação de empresas à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q13 - Caso deseje, insira seus comentários sobre a resposta ao item 12 do questionário:	-	-	-	-
Q14 - O *roadmap* auxilia na identificação de processos, políticas e procedimentos relevantes para a adequação de empresas à LGPD?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q15 - Caso deseje, insira seus comentários sobre a resposta ao item 14 do questionário:	-	-	-	-
Q16 - O *roadmap* tem aplicabilidade para empresas de setores que não o de tecnologia da informação?	Concordo totalmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q17 - Caso deseje, insira seus comentários sobre a resposta ao item 16 do questionário:	-	-	-	A estrutura do *roadmap* é completa e acessível para

				que seja totalmente aplicável a qualquer empresa, independente do seu ramo de atividade.
Q18 - O *roadmap* tem aplicabilidade para empresas de qualquer porte?	Concordo parcialmente	Concordo totalmente	Concordo totalmente	Concordo totalmente
Q19 - Caso deseje, insira seus comentários sobre a resposta ao item 18 do questionário:	De qualquer porte e que se enquadrem na LGPD (quase todas!)			As orientações mencionadas na fase de Preparação foram pertinentes para que mesmo empresas de pequeno porte possam nomear os seus responsáveis e aplicarem o *roadmap* para adequação à LGPD.
Q20 - Você tem alguma sugestão de melhoria ou modificação ao *roadmap*?		Com certeza o *roadmap* dá um direcionamento embasado nos normativas de ISO, mas ampliar o tema de medidas técnicas dando uma visão mais ampla de defesa cibernética abordando o NIST por exemplo e segurança em camadas para proteger a informação e garantir a privacidade, seria formidável.		

Fonte: Resultado da pesquisa

Uma sugestão valiosa surgiu durante a etapa de avaliação: a inclusão de uma etapa de elaboração de cronograma de projeto. Esta sugestão foi prontamente integrada ao *design* do *roadmap*, com o objetivo de garantir a criação de um

cronograma alinhado com as necessidades e peculiaridades de cada organização, incluindo complexidade, orçamento, recursos humanos e tecnológicos, entre outros aspectos relevantes.

Com base nas respostas apresentadas observa-se um consenso dos avaliadores na quase totalidade das questões, com concordância total em relação à relevância do RAEL, a suficiência das etapas para a adequação de empresas à LGPD e a ordem na qual as etapas são apresentadas no *roadmap*, segundo os avaliadores, são adequadas.

Os avaliadores também concordam totalmente que as informações de cada etapa são suficientes para prover orientação para o processo de adequação à LGPD e que o *roadmap* é relevante para a identificação de processos a serem implementados, bem como auxilia na identificação de processos, políticas e procedimentos relevantes para a adequação de empresas à LGPD. Além disso, afirmam que o *roadmap* tem aplicabilidade para empresas de setores que não o de tecnologia da informação e comunicação, setor ao qual pertence a XYZ, empresa na qual o *roadmap* foi demonstrado.

A única questão que apresentou diferença de opinião foi quanto à aplicabilidade do *roadmap* para empresas de qualquer porte. Os avaliadores 2 e 3 concordam totalmente quanto à aplicabilidade em empresas de qualquer porte, e o avaliador 1 concordou parcialmente. Nos comentários sobre a respostas a esta questão o avaliador 1 comenta: “De qualquer porte e que se enquadrem na LGPD (quase todas!)”, ou seja, a observação do avaliador 1 não contesta a aplicabilidade a empresas de qualquer porte, mas apenas observa que nem todas as empresas têm obrigação de enquadramento, e, portanto, o *roadmap* aplica-se a empresas de qualquer porte que se enquadrem na LGPD, que, na opinião do avaliador 1, são quase todas as empresas.

O avaliador 2 teceu um comentário final em que menciona que a ampliação do tema de medidas técnicas dando uma visão mais ampla de defesa cibernética abordando o *NIST* e segurança em camadas para proteger a informação e garantir a privacidade, seria formidável.

Com relação ao comentário, o *NIST Cibersecurity Framework* foi empregado como uma das referências no *roadmap,* estando em linha com a sugestão. A sugestão da aplicação de segurança em camadas para proteger a informação e garantir a privacidade não foi incluída no *roadmap* por direcionar a tomada de decisão para uma

abordagem técnica, a qual pode ser apropriada para algumas empresas, mas não ser aplicável em outras, dependendo de diversos fatores para sua adoção e por entrar em critérios técnicos que são muito específicos do ambiente computacional e de segurança da informação de cada organização, além de entrar no mérito do “como” fazer, enquanto o objetivo do *roadmap* é focar no “o quê” fazer.

Por meio das respostas obtidas é possível avaliar que o objetivo geral desta pesquisa foi atingido, com o desenvolvimento de um *roadmap* para adequação de empresas à LGPD, que sirva como guia de apoio às organizações brasileiras no processo de adequação à LGPD.

4.6 Resultado da etapa de comunicação

A etapa de comunicação deste trabalho consiste, em primeiro lugar, na própria elaboração desta dissertação, e sua apresentação à banca avaliadora. Além disso, as etapas intermediárias do desenvolvimento da pesquisa foram comunicadas por meio da apresentação e publicação nos anais do congresso em 3 artigos:

1. **“Uso da inteligência artificial na adequação à GDPR – Um estudo bibliográfico”** – apresentado no XVII SIMPROFI – 2022;
2. **“Métodos de Apoio à Implementação da LGPD – Um Estudo Bibliográfico”** – apresentado no VII SAEPRO – 2023;
3. **“Desafios na implementação da LGPD nas organizações - Resultado de uma *survey”*** – apresentado no XVIII SIMPROFI – 2023.

Um artigo com o resultado da dissertação está em elaboração e será submetido à apreciação de periódicos com *qualis* B2 ou superior visando sua publicação e divulgação do resultado da pesquisa à comunidade acadêmica.

Segundo relato do proprietário da empresa XYZ o RAEL está sendo aplicado como ferramenta de apoio no processo de adequação à LGPD.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do *roadmap* relatado ao longo do presente trabalho teve por objetivo responder à questão de pesquisa: como estruturar um *roadmap* que sirva de apoio a organizações brasileiras no processo de adequação à LGPD?

Para tanto, este trabalho contou com a revisão sistemática da bibliografia, que possibilitou a identificação das ferramentas e métodos para implementação da LGPD e servindo de base para a elaboração da pesquisa *survey*. Esta pesquisa, por sua vez, buscou capturar a percepção de profissionais de empresas brasileiras em relação ao processo de adequação de suas organizações à LGPD.

A revisão sistemática da bibliografia identificou métodos em desenvolvimento ou já implementados, porém, nenhum deles com foco no processo de implementação geral da LGPD, e sim em etapas ou processos específicos, conforme relatado no item 2.1.1.

A pesquisa *survey* trouxe também indicativos de que alguns dos principais desafios para o processo de adequação à LGPD apontados em outros estudos não foram corroborados pelas respostas dos participantes. Dificuldades relacionadas a ferramentas, recursos financeiros e preparo dos profissionais das equipes de tecnologia da informação e de segurança da informação não foram confirmadas pelos participantes da *survey*. A única exceção foi a dificuldade de contratação de profissionais.

Outro achado importante que surgiu dos resultados da pesquisa foi o descasamento entre a percepção dos profissionais quanto ao nível de adequação de suas organizações e as medidas, políticas e procedimentos implementados por elas.

Conforme já relatado no item 2.2.3.4, nenhuma das políticas foi implementada na totalidade das organizações pesquisada, e mesmo nas 6 empresas com nota 10, somente 2 dos 7 instrumentos pesquisados foram implementados em todas as 6: A política de segurança da informação e procedimentos de monitoramento de incidentes.

Com relação às medidas implementadas, a situação é até pior, pois nenhuma das empresas implementou as 6 medidas pesquisadas, e nem mesmo nenhuma empresa nota 10 implementou todas as 6 medidas pesquisadas.

Como estas medidas, políticas e procedimentos estão embasados na LGPD, seria de se esperar que a grande maioria das empresas as implementasse na sua

totalidade, salvo exceções.

Tais achados são indicativos de futuros estudos a serem desenvolvidos para de entender a causa da divergência entre percepções dos pesquisados e os procedimentos e métodos implementados.

O desenvolvimento do RAEL foi realizado com base na DSRM, utilizando como apoio as metodologias de *Design Thinking* e *Scrum*, além das informações obtidas na revisão da bibliografia e da pesquisa *survey*, bem como da família de normas ISO NBR/IEC, do *NIST Cibersecurity Framework* e *NIST Privacy Framework.*

A etapa de demonstração do RAEL possibilitou obter melhorias no *design* e a confirmação de sua aplicabilidade na empresa XYZ.

A etapa de avaliação do RAEL permitiu coletar impressões dos avaliadores, corroborando a expectativa de que o *roadmap* desenvolvido atende ao objetivo geral da pesquisa.

Dentre as questões apresentadas aos avaliadores, foram incluídas questões que abordam a clareza do RAEL, sua facilidade de entendimento, a suficiência das etapas para a adequação de empresas à LGPD e a aplicabilidade do *roadmap* a empresas de todos os portes e segmentos.

É importante salientar que o RAEL se propõe a ser um instrumento de apoio na adequação à LGPD, ou seja, ele não apenas serve para o processo de implementação da LGPD, que é uma etapa inicial, mas também pode ser utilizado por empresas que já tenham implementado, mas que desejam validar seu nível de aderência à lei. Sendo assim, é de ampla aplicação para empresas de todos os portes, setores e nos mais diversos estágios de implementação da LGPD.

Um fator limitante da pesquisa foi a realização da demonstração em uma única empresa, do setor de data center, o que pode motivar novos estudos e avaliações em empresas de diferentes setores.

Do ponto de vista da gestão e da tecnologia em sistemas produtivos, esta pesquisa traz uma contribuição por meio do artefato *roadmap*¸ que poderá ser útil no processo de adequação das organizações brasileiras à LGPD, para a compreensão destas organizações quanto aos requisitos a serem atendidos e para que possam assegurar a proteção dos dados privados de clientes, usuários e outros.

Sob a perspectiva acadêmica, esta pesquisa contribui para a discussão da gestão da segurança de informações e da privacidade de dados e para novas pesquisas envolvendo o contexto da segurança da informação, da privacidade dos

dados e da adequação de empresas à legislação relacionada ao tema.

Este estudo visa preencher uma lacuna entre pesquisa e prática na área de engenharia de produção, ampliando o debate sobre o direito à privacidade e à proteção de dados pessoais nas organizações brasileiras, contribuindo para a conformidade das empresas à legislação de privacidade.

Na conclusão e formalização desta dissertação de mestrado, após a aprovação e formalização do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, o pesquisador submeterá um artigo com o relato do produto desenvolvido ao longo deste trabalho de pesquisa para a comunicação à comunidade acadêmica. Isso permitirá que pesquisadores de áreas correlatas ao tema tenham acesso aos resultados da pesquisa, ao produto *roadmap* desenvolvido e à sua aplicação em empresas no processo de adequação à LGPD, propiciando o desenvolvimento de novas iterações e futuras pesquisas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 38500: Governança corporativa de tecnologia da informação.** Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2013.

ARAÚJO, Eric et al. **Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes**. In: XVII Brazilian Symposium on Information Systems. 2021. p. 1-9.

BASON, Christian; AUSTIN, Robert D. **The right way to lead design thinking.** Harvard Business Review, v. 97, n. 2, p. 82-91, 2019.

BLAND, J. M.; ALTMAN, D. G. **Statistics notes: Cronbach's alpha**. British Medical Journal, v.314, n.7080, p. 572, 1997.

BRASIL. **"Lei geral de proteção de dados pessoais (LGPD)"** Secretaria-Geral. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso 08 Set, 2022.

BROWN, Tim. **When everyone is doing design thinking, is it still a competitive advantage**. Harvard Business Review, v. 27, 2015.

BROWN, Tim et al. **Design Thinking: uma metodologia ponderosa para decretar o fim das velhas ideias.** Rio de Janeiro: Elsevier, 2010.

CANEDO, Edna; CERQUEIRA, Anderson; GRAVINA, Rogério; RIBEIRO, Vanessa; CAMÕES, Renato; REIS, Vinicius; MENDONÇA, Fábio; SOUSA JR., Rafael; **Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD).** In: Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS 2021) - Volume 1, pages 19-30.

CARVALHO, Marly M.; FLEURY, André; LOPES, Ana Paula. **An overview of the literature on technology roadmapping (TRM): Contributions and trends**. Technological Forecasting and Social Change, v. 80, n. 7, p. 1418-1437, 2013.

CORRALES-ESTRADA, Martha. **Design thinkers' profiles and design thinking solutions.** Academia Revista Latinoamericana de Administracion, v. 33, n. 1, p. 9-24, 2020.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues. **Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais**. Revista brasileira de direito civil em perspectiva, v. 5, n. 2, p. 22-41, 2019.

CASTRO, Evandro Thalles Vale; SILVA, Geovana RS; CANEDO, Edna Dias. **Ensuring privacy in the application of the Brazilian general data protection law**

(LGPD). In: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. 2022. p. 1228-1235.

CANEDO, Edna et al. **Perceptions of ICT practitioners regarding software privacy.** Entropy, v. 22, n. 4, p. 429, 2020.

CANEDO, Edna et al. **Perceptions of ICT practitioners regarding software privacy.** Entropy, v. 22, n. 4, p. 429, 2020.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, José Antônio Valle. **Design Science Research.** Springer Books, p. 67-102, 2015.

EUROPEAN UNION. **General Data Protection. GDPR.** Disponível em < https://gdpr-info.eu>. Acesso 08 Set, 2023.

FARRUKH, Clare; PHAAL, Rob; PROBERT, David. **Technology roadmapping: linking technology resources into business planning**. International Journal of Technology Management, v. 26, n. 1, p. 2-19, 2003.

FERRÃO, Sâmmara Éllen Renner et al. **Diagnostic of data processing by Brazilian organizations—a low compliance issue**. Information, v. 12, n. 4, p. 168, 2021.

FREITAS, M. C.; SILVA, Miguel. **GDPR Compliance in SMEs: There is much to be done.** Journal of Information Systems Engineering & Management, v. 3, n. 4, p. 30, 2018.

GALVIN, Robert. **Science Roadmaps**. Science, v. 280, n. 5365, p. 803-803, 1998.

GARCIA, Marie L.; BRAY, Olin H. **Fundamentals of technology roadmapping**. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 1997.

HIRATA, Alessandro. **O Facebook e o direito à privacidade.** Revista de Informação Legislativa, v. 51, n. 201, p.17-27, 2014.

HORA, H. R. M.; MONTEIRO, G. T. R.; ARICA, J. **Confiabilidade em Questionários para Qualidade: Um estudo com o Coeficiente Alfa de Cronbach**. Produto & Produção, v.11, n.2, p.85-103, 2010.

IMAI, Ken'ichi et al. **Managing the new product development process: How Japanese companies learn and unlearn**. 1984.

ISAAK, Jim; HANNA, Mina J. **User data privacy: Facebook, Cambridge Analytica, and privacy protection.** Computer, v. 51, n. 8, p. 56-59, 2018.

KERR, Clive; PHAAL, Robert. **Visualizing roadmaps: A design-driven approach**. 2015.

KOLKO, Jon. **Design Thinking Comes of Age**. Harvard Business Review, 2015.

KOSTOFF, Ronald N.; SCHALLER, Robert R. **Science and technology roadmaps**.

IEEE Transactions on engineering management, v. 48, n. 2, p. 132-143, 2001.

LACERDA, Daniel Pacheco et al. **Design Science Research: método de pesquisa para a engenharia de produção**. Gestão & produção, v. 20, p. 741-761, 2013.

LAYTON, R.; BARANES, E. **GDPR: Short Run Outputs vs. Long Term Welfare. Mapping the EU's General Data Protection Regulation to Best Practices for Online Privacy**, 2017.

LOUZEIRO, Matheus Lustosa et al. **General Data Protection Law: Observations and Analysis of the Compliance Level of Organizations**. In: EGOV-CeDEM-ePart-*. 2021. p. 325-329.

MUNCINELLI, Gianfranco et al. **Components of the Preliminary Conceptual Model for Process Capability in LGPD (Brazilian Data Protection Regulation)**. Context. 2020.

LIEDTKA, Jeanne. **Why design thinking works**. Harvard Business Review, v. 96, n. 5, p. 72-79, 2018.

LINDBERG, Tilmann; MEINEL, Christoph; WAGNER, Ralf. **Design thinking: A fruitful concept for IT development?** Design thinking: Understand–improve–apply, p. 3-18, 2011.

MÜNCH, Jürgen; TRIEFLINGER, Stefan; LANG, Dominic. **Product roadmap–from vision to reality: a systematic literature review**. In: 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). IEEE, 2019. p. 1-8.

MUNCINELLI, Gianfranco et al. **Developing a Conceptual Model for Process Capability in the Brazilian Data Protection Regulation Context.** Journal of Industrial Integration and Management, v. 6, n. 04, p. 407-427, 2021.

PEFFERS, Ken et al. **A design science research methodology for information systems research**. Journal of management information systems, v. 24, n. 3, p. 45-77, 2007.

PEFFERS, K., et al. **Design science research in information systems: advances in theory andpractice.** 1st edition. Berlin: Springer, 2012. 438 p

PHAAL, Robert et al. **Starting-up roadmapping fast**. Research-Technology Management, v. 46, n. 2, p. 52-59, 2003.

PHAAL, Robert; FARRUKH, Clare JP; PROBERT, David R. **Technology roadmapping—A planning framework for evolution and revolution**. Technological Forecasting & Social Change, v. 71, p. 5-26, 2004.

PHAAL, Robert; FARRUKH, Clare; PROBERT, David. **Customizing roadmapping.** Research-Technology Management, v. 47, n. 2, p. 26-37, 2004.

PINSONNEAULT, Alain; KRAEMER, Kenneth. **Survey research methodology in management information systems: an assessment.** Journal of management information systems, v. 10, n. 2, p. 75-105, 1993.

RIBEIRO, Renato; CANEDO, Edna. **Using MCDA for selecting criteria of LGPD compliant personal data security.** In: The 21st Annual International Conference on Digital Government Research. 2020. p. 175-184.

