



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

Lei de Acesso à Informação (LAI): Uma Análise Multicritério sobre os Principais Riscos do Compartilhamento de Dados

Jorge Vinícios da Rocha Moreira

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador

Prof. Dr. João Gabriel de Moraes Souza

Brasília
2026

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

JM8318l
l Jorge Vinivios da Rocha, Moreira
Lei de Acesso à Informação (LAI): Uma Análise
Multicritério sobre os Principais Riscos do Compartilhamento
de Dados / Moreira Jorge Vinivios da Rocha; orientador Souza
João Gabriel de Moraes. Brasília, 2026.
132 p.

Dissertação(Mestrado em Ciência da Informação)
Universidade de Brasília, 2026.

1. Lei de Acesso à Informação. 2. Riscos . 3.
Compartilhamento de Dados. 4. Tomada de Decisão. 5. Análise
Multicritério. I. João Gabriel de Moraes, Souza, orient. II.
Título.



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

Lei de Acesso à Informação (LAI): Uma Análise Multicritério sobre os Principais Riscos do Compartilhamento de Dados

Jorge Vinícios da Rocha Moreira

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. João Gabriel de Moraes Souza (Orientador)
CIC/UnB

Profa. Dra. Simone Borges Simão Monteiro Profa. Dra. Viviane Vasconcellos Ferreira Grubisic
Universidade de Brasília Universidade Federal de Santa Catarina

Profa. Dra. Edna Dias Canedo
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 16 de março de 2026

Dedicatória

Dedico este trabalho, parafraseando a obra “Vidas Secas” de Graciliano Ramos (1938), eu dedico este trabalho a vocês escolheram me acompanhar; apoiar e ajudar; tiveram de se adaptar às minhas faltas e ausências; abdicaram de muito e mesmo assim, optaram por ser sombra, força e descanso na minha jornada de aprendizado.

Dedico este trabalho ao meu Sr. Jesus Cristo, uma vez que "tudo foi feito por meio dele, e sem ele nada do que foi feito teria sido feito".

À minha mãe, e ao meu pai (in memoriam), por me mostrarem que “o que Deus quer, é ver a gente ser capaz de ficar alegre no meio da alegria, e ainda mais alegre no meio da tristeza!”, e por acreditarem que o investimento em educação está entre as melhores coisas que podemos fazer nesta vida.

À minha esposa, a Flor que traz cor à minha vida, pela sua perseverança, juntos, temos aprendido que “o correr da vida embrulha tudo, e o que ela quer da gente é coragem”, para tentarmos ser mais e melhor, um para o outro.

As minhas irmãs e ao meu irmão; porque, com vocês eu aprendi o sentido da vida coletiva, e que “o mais importante e bonito do mundo é isto: que as pessoas não estão sempre iguais, ainda não foram terminadas, mas que elas vão sempre mudando” e que eu preciso de tempo e presença para perceber isto.

As minhas sobrinhas e sobrinho, por serem exemplos de determinação, força e resiliência para mim, sempre me lembrando que “viver é muito perigoso; e não é não!”.

Agradecimentos

Agradeço ao meu orientador, Professor Dr. João Gabriel de Moraes Souza, pelo direcionamento, apoio e confiança nos potenciais do pesquisador e da pesquisa. O seu direcionamento e participação como “timoneiro” de águas, muitas vezes agitadas, horas claras e horas turvas, foi importante.

Aos outros professores do Programa de Pós-Graduação em Computação Aplicada (PPCA/UnB), a minha gratidão pelos ensinamentos e orientações técnicas que me prepararam para que eu conseguisse ver mais longe nas “grandes navegações” da busca pelo conhecimento acadêmico.

Aos amigos e parceiros da turma “PPCA 2023.2”, eu lhes dedico a minha gratidão por cada apoio, conquista, batalhas e amizades construídas, especialmente pelo ensino que “guerra é guerra”, e que nela precisamos caminhar com estratégia!

Resumo

Esta dissertação analisa os principais riscos do compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação, com vistas a fundamentar e estruturar um framework de governança alinhado à ABNT NBR ISO 31000:2018. O estudo parte da lacuna existente entre a previsão normativa de transparência e a ausência de modelos decisórios capazes de incorporar o risco como variável relevante no tratamento de pedidos formulados com base na Lei de Acesso à Informação. Trata-se de pesquisa aplicada, exploratória, bibliográfica e documental, com abordagem predominantemente quantitativa e suporte qualitativo na seleção, validação e interpretação dos riscos. O percurso metodológico compreendeu revisão bibliométrica com apoio da TEMAC e do software VOSviewer®, análise normativa e documental, identificação e organização tipológica dos riscos, bem como a aplicação integrada da FMEA, da AHP-AIJ e da normalização Mini-Max para sua hierarquização. hierarquizar os riscos do processo analisado e identificar, entre os mais críticos, transparência excessiva, exposição indevida de dados e violação de direitos. Como principal contribuição aplicada, a pesquisa fundamenta e estrutura o LAI-Risk Governance Framework (LAI-RGF), concebido para converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional no setor público.