RINNE, Martin. **Technology roadmaps: Infrastructure for innovation.** Technological Forecasting and Social Change, v. 71, n. 1-2, p. 67-80, 2004.

SCHWABER, Ken; SUTHERLAND, Jeff. **The scrum guide.** Scrum Alliance, v. 21, n. 1, p. 1-38, 2011.

SILVA, Paulo Henrique; BENITTI, Fabiane; WANGHAM, Michelle. **Framework for the development of computational solutions for the support of requirements engineering with a focus on data protection.** In: Proceedings of the XXXVI Brazilian Symposium on Software Engineering. 2022. p. 419-424.

SIMON, H. (1996). **The Sciences of the Artificial (3rd ed),** Cambridge, MA: MIT Press.

SUTHERLAND, Jeff; SCHWABER, Ken. **The scrum guide. The definitive guide to scrum: The rules of the game.** Scrum. org, v. 268, p. 19, 2013.

SUTHERLAND, Jeff. **SCRUM: A arte de fazer o dobro de trabalho na metade do tempo**. Leya, 2014.

SRNICEK, N. **Platform capitalism**. Cambridge: Polity Press, 2017.

TAKEUCHI, Hirotaka; NONAKA, Ikujiro. **The new product development game**. Harvard business review, v. 64, n. 1, p. 137-146, 1986.

APÊNDICE A – TCLE APRESENTADO AOS RESPONDENTES DA PESQUISA

Observação... Como o formulário da pesquisa elaborado não permitia a inserção de uma caixa de concordância, o termo foi modificado conforme abaixo:

DESAFIOS NA IMPLEMENTAÇÃO DA LGPD NAS ORGANIZAÇÕES

A pesquisa leva cerca de 7 minutos para ser concluída.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado a participar da pesquisa **Desafios na implementação da LGPD nas organizações** e sua seleção foi por conveniência em virtude de nossas conexões profissionais e na rede social LinkedIn.

Sua contribuição muito engrandecerá nosso trabalho pois participando desta pesquisa.

Você nos trará uma visão específica pautada na sua experiência sobre o assunto. Esclarecemos, contudo, que sua participação não é obrigatória. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição proponente.

O(s) objetivo(s) deste estudo são avaliar os principais desafios enfrentados pelas organizações no processo de adequação à LGPD em organizações de diferentes portes e setores.

As informações obtidas por meio desta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação. Os dados serão divulgados de forma a não possibilitar sua identificação, protegendo e assegurando sua privacidade.

A qualquer momento você poderá tirar suas dúvidas sobre o projeto e sua participação.

Ao final desta pesquisa, o trabalho completo será disponibilizado no site do Programa de Mestrado.

Ao continuar com o preenchimento do formulário você declaro que entendeu os objetivos de sua participação na pesquisa e concorda em participar. Registra também que concorda com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

APÊNDICE B – QUESTIONÁRIO DA *SURVEY*

Acessível pelo link: https://forms.office.com/r/MT76UpWd4z

Item	Questão	Referência
Q1	Qual seu tempo de experiência profissional? • Menos de 1 ano • 1 a 3 anos • 3 a 5 anos • 5 a 10 anos • Mais de 10 anos	Ferrão et al (2021)
Q2	Qual o porte de sua empresa quanto ao número de funcionários? • Até 10 funcionários • Entre 10 e 50 funcionários • Entre 50 e 100 funcionários • Entre 100 e 250 funcionários • Entre 250 e 500 funcionários • Entre 500 e 1000 funcionários • Mais de 1000 funcionários	Freitas e Silva (2018) Ferrão et al (2021)
Q3	Qual o setor de atuação de sua Organização? • Financeiro • Tecnologia • Indústria • Jurídico • Serviços • Saúde • Telecomunicações • Comércio • Agricultura / Pecuária • Construção Civil • Educação • Turismo • Outro (indique)	Freitas e Silva (2018) Ferrão et al (2021)
Q4	Qual seu departamento dentro de sua organização? • Tecnologia da Informação • Segurança da Informação • Auditoria e/ou *Compliance* • Jurídico • Recursos Humanos • Outro (indique)	Freitas e Silva (2018) Ferrão et al (2021)
Q5	Qual seu nível hierárquico dentro de sua organização? • estagiário / *trainee* / Júnior • Pleno ou Sênior • Coordenador / Supervisor • Gerente	Freitas e Silva (2018)

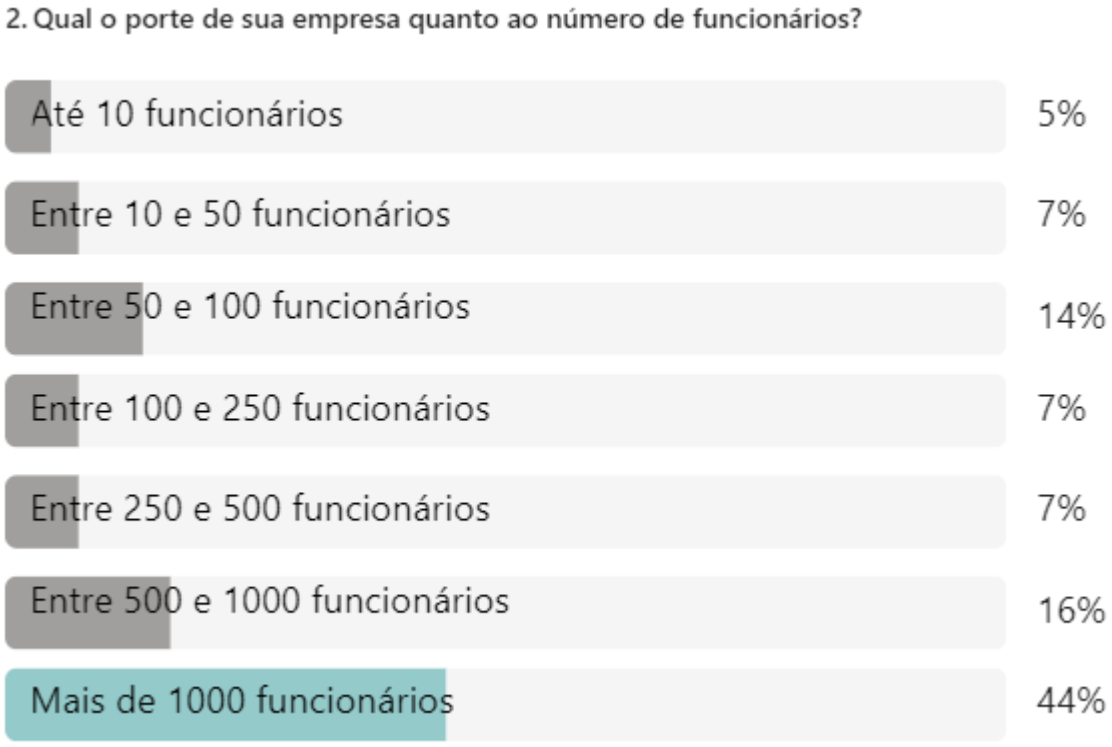
	• Diretor	
Q6	Com relação ao processo de implementação da LGPD, indique o seu grau de envolvimento? • Não estou envolvido(a) no processo • Estou pouco envolvido(a) no processo • Estou moderadamente envolvido(a) no processo • Estou bastante envolvido(a) no processo • Estou completamente envolvido(a) no processo	Freitas e Silva (2018)
Q7	Numa escala de 1 a 10, qual sua percepção do nível de adequação de sua organização à LGPD, sendo 1 totalmente não adequado e 10 totalmente adequado?	Louzeiro et al (2021)
Q8	Em que medida você concorda que sua empresa tem recursos financeiros suficientes para implementar as medidas necessárias para cumprir a LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Layton e Baranes (2017) Freitas e Silva (2018) Ferreira et al (2022)
Q9	Sua empresa teve facilidade de identificar ferramentas e métodos que apoiassem / facilitassem o processo de adequação à LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Layton e Baranes (2017) Freitas e Silva (2018)
Q10	Em que medida você concorda que sua empresa tem conhecimento suficiente sobre a LGPD para implementá-la adequadamente? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Ferreira et al (2022) Ferrão et al (2021) Canedo et al (2020)
Q11	Sua empresa teve (ou tem) dificuldades de contratar profissionais qualificados para trabalhar no processo de adequação à LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Layton e Baranes (2017) Freitas e Silva (2018) Ferreira et al (2022)
Q12	Em que medida você concorda que a equipe de TI e segurança da informação da sua empresa está suficientemente capacitada para implementar a LGPD? • Concordo totalmente	Ferrão et al (2021) Canedo et al (2020)

	• Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	
Q13	Sua organização tem políticas e procedimentos relativos à (selecione todas as opções válidas): • Política de Segurança da Informação; • Descarte de Informações após seu processamento e uso; • Monitoramento de incidentes de segurança; • Plano de ação e comunicação em caso de incidentes de vazamento de dados; • Registro e monitoramento de processamento de dados; • Política de coleta, tratamento e uso de dados; • Atendimento às solicitações dos proprietários dos dados (retificação / descarte).	Ferrão et al (2021) Canedo et al (2020) Freitas e Silva (2018)
Q14	Você considera que as políticas e procedimentos de sua organização são adequadas e suficientes para assegurar o atendimento aos requisitos da LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Ferrão et al (2021) Canedo et al (2020) Freitas e Silva (2018)
Q15	Sua empresa realiza treinamento periódico dos seguintes grupos de colaboradores para conscientização sobre a LGPD (escolha todas as opções que considerar válidas): • Colaboradores de TI; • Colaboradores de Segurança da Informação; • Colaboradores do Jurídico; • Colaboradores de Recursos Humanos; • Colaboradores de Todas as áreas da Organização; • Outros (especificar).	Ferreira et al (2022) Freitas e Silva (2018)
Q16	Em sua opinião, sua empresa tomou medidas para atendimento aos seguintes aspectos relativos à LGPD: • Obtenção formal de consentimento para coleta, tratamento e processamento de dados de usuários; • Atendimento às solicitações dos proprietários dos dados; • Auditoria periódica dos processos para atendimento à LGPD; • Termos de responsabilidade assinados por todos os seus funcionários, colaboradores e parceiros; • Inclusão de cláusulas contratuais relativas à proteção de dados em todos os contratos firmados; • Medidas de proteção dos dados tais como criptografia, anonimização.	Ferrão et al (2021) Canedo et al (2020)
Q17	Os dados coletados por sua organização são aqueles	Canedo et al (2020)

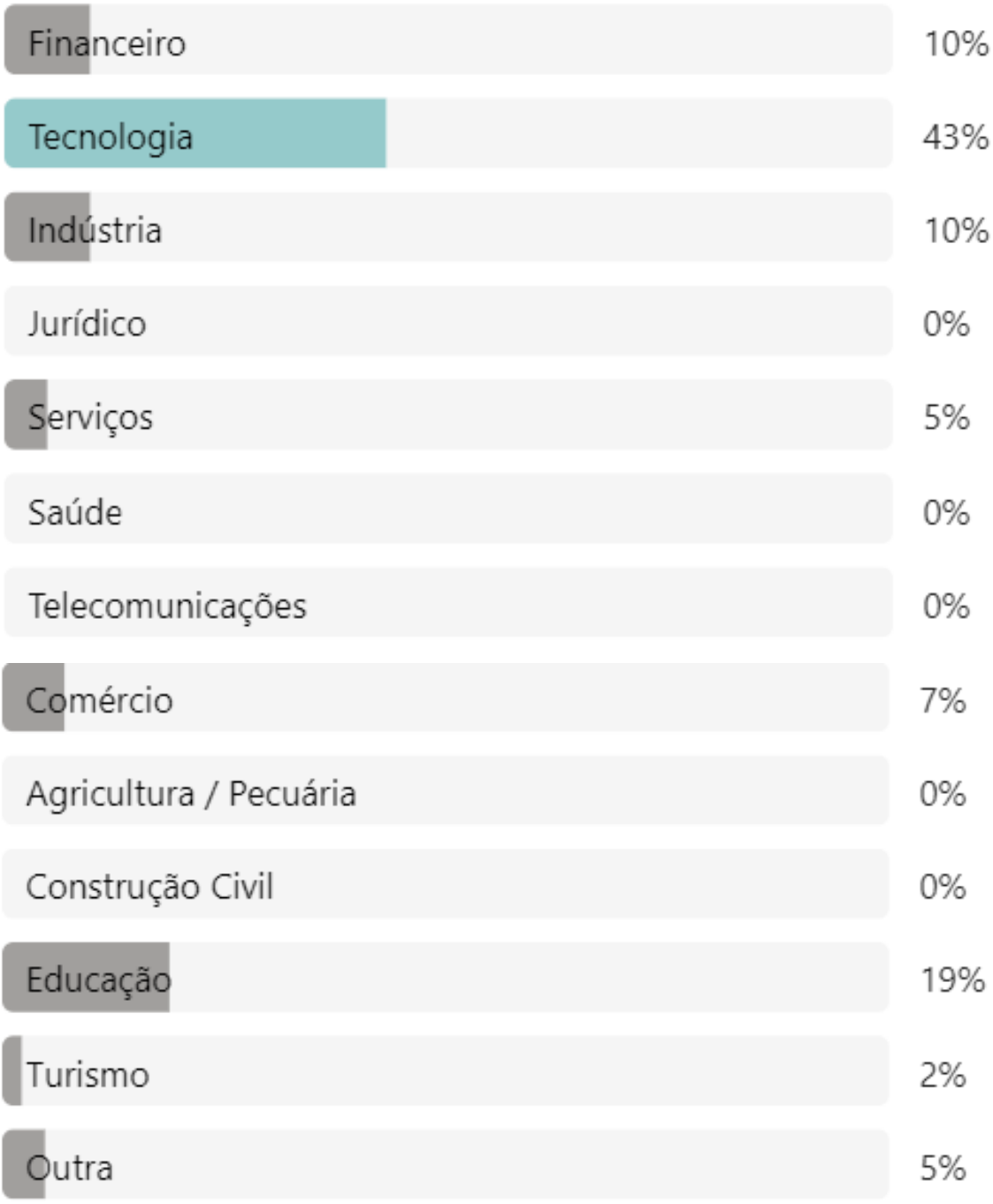
	estritamente necessários para cumprir os objetivos para os quais foram coletados? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente	Freitas e Silva (2018)

Fonte: Resultado da pesquisa

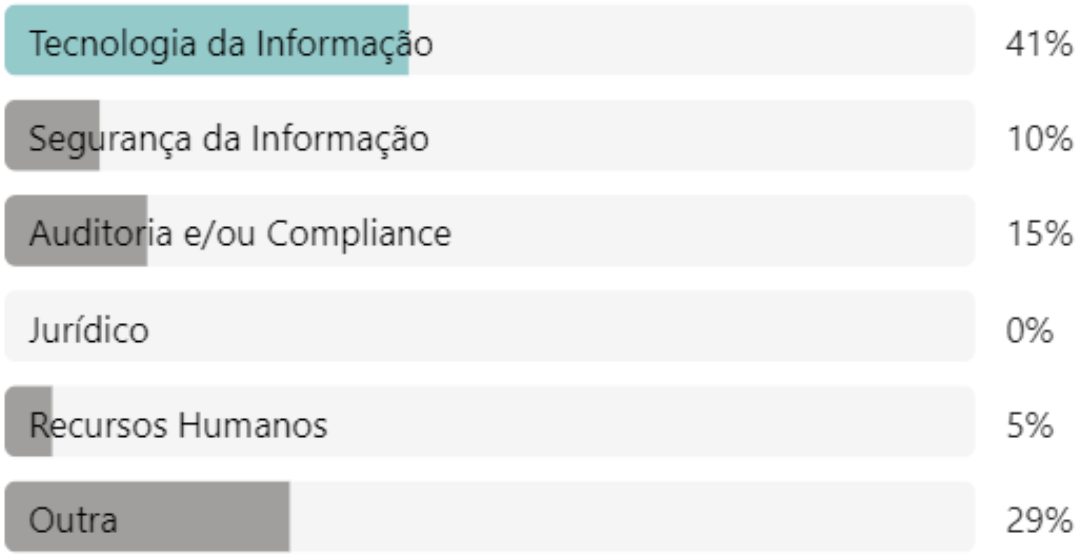
APÊNDICE C – RESULTADOS DA *SURVEY*: DESAFIOS NA IMPLEMENTAÇÃO DA LGPD NAS ORGANIZAÇÕES



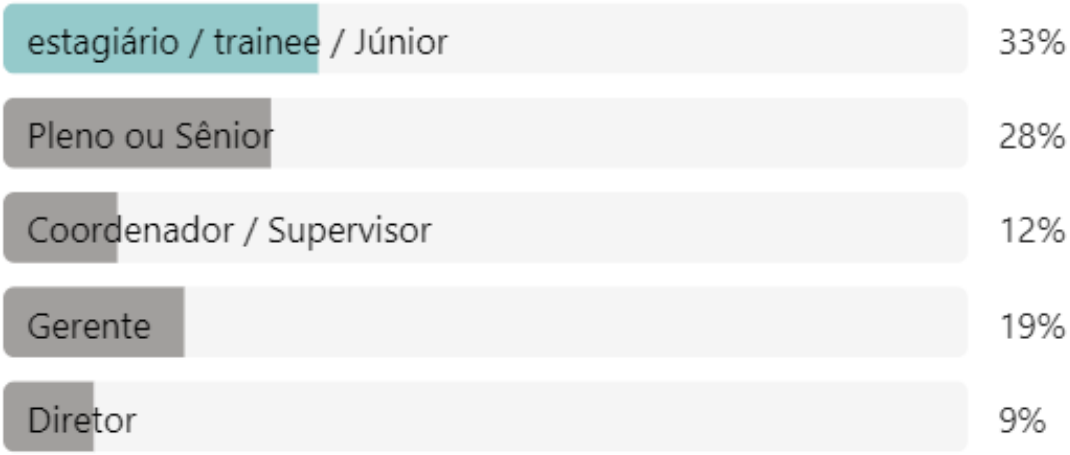
3. Qual o setor de atuação de sua Organização



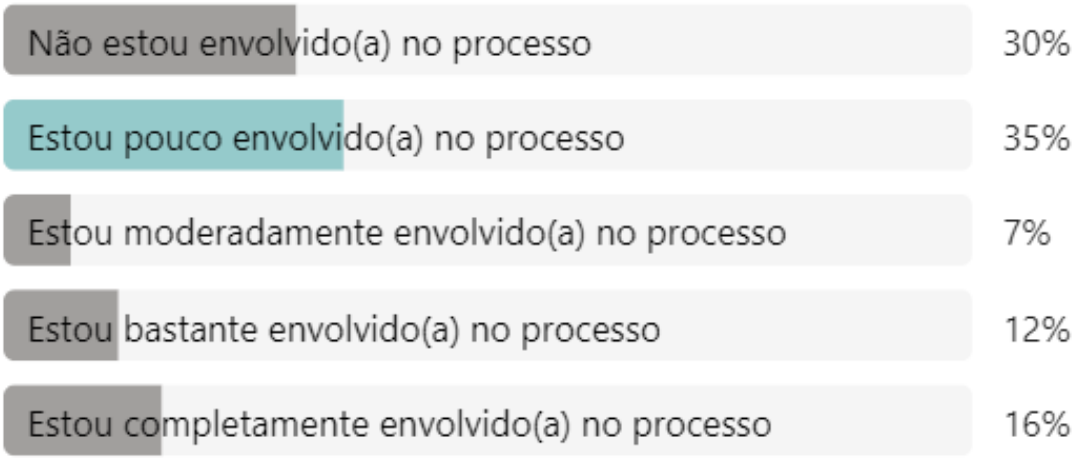
4. Qual seu departamento dentro de sua organização?