Palavras-chave: compartilhamento de dados; Lei de acesso à informação; riscos; tomada de decisão; análise multicritério

Abstract

This dissertation analyzes the main risks associated with public data sharing in the process of responding to access to information requests, with the aim of grounding and structuring a governance framework aligned with ABNT NBR ISO 31000:2018. The study is based on the gap between the normative provision of transparency and the absence of decision-making models capable of incorporating risk as a relevant variable in the handling of requests submitted under Brazil's Access to Information Law. This is an applied, exploratory, bibliographic, and documentary study, with a predominantly quantitative approach and qualitative support in the selection, validation, and interpretation of risks. The methodological path comprised a bibliometric review supported by TEMAC and the VOSviewer® software, normative and documentary analysis, identification and typological organization of risks, as well as the integrated application of FMEA, AHP-AIJ, and Min-Max normalization for their prioritization. It also enabled the prioritization of the risks in the analyzed process and the identification, among the most critical, of excessive transparency, undue data exposure, and rights violations. As its main applied contribution, the study grounds and structures the LAI-Risk Governance Framework (LAI-RGF), designed to convert risk prioritization into institutional decisions, treatment measures, and organizational learning in the public sector.

Keywords: compartilhamento de dados; Lei de acesso à informação; riscos; tomada de decisão; análise multicritério

Sumário

1	Introdução	1
1.1	Justificativa	1
1.2	Problema de Pesquisa	3
1.3	Objetivos	4
1.3.1	Objetivo Geral	4
1.3.2	Objetivos Específicos	4
1.4	Contribuições da Pesquisa	4
1.5	Estrutura da Pesquisa	5
2	Embasamento Teórico	6
2.1	Referencial Teórico	6
2.2	Aplicação da Teoria do Enfoque Meta Analítico (TEMAC)	8
2.2.1	Preparação da Pesquisa (Etapa 1)	9
2.2.2	Apresentação e Inter-relação dos Dados (Etapa 2)	10
2.2.3	Detalhamento, Modelo Integrador e Validação por Evidências (Etapa 3)	15
2.3	Sociedade da Informação	25
2.4	Acesso à Informação	26
2.5	Compartilhamento de Dados	32
2.6	Riscos	35
2.7	Processo de Tomada de Decisão	37
2.8	Análise de Modos e Efeitos de Falha (FMEA)	39
2.9	Análise Hierárquica de Processo (AHP)	44
2.9.1	Estruturação do Problema	45
2.9.2	Definição das Prioridades	46
2.9.3	Avaliação da Consistência Lógica	48
2.10	Algoritmo Mini-Max	49

3	Metodologia	51
3.1	Levantamento Bibliográfico	52
3.2	Fase de Identificação	53
3.3	Fase de Priorização	53
3.4	Hierarquização e Normalização	55
3.5	Ranking de Riscos	58
3.6	Governança dos Riscos	59
4	Resultados e Discussão	61
4.1	Perfil dos Participantes	61
4.2	Análise Sistemática dos Modos de Falha e seus Efeitos (FMEA)	62
4.3	Análise Hierárquica de Processos (AHP)	66
4.3.1	Estruturação do Problema	66
4.3.2	Definição das Prioridades	67
4.3.3	Avaliação da Consistência Lógica	69
4.3.4	Matriz AHP Consolidada (AHP-AIJ)	70
4.4	Modelo de Normalização – FMEA e AHP-AIJ	73
4.4.1	Normalização e Ranqueamento	73
4.5	<i>Framework</i> de Gestão de Riscos	75
5	Considerações Finais	85
5.1	Objetivos e Resultados Obtidos na Pesquisa	85
5.2	Limitações da Pesquisa	86
5.3	Sugestões para Trabalhos Futuros	87
	Referências	88
	Apêndice	103
A	Modelo Integrador da Teoria do Enfoque Meta Analítico (TEMAC)	104
B	Formulário On-line para Hierarquização Utilizando a Análise de Modos e Efeitos de Falha (FMEA)	106
C	Lista de tipologia conforme INC MP/CGU nº 1/2016 e riscos priorizados por especialistas	108
D	Análise de Modos e Efeitos de Falha (FMEA) utilizando o Formulário on-line para hierarquização	110

E	Processo de Execução da Análise Hierárquica de Processos (AHP) de cada Respondente (Peso Local e Peso Global)	112
E.1	Respondente 01	113
E.2	Respondente 02	114
E.3	Respondente 03	115
E.4	Respondente 04	116
E.5	Respondente 05	117

Lista de Figuras

2.1	Etapas do TEMAC [Mariano & Rocha, 2017].	9
2.2	Composição do referencial teórico inspirada em [Mariano & Rocha, 2017]. . .	10
2.3	Evolução Anual das Pesquisas Sobre o Tema	12
2.4	Análise das Revistas mais relevantes – Lei de Bradford [Scopus, 2025]. . . .	13
2.5	Análise das Universidades que mais publicam [Scopus, 2025].	14
2.6	Funcionalidades do VOSviewer® [Berriel & Santos, 2020].	16
2.7	Técnica de Cocitação e Pareamento Bibliográfico [Zupic & Čater, 2014]. . .	17
2.8	Mapa de Densidade de Cocitação de Obras [Van Eck & Waltman, 2010] . .	18
2.9	Mapa de Densidade de Cocitação de Autores [Van Eck & Waltman, 2010].	18
2.10	Mapa de Densidade de Análise de Acoplamento [Zupic & Čater, 2014]. . .	20
2.11	Espelho de pesquisa <i>Hierarchical Process Analysis “Risks”</i> [Zupic & Čater, 2014].	21
2.12	Histórico de Publicações das Leis de Liberdade de Informação.	27
2.13	Tipos de Respostas a Pedidos de Acesso à Informação.	30
2.14	Distribuição de demandantes da LAI no Brasil.	31
2.15	Fases do Ciclo de Vida do Tratamento de Dados [gui, 2020].	33
2.16	Fluxo de aplicação da AHP [Santos & Cruz, 2013].	45
2.17	Estrutura de Decisão Hierárquica [Santos & Cruz, 2013].	46
2.18	Escala de prioridades de Thomas L. Saaty [Saaty, 2008]	47
2.19	Matriz de julgamento par-a-par [Santos & Cruz, 2013].	47
2.20	Índice de Consistência Aleatória (RI) [Saaty, 1977, Saaty, 2008].	49
3.1	Fluxo metodológico adotado na pesquisa.	52
3.2	Processo de priorização	54
3.3	Matriz FMEA	56
3.4	Análise Hierárquica de Processos.	57
3.5	Fluxo de Normalização dos Valores dos Riscos.	58
4.1	Dados Demográficos dos Respondentes	62
4.2	Valores Individuais de NPR por Respondentes	63

4.3	Média do Valor de NPR	64
4.4	Média do Valor de NPR	65
4.5	Estrutura de Decisão Hierárquica	67
4.6	Ranqueamento de Riscos por Respondentes	68
4.7	Consistência Lógica dos Critérios	70
4.8	Pesos Locais e Pesos Globais das Alternativas (AHP-AIJ).	71
4.9	Ranking Global (Alternativas)	72
4.10	Valores Normalizados de FMEA e AHP	73
4.11	Comparativo dos Valores Normalizados	74
4.12	Processo de Gestão de Riscos ABNT NBR ISO 31000:2018.	76
4.13	<i>Framework</i> de Gestão de Riscos de Compartilhamento da LAI.	77
4.14	Ocorrência dos Risco Prioritários no LAI-RGF.	81
B.1	Formulário on-line para hierarquização utilizando a Análise de Modos e Efeitos de Falha (FMEA)	107
D.1	Análise de Modos e Efeitos de Falha (FMEA) utilizando o Formulário on-line para hierarquização.	111
E.1	Heatmap - pesos globais e locais das alternativas por critério para o respondente 01.	113
E.2	Heatmap - pesos globais e locais das alternativas por critério para o respondente 02.	114
E.3	Heatmap - pesos globais e locais das alternativas por critério para o respondente 03.	115
E.4	Heatmap - pesos globais e locais das alternativas por critério para o respondente 04.	116
E.5	Heatmap - pesos globais e locais das alternativas por critério para o respondente 05.	117

Lista de Tabelas

2.1	Principais autores por <i>Clusters</i> . Elaborada pelo autor, (2025).	19
2.2	Aplicação dos Princípios de Transparência na LAI do Brasil. Elaborado pelo autor	29
2.3	Escala de Ocorrência de uma Falha. Adaptado de [Ben-Daya & Raouf, 1996] e [Wang et al., 2009].	41
2.4	Escala de Gravidade (Severidade). Adaptado de [Wang et al., 2009].	42
2.5	Escala de Detecção de uma Falha. Adaptado de [Wang et al., 2009].	43
4.1	Plano de Implementação do LAI-RGF. Elaborada pelo autor, 2025.	80
A.1	Modelo Integrador da Teoria do Enfoque Meta Analítico (TEMAC).	105
C.1	Lista de tipologia conforme INC MP/CGU nº 1/2016 e riscos priorizados por especialistas.	109

Lista de Abreviaturas e Siglas

ABNT Associação Brasileira de Normas Técnicas.

AHP *Analytic Hierarchy Process*.

AHP-AIJ *Analytic Hierarchy Process* com agregação de julgamentos individuais.

CCGD Comitê Central de Governança de Dados.