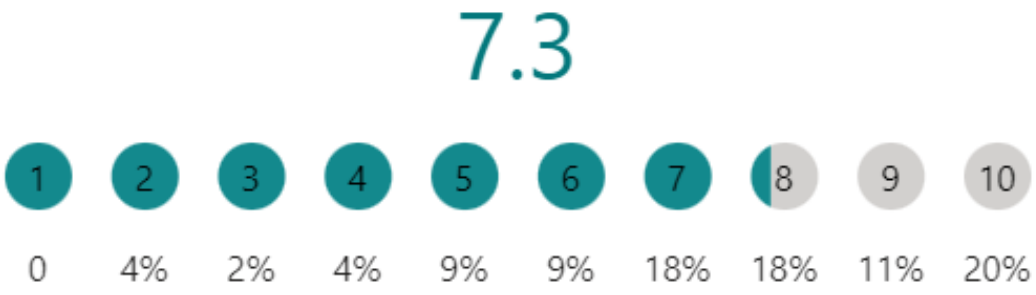
5. Qual seu nível hierárquico dentro de sua organização



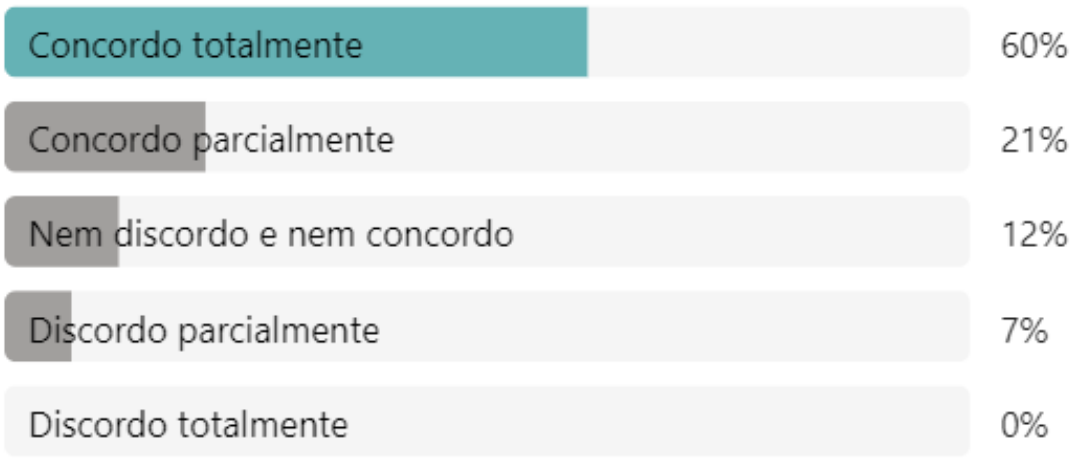
6. Com relação ao processo de implementação da LGPD, indique o seu grau de envolvimento:



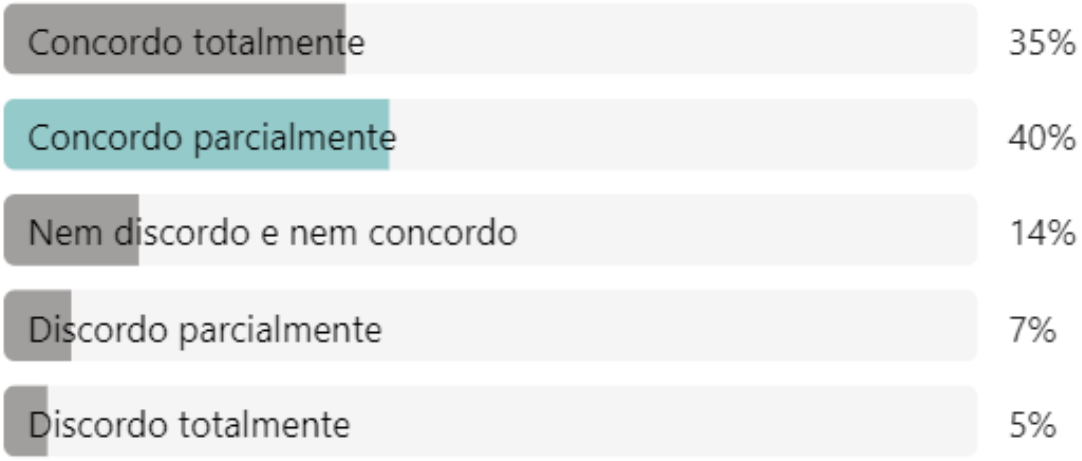
7. Numa escala de 1 a 10, qual sua percepção do nível de adequação de sua organização à LGPD, sendo 1 totalmente nã...



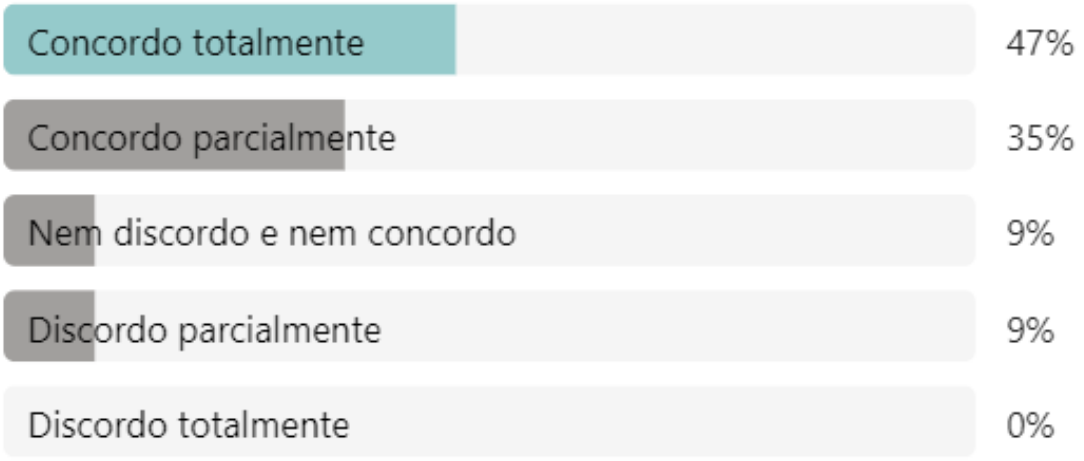
8. Em que medida você concorda que sua empresa tem recursos financeiros suficientes para implementar as medidas...



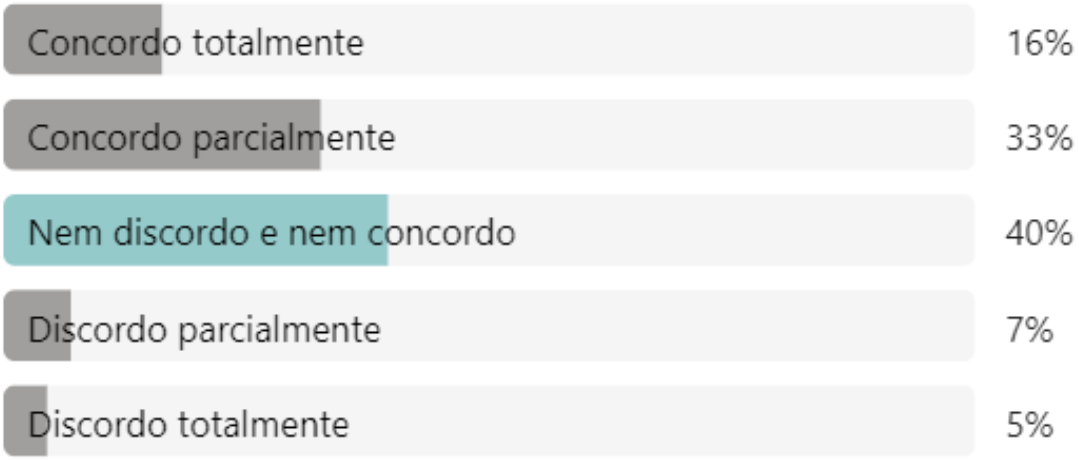
9. Sua empresa teve facilidade de identificar ferramentas e métodos que apoiassem / facilitassem o processo de...



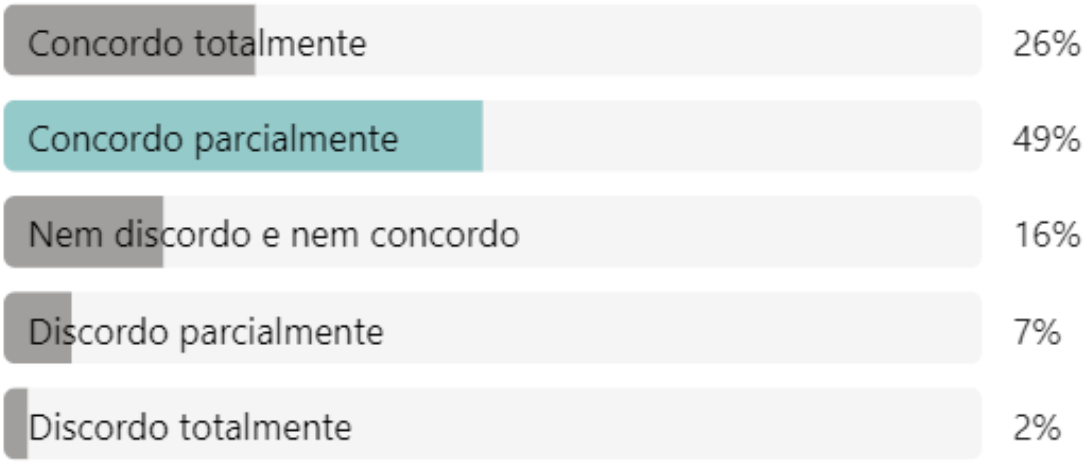
10. Em que medida você concorda que sua empresa tem conhecimento suficiente sobre a LGPD para implementá-la...



11. Sua empresa teve (ou tem) dificuldades de contratar profissionais qualificados para trabalhar no processo de...



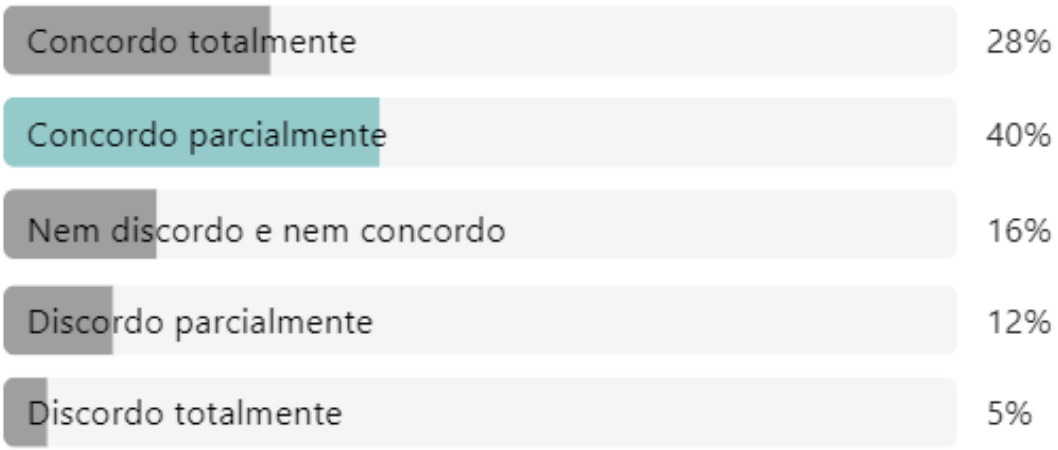
12. Em que medida você concorda que a equipe de TI e segurança da informação da sua empresa está suficientemente...



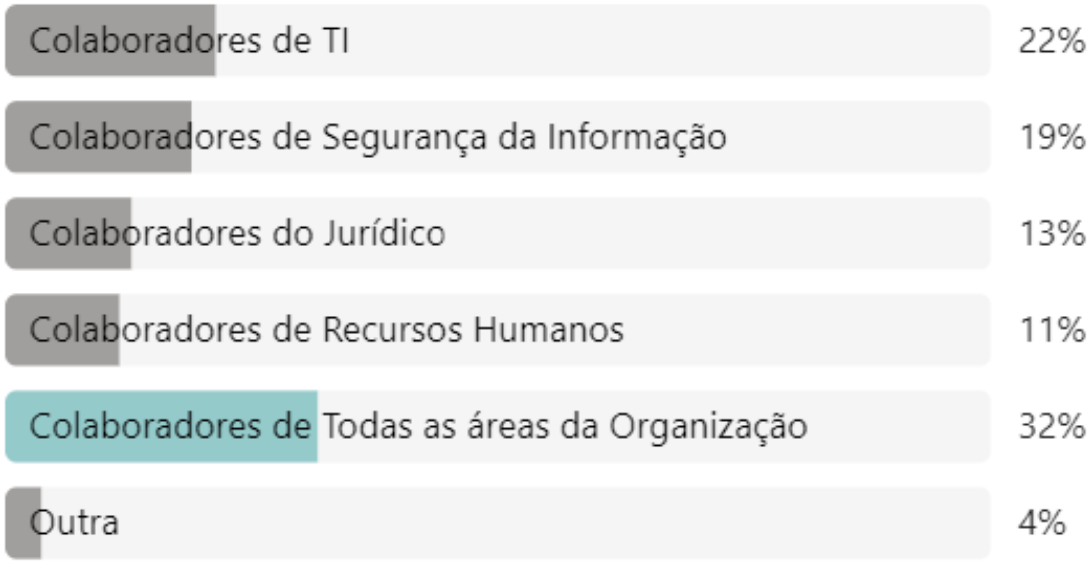
13. Sua organização tem políticas e procedimentos relativos à (selecione todas as opções válidas):

Política de Segurança da Informação	19%
Descarte de Informações após seu processamento e uso	12%
Atendimento às solicitações dos proprietários dos dados (retificação / descarte)	15%
Monitoramento de incidentes de segurança	16%
Plano de ação e comunicação em caso de incidentes de vazamento de dados	12%
Registro e monitoramento de processamento de dados	12%
Política de coleta, tratamento e uso de dados	14%
Outra	1%

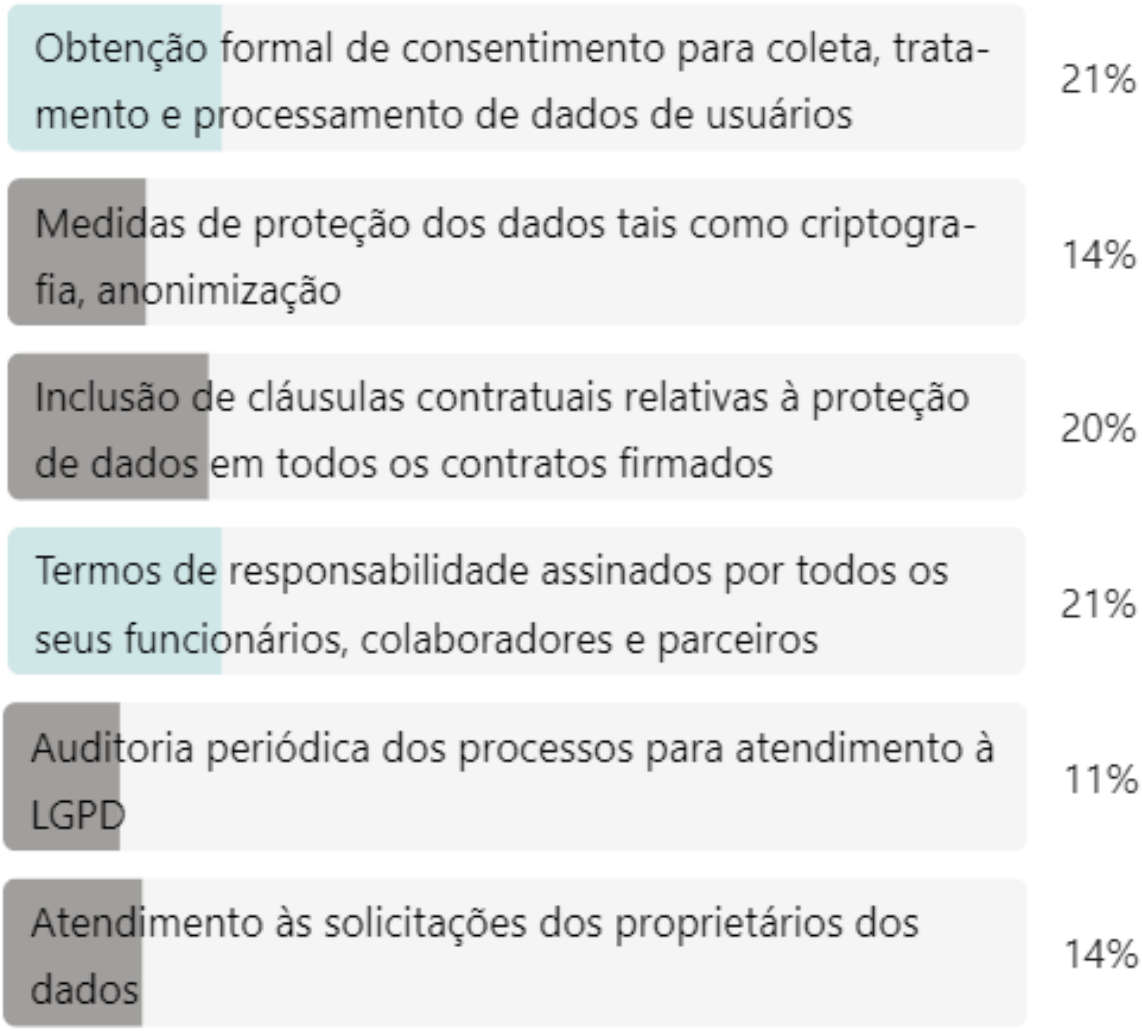
14. Você considera que as políticas e procedimentos de sua organização são adequadas e suficientes