CGU Controladoria-Geral da União.

CMRI Comissão Mista de Reavaliação de Informações.

CSCRM *Cyber Supply Chain Risk Management*.

CSF *Cybersecurity Framework*.

CTRIC Centro de Tratamento e Resposta a Incidentes Cibernéticos.

DAG Dados Abertos Governamentais.

DANP *Decision-Making Trial and Evaluation Laboratory with Analytic Network Process*.

EGR Estrutura de Gestão de Riscos.

Fala.BR Plataforma Integrada de Ouvidoria e Acesso à Informação.

FMEA *Failure Mode and Effects Analysis*.

FOI *Freedom of Information*.

Gov.BR Plataforma digital de serviços públicos do Governo Federal.

IA Inteligência Artificial.

INC MP/CGU nº 1/2016 Instrução Normativa Conjunta do Ministério do Planejamento e da Controladoria-Geral da União nº 1, de 2016.

IoT *Internet of Things*.

ISO *International Organization for Standardization*.

LAI Lei de Acesso à Informação.

LAI-RGF *LAI-Risk Governance Framework*.

LGPD Lei Geral de Proteção de Dados Pessoais.

MCI Marco Civil da Internet.

NBR Norma Brasileira Regulamentadora.

NIST *National Institute of Standards and Technology*.

NPR Número de Prioridade de Riscos.

ONG Organização Não Governamental.

ONU Organização das Nações Unidas.

PG Peso Global.

PL Peso Local.

PNDA Política Nacional de Dados Abertos.

PPCA/UnB Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília.

PR Presidência da República.

RI Índice de Consistência Aleatória.

RICI Revista Ibero-Americana de Ciência da Informação.

SBC Sociedade Brasileira de Computação.

SGD Secretaria de Governo Digital.

SGD/ME Secretaria de Governo Digital do Ministério da Economia.

SISBIN Sistema Brasileiro de Inteligência.

SNAI/CGU Secretaria Nacional de Acesso à Informação da Controladoria-Geral da União.

SUS Sistema Único de Saúde.

TEMAC Teoria do Enfoque Meta-Analítico Consolidado.

TIC Tecnologia da Informação e Comunicação.

TSE Tribunal Superior Eleitoral.

UF Unidade Federativa.

UnB Universidade de Brasília.

VOS *Visualization of Similarities*.

WoS *Web of Science*.

Capítulo 1

Introdução

1.1 Justificativa

O acesso à informação é um direito constitucional indispensável ao controle social, à transparência pública e à qualificação da democracia. No Brasil este direito é regulado pela Lei federal nº 12.527, de 18 de novembro de 2011 - **Lei de Acesso à Informação (LAI)**, atualizada pelo Decreto Federal nº 11.527, de 16 de maio de 2023 e pelo decreto Federal nº 7.724, de 16 de maio de 2012. Embora esse marco normativo tenha estruturado e ampliado o direito de acesso à informações produzidas ou custodiadas por entidades públicas, [Martín-Martín et al., 2018a] destacam que a “LAI tem sido pouco estudada e muito descumprida, sendo eminente a necessidade de investigá-la em contextos diversos e de aumentar o monitoramento para garantir que ela seja respeitada”.

A literatura recente evidencia a persistência de uma lacuna entre a transparência formalmente assegurada em lei e sua efetiva concretização no plano institucional, demonstrando que a simples existência de um dispositivo normativo não é suficiente para garantir transparência material, qualidade da informação compartilhada ou consistência decisória na administração pública [Trautendorfer et al., 2025]. Nesse contexto, decisões relacionadas a pedidos fundamentados na LAI tendem, com frequência, a permanecer restritas a uma lógica binária de concessão ou negativa de acesso, sem incorporar, de modo estruturado, os riscos inerentes ao processo de coleta, tratamento e compartilhamento de dados [Matey et al., 2025].

Tal constatação torna-se ainda mais sensível quando se observa o compartilhamento de dados, embora regulado por diretrizes de governança e interoperabilidade no âmbito da administração pública, permanece exposto a vulnerabilidades que ultrapassam a dimensão estritamente jurídica do problema.

Mesmo diante de referenciais como o decreto federal nº 10.046, de 9 de outubro de 2019, a operação concreta desse processo pode produzir efeitos adversos relevantes, como invasão

de privacidade em detrimento da segurança [Adeyeye, 2024]; consentimento insuficientemente esclarecido quanto ao uso dos dados [Beardsley et al., 2020] e compartilhamento excessivo, com potencial de ampliação de exclusões, assimetrias e estigmatizações sociais [Landström, 2024]. Em uma sociedade digital intensiva em dados, o compartilhamento deixa de ser mero ato administrativo acessório e passa a ocupar posição estratégica no ciclo de tratamento da informação, exigindo mecanismos capazes de articular transparência, proteção de direitos, segurança institucional e responsabilidade decisória.