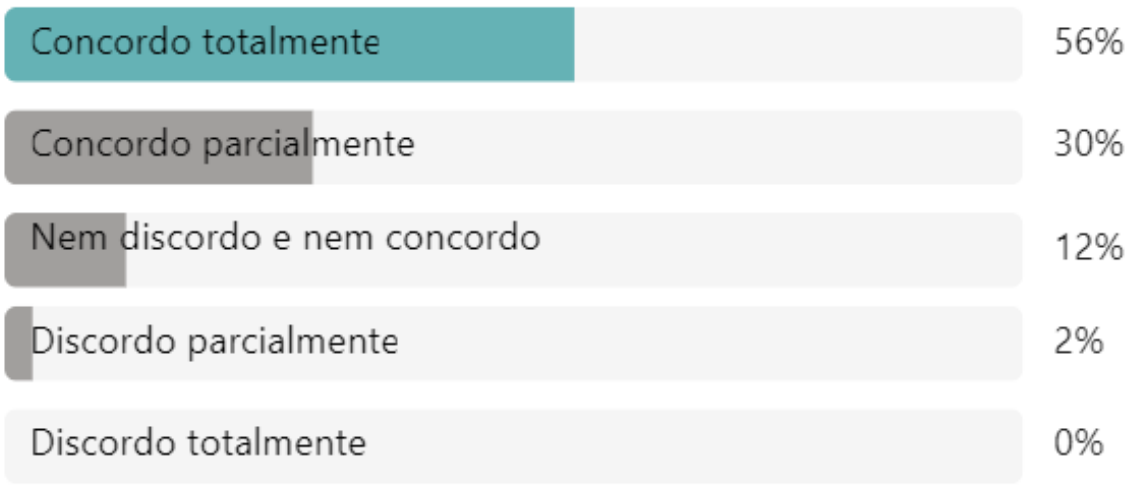
15. Sua empresa realiza treinamento periódico dos seguintes grupos de colaboradores para



16. Em sua opinião, sua empresa tomou medidas para atendimento aos seguintes aspectos relativos à LGPD:



17. Os dados coletados por sua organização são aqueles estritamente necessários para cumprir os objetivos para os quais foram coletados



APÊNDICE D – ELEMENTOS DA NBR ISO/IEC 27002 BASE PARA ELABORAÇÃO DO ROADMAP

Item	Teor	Elementos para o *ROADMAP*	Exigência
5.1	Políticas de segurança da informação	• Controle: Política de Segurança da Informação e políticas específicas devem ser definidas, aprovadas pela gestão, publicadas, comunicadas, reconhecidas por partes interessadas relevantes e revisadas em intervalos planejados, no momento em que mudanças significativas ocorrerem. • Propósito: Garantir adequação contínua, eficácia da direção de gestão e suporte para Segurança da Informação, de acordo com requisitos de negócio, legais, estatutários, regulatórios e contratuais.	Requerido
5.2	Papéis e Responsabilidades pela Segurança da Informação	• Controle: Papéis e responsabilidades de Segurança da Informação devem ser definidos e alocados de acordo com as necessidades da organização • Propósito: Estabelecer uma estrutura definida, aprovada e compreendida para a implementação, operação e gerenciamento de Segurança da Informação na organização.	Desejável
5.3	Segregação de Funções	• Controle: Funções e áreas de responsabilidade conflitantes devem ser segregadas. • Propósito: Reduzir os riscos de fraude, erro e contorno de controles de Segurança da Informação.	Requerido
5.4	Responsabilidades de Gestão	• Controle: A direção deve exigir que todo o pessoal aplique a Segurança da Informação de acordo com a Política de Segurança da Informação estabelecida, políticas de tópicos específicos e procedimentos da organização. • Propósito: Garantir entendimento da gestão em seu papel de Segurança da Informação e realizar ações visando garantir que todos os colaboradores estejam conscientes e cumpram suas responsabilidades de Segurança da	Requerido

		Informação.	
5.5	Contato com Autoridades	• Controle: A organização deve estabelecer e manter contato com autoridades relevantes. • Propósito: Garantir que o fluxo apropriado de informação ocorra entre a organização e autoridades relevantes legais, regulatórias e de supervisão, respeitando a Segurança da Informação.	Requerido
5.7	Inteligência contra Ameaças	• Controle: Informações relacionadas às ameaças de Segurança da Informação devem ser coletadas e analisadas, a fim de produzir inteligência contra ameaças. • Propósito: Prover conhecimento sobre o ambiente de ameaças da organização para a tomada de ações de mitigação apropriadas	Desejável
5.8	Segurança da Informação no Gerenciamento de Projetos	• Controle: Segurança da Informação deve ser integrada ao gerenciamento de projetos. • Propósito: Assegurar que os riscos de Segurança da Informação relacionados aos projetos e às entregas são efetivamente abordados no gerenciamento de projetos por todo o ciclo de vida do projeto.	Desejável
5.9	Inventário de Informações e outros Ativos Associados	• Controle: Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido. • Propósito: Identificar informações da organização e outros ativos associados, a fim de preservar sua Segurança da Informação e atribuir a propriedade adequada.	Requerido
5.10	Uso Aceitável de Informações e outros Ativos Associados	• Controle: Regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados devem ser identificadas, documentadas e implementadas. • Propósito: Assegurar que informações e outros ativos associados tenham proteção, uso e manuseio adequados.	Desejável
5.12	Classificação das Informações	• Controle: Informações devem ser classificadas de acordo com as necessidades da organização em Segurança da Informação, baseadas nos	Requerido

		requisitos de confidencialidade, integridade, disponibilidade e requisitos relevantes das partes interessadas. • Propósito: Assegurar a identificação e entendimento das necessidades de proteção da informação, de acordo com sua importância para a organização.	
5.13	Rotulagem das Informações	• Controle: Um conjunto adequado de procedimentos para rotulagem das informações deve ser desenvolvido e implementado, de acordo com o esquema de classificação das informações adotado pela organização. • Propósito: Facilitar as comunicações a respeito da classificação das informações e automação do suporte de processamento e gerenciamento das informações.	Desejável
5.14	Transferência das Informações	• Controle: Regras, procedimentos e acordos de transferência das informações devem ocorrer em todos os tipos de instalações de transferência na organização, entre ela e partes interessadas. • Propósito: Manter a segurança das informações transferidas na organização e em qualquer parte interessada externa.	Requerido
5.15	Controle de Acesso	• Controle: Regras para o controle físico e lógico de acesso às informações e outros ativos associados devem ser estabelecidos e implementados, conforme os requisitos de negócio e Segurança da Informação. • Propósito: Garantir acesso autorizado e prever acesso não autorizado às informações e aos outros ativos associados.	Requerido
5.18	Direitos de Acesso	• Controle: Direitos de acesso a informações e outros ativos associados devem ser provisionados, revisados, modificados e removidos, de acordo com políticas de tópicos específicos da organização e regras para controle de acesso. • Propósito: Garantir que o acesso a informações e outros ativos associados estejam definidos e autorizados de acordo com os requisitos de	Requerido

		negócio.	
5.19	Segurança da Informação nas relações com Fornecedores	• Controle: Processos e procedimentos devem ser definidos e implementados, a fim de gerenciar os riscos de Segurança da Informação associados com o uso de produtos ou serviços de fornecedores. • Propósito: Manter o nível acordado de Segurança da Informação nos relacionamentos com fornecedores	Requerido
5.20	Abordagem da Segurança da Informação nos Contratos de Fornecedores	• Controle: Requisitos relevantes de Segurança da Informação devem ser estabelecidos e acordados com cada fornecedor, conforme os seus tipos de relacionamento. • Propósito: Manter um nível acordado de Segurança da Informação nos relacionamentos com fornecedores.	Requerido
5.23	Segurança da Informação para Uso de Serviços em Nuvem	• Controle: Processos para aquisição, uso, gerenciamento e saída de serviços em nuvem devem ser estabelecidos de acordo com os requisitos de Segurança da Informação da organização. • Propósito: Especificar e gerenciar Segurança da Informação para uso nos serviços em nuvem.	Requerido
5.24	Planejamento e preparação de Gerenciamento de Incidentes de Segurança da Informação	• Controle: A organização deve planejar-se e preparar-se para o gerenciamento de incidentes de Segurança da Informação, por meio da definição, estabelecimento e comunicação dos processos, funções e responsabilidades relativos a gestão de incidentes de Segurança da Informação. • Propósito: Assegurar uma resposta rápida, eficaz, consistente e ordenada aos incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança da informação.	Desejável
5.25	Avaliação e Decisão sobre Eventos de Segurança da Informação	• Controle: A organização deve avaliar os eventos de Segurança da Informação e decidir se os categoriza como incidentes. • Propósito: Garantir categorização eficaz e	Requerido

		priorização dos eventos de Segurança da Informação.	
5.26	Resposta aos Incidentes de Segurança da Informação	• Controle: Incidentes de Segurança da Informação devem ser respondidos de acordo com os procedimentos documentados. • Propósito: Garantir respostas eficientes e eficazes aos incidentes de Segurança da Informação	Requerido
5.31	Requisitos Legais, Estatutários, Regulatórios e Contratuais	• Controle: Os requisitos legais, estatutários, regulatórios e contratuais relevantes para a Segurança da Informação e a abordagem organizacional para atender a esses requisitos devem passar por identificação, documentação e atualização constante. • Propósito: Garantir conformidade com requisitos legais, estatutários, regulatórios e contratuais relacionados à Segurança da Informação.	Requerido
5.33	Proteção de Registros	• Controle: Registros devem possuir proteção contra perda, destruição, falsificação e acesso e liberação não autorizados. • Propósito: Garantir conformidade com requisitos legais, estatutários, regulatórios e contratuais, assim como expectativas da comunidade ou sociedade relacionadas a proteção e disponibilidade dos registros.	Requerido
5.34	Privacidade e Proteção de DP	• Controle: A organização deve identificar e atender aos requisitos a respeito da preservação da privacidade e proteção de DP, de acordo com leis e regulações aplicáveis e requisitos contratuais. • Propósito: Assegurar o *compliance* dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de DP.	Requerido
5.36	Conformidade com Políticas, Regras e Padrões de Segurança da Informação	• Controle: Conformidade com Política de Segurança da Informação organizacional, políticas de tópicos específicos, regras e padrões devem passar regularmente por revisão. • Propósito: Garantir que a Segurança da	Requerido

		Informação seja implementada e operada de acordo com a Política de Segurança da Informação organizacional, as políticas de tópicos específicos, as regras e os padrões.	
5.37	Procedimentos Operacionais Documentados	• Controle: Procedimentos operacionais para recursos de processamento de informações devem ser documentados e deixados disponíveis aos colaboradores que os necessitem. • Propósito: Garantir o funcionamento correto e seguro dos recursos de processamento de informações.	Requerido
6.2	Termos e Condições de Contratação	• Controle: Os acordos contratuais de trabalho devem indicar as responsabilidades dos colaboradores e da organização com a Segurança da Informação. • Propósito: Garantir entendimento dos colaboradores sobre suas responsabilidades de Segurança da Informação, relativas às suas funções.	Requerido
6.3	Conscientização, educação e treinamento em segurança da informação	• Controle: O pessoal da organização e partes interessadas relevantes devem receber conscientização sobre Segurança da Informação, educação, treinamento e atualizações da Política de Segurança da Informação, bem como políticas de tópicos específicos e procedimentos, relevantes para as suas funções. • Propósito: Assegurar que o pessoal e as partes interessadas pertinentes estejam cientes e cumpram suas responsabilidades de Segurança da Informação.	Requerido
6.4	Processo Disciplinar	• Controle: Um processo disciplinar deve ser formalizado e comunicado, a fim de tomar ações contra colaboradores e partes interessadas relevantes que tenham cometido violações na Política de Segurança da Informação. • Propósito: Garantir que colaboradores e outras partes interessadas relevantes entendam as consequências de violação da Política de Segurança da Informação, bem como dissuadir e	Desejável

		lidar adequadamente com os que cometerem a infração.	
6.6	Acordos de Confidencialidade ou Não Divulgação	• Controle: Acordos de confidencialidade ou não divulgação que reflitam as necessidades organizacionais para a proteção da informação deve passar por identificação, documentação, revisão regular e assinatura pelos colaboradores e outras partes interessadas relevantes. • Propósito: Manter confidencialidade das informações acessíveis pelos colaboradores ou partes externas.	Requerido
6.7	Trabalho Remoto	• Controle: Medidas de segurança devem ser implementadas quando os colaboradores estão trabalhando remotamente, a fim de proteger as informações acessadas, processadas ou armazenadas fora das instalações da organização. • Propósito: Garantir a Segurança da Informação enquanto os colaboradores estão trabalhando remotamente.	Requerido
6.8	Relato de Eventos de Segurança da Informação	• Controle: A organização deve fornecer um mecanismo para as pessoas reportarem eventos de Segurança da Informação observados ou suspeitos por meio de canais adequados, em tempo hábil. • Propósito: Oferecer apoio em tempo hábil a relatos, consistentes e eficazes de eventos de segurança da informação que podem ser identificados pelo pessoal.	Requerido
7.1	Perímetros de Segurança Física	• Controle: Perímetros de segurança devem ser definidos e usados, a fim de proteger áreas que contêm informações e outros ativos associados. • Propósito: Prevenir acesso físico não autorizado, dano e interferências a informações organizacionais e outros ativos associados.	Requerido
7.2	Entrada Física	• Controle: Áreas de segurança devem ser protegidas por controles de entrada e pontos de acesso apropriados. • Propósito: Assegurar que ocorra apenas acesso	Requerido

		físico autorizado às informações da organização e outros ativos associados.	
7.7	Mesa limpa e tela limpa	• Controle: Regras claras de mesa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de tratamento das informações sejam definidas e adequadamente aplicadas. • Propósito: Reduzir os riscos de acesso não autorizado, perda e dano a informações em mesas, telas e outros locais acessíveis durante e fora dos horários normais de trabalho.	Requerido
7.10	Mídia de Armazenamento	• Controle: A mídia de armazenamento deve admitir gerenciamento por meio do ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e requisitos de manuseio da organização. • Propósito: Assegurar a divulgação, modificação, remoção ou destruição de informações apenas de forma autorizada sobre as mídias de armazenamento.	Requerido
8.1	Dispositivos *endpoint* do Usuário	• Controle: A organização deve estabelecer uma política específica por tema sobre configuração segura e manuseio de dispositivos *endpoint* do usuário. Informações armazenadas, processadas ou acessíveis por meio de dispositivos *endpoint* de usuários devem ser protegidas. • Propósito: Proteger as informações contra os riscos provocados pelo uso de dispositivos *endpoint* do usuário.	Requerido
8.2	Direitos de Acessos Privilegiados	• Controle: A atribuição e a utilização de direitos de acesso privilegiados devem ser restringidas e geridas. • Propósito: Assegurar que apenas usuários, componentes de software e serviços autorizados recebam direitos de acessos privilegiados.	Requerido
8.3	Restrição de acesso à Informação	• Controle: Acesso à informação e outros ativos associados devem ser restritos de acordo com a políticas específica estabelecida no controle de acesso.	Requerido

		• Propósito: Assegurar somente acesso autorizado e impedir acesso não autorizado a informações e outros ativos associados.	
8.5	Autenticação Segura	• Controle: Tecnologias e procedimentos de autenticação segura devem ser implementados baseados em restrições de acesso à informação e à política específica por tema de controle de acesso. • Propósito: Assegurar que um usuário ou uma entidade seja autenticada com segurança, quando o acesso a sistemas, aplicações e serviços é concedido.	Requerido
8.7	Proteção contra *Malware*	• Controle: A proteção contra *malware* deve ser implementada e apoiada pela conscientização adequada do usuário. • Propósito: Assegurar que informações e outros ativos associados estejam protegidos contra *malware*.	Requerido
8.8	Gerenciamento de Vulnerabilidades Técnicas	• Controle: Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas e a exposição da organização a tais vulnerabilidades deve ser avaliadas, tomando medidas adequadas. • Propósito: Evitar a exploração de vulnerabilidades técnicas.	Desejável
8.10	Exclusão de Informações	• Controle: Informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias. • Propósito: Evitar a exposição desnecessária de informações sensíveis e estar em *compliance* com requisitos legais, estatutários, regulatórios e contratuais para a exclusão de informações.	Requerido
8.11	Mascaramento de Dados	• Controle: Mascaramento de dados deve ser utilizado de acordo com políticas de tópicos específicos de controle de acesso e outros relacionados, bem como requisitos de negócio, levando em consideração a legislação aplicável.	Requerido