Sob a ótica da tomada de decisão, essa lacuna é ainda mais relevante. Decidir, em sentido estrito, implica escolher entre cursos possíveis de ação diante de um problema concreto. No entanto, a literatura mostra que decisões humanas e institucionais frequentemente se apoiam em heurísticas, automatismos e atalhos cognitivos, em vez de serem conduzidas por exame sistemático das consequências e dos riscos envolvidos [Plassmann et al., 2005].

No ambiente da LAI, isso significa que pedidos de acesso podem ser avaliados a partir de critérios formais insuficientes para captar os impactos operacionais, legais, reputacionais e informacionais implicados no compartilhamento de dados públicos. Tal cenário reforça a necessidade de deslocar a análise do campo exclusivamente normativo para uma abordagem que incorpore o risco como variável relevante do processo decisório.

Estudar o compartilhamento de dados motivado pela LAI justifica-se, não apenas por sua escala e aplicabilidade no serviço público ou atualidade normativa e institucional, mas pela sua capacidade de revelar tensões estruturais entre publicidade, privacidade, segurança e integridade do processo decisório. Essa investigação é relevante para explicitar vulnerabilidades relacionadas à intrusão na esfera privada [Prosser, 1960], à integridade contextual dos fluxos informacionais e às formas contemporâneas de vigilância e monitoramento em ambientes mediados por dados. Ao mesmo tempo, a pesquisa se conecta à necessidade de fortalecer práticas de governança capazes de internalizar medidas de proteção desde a concepção e por padrão, em linha com os princípios de *privacy by design* [Cavoukian, 2010] e *privacy by default* [Bygrave, 2017], bem como de reforçar a conformidade com os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) e com a cultura de segurança da informação.

Além de sua relevância teórica, a pesquisa possui justificativa aplicada clara. A incorporação da análise de riscos ao processo de atendimento a pedidos de acesso à informação pode contribuir para reduzir danos reputacionais, aumentar a confiança da sociedade, padronizar critérios de decisão e fortalecer a maturidade institucional no tratamento de situações sensíveis. Mais do que identificar riscos isolados, o estudo busca responder a uma carência concreta da administração pública: a ausência de modelos estruturados e replicáveis capazes de traduzir riscos priorizados em ações institucionais proporcionais,

rastreáveis e orientadas por evidências. Nesse sentido, a investigação dialoga com a necessidade de ampliar os estudos sobre LAI para além do arcabouço jurídico-normativo, aproximando-os de metodologias e ferramentas de análise de risco aptas a qualificar o processo decisório em contextos de compartilhamento de dados e produção de insumos para a construção de uma resposta aplicada de governança.

A partir dessa base, a pesquisa fundamenta a estruturação do *LAI-Risk Governance Framework* (LAI-RGF), concebido como um *framework* de governança alinhado à Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira Regulamentadora (NBR) *International Organization for Standardization* (ISO) 31000:2018, capaz de converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional no setor público. Assim, a justificativa deste trabalho baseia-se não apenas na relevância do tema, mas na necessidade de oferecer uma resposta metodológica e institucional à insuficiência de decisões binárias em contextos complexos de compartilhamento de dados baseados na Lei de Acesso à Informação.

1.2 Problema de Pesquisa

No Brasil, o acesso a informações que foram produzidas ou são custodiadas pelo Estado é regulamentado pela LAI. No processo de operação das garantias deste direito, a tomada de decisão é majoritariamente binária / booleana [Trbojevic, 2005], focada em conceder ou negar acesso à informação solicitada. Essa abordagem ignora os riscos como um fator a ser considerado, em especial os riscos relacionados ao processo de compartilhamento, que ocorre no atendimento aos pedidos dos usuários da LAI.

A ausência de modelos estruturados e replicáveis para a governança dos riscos do processo de compartilhamento pode afetar a estrutura de segurança da informação institucional. A pesquisa trata da incorporação dos riscos como fator estrutural no processo decisório de atendimento a pedidos de acesso à informação em órgãos públicos. Ao integrar abordagens analíticas e práticas administrativas, esta pesquisa aplica parâmetros capazes de contribuir para a avaliação e formulação de políticas públicas mais equilibradas, fortalecendo a governança de dados, a proteção da privacidade e a segurança institucional.

Os achados oferecem subsídios concretos para a proposição de um modelo específico capaz de auxiliar na tomada de decisão estratégica pela administração pública federal, que seja sensível ao contexto da sociedade e coerente com a impessoalidade, legalidade, eficiência, moralidade e publicidade, devidos à administração pública.

1.3 Objetivos

1.3.1 Objetivo Geral

Analisar os principais riscos do compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação.