		• Propósito: Limitar a exposição de dados sensíveis, incluindo DP, e cumprir requisitos legais, estatutários, regulatórios e contratuais.	
8.12	Prevenção de Vazamento de Dados	• Controle: Medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis. • Propósito: Detectar e prevenir divulgação e extração não autorizada de informações por indivíduos ou sistemas.	Requerido
8.15	*Log*	• Controle: *Logs* que registram atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados. • Propósito: Registrar eventos, gerar evidências, garantir a integridade das informações de *log*, prevenir contra acesso não autorizado, identificar eventos de Segurança da Informação que podem levar a um incidente e apoiar as investigações.	Requerido
8.16	Atividades de Monitoramento	• Controle: Redes, sistemas e aplicações devem ser monitorados em razão de comportamento anômalo e ações apropriadas devem ser tomadas a fim de avaliar potenciais incidentes de Segurança da Informação. • Propósito: Detectar comportamento anômalo e possíveis incidentes de Segurança da Informação.	Desejável
8.20	Segurança de Redes	• Controle: Redes e seus dispositivos devem ser protegidos, gerenciados e controlados, a fim de salvaguardar as informações em sistemas e aplicações. • Propósito: Proteger as informações nas redes e seus recursos de processamento de informações contra comprometimentos.	Requerido
8.21	Segurança de Serviços de Rede	• Controle: Mecanismos de segurança, níveis de serviço e requisitos de serviço de rede devem ser identificados, implementados e monitorados.	Requerido

		• Propósito: Assegurar a segurança no uso dos serviços de rede.	
8.22	Segregação de Redes	• Controle: Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização. • Propósito: Dividir a rede em perímetros de segurança e controlar o tráfego entre eles, conforme as necessidades do negócios.	Requerido
8.24	Uso de Criptografia	• Controle: Regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográficas, devem ser definidas e implementadas. • Propósito: Assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, a autenticidade ou a integridade das informações, conforme requisitos de negócios e Segurança da Informação, considerando premissas legais, estatutárias, regulatórias e contratuais relacionadas à criptografia.	Requerido
8.25	Ciclo de Vida de Desenvolvimento Seguro	• Controle: Regras para o desenvolvimento seguro de software e sistemas devem ser estabelecidas e aplicadas. • Propósito: Garantir que a Segurança da Informação seja projetada e implementada dentro do ciclo de vida de desenvolvimento seguro de softwares e sistemas.	Desejável
8.26	Requisitos de Segurança de Aplicações	• Controle: Requisitos de Segurança da Informação devem ser identificados, especificados e aprovados durante o desenvolvimento ou aquisição de aplicações. • Propósito: Assegurar que todos os requisitos de segurança da informação sejam identificados e abordados ao desenvolver ou adquirir aplicações.	Requerido
8.27	Princípios de Arquitetura e Engenharia de Sistemas Seguros	• Controle: Princípios para engenharia em sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados a quaisquer atividades de desenvolvimento de sistemas de informação.	Desejável

		• Propósito: Assegurar que os sistemas de informação sejam projetados, implementados e operados com segurança dentro do ciclo de vida de desenvolvimento.	
8.30	Desenvolvimento Terceirizado	• Controle: A organização deve dirigir, monitorar e revisar as atividades relacionadas à terceirização de desenvolvimento de sistemas. • Propósito: Assegurar que as medidas de Segurança da Informação requeridas pela organização sejam implementadas na terceirização do desenvolvimento de sistemas.	Desejável

Fonte: Adaptado de Associação Brasileira de Normas e Técnicas. NBR ISO/IEC 27002 3ª. e, (2022).

APÊNDICE E – VISÃO GERAL DAS ETAPAS DO RAEL

ETAPA	TÍTULO	OBJETIVO
1	Avaliar necessidade de adequação à LGPD	A empresa deve avaliar se está enquadrada nos requisitos de obrigatoriedade de adequação à LGPD. Além disso, deve verificar se existem normas, regulamentos, portarias ou outras normativas emitidas por órgãos regulatórios, agências governamentais e outras associações específicas do setor de atuação da organização que possam incluir regras específicas a serem seguidas pela organização, as quais devam também ser consideradas ao longo de todo o processo.
2	Constituir um comitê Interno para Acompanhamento da LGPD	Nomear as pessoas dentro da organização que serão responsáveis pelo acompanhamento do projeto de adequação à LGPD e que darão o apoio e suporte necessários ao DPO e às áreas envolvidas. As responsabilidades do comitê incluem a seleção do DPO, que se reportará a este comitê, bem como decidir pontos essenciais do processo para os quais o DPO não tenha alçada. Em organizações de menor porte este comitê pode ser formado pelos sócios/proprietários da empresa e, quando houver uma estrutura organizacional mais adequada, deve considerar a participação de todos os stakeholders relevantes para o processo, que pode incluir representantes dos investidores, diretores de áreas chaves tais como Segurança da Informação, Tecnologia, Jurídico, Marketing e Recursos Humanos
3	Nomear o encarregado de Proteção de Dados (DPO)	A empresa deve designar um encarregado de proteção de dados (DPO) para monitorar o cumprimento da LGPD. O DPO é responsável por garantir a conformidade com a LGPD dentro da empresa, além de ser o ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO deve também reportar-se ao comitê gestor da LGPD na organização, provendo informação, solicitando apoio e submetendo ao comitê decisões chaves do processo para as quais não tenha plena liberdade de atuação.

4	Mapear / Identificar os dados pessoais / sensíveis tratados pela empresa e seu fluxo dentro da organização desde a coleta até o descarte	A empresa deve fazer um inventário para identificar, documentar e classificar os dados) que são coletados, armazenados, processados e compartilhados dentro da organização, bem como os meios utilizados para isso. Estes dados coletados devem ser classificados com relação ao seu teor (se dados pessoais, dados pessoais sensíveis, dados anonimizados, pseudoanonimizados). Além disso, deve mapear os fluxos pelos quais estas informações são coletadas, tratadas e descartadas pela empresa, de forma a identificar todos os processos que demandem revisão para averiguar sua adequação ao cumprimento dos requisitos da LGPD. A empresa deve iniciar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), também conhecido pela sigla DPIA em inglês. As informações que constam deste relatório deverão ser incluídas / revisadas / atualizadas ao longo de todo o processo de adequação a fim de assegurar o atendimento aos requisitos da LGPD.
5	Analisar a base legal para o tratamento de dados	A empresa deve avaliar se possui uma base legal válida para coletar, armazenar e processar os dados pessoais. Essas bases podem incluir consentimento, contrato, cumprimento de obrigação legal ou interesse legítimo. Esta avaliação deve considerar também uma análise quanto à suficiência dos dados coletados e processados, ou seja, os dados coletados e processados são aqueles estritamente necessários? A análise deve incluir também avaliação quanto à proporcionalidade do processamento realizado. São processadas as informações estritamente necessárias? O processamento é realmente necessário? Não existe outra maneira de alcançar o mesmo resultado?
6	Análise de riscos	A empresa deve avaliar os riscos envolvidos na coleta, tratamento, transferência, descarte e qualquer outra etapa relacionada a dados pessoais/sensíveis de usuários/clientes e colaboradores e adotar medidas para gerenciamento

		destes riscos que atendam aos requisitos da LGPD.
7	Elaborar cronograma geral do projeto	Elaborar um cronograma que sirva como guia geral do projeto considerando a criticidade dos riscos identificados e as medidas de gerenciamento
8	Elaborar ou revisar as Políticas e procedimentos de Segurança da Informação, Proteção, Privacidade e Tratamento de Dados	A empresa deve elaborar políticas e procedimentos (ou revisar as existentes, se houver), com objetivo de definir papéis e responsabilidades de cada um dos envolvidos na gestão da segurança das informações e dos dados pessoais, as medidas a serem implementadas visando a proteção dos dados, gestão do acesso, proteção, monitoramento de incidentes, descarte de informações após uso e outros procedimentos necessários para atendimento aos requisitos da lei. Devem também ser elaborados os termos de responsabilidade a serem assinados por colaboradores e parceiros relativos ao sigilo e proteção dos dados processados pela organização, bem como os termos de autorização a serem assinados pelos usuários, clientes e colaboradores da empresa, detalhando o tipo de procedimento de tratamento de dados realizados, os compartilhamentos de dados realizados com parceiros da empresa, explicitando quais estes parceiros e os fins para os quais estas informações são tratadas e/ou compartilhadas. A empresa deve levar em conta os riscos envolvidos no tratamento de dados pessoais, definindo procedimentos e medidas para minimizar estes riscos e, quando possível e viável, eliminá-los por completo.
9	Revisar contratos com parceiros, fornecedores e demais envolvidos	A empresa deve revisar os contratos com fornecedores, parceiros e demais envolvidos a fim de incluir cláusulas de conformidade que assegurem a aplicação de medidas protetivas adequadas para os dados pessoais de clientes da organização acessados, tratados e processados por estes fornecedores. Toda e qualquer alteração nos contratos existentes, bem como elaboração de novos contratos com outros fornecedores e parceiros deve ser sempre seguida de

		atualização dos Termos de Autorização e nova coleta de autorização dos titulares de dados tendo em vista a lei estabelecer que a autorização deve ser explícita, e não genérica.
10	Obter o consentimento dos titulares dos dados	A empresa deve obter o consentimento explícito e formal dos titulares dos dados para coletar, tratar, processar e compartilhar seus dados pessoais. O termo deve conter as informações referentes à quais informações são coletadas, qual o objetivo, tempo de retenção, tipo de tratamento, propósito do tratamento, bem como deve explicitar que informações são transferidas / compartilhadas com outros parceiros e com qual propósito e finalidade e outras informações pertinentes para assegurar a transparência do processo ao titular dos dados. Implementar medidas para estabelecer de forma clara nos serviços de comunicação da empresa a publicação das políticas de privacidade e contato com a área responsável para que os direitos de titulares possam ser exercidos/solicitados.
11	Preparação dos profissionais envolvidos	A empresa deve conscientizar seus colaboradores, fornecedores e demais envolvidos diretamente no processo sobre a importância da LGPD e como ela impacta o negócio. Além disso deve treiná-los e capacitá-los para garantir que entendam os requisitos da LGPD, as boas práticas de proteção de dados pessoais e as políticas e procedimentos de proteção de dados da empresa e as ferramentas, técnicas e métodos a serem implementados para assegurar a efetiva proteção dos dados com base nos requisitos da lei.
12	Implementar medidas técnicas para garantir a segurança dos dados	A empresa deve implementar medidas de segurança para proteger os dados pessoais que coleta e processa. Isso inclui medidas técnicas e organizacionais, como implementação de sistemas de segurança e a elaboração de políticas e procedimentos internos, criptografia, anonimização, autenticação, controle de acesso e gestão de incidentes visando a prevenção de acessos não autorizados e a minimização de riscos de vazamentos.

13	Avaliar e implementar medidas para transferência internacional	Na hipótese de a empresa realizar a transferência internacional de dados, deve avaliar se atende aos requisitos estabelecidos nos artigos 33 a 36 da LGPD e definir procedimentos específicos para este caso.
14	Estabelecer um processo de gerenciamento e resposta a incidentes de segurança	A empresa deve estabelecer um processo para lidar com incidentes de segurança, incluindo um plano de resposta a incidentes de segurança, para lidar com vazamentos ou outras situações que possam afetar a segurança e/ou violar os dados pessoais, incluindo procedimentos para comunicação à autoridade nacional e ao titular dos dados em prazo razoável e conforme definido no parágrafo 1 do artigo 48.
15	Implementar medidas para eliminação dos dados ao término do tratamento	A empresa deve definir procedimentos para eliminação dos dados após o fim do período de tratamento, quando a finalidade tiver sido alcançada, quando os dados deixem de ser necessários ou pertinentes à finalidade específica para a qual foram coletados ou por solicitação do titular.
16	Manter registros das atividades de tratamento de dados	A empresa deve manter registros de todas as atividades de tratamento de dados pessoais realizadas, incluindo informações sobre os titulares dos dados, finalidades do tratamento, dados compartilhados, entre outras informações. Além disso, deve elaborar um relatório de impacto à proteção de dados pessoais conforme estabelecido no artigo 38 da LGPD.
17	Atendimento aos direitos dos titulares	A empresa deve garantir o atendimento aos direitos dos titulares dos dados, como o direito de acesso, correção, exclusão, portabilidade e oposição ao tratamento de seus dados pessoais.
18	Treinamento, Conscientização e Capacitação - demais profissionais da organização.	A empresa deve conscientizar os demais colaboradores, fornecedores e prestadores de serviço sobre a importância da LGPD e como ela impacta o negócio. Além disso deve treiná-los e capacitá-los para garantir que entendam os requisitos da LGPD, as boas práticas de proteção de dados pessoais e as políticas e procedimentos de proteção de dados da empresa, bem como os procedimentos para atendimento à clientes e usuários e para direcionamento de suas solicitações relativas ao tema.

19	Implementar um processo de monitoramento que assegure a revisão e atualização periódica dos processos, políticas e procedimentos relacionados à LGPD	A fim de assegurar a manutenção e validade dos processos implementados, deve ser realizado monitoramento e revisão periódica dos processos, dos fluxos de dados, dos contratos com parceiros e fornecedores e todo e qualquer outro aspecto que possa demandar mudanças nos processos implementados nas etapas anteriores, de forma a assegurar a constante adequação da empresa aos requisitos da LGPD.
20	Realizar auditorias regulares	A empresa deve realizar auditorias regulares para garantir que esteja em conformidade com a LGPD e para identificar possíveis riscos e vulnerabilidades em seu sistema de proteção de dados.

Fonte: Resultado da pesquisa

APÊNDICE F – DETALHAMENTO DAS ETAPAS DO RAEL

# ETAPA	1
FASE	PREPARAÇÃO
ETAPA	Avaliar necessidade de adequação à LGPD
OBJETIVO (POR QUÊ?)	A empresa deve avaliar se está enquadrada nos requisitos de obrigatoriedade de adequação à LGPD. Além disso, deve verificar se existem normas, regulamentos, portarias ou outras normativas emitidas por órgãos regulatórios, agências governamentais e outras associações específicas do setor de atuação da organização que possam incluir regras específicas a serem seguidas pela organização, as quais devam também ser consideradas ao longo de todo o processo.
REFERÊNCIA ISO 27002	NÃO SE APLICA
ENTRADAS	Artigos 3 A 7 da LGPD, normas e regulamentos específicos para o setor de atuação da empresa que possam afetar também as questões de proteção de dados.
SAIDAS ENTREGAS "O QUÊ?"	Análise do enquadramento da empresa aos artigos 3 a 7 da LGPD e a outras normas e regulamentos que devam ser levados em consideração ao longo do processo de adequação.
ETAPA ANTECESSORA (REQUERIDA)	NÃO HÁ
ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ARTIGOS 3 A 7 Outras normas e regulamentos que se apliquem
# ETAPA	**2**
FASE	PREPARAÇÃO
ETAPA	Constituir um comitê Interno para Acompanhamento da LGPD
OBJETIVO (POR QUÊ?)	Nomear as pessoas dentro da organização que serão responsáveis pelo acompanhamento do projeto de adequação à LGPD e que darão o apoio e suporte necessários ao DPO e às áreas envolvidas. As responsabilidades do comitê incluem a seleção do DPO, que se reportará a este comitê, bem como decidir pontos essenciais do processo para os quais o DPO não tenha alçada. Em organizações de menor porte este comitê pode ser formado pelos sócios/proprietários da empresa e, quando houver uma estrutura organizacional mais adequada, deve considerar a participação de todos os stakeholders relevantes para o processo, que pode incluir representantes dos investidores, diretores de áreas chaves tais como Segurança da Informação, Tecnologia, Jurídico, Marketing e Recursos Humanos
REFERÊNCIA ISO 27002	5.2
ENTRADAS	NÃO HÁ
SAIDAS / ENTREGAS ("O QUÊ?")	Organograma do Comitê

ETAPA ANTECESSORA (REQUERIDA)	NÃO HÁ
ÁREAS / FUNÇÕES ENVOLVIDAS	COMITÊ EXECUTIVO, SÓCIOS, PROPRIETÁRIOS, REPRESENTANTES DE ÁREAS RELEVANTES NO PROCESSO TAIS COMO TI, SEGURANÇA DA INFORMAÇÃO, MARKETING, JURÍDICO, RH
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	A lei não exige um comitê, apenas o DPO. No entanto, o comitê é uma boa prática especialmente nos casos em que o DPO seja um prestador de serviço externo que não tenha intimidade com a estrutura e a realidade da empresa, facilitando a comunicação e o alinhamento das expectativas da organização à visão do consultor externo
# ETAPA	**3**
FASE	PREPARAÇÃO
ETAPA	Nomear o encarregado de Proteção de Dados (DPO)
OBJETIVO (POR QUÊ?)	A empresa deve designar um encarregado de proteção de dados (DPO) para monitorar o cumprimento da LGPD. O DPO é responsável por garantir a conformidade com a LGPD dentro da empresa, além de ser o ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO deve também reportar-se ao comitê gestor da LGPD na organização, provendo informação, solicitando apoio e submetendo ao comitê decisões chaves do processo para as quais não tenha plena liberdade de atuação
REFERÊNCIA ISO 27002	5.2
ENTRADAS	Requisitos e competências do DPO podem variar conforme o perfil da organização, podendo incluir profissionais com experiência em gestão de Tecnologia da Informação e Comunicação, Segurança da Informação, Auditoria de Sistemas, Controles Internos e Compliance, com vivência de processos de gestão de informações
SAIDAS / ENTREGAS ("O QUÊ?")	Nomeação do profissional que realizará o papel de DPO na organização
ETAPA ANTECESSORA (REQUERIDA)	1
ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART. 6 INCISO X ART 41.
# ETAPA	**4**
FASE	PREPARAÇÃO
ETAPA	Mapear / Identificar os dados pessoais/sensíveis tratados pela empresa e seu fluxo dentro da organização desde a coleta até o descarte