1.3.2 Objetivos Específicos

1. Construir um referencial teórico sobre os riscos relacionados ao compartilhamento de dados públicos no contexto da **LAI**.
2. Identificar e organizar, por tipologia, os principais riscos associados ao compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação.
3. Hierarquizar os principais riscos associados ao compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação.
4. Fundamentar e estruturar um *framework* de governança, alinhado à **ABNT NBR ISO 31000:2018**, capaz de converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional no setor público.

1.4 Contribuições da Pesquisa

Ao analisar, de forma estruturada, os principais riscos associados ao compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação, esta pesquisa busca contribuir para o campo da governança pública e da gestão de riscos na execução dos princípios, objetivos e iniciativas da Estratégia Federal de Governo Digital do Brasil, ciclo de 2024–2027, fortalecendo a transparência, segurança cibernética e proteção dos dados da população brasileira.

O estudo amplia a discussão sobre a relação entre transparência pública, compartilhamento de dados, proteção de informações sensíveis e tomada de decisão institucional orientada por riscos, reunindo literatura acadêmica e normativa aplicável ao contexto da **LAI**.

No plano metodológico, a pesquisa contribui ao articular procedimentos de identificação, organização tipológica e hierarquização de riscos por meio de abordagem multicritério, permitindo maior sistematização analítica do problema investigado. Ao combinar técnicas de priorização e julgamento especializado, o estudo oferece uma base estruturada

para compreender quais riscos assumem maior criticidade no contexto do atendimento a pedidos de acesso à informação.

Como principal contribuição aplicada, a dissertação fundamenta e estrutura o **LAI-RGF**, concebido como um *framework* de governança alinhado à **ABNT NBR ISO 31000:2018**. O modelo proposto foi desenvolvido para converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional, oferecendo suporte à atuação de órgãos públicos no tratamento de situações que demandam equilíbrio entre transparência, conformidade legal, segurança da informação, proteção de dados e *accountability*.

Assim, a pesquisa não se limita à identificação e hierarquização de riscos, mas avança na proposição de um arranjo de governança orientado por riscos, com potencial de apoiar a melhoria dos processos decisórios no setor público. Desse modo, a dissertação pretende contribuir tanto para o avanço do debate acadêmico quanto para o aprimoramento de práticas institucionais relacionadas ao atendimento de pedidos de acesso à informação.

1.5 Estrutura da Pesquisa

A dissertação está organizada em cinco capítulos:

- **Capítulo 1** – Apresenta a introdução, justificativa, problema de pesquisa e os objetivos;
- **Capítulo 2** – Trata da revisão da literatura acadêmica e normativa;
- **Capítulo 3** – Descreve os procedimentos metodológicos da pesquisa;
- **Capítulo 4** – Apresenta os resultados;
- **Capítulo 5** – Reúne as considerações finais, contribuições, limitações e agenda de pesquisas futuras.

As referências e os apêndices compõem os elementos pós-textuais.

Capítulo 2

Embasamento Teórico

2.1 Referencial Teórico

Com o intuito de proporcionar robustez e amplitude ao estudo, foi realizada uma busca bibliográfica [Garousi et al., 2019] por publicações relevantes para agregar conhecimento à pesquisa, elucidar as questões centrais do problema e fornecer subsídios para a formulação da proposta metodológica.

Uma vez que uma revisão sistemática não oferece *insights* sobre o “estado da prática” [Garousi & Mantyla, 2016, Garousi et al., 2019], foi realizada a análise da literatura cinzenta, ou seja, de documentos normativos, jurídicos, técnicos e administrativos basilares para a tomada de decisão relacionada com a governança de riscos no compartilhamento de dados fundamentados na LAI.

O direito de acesso à informação previsto pela Constituição Federal da República Federativa do Brasil de 1988, no seu inciso XIV do artigo 5º, foi regulamentado pela Lei Federal nº 12.527, de 18 de novembro de 2011 – LAI, que dispõe sobre o acesso à informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, garantindo o direito constitucional à população, sendo um “recurso” indispensável para a formulação de políticas públicas e o controle social, atualizada pelo Decreto Federal nº 11.527, de 16 de maio de 2023.

A governança no compartilhamento de dados no âmbito da Administração Pública Federal é regida pelo Decreto Federal nº 10.046, de 9 de outubro de 2019, que se articula diretamente com os dispositivos da LAI. A Resolução nº 2, de 16 de março de 2020, do Comitê Central de Governança de Dados (CCGD) normatiza o decreto e estabelece critérios e categorias para a classificação dos dados compartilhados.

Já o Guia de Boas Práticas para Implementação da LGPD (2020) na Administração Pública Federal complementa o processo com orientações técnicas, canais de comunicação com titulares de dados e a conceituação do ciclo de vida do tratamento de dados. Ante

a crescente popularização dos recursos tecnológicos de **Inteligência Artificial (IA)** no tratamento de dados, o Relatório Internacional Independente sobre Segurança em IA [UK Government, 2025], desenvolvido com a participação de pesquisador brasileiro, também é fonte relevante de informações, trazendo alertas sobre ameaças emergentes do uso de tecnologias de automação que impactam diretamente no processo de compartilhamento de dados.

O Relatório da **Organização das Nações Unidas (ONU)** sobre Inteligência Artificial – *Governing AI for Humanity* [United Nations, 2023] – propõe sete funções institucionais para a governança global da IA relacionadas ao acesso à informação, tendo igual relevância ao relatório anterior. O Código de Práticas de Governança Cibernética [Financial Reporting Council, 2024], publicado no Reino Unido, estabelece um modelo de responsabilidade diretiva para a alta gestão sobre riscos de segurança cibernética. Já o *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)* de 2025 [National Institute of Standards and Technology, 2026] é um modelo norte-americano de maturidade de gestão de riscos cibernéticos que dialoga diretamente com a estruturação dos sistemas de informação da administração pública, ao promover ações contínuas de identificação, proteção, detecção, resposta e recuperação. O CSF é aplicável a todo o ciclo de vida da informação gerida sob a LAI. Esses princípios e conceitos fortalecem a tomada de decisão estratégica e ressaltam a importância da governança de riscos do processo de compartilhamento de dados.

O NIST SP 800-61r3, versão 2.0 de 2025 (Rev. 3) [Nelson et al., 2025], é um guia técnico essencial para a resposta a incidentes de segurança, orientando quanto ao processo de detecção e gestão de riscos e eventos de violação de dados. Complementarmente, o NIST SP 800-53, Revisão 5.2.0, de 2025 [nis,], discorre sobre controles de segurança e privacidade para sistemas de informação, fornecendo um conjunto de práticas aplicáveis à proteção de dados durante o processamento e o compartilhamento. Por fim, o Regulamento (UE) 2024/1689 do Parlamento Europeu sobre Inteligência Artificial [European Union, 2024] propõe uma abordagem baseada em risco e impõe restrições ao uso de sistemas de IA em contextos sensíveis. Sua categorização dos sistemas em níveis de risco (inaceitável, alto, limitado, mínimo) oferece uma matriz analítica útil para hierarquizar riscos no compartilhamento de dados automatizados sob a LAI.

Foi possível identificar um grupo de pesquisas que tratam da LAI de forma isolada ou transversalmente com outros normativos brasileiros como a LGPD, a Lei Federal nº 12.965, de 23 de abril de 2014 – **Marco Civil da Internet (MCI)** – e a **Política Nacional de Dados Abertos (PNDA)**, instituída pelo Decreto Federal nº 8.777, de 11 de maio de 2016. Investigações comparativas da legislação brasileira com outros países, tratativas sobre proposições e alterações feitas nas LAI em contexto global, com recorte para o

Brasil em tempos de pandemia, também foram encontradas. Porém, ficou evidente a ausência de pesquisas que tragam a perspectiva de identificação e análise dos riscos de compartilhamento de dados relacionados à operação da LAI do Brasil, o que confere considerável destaque e relevância à presente investigação.

2.2 Aplicação da Teoria do Enfoque Meta Analítico (TEMAC)

A literatura descreve e ressalta a importância de índices relacionados com os resultados das Leis da Bibliometria: a Lei de Bradford, a Lei de Lotka, a Lei de Zipf, a Lei do Elitismo e a Lei do 80/20, com abordagem meta-analítica e uso do **VOSviewer** (versão 1.6.20), e a Lei da Obsolescência da literatura [Aytac et al., 2025, Rodrigues et al., 2024, Kwilinski & Kardas, 2024, Nisonger, 2008, Guedes & Borschiver, 2007, Urbizagástegui Alvarado, 2002].

Para Abramo & D'Angelo (2011), uma boa revisão da literatura deve possuir precisão, explicada pelo grau de proximidade das medidas dos indicadores de desempenho e outros indicadores. Por isso, a revisão bibliométrica [Passas, 2024] foi a base para a construção da estrutura metodológica da pesquisa e dos grupos de riscos utilizados.

A **Teoria do Enfoque Meta-Analítico Consolidado (TEMAC)** de [Mariano & Rocha, 2017] é eficaz para integrar e sintetizar grandes volumes de dados bibliográficos, permitindo a avaliação detalhada e comparativa dos fatores influenciadores identificados e a sua organização processual em etapas de execução com objetivos específicos, claros e respaldados nas leis da bibliometria. As três etapas da **TEMAC**, representadas na Figura 2.1, foram aplicadas no estudo.