OBJETIVO (POR QUÊ?)	A empresa deve fazer um inventário para identificar, documentar e classificar os dados) que são coletados, armazenados, processados e compartilhados dentro da organização, bem como os meios utilizados para isso. Estes dados coletados devem ser classificados com relação ao seu teor (se dados pessoais, dados pessoais sensíveis, dados anonimizados, pseudoanonimizados). Além disso, deve mapear os fluxos pelos quais estas informações são coletadas, tratadas e descartadas pela empresa, de forma a identificar todos os processos que demandem revisão para averiguar sua adequação ao cumprimento dos requisitos da LGPD. A empresa deve iniciar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), também conhecido pela sigla DPIA em inglês. As informações que constam deste relatório deverão ser incluídas / revisadas / atualizadas ao longo de todo o processo de adequação a fim de assegurar o atendimento aos requisitos da LGPD.
REFERÊNCIA ISO 27002	5.9, 5.12, 5.13
ENTRADAS	LGPD ISO 27002 Dicionários de Dados dos sistemas Modelos de Dados dos sistemas Outros documentos dos sistemas, tais como manuais de fornecedor, Diagramas de Dados etc. Documentos de qualquer tipo e em qualquer meio que sejam utilizados para coleta, registro e processamento de dados pessoais e/ou dados pessoais sensíveis de clientes e/ou colaboradores da empresa
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Matriz de Dados pessoais e sensíveis, contendo sua origem (sistema, formulário ou outro tipo de documento), forma de registro e de guarda destes dados, período de retenção, classificação dos dados quanto ao tipo e criticidade, método de descarte e qualquer outra informação relevante para identificação e rastreamento do processo de coleta e tratamento destes dados
ETAPA ANTECESSORA (REQUERIDA)	3
ÁREAS / FUNÇÕES ENVOLVIDAS	TI, SEGURANÇA DA INFORMAÇÃO, DPO, MARKETING
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART. 5 ART. 38
# ETAPA	**5**
FASE	PREPARAÇÃO
ETAPA	Analisar a base legal para o tratamento de dados
OBJETIVO (POR QUÊ?)	A empresa deve avaliar se possui uma base legal válida para coletar, armazenar e processar os dados pessoais. Essas bases podem incluir consentimento, contrato, cumprimento de obrigação legal ou interesse

	legítimo. Esta avaliação deve considerar também uma análise quanto à suficiência dos dados coletados e processados, ou seja, os dados coletados e processados são aqueles estritamente necessários? A análise deve incluir também avaliação quanto à proporcionalidade do processamento realizado. São processadas as informações estritamente necessárias? O processamento é realmente necessário? Não existe outra maneira de alcançar o mesmo resultado?
REFERÊNCIA ISO 27002	5.31
ENTRADAS	RIPD, LGPD, ISO 27002 e outras leis, normas e regulamentos às quais a empresa esteja sujeita por atuar em um determinado setor, por força de contrato ou exigências do negócio.
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Artigos, parágrafos e trechos de legislação, regulamentações, portarias, normas que embasam o tratamento de dados pessoais de clientes e funcionários.
ETAPA ANTECESSORA (REQUERIDA)	4
ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO, DPO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 4, 6 E 7 ART 10 ART 11 ART 16 PARA PESSOAS JURÍDICAS DE DIREITO PÚBLICO: ART 23 A 32.
# ETAPA	**6**
FASE	PREPARAÇÃO
ETAPA	Análise de riscos
OBJETIVO (POR QUÊ?)	A empresa deve avaliar os riscos envolvidos na coleta, tratamento, transferência, descarte e qualquer outra etapa relacionada a dados pessoais/ sensíveis de usuários/clientes e colaboradores e adotar medidas para gerenciamento destes riscos que atendam aos requisitos da LGPD
REFERÊNCIA ISO 27002	A ISO 27002 não endereça riscos, eles devem ser tratados com base na norma ISO 27005
ENTRADAS	RIPD, LGPD, ISO 27002, 27005, Matriz de dados pessoais e sensíveis por sistema, mapas e diagramas de sistemas e de infraestrutura tecnológica, dentre outros.
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Mapa de Riscos com ações de mitigação implementadas ou a implementar e classificados por criticidade.
ETAPA ANTECESSORA (REQUERIDA)	5
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO

ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 50.
# ETAPA	**7**
FASE	PREPARAÇÃO
ETAPA	Elaborar cronograma geral do projeto
OBJETIVO (POR QUÊ?)	Elaborar um cronograma que sirva como guia geral do projeto considerando a criticidade dos riscos identificados e as medidas de gerenciamento
REFERÊNCIA ISO 27002	5.8
ENTRADAS	Mapa de Riscos com ações de mitigação implementadas ou a implementar e classificados por criticidade
SAIDAS / ENTREGAS ("O QUÊ?")	Cronograma geral do projeto com as etapas a serem implementadas
ETAPA ANTECESSORA (REQUERIDA)	6
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	A lei não exige um cronograma, mas como o prazo para adequação à lei já expirou, as empresas são passíveis de aplicação de sanções, é recomendável que seja elaborado um cronograma para gerenciamento adequado do projeto e atendimento aos requisitos da lei com a máxima celeridade possível.
# ETAPA	**8**
FASE	IMPLEMENTAÇÃO
ETAPA	Elaborar ou revisar as Políticas e procedimentos de Segurança da Informação, Proteção, Privacidade e Tratamento de Dados
OBJETIVO (POR QUÊ?)	A empresa deve elaborar políticas e procedimentos (ou revisar as existentes, se houver), com objetivo de definir papéis e responsabilidades de cada um dos envolvidos na gestão da segurança das informações e dos dados pessoais, as medidas a serem implementadas visando a proteção dos dados, gestão do acesso, proteção, monitoramento de incidentes, descarte de informações após uso e outros procedimentos necessários para atendimento aos requisitos da lei. Devem também ser elaborados os termos de responsabilidade a serem assinados por colaboradores e parceiros relativos ao sigilo e proteção dos dados processados pela organização, bem como os termos de autorização a serem assinados pelos usuários, clientes e colaboradores da empresa, detalhando o tipo de procedimento de tratamento de dados realizados, os compartilhamentos de dados realizados com parceiros da empresa, explicitando quais estes parceiros e os fins para os quais estas informações são tratadas e/ou compartilhadas. A empresa deve levar em conta os riscos envolvidos no tratamento de dados pessoais, definindo procedimentos e medidas para minimizar estes riscos e, quando possível e viável, eliminá-los por completo.
REFERÊNCIA ISO 27002	5.1, 5.31, 5.34, 5.37

ENTRADAS	RIPD, LGPD, ISO 27001, 27002, 27701, NIST PRIVACY FRAMEWORK, NIST CIBERSECURITY FRAMEWORK NORMAS ISO AUXILIARES: 27032, 27033, 27034, 27017, 27018 Outras leis, normas e regulamentos às quais a empresa esteja sujeita por atuar em um determinado setor, por força de contrato ou exigências do negócio
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Políticas e procedimentos de Segurança da Informação, Política de proteção de dados e de privacidade, monitoramento e gerenciamento de incidentes e outros que a empresa identifique serem necessários, Termo de Uso / Aceite das políticas de privacidade da organização a serem assinados / aceitos pelos usuários, clientes e colaboradores / Procedimentos para tratamento de dados, transferência de dados, descarte de dados, remoção de dados a pedido do titular.
ETAPA ANTECESSORA (REQUERIDA)	7
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 12. ART 50.
# ETAPA	**9**
FASE	IMPLEMENTAÇÃO
ETAPA	Revisar contratos com parceiros, fornecedores e demais envolvidos
OBJETIVO (POR QUÊ?)	A empresa deve revisar os contratos com fornecedores, parceiros e demais envolvidos a fim de incluir cláusulas de conformidade que assegurem a aplicação de medidas protetivas adequadas para os dados pessoais de clientes da organização acessados, tratados e processados por estes fornecedores. Toda e qualquer alteração nos contratos existentes, bem como elaboração de novos contratos com outros fornecedores e parceiros deve ser sempre seguida de atualização dos Termos de Autorização e nova coleta de autorização dos titulares de dados tendo em vista a lei estabelecer que a autorização deve ser explícita, e não genérica.
REFERÊNCIA ISO 27002	5.19, 5.20, 5.23, 8.30
ENTRADAS	RIPD, LGPD, ISO 27002, 27036 Políticas de privacidade elaboradas pela organização, contratos com fornecedores e parceiros que realizam processamento / tratamento de dados dos titulares. Outras leis, normas e regulamentos às quais a empresa esteja sujeita por atuar em um determinado setor, por força de contrato ou exigências do negócio
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Contratos com fornecedores e parceiros que realizam processamento / tratamento de dados pessoais dos titulares revisados/atualizados para atendimento aos requisitos da LGPD.

ETAPA ANTECESSORA (REQUERIDA)	8
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, JURÍDICO, TI, SEGURANÇA DA INFORMAÇÃO, CONTRATOS, COMPRAS
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART. 9 INCISO VI ART 14 § 3 ART 18 § 6 ART 33 INCISO II ART 37 A 40 ART 42 A 44 ART 46 E 47 ART 52

# ETAPA	**10**
FASE	IMPLEMENTAÇÃO
ETAPA	Obter o consentimento dos titulares dos dados
OBJETIVO (POR QUÊ?)	A empresa deve obter o consentimento explícito e formal dos titulares dos dados para coletar, tratar, processar e compartilhar seus dados pessoais. O termo deve conter as informações referentes à quais informações são coletadas, qual o objetivo, tempo de retenção, tipo de tratamento, propósito do tratamento, bem como deve explicitar que informações são transferidas / compartilhadas com outros parceiros e com qual propósito e finalidade e outras informações pertinentes para assegurar a transparência do processo ao titular dos dados. Implementar medidas para estabelecer de forma clara nos serviços de comunicação da empresa a publicação das políticas de privacidade e contato com a área responsável para que os direitos de titulares possam ser exercidos/solicitados.
REFERÊNCIA ISO 27002	5.10, 5.34
ENTRADAS	RIPD, LGPD, Termo de Uso / Aceite das políticas de privacidade da organização a serem assinados / aceitos pelos clientes, usuários, colaboradores. Os termos devem diferenciados e conter as informações pertinentes para cada uma destas categorias (clientes, usuários e colaboradores).
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Procedimentos para obtenção de consentimento dos titulares dos dados, incluindo clientes, fornecedores e colaboradores e suspensão dos serviços quando não houver consentimento. Identificar meios que permitam assegurar a evidência formal de consentimento dos titulares dos dados.
ETAPA ANTECESSORA (REQUERIDA)	9

ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, SEGURANÇA DA INFORMAÇÃO, RH, DPO, MARKETING, RELAÇÕES COM CLIENTES
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 7 INCISO I E § 3, 4, 5 E 7 ART 8 ART 9 § 1, 2 E 3 ART 11 INCISO I ART 14 § 1, 3, 4 E 5 NA HIPÓTESE DE TRANSFERÊNCIA INTERNACIONAL DE DADOS: ART 33 INCISO VIII
# ETAPA	**11**
FASE	IMPLEMENTAÇÃO
ETAPA	Preparação dos profissionais envolvidos
OBJETIVO (POR QUÊ?)	A empresa deve conscientizar seus colaboradores, fornecedores e demais envolvidos diretamente no processo sobre a importância da LGPD e como ela impacta o negócio. Além disso deve treiná-los e capacitá-los para garantir que entendam os requisitos da LGPD, as boas práticas de proteção de dados pessoais e as políticas e procedimentos de proteção de dados da empresa e as ferramentas, técnicas e métodos a serem implementados para assegurar a efetiva proteção dos dados com base nos requisitos da lei.
REFERÊNCIA ISO 27002	6.2 A 6.7
ENTRADAS	LGPD, Políticas e Procedimentos de Segurança da Informação e Privacidade elaboradas pela organização, ISO 27002, NIST PRIVACY FRAMEWORK e outras normas que possam servir de base para elaboração de material de treinamento e capacitação.
SAIDAS / ENTREGAS ("O QUÊ?")	Material de treinamento, manuais e instruções específicas para cada área envolvida. Registro de pessoal treinado, avaliação de aprendizagem do pessoal.
ETAPA ANTECESSORA (REQUERIDA)	9
ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, SEGURANÇA DA INFORMAÇÃO, RH, DPO, MARKETING
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 19 § 1 ART 46 A 50
# ETAPA	**12**
FASE	IMPLEMENTAÇÃO
ETAPA	Implementar medidas técnicas para garantir a segurança dos dados
OBJETIVO (POR QUÊ?)	A empresa deve implementar medidas de segurança para proteger os dados pessoais que coleta e processa. Isso inclui medidas técnicas e organizacionais, como implementação de sistemas de segurança e a elaboração de políticas e procedimentos internos, criptografia, anonimização, autenticação, controle de acesso e gestão de incidentes visando a prevenção de acessos não autorizados e a minimização de riscos de vazamentos.
REFERÊNCIA ISO 27002	5.2, 5.3, 5.4, 5.36, 5.37, 5.7, 5.8, 7.1, 7.2, 7.7, 7.10, 8.1. 8.2, 8.3, 8.5, 8.7, 8.8, 8.11, 8.12, 8.20, 8.21, 8.22, 8.24, 8.25, 8.26, 8.27

ENTRADAS	RIPD, LGPD, ISO 27002, 27017, 27018, 27032, 27033, 27034 NIST PRIVACY FRAMEWORK NIST CIBERSECURITY FRAMEWORK Políticas e Procedimentos de Segurança da Informação e Privacidade elaboradas pela organização
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Procedimentos para tratamento e proteção de dados
ETAPA ANTECESSORA (REQUERIDA)	11
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 19 § 1 ART 46 E 47 ART 49 E 50
# ETAPA	**13**
FASE	IMPLEMENTAÇÃO
ETAPA	Avaliar e implementar medidas para transferência internacional
OBJETIVO (POR QUÊ?)	Na hipótese de a empresa realizar a transferência internacional de dados, deve avaliar se atende aos requisitos estabelecidos nos artigos 33 a 36 da LGPD e definir procedimentos específicos para este caso.
REFERÊNCIA ISO 27002	5.19, 5.20, 5.23, 8.20, 8.21
ENTRADAS	RIPD, LGPD, ISO 27002, 27010, 27017, 27018, 27032, 27033, 27034 NIST PRIVACY FRAMEWORK NIST CIBERSECURITY FRAMEWORK Políticas e Procedimentos de Segurança da Informação e Privacidade elaboradas pela organização
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Procedimentos para transferência internacional de dados em conformidade com a legislação e contratos vigentes.
ETAPA ANTECESSORA (REQUERIDA)	9
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO, JURÍDICO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 33 A 36
# ETAPA	**14**
FASE	IMPLEMENTAÇÃO
ETAPA	Estabelecer um processo de gerenciamento e resposta a incidentes de segurança
OBJETIVO (POR QUÊ?)	A empresa deve estabelecer um processo para lidar com incidentes de segurança, incluindo um plano de resposta a incidentes de segurança, para lidar com vazamentos ou outras situações que possam afetar a segurança e/ou violar os dados pessoais, incluindo procedimentos para comunicação à autoridade nacional e ao titular dos dados em prazo razoável e conforme definido no parágrafo 1 do artigo 48 da lei.
REFERÊNCIA ISO 27002	5.24, 5.25, 5.26, 5.5, 5.7, 6.8, 8.15, 8.16
ENTRADAS	RIPD, LGPD, Políticas de Segurança da Informação e Privacidade

	elaboradas pela Organização, ISO 27002, 27004, NIST PRIVACY FRAMEWORK, NIST CIBERSECURITY FRAMEWORK.
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Procedimentos para monitoramento, gerenciamento e resposta à incidentes de segurança. Procedimento para comunicação de incidente de segurança à titulares dos dados, ANPD e demais partes interessadas.
ETAPA ANTECESSORA (REQUERIDA)	13
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO, JURÍDICO, MARKETING, RELAÇÕES COM CLIENTES, RELAÇÕES PÚBLICAS
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 48 ART 50 ART 52 INCISOS V, VI, X, XI E XII.
# ETAPA	**15**
FASE	IMPLEMENTAÇÃO
ETAPA	Implementar medidas para eliminação dos dados ao término do tratamento
OBJETIVO (POR QUÊ?)	A empresa deve definir procedimentos para eliminação dos dados após o fim do período de tratamento, quando a finalidade tiver sido alcançada, quando os dados deixem de ser necessários ou pertinentes à finalidade específica para a qual foram coletados ou por solicitação do titular.
REFERÊNCIA ISO 27002	8.10
ENTRADAS	RIPD, LGPD, ISO 27002, Políticas de Segurança da Informação e Privacidade elaboradas pela Organização, Termo de Uso / Aceite das políticas de privacidade da organização assinados / aceitos pelos clientes, usuários, colaboradores
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD atualizado, Procedimento para eliminação / remoção de dados ao término do tratamento.
ETAPA ANTECESSORA (REQUERIDA)	13
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO, JURÍDICO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 15 ART 16 ART 18 INCISO VI
# ETAPA	**16**
FASE	MANUTENÇÃO
ETAPA	Manter registros das atividades de tratamento de dados
OBJETIVO (POR QUÊ?)	A empresa deve manter registros de todas as atividades de tratamento de dados pessoais realizadas, incluindo informações sobre os titulares dos dados, finalidades do tratamento, dados compartilhados, entre outras informações. Além disso, deve elaborar um relatório de impacto à proteção de dados

	pessoais conforme estabelecido no artigo 38 da LGPD.
REFERÊNCIA ISO 27002	5.33, 8.15, 8.16
ENTRADAS	RIPD, LGPD, Políticas e procedimentos de Segurança da Informação e Privacidade elaboradas pela organização, em especial no que tange aos aspectos relativos ao tratamento de dados.
SAIDAS / ENTREGAS ("O QUÊ?")	Registro formal das atividades de tratamento de dados detalhando processo, responsáveis, data de início, término, ocorrências durante o processamento.
ETAPA ANTECESSORA (REQUERIDA)	15
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, TI, SEGURANÇA DA INFORMAÇÃO
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 9 ART 10 § 2 ART 37 A 40.
# ETAPA	**17**
FASE	MANUTENÇÃO
ETAPA	Atendimento aos direitos dos titulares
OBJETIVO (POR QUÊ?)	A empresa deve garantir o atendimento aos direitos dos titulares dos dados, como o direito de acesso, correção, exclusão, portabilidade e oposição ao tratamento de seus dados pessoais.
REFERÊNCIA ISO 27002	5.34
ENTRADAS	RIPD, LGPD, Políticas e procedimentos de Segurança da Informação e Privacidade elaboradas pela organização, Termo de Uso / Aceite das políticas de privacidade da organização aprovados pelos usuários. Formulário de solicitação de remoção de dados pelo Titular.
SAIDAS / ENTREGAS ("O QUÊ?")	Divulgação em meios adequados dos direitos dos titulares. Registro das atividades de atendimento aos direitos dos titulares aceitas e recusadas, com as devidas justificativas. Registro das atividades de atendimento aos direitos dos titulares aceitas e recusadas, com as devidas justificativas.
ETAPA ANTECESSORA (REQUERIDA)	15
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO, JURÍDICO, TI, SEGURANÇA DA INFORMAÇÃO, RH, MARKETING, RELAÇÕES COM CLIENTES
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 8 § 5 E 6. ART 9 ART 14 § 2 E 6 ART 15 INCISO III ART 17 a 22 ART 45 ART 48 ART 50 ART 52 § 7

	ART 60.
# ETAPA	**18**
FASE	MANUTENÇÃO
ETAPA	Treinamento, Conscientização e Capacitação - demais profissionais da organização.
OBJETIVO (POR QUÊ?)	A empresa deve conscientizar os demais colaboradores, fornecedores e prestadores de serviço sobre a importância da LGPD e como ela impacta o negócio. Além disso deve treiná-los e capacitá-los para garantir que entendam os requisitos da LGPD, as boas práticas de proteção de dados pessoais e as políticas e procedimentos de proteção de dados da empresa, bem como os procedimentos para atendimento à clientes e usuários e para direcionamento de suas solicitações relativas ao tema.
REFERÊNCIA ISO 27002	6.2 A 6.7
ENTRADAS	RIPD, LGPD, Políticas de Segurança da Informação e Privacidade elaboradas pela organização, ISO 27002, NIST PRIVACY FRAMEWORK e outras normas que possam servir de base para elaboração de material de treinamento e capacitação.
SAIDAS ENTREGAS "O QUÊ?"	Material de treinamento, manuais e instruções gerais para os colaboradores da empresa. Registro de pessoal treinado, avaliação de aprendizagem do pessoal.
ETAPA ANTECESSORA (REQUERIDA)	15
ÁREAS / FUNÇÕES ENVOLVIDAS	JURÍDICO, TI, SEGURANÇA DA INFORMAÇÃO, RH, DPO, MARKETING
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 19 § 1 ART 46 A 50
# ETAPA	**19**
FASE	MANUTENÇÃO
ETAPA	Implementar um processo de monitoramento que assegure a revisão e atualização periódica dos processos, políticas e procedimentos relacionados à LGPD
OBJETIVO (POR QUÊ?)	A fim de assegurar a manutenção e validade dos processos implementados, deve ser realizado monitoramento e revisão periódica dos processos, dos fluxos de dados, dos contratos com parceiros e fornecedores e todo e qualquer outro aspecto que possa demandar mudanças nos processos implementados nas etapas anteriores, de forma a assegurar a constante adequação da empresa aos requisitos da LGPD.
REFERÊNCIA ISO 27002	5.31, 5.36, 5.37
ENTRADAS	RIPD, Documentação dos processos implementados, novas demandas de coleta, alteração nos dados coletados, alteração nos contratos com parceiros, alterações nas regras de negócio que gerem mudança nos dados coletados ou nos processos de tratamento realizados pela empresa ou por seus parceiros.
SAIDAS / ENTREGAS ("O QUÊ?")	RIPD revisado e atualizado, requisições de mudança nos processos, políticas, procedimentos, contratos, termos de consentimento e outros

	documentos base para adequação à LGPD, de acordo com o tipo de mudança ocorrida.
ETAPA ANTECESSORA (REQUERIDA)	17
ÁREAS / FUNÇÕES ENVOLVIDAS	DPO E ÁREAS ENVOLVIDAS NOS PROCESSOS A SEREM ATUALIZADOS
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 50
# ETAPA	**20**
FASE	MANUTENÇÃO
ETAPA	Realizar auditorias regulares
OBJETIVO (POR QUÊ?)	A empresa deve realizar auditorias regulares para garantir que esteja em conformidade com a LGPD e para identificar possíveis riscos e vulnerabilidades em seu sistema de proteção de dados.
REFERÊNCIA ISO 27002	5.36
ENTRADAS	RIPD, LGPD, Políticas de Segurança da Informação e Privacidade elaboradas pela organização, Procedimentos para tratamento e proteção de dados, Procedimento para eliminação / remoção de dados ao término do tratamento e outras políticas, procedimentos e documentos definidas pela organização e pertinentes ao processo.
SAIDAS / ENTREGAS ("O QUÊ?")	Relatório de avaliação dos procedimentos abaixo com relação à sua adequação aos requisitos da lei: RIPD; Obtenção de consentimento do titular e de colaboradores da organização; Revisão das políticas e procedimentos de segurança da informação, privacidade e tratamento de dados; Contratos com fornecedores e terceiros; Medidas técnicas para garantir a segurança dos dados; Medidas para transferências internacionais de dados; Gerenciamento e resposta a incidentes de segurança; Medidas para eliminação dos dados ao término do tratamento; Registro das atividades de tratamento de dados; Atendimento aos direitos dos titulares; Treinamento e capacitação dos profissionais envolvidos; Treinamento e capacitação dos demais profissionais da organização; Relatório de avaliação do nível de aderência dos processos efetivamente executados aos procedimentos definidos.
ETAPA ANTECESSORA (REQUERIDA)	19
ÁREAS / FUNÇÕES ENVOLVIDAS	AUDITORIA INTERNA, SEGURANÇA DA INFORMAÇÃO, DPO, TI
ARTIGO DA LGPD BASE PARA A EXECUÇÃO DA ETAPA	ART 50

Fonte: Resultado da pesquis

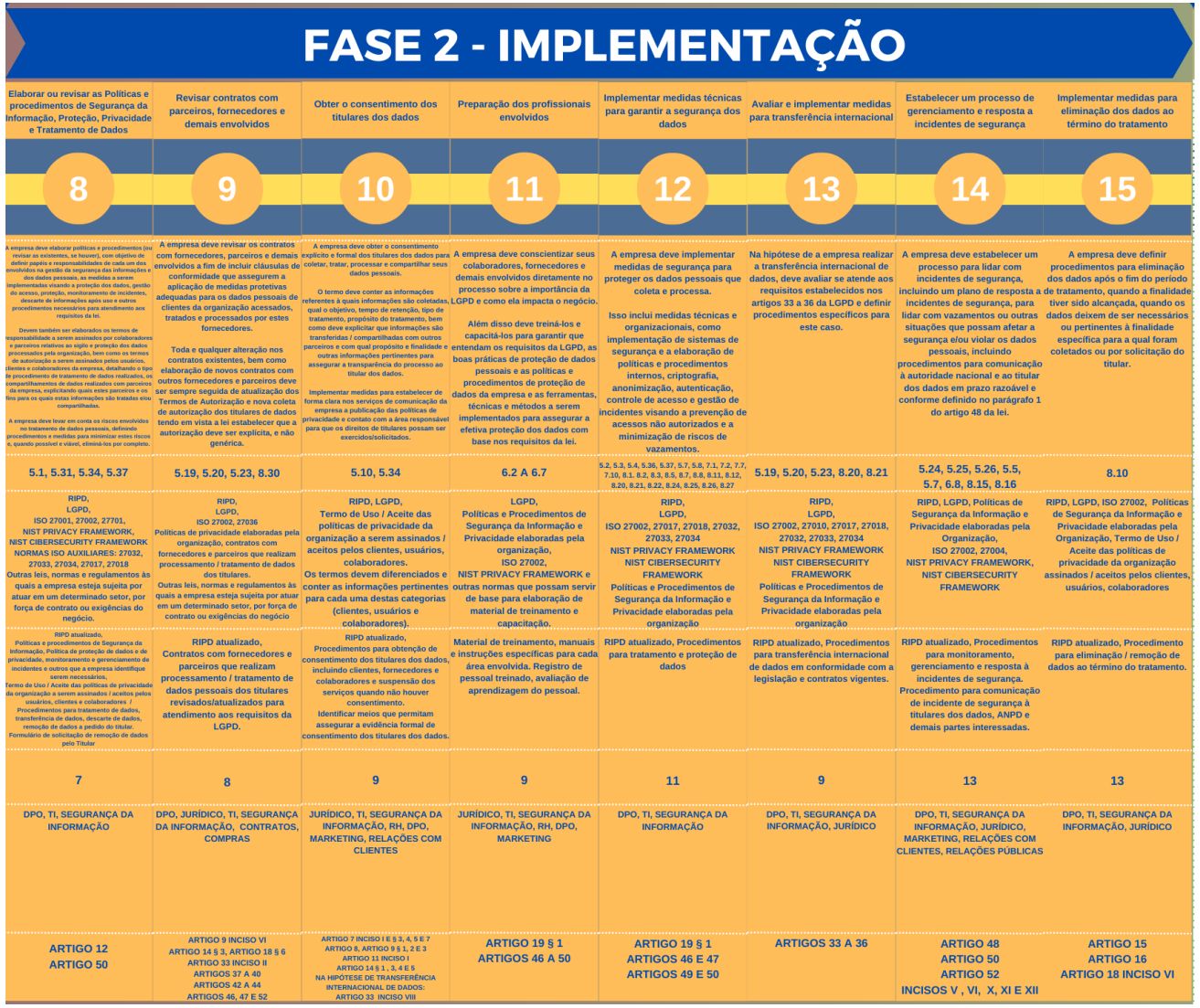
APÊNDICE G – FASE 1 - PREPARAÇÃO – RAEL

FASE 1 - PREPARAÇÃO

Etapa	1 – Avaliar necessidade de adequação à LGPD	2 – Constituir um comitê interno para Acompanhamento da LGPD	3 – Nomear o encarregado de Proteção de Dados (DPO)	4 – Mapear / Identificar os dados pessoais / sensíveis tratados pela empresa e seu fluxo dentro da organização desde a coleta até o descarte	5 – Analisar a base legal para o tratamento de dados	6 – Análise de riscos	7 – Elaborar cronograma geral do projeto
Objetivo	A empresa deve avaliar se está enquadrada nos requisitos de obrigatoriedade de adequação à LGPD. Além disso, deve verificar se existem normas, regulamentos, portarias ou outras normativas emitidas por órgãos regulatórios, agências governamentais e outras associações específicas do setor de atuação da organização que possam incluir regras específicas a serem seguidas pela organização, as quais devam também ser consideradas ao longo de todo o processo.	Nomear as pessoas dentro da organização que serão responsáveis pelo acompanhamento do projeto de adequação à LGPD e que darão o apoio e suporte necessários ao DPO e às áreas envolvidas. As responsabilidades do comitê incluem a seleção do DPO, que se reportará a este comitê, bem como decidir pontos essenciais do processo para os quais o DPO não tenha alçada. Em organizações de menor porte este comitê pode ser formado pelos sócios/proprietários da empresa e, quando houver uma estrutura organizacional mais adequada, deve considerar a participação de todos os stakeholders relevantes para o processo, que pode incluir representantes dos investidores, diretores de áreas chaves tais como Segurança da Informação, Tecnologia, Jurídico, Marketing e Recursos Humanos	A empresa deve designar um encarregado de proteção de dados (DPO) para monitorar o cumprimento da LGPD. O DPO é responsável por garantir a conformidade com a LGPD dentro da empresa, além de ser o ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO deve também reportar-se ao comitê gestor da LGPD na organização, provendo informação, solicitando apoio e submetendo ao comitê decisões chaves do processo para as quais não tenha plena liberdade de atuação	A empresa deve fazer um inventário para identificar, documentar e classificar os dado(s) que são coletados, armazenados, processados e compartilhados dentro da organização, bem como os meios utilizados para isso. Estes dados coletados devem ser classificados com relação ao seu teor (se dados pessoais, dados pessoais sensíveis, dados anonimizados, pseudoanonimizados). Além disso, deve mapear os fluxos pelos quais estas informações são coletadas, tratadas e descartadas pela empresa, de forma a identificar todos os processos que demandem revisão para averiguar sua adequação ao cumprimento dos requisitos da LGPD. A empresa deve iniciar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), também conhecido pela sigla DPIA em inglês. As informações que constam deste relatório deverão ser incluídas / revisadas / atualizadas ao longo de todo o processo de adequação a fim de assegurar o atendimento aos requisitos da LGPD.	A empresa deve avaliar se possui uma base legal válida para coletar, armazenar e processar os dados pessoais. Essas bases podem incluir consentimento, contrato, cumprimento de obrigação legal ou interesse legítimo. Esta avaliação deve considerar também uma análise quanto à suficiência dos dados coletados e processados, ou seja, os dados coletados e processados são aqueles estritamente necessários? A análise deve incluir também avaliação quanto à proporcionalidade do processamento realizado. São processadas as informações estritamente necessárias? O processamento é realmente necessário? Não existe outra maneira de alcançar o mesmo resultado?	A empresa deve avaliar os riscos envolvidos na coleta, tratamento, transferência, descarte e qualquer outra etapa relacionada a dados pessoais/ sensíveis de usuários/clientes e colaboradores e adotar medidas para gerenciamento destes riscos que atendam aos requisitos da LGPD	Elaborar um cronograma que sirva como guia geral do projeto considerando a criticidade dos riscos identificados e as medidas de gerenciamento
Item ISO 27002	Não se aplica	5.2	5.2	5.9, 5.12, 5.13	5.31	A ISO 27002 não endereça riscos, eles devem ser tratados com base na norma ISO 27005	5.8
Entradas	Artigos 3 A 7 da LGPD, normas e regulamentos específicos para o setor de atuação da empresa que possam afetar também as questões de proteção de dados.	Não há	Requisitos e competências do DPO podem variar conforme o perfil da organização, podendo incluir profissionais com experiência em gestão de Tecnologia da Informação e Comunicação, Segurança da Informação, Auditoria de Sistemas, Controles Internos e Compliance, com vivência de processos de gestão de informações	LGPD ISO 27002 Dicionários de Dados dos sistemas Modelos de Dados dos sistemas Outros documentos dos sistemas, tais como manuais de fornecedor, Diagramas de Dados etc. Documentos de qualquer tipo e em qualquer meio que sejam utilizados para coleta, registro e processamento de dados pessoais e/ou dados pessoais sensíveis de clientes e/ou colaboradores da empresa	RIPD, LGPD, ISO 27002 e outras leis, normas e regulamentos às quais a empresa esteja sujeita por atuar em um determinado setor, por força de contrato ou exigências do negócio.	RIPD, LGPD, ISO 27002, 27005, Matriz de dados pessoais e sensíveis por sistema, mapas e diagramas de sistemas e de infraestrutura tecnológica, dentre outros.	Mapa de Riscos com ações de mitigação implementadas ou a implementar e classificados por criticidade
Saídas / Entregas	Análise do enquadramento da empresa aos artigos 3 a 7 da LGPD e a outras normas e regulamentos que devam ser levados em consideração ao longo do processo de adequação.	Organograma do Comitê	Nomeação do profissional que realizará o papel de DPO na organização	RIPD atualizado, Matriz de Dados pessoais e sensíveis, contendo sua origem (sistema, formulário ou outro tipo de documento), forma de registro e de guarda destes dados, período de retenção, classificação dos dados quanto ao tipo e criticidade, método de descarte e qualquer outra informação relevante para identificação e rastreamento do processo de coleta e tratamento destes dados	RIPD atualizado, Artigos, parágrafos e trechos de legislação, regulamentações, portarias, normas que embasam o tratamento de dados pessoais de clientes e funcionários.	RIPD atualizado, Mapa de Riscos com ações de mitigação implementadas ou a implementar e classificados por criticidade.	Cronograma geral do projeto com as etapas a serem implementadas
Etapa Antecessora	Não há	Não Há	1	3	4	5	6
Áreas / Funções Envolvidas	JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO	COMITÊ EXECUTIVO, SÓCIOS, PROPRIETÁRIOS, REPRESENTANTES DE ÁREAS RELEVANTES NO PROCESSO TAIS COMO TI, SEGURANÇA DA INFORMAÇÃO, MARKETING, JURÍDICO, RH	COMITÊ INTERNO DA LGPD, JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO	TI, SEGURANÇA DA INFORMAÇÃO, DPO, MARKETING	JURÍDICO, TI, RH E SEGURANÇA DA INFORMAÇÃO, DPO	DPO, TI, SEGURANÇA DA INFORMAÇÃO	DPO, TI, SEGURANÇA DA INFORMAÇÃO
Artigo(s) da LGPD	ARTIGOS 3 A 7 Outras normas e regulamentos que se apliquem	A lei não exige um comitê, apenas o DPO. No entanto, o comitê é uma boa prática especialmente nos casos em que o DPO seja um prestador de serviço externo que não tenha intimidade com a estrutura e a realidade da empresa, facilitando a comunicação e o alinhamento das expectativas da organização à visão do consultor externo	ARTIGO 6 INCISO X ARTIGO 41	ARTIGO 5 ARTIGO 38	ARTIGOS 4, 6 E 7 ARTIGOS 10, 10 E 16 PARA PESSOAS JURÍDICAS DE DIREITO PÚBLICO: ART 23 A 32	ARTIGO 50	A lei não exige um cronograma, mas como o prazo para adequação à lei já expirou, as empresas são passíveis de aplicação de sanções, é recomendável que seja elaborado um cronograma para gerenciamento adequado do projeto e atendimento aos requisitos da lei com a máxima celeridade possível.

Fonte: Resultado da pesquisa

APÊNDICE H – FASE 2 - IMPLEMENTAÇÃO – RAEL



Fonte: Resultado da pesquisa

APÊNDICE I – FASE 3 - MANUTENÇÃO – RAEL

Fonte: Resultado da Pesquisa

APÊNDICE J – VISÃO GERAL DO RAEL COM TODAS AS FASES

Fonte: Resultado da pesquisa

APÊNDICE K – AVALIAÇÃO DA ETAPA DE DEMONSTRAÇÃO DO RAEL

CÓDIGO DA ETAPA	ETAPA	COMENTÁRIO	ORIGEM	RÉPLICA	AÇÃO
B	Nomear o encarregado de Proteção de Dados (DPO)	NOS OBJETIVOS DA ETAPA: Muitas vezes o DPO é um agente externo à empresa, com pouco conhecimento sobre os processos internos. Dessa forma, entendo que inicialmente, avaliada a necessidade de adequação à LGPD, antes de nomear um DPO, deve-se criar um comitê com pessoas familiarizadas com os processos da empresa que será responsável por coordenar o processo. Daí nomear um DPO que poderá fazer parte desse comitê.	PLANILHA	Concordo com a observação, que é totalmente pertinente. A sugestão será acatada, com a inclusão de um item anterior à nomeação do DPO, para formação do comitê gestor da LGPD, que deve prover *sponsorship* e guiar o processo sob a ótica da alta gestão da empresa.	Incluir etapa de elaboração do conselho gestor da LGPD
C	Mapear / Identificar os dados pessoais / sensíveis tratados pela empresa	NOS OBJETIVOS DA ETAPA: Tão importante quanto identificar os dados é mapear o fluxo dos mesmos dentro da empresa. No fluxo podem ser identificados vários detalhes que tem potencial para afetar a privacidade.	PLANILHA	Concordo, não está claro no conteúdo do *roadmap* que este mapeamento incluiria o fluxo dos dados.	Alterar o teor do item para enfatizar o mapeamento dos dados pessoais / sensíveis, bem como o fluxo destes dados na empresa.
C	Mapear / Identificar os	NO ITEM OBJETIVO: Talvez adicionar a	PLANILHA	Concordo, a classificação dos dados	Alterar o teor do item para incluir também o

	dados pessoais / sensíveis tratados pela empresa	palavra "classificar": pessoais / pessoais sensíveis / pessoais anonimizados		também é importante nesta etapa, pois nem todos os dados têm a mesma criticidade e deve ter o mesmo nível de tratamento.	termo classificação dos dados quanto à sua criticidade, necessidade de anonimização / proteção.
C	Mapear / Identificar os dados pessoais / sensíveis tratados pela empresa	NAS ENTRADAS: As entradas não precisam ter necessariamente somente foco sistêmico. É possível que dados pessoais sejam coletados por papel, formulário, documento ou até por um humano atendendo o outro. E podem ser armazenados e tratados nesse formato. Daí também a importância do fluxo.	PLANILHA	Concordo, o foco sistêmico dá ênfase do *roadmap* para empresas de médio a grande porte.	Alterar o teor do item para não focar apenas em sistemas, mas nos meios em que as informações sejam mantidas, quer sejam sistemas, planilhas ou outros.
E	Análise de riscos tecnológicos	TÍTULO DA ETAPA: Penso que o título deveria ser apenas "Análise de riscos". Isso porque temos outros tipos de risco que não tecnológicos que precisam ser avaliados. Como por exemplo no próprio processo de coleta do dado. Imagine uma atendente pedindo o CPF verbalmente. Muito importante nessa etapa também é classificar o risco	PLANILHA	Concordo, o enfoque sistêmico dá sempre um viés muito específico e que deixa de cobrir outros aspectos tão importantes quanto e que acabam sendo deixados de fora quando a ênfase fica apenas nos sistemas da empresa. Concordo também que a classificação dos riscos é importante para a priorização das ações de adequação.	Alterar a redação do item para revisar os riscos relativos à privacidade de dados, independente de em que meio. Incluir na redação do item a classificação dos riscos para posterior priorização das ações de adequação. Alterar também o item que trata da implementação das ações para incluir no critério de priorização das medidas a classificação dos riscos

		(baixo/moderado/alto) para lá na frente, na implementação, criar medidas de mitigação de acordo com a classificação do risco.			
E	Análise de riscos tecnológicos	NOS OBJETIVOS DA ETAPA: No tratamento, coleta etc.	PLANILHA	Concordo, o enfoque sistêmico dá sempre um viés muito específico e que deixa de cobrir outros aspectos tão importantes quanto e que acabam sendo deixados de fora quando a ênfase fica apenas nos sistemas da empresa. Concordo também que a classificação dos riscos é importante para a priorização das ações de adequação.	Alterar a redação do item para revisar os riscos relativos à privacidade de dados, independente de em que meio. Incluir na redação do item a classificação dos riscos para posterior priorização das ações de adequação. Alterar também o item que trata da implementação das ações para incluir no critério de priorização das medidas a classificação dos riscos
E	Análise de riscos tecnológicos	NAS SAÍDAS/ENTREGAS: Pois é, penso que as saídas devem incluir outros mapeamentos de risco que não estejam somente ligados à sistemas tecnológicos.	PLANILHA	Concordo, o enfoque sistêmico dá sempre um viés muito específico e que deixa de cobrir outros aspectos tão importantes quanto e que acabam sendo deixados de fora quando a ênfase fica apenas nos sistemas da empresa. Concordo também que a classificação dos riscos é importante para a priorização das ações de adequação.	Alterar a redação do item para revisar os riscos relativos à privacidade de dados, independente de em que meio. Incluir na redação do item a classificação dos riscos para posterior priorização das ações de adequação. Alterar também o item que trata da implementação das ações para incluir no critério de priorização das medidas a classificação dos riscos

F	Elaborar ou revisar as políticas e procedimentos de segurança da informação, privacidade e tratamento de dados	NOS OBJETIVOS: Não seria legal mencionar algo em relação à elaboração de um DPIA ? (art.38) Ou em outra fase?	PLANILHA	A sugestão de inclusão do DPIA é válida, só não sei se aqui ou em outra fase, como apontado no próprio comentário.	Foi incluída a elaboração do DPIA (na verdade, foi utilizado o termo RPID, em português) como saída da etapa 4. Todas as demais etapas à partir da 4 foram revisadas para incluir na entrada o RIPD e na saída o RIPD atualizado, quando pertinente.
F	Elaborar ou revisar as políticas e procedimentos de segurança da informação, privacidade e tratamento de dados	NAS SAÍDAS/ENTREGAS: É preciso criar também uma política de proteção de dados que deve fornecer diretrizes gerais para os problemas de privacidade de dados relacionados à coleta, uso, processamento, divulgação, monitoramento etc. dos dados pessoais dentro da empresa.	PLANILHA	O que eu havia mencionado como sendo procedimento de privacidade seria o que corresponderia à esta política de proteção de dados, mas creio que a mudança na redação seja benéfica, deixando mais específico o teor desta política e sua abrangência	Alterar a redação no que diz respeito à procedimentos de segurança da informação, privacidade para deixar mais específica a implementação de uma política de proteção de dados e sua abrangência.
G	Revisar contratos com parceiros, fornecedores e demais envolvidos	Talvez pudesse existir uma etapa com foco na implementação de um SGPD (sistema de gerenciamento de proteção de dados) com objetivo de implementar, monitorar, avaliar e melhorar as políticas, planos, procedimentos, práticas, controles e ferramentas técnicas. Dá para usar como	PLANILHA	A própria LGPD é uma exigência de implementação de um sistema com este foco, entendo que as medidas sugeridas para implementação ao longo do *roadmap* visam justamente implementar tal sistema, mesmo que ele não seja formalmente assim designado.	As políticas e procedimentos apontados como saídas ao longo das etapas do *Roadmap* tem por objetivo o gerenciamento de proteção de dados, o processo como um todo visa justamente o gerenciamento de proteção de dados, que é o foco da LGPD. A GDPR tem uma abrangência relativamente diferente, podendo levar à

		base as "medidas técnicas e organizacionais" da GDPR			questionamentos sobre o objetivo do *roadmap*.
H	Obter o consentimento dos titulares dos dados	OBJETIVO DA ETAPA: Penso ser importante mencionar que a coleta deve conter o objetivo, tempo, finalidade etc.	PLANILHA	Concordo... Elaborar melhor o teor do consentimento incluindo o que ele deve contemplar torna o documento mais consistente.	Revisar o item e incluir a menção no termo de consentimento dos titulares de dados do objetivo da coleta e tratamento, tempo de retenção, finalidade, etc.
M	Implementar medidas para eliminação dos dados ao término do tratamento	SAÍDAS/ENTREGAS: Talvez fosse interessante mencionar também sobre a necessidade de se estabelecer de forma clara nos serviços de comunicação da empresa a publicação das políticas de privacidade e contato com a área responsável para que os direitos de titulares etc. possam ser exercidos / solicitados. (art. 18)	PLANILHA	Concordo, não sei apenas se seria neste item ou em outro, como na própria obtenção do consentimento, ou se incluiria um item sobre implementação de medidas para divulgação das políticas de tratamento de dados e privacidade da empresa.	Avaliar de que forma implementar a sugestão, se no próprio item, em outro ou por meio da inclusão de um novo item. Requer a revisão do *roadmap* para verificar como contemplar este item.
N	Manter registros das atividades de tratamento de dados	INCLUIR ETAPA: Entendo que falte uma etapa de revisão dos dados que são coletados. Por exemplo, a atividade pode mudar e existirem dados que não são mais necessários.	PLANILHA	Concordo, avaliar de que forma implementar, por ser um processo contínuo, talvez um procedimento de revisão periódico seja o melhor.	Definida uma etapa denominada: Implementar um processo de monitoramento que assegure a revisão e atualização periódica dos processos, políticas e procedimentos relacionados à LGPD
GERAL	*ROADMAP* COMO UM TODO	GERAL: Qual o público-alvo do *Roadmap*? Não ficou	ENTREVISTA	Realmente a explicitação do *roadmap* tendo como	Incluir no modelo título do *roadmap,* onde deve constar o seu propósito

		claro, mas pela forma como foi desenvolvido o público-alvo são empresas de grande porte. É importante, se ele for destinado à um nicho específico, deixar isso claro.		público-alvo empresas de TI não foi incluída na versão encaminhada para avaliação.	como sendo empresas em geral. Além disso, revisar o *roadmap* como um todo ajustando terminologia para que possa ser também lido e utilizado por outras empresas.
GERAL	ÁREAS ENVOLVIDAS (COMO UM TODO, E NÃO DE UM ÍTEM ESPECÍFICO)	ÁREAS ENVOLVIDAS: O GERAL: ÁREAS ENVOLVIDAS pressupõe que existam estas estruturas departamentais, o que, novamente, indica um foco em empresas de grande porte. Se este não for o único foco, deve-se deixar claro que não são áreas, mas sim atividades, que podem ser realizadas por uma ou duas pessoas, dependendo da organização, ou até mesmo serem todas realizadas por uma única pessoa, no caso das pequenas e médias empresas.	ENTREVISTA	Concordo, a terminologia empregada acaba por direcionar a aplicação do *roadmap* para empresas de grande porte.	Revisar o *roadmap* como um todo ajustando terminologia para que, embora seja voltado a empresas de TI, possa ser também lido e utilizado por outras empresas
GERAL	FOCO EM SISTEMAS	FOCO DO *ROADMAP*: O *roadmap* tem um foco muito grande em mencionar ajustes, correções, implementações em sistemas informatizados. No entanto, pequenas	ENTREVISTA	Entendo ser uma adição importante o ajuste da terminologia para que se adeque não apenas a sistemas, pois dados pessoais sensíveis podem existir também em outros meios e devem também ser	Revisar todo o *roadmap* com a aplicação de uma terminologia mais ampla que não restrinja o escopo apenas à revisão sistêmica, mas sim, revisão de todas as informações pessoais.

		empresas talvez não tenham um sistema informatizado, mas nem por isso deixam de ter que atender à LGPD quando ela coletar e tratar dados de clientes.		tratados e endereçados	
GERAL	ESTRUTURA DO *ROADMAP*	GERAL: Apesar dos comentários realizados, o *roadmap* em si é uma ideia excelente, que com certeza será muito útil para empresas, pois serve como um guia geral, e com pequenos ajustes pode se tornar uma valiosa ferramenta de apoio e orientação para empresas no seu processo de adequação à LGPD	ENTREVISTA	O ajuste da terminologia do *roadmap para* que o mesmo possa ser utilizado por empresas de qualquer setor e de qualquer porte é relevante, e será considerado na revisão.	Revisar o *roadmap* como um todo ajustando terminologia para que, embora seja voltado a empresas de TI, possa ser também lido e utilizado por outras empresas
GERAL	USAR A GDPR com base para melhorar o teor do *roadmap*.	USO DA GDPR: Embora a LGPD tenha se baseado na GDPR, tem grandes lacunas no que diz respeito ao aprofundamento do tema. A impressão é de que a LGPD tenha sido elaborada às pressas com um sumário dos principais itens da GDPR, mas trata alguns temas de forma superficial, sem detalhe, e quando buscamos o mesmo tema na GDPR	ENTREVISTA	Toda sugestão que possa melhorar o *design* e a relevância da ferramenta são importantes e serão consideradas na revisão.	Como melhoria futura, revisar a GDPR e identificar se, conforme sugestão, a mesma pode indicar medidas mais específicas e que possam servir também para a adequação de empresas à LGPD.

	percebe-se que lá os itens têm mais detalhe e estão explicados de forma mais clara. Por este motivo, recomendo a revisão do *ROADMAP* com um enfoque da GDPR no sentido de prover maiores detalhes sobre o que deve ser feito.

Fonte: Resultado da pesquisa

APÊNDICE L – TCLE APRESENTADO AOS AVALIADORES

Avaliação do RAETEL - *Roadmap* para Adequação de Empresas de TEcnologia à LGPD

O questionário tem por objetivo obter as impressões do entrevistado quanto ao RAETEL - *Roadmap* para Adequação de Empresas de TEcnologia à LGPD. São coletadas informações com relação ao perfil do entrevistado, bem como suas avaliações com relação ao *Roadmap* quanto à sua relevância, completude, facilidade de entendimento, aplicação e pertinência.

A pesquisa leva entre 8 e 20 minutos para ser concluída, dependendo dos comentários sobre algumas questões.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado a participar da avaliação do *ROADMAP* **RAETEL** - ***R****oadmap* para **A**dequação de **E**mpresas de **TE**cnologia à **L**GPD e sua seleção foi por conveniência em virtude de nossas conexões profissionais e de sua experiência profissional ser considerada relevante para prover um feedback adequado sobre o *roadmap*.

O(s) objetivo(s) do RAETEL é servir de apoio à empresas do setor de tecnologia da informação no processo de adequação à LGPD (quer seja uma empresa que já tenha se adequado, servindo de apoio para avaliar sua adequação, ou uma empresa que ainda não tenha se adequado, apontando as etapas a serem cumpridas para adequação da empresa).

As informações obtidas por meio desta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação.
Os dados serão divulgados de forma a não possibilitar sua identificação, protegendo e assegurando sua privacidade.

A qualquer momento você poderá tirar suas dúvidas sobre o projeto e sua participação.

Ao final desta pesquisa, o trabalho completo será disponibilizado no site do Programa de Mestrado.

Ao continuar com o preenchimento do formulário você declara que entendeu os objetivos de sua participação na pesquisa e concorda em participar. Registra também que concorda com o tratamento de seus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Sua contribuição muito engrandecerá nosso trabalho pois você nos trará uma visão específica pautada na sua experiência sobre o assunto.

Esclarecemos, contudo, que sua participação não é obrigatória. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição proponente.

Caso deseje obter acesso aos resultados da pesquisa, pode enviar solicitação por e-mail para mauricio.munhoz@cpspos.sp.gov.br

APÊNDICE M – QUESTIONÁRIO PARA AVALIAÇÃO DO RAEL

Item	Questão
Q1	Qual seu tempo de experiência profissional? • Menos de 1 ano • 1 a 3 anos • 3 a 5 anos • 5 a 10 anos • Mais de 10 anos
Q2	Qual seu departamento dentro de sua organização? • Tecnologia da Informação • Segurança da Informação • Auditoria de Sistemas • Controles Internos • *Compliance* • Outro (indique)
Q3	Qual seu nível hierárquico dentro de sua organização? • estagiário / *trainee* / Júnior • Pleno ou Sênior • Coordenador / Supervisor • Gerente • Diretor
Q4	As etapas do *roadmap* são relevantes para a adequação de empresas à LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente
Q5	Caso deseje, insira seus comentários sobre a resposta ao item 4 do questionário:
Q6	As etapas do *roadmap* são suficientes para a adequação de empresas à LGPD? • Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente
Q7	Caso deseje, insira seus comentários sobre a resposta ao item 6 do questionário:
Q8	As etapas do *roadmap* estão em uma ordem adequada para o desenvolvimento do processo de adequação à LGPD?

- Concordo totalmente
- Concordo parcialmente
- Nem discordo e nem concordo
- Discordo parcialmente
- Discordo totalmente

Q9 Caso deseje, insira seus comentários sobre a resposta ao item 8 do questionário:

Q10 As informações que constam de cada etapa do *roadmap* são suficientes para prover orientação para a adequação à LGPD?

- Concordo totalmente
- Concordo parcialmente
- Nem discordo e nem concordo
- Discordo parcialmente
- Discordo totalmente

Q11 Caso deseje, insira seus comentários sobre a resposta ao item 10 do questionário:

Q12 O *roadmap* é relevante para a identificação de processos a serem implementados para a adequação de empresas à LGPD?

- Concordo totalmente
- Concordo parcialmente
- Nem discordo e nem concordo
- Discordo parcialmente
- Discordo totalmente

Q13 Caso deseje, insira seus comentários sobre a resposta ao item 12 do questionário:

Q14 O *roadmap* auxilia na identificação de processos, políticas e procedimentos relevantes para a adequação de empresas à LGPD?

- Concordo totalmente
- Concordo parcialmente
- Nem discordo e nem concordo
- Discordo parcialmente
- Discordo totalmente

Q15 Caso deseje, insira seus comentários sobre a resposta ao item 14 do questionário:

Q16 O *roadmap* tem aplicabilidade para empresas de setores que não o de tecnologia da informação?

- Concordo totalmente
- Concordo parcialmente
- Nem discordo e nem concordo
- Discordo parcialmente
- Discordo totalmente

Q17 Caso deseje, insira seus comentários sobre a resposta ao item 16 do questionário:

Q18 O *roadmap* tem aplicabilidade para empresas de qualquer porte?

	• Concordo totalmente • Concordo parcialmente • Nem discordo e nem concordo • Discordo parcialmente • Discordo totalmente
Q19	Caso deseje, insira seus comentários sobre a resposta ao item 18 do questionário:
Q20	Você tem alguma sugestão de melhoria ou modificação ao *roadmap*?

Fonte: Resultado da pesquisa