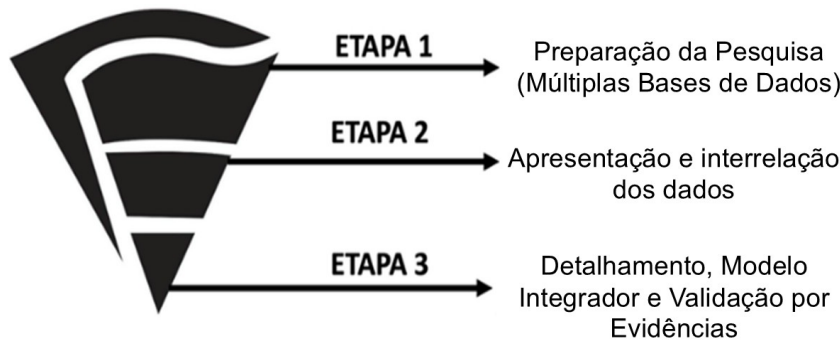


Figura 2.1: Etapas do TEMAC [Mariano & Rocha, 2017].

2.2.1 Preparação da Pesquisa (Etapa 1)

A primeira etapa responde questões como: Qual o descritor, *string* ou palavra-chave da pesquisa? Qual o campo espaço-tempo da pesquisa? Quais as bases de dados serão utilizadas? Quais áreas de conhecimento serão utilizadas? E foi aplicada como explicado abaixo:

1. **Definição dos Filtros (análise bibliométrica):** utilizou-se a tag “*access to information law*” para ser mais específico na busca. A partir dela, as tags “*risk*”, “*data sharing*” e “*Hierarchical Process Analysis*” foram pesquisadas.
2. **Seleção da Base de Dados:** os estudos mostram que existem diferenças no grau de cobertura dos bancos de dados em assuntos específicos [GONZÁLEZ-VALIENTE & LÓPEZ-MESA, 2022, Harzing & Alakangas, 2016]; por este motivo, para garantir maior cobertura de referencial teórico com publicações mais relevantes, a pesquisa foi expandida para as bases de dados [Mariano & Rocha, 2017] *Web of Science* (WoS) [Martín-Martín et al., 2018b], Scopus Elsevier [Baas et al., 2020b, Baas et al., 2020a] e Google Acadêmico [Sinha et al., 2015, Wang et al., 2019, Wang et al., 2020, Shintaku et al., 2015]; e outras bases de dados como provedores secundários, tais como Emerald Insight, *Revista Ibero-Americana de Ciência da Informação* (RICI), IEEE Xplore, Research Gate, Scielo, Scielo Brasil, ProQuest, Science Direct, Taylor & Francis, *Sociedade Brasileira de Computação* (SBC) e Nature.

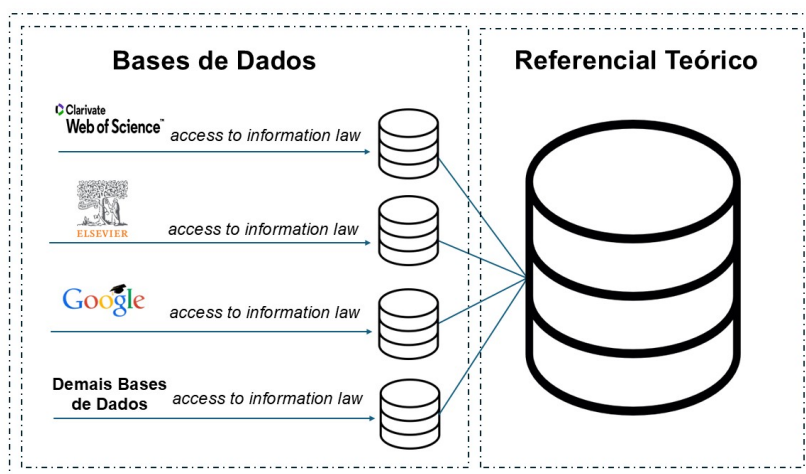


Figura 2.2: Composição do referencial teórico inspirada em [Mariano & Rocha, 2017].

3. **Definição do campo e espaço-tempo da pesquisa:** foram analisados pela perspectiva do serviço público executado no Executivo Federal, nos anos de 2014 a 2024.
4. **Coleta de Dados (análise bibliométrica):** executada com coletas entre o período de junho/2024 e setembro/2025.
5. **Áreas do Conhecimento:** a pesquisa obteve achados em volume e representatividade nas áreas conforme especificado a seguir, cabendo destaques para Ciências Sociais, Ciência da Informação, Biblioteconomia e Ciência da Computação.

2.2.2 Apresentação e Inter-relação dos Dados (Etapa 2)

Os dados coletados são inter-relacionados e os resultados apresentados nessa fase. Atualmente são inúmeras as opções de demonstração dos resultados oferecidas, sendo também possível identificar resultados nas pesquisas de enfoque meta-analítico destacando um padrão informal em consonância com os princípios bibliométricos, esperados por editoras e revisores de revistas.

[Guedes & Borschiver, 2007], [Nisonger, 2008], [Rodrigues et al., 2024], [Kwilinski & Kardas, 2024] e [Aytac et al., 2025] destacaram: (i) análise de revistas mais relevantes – Lei de Bradford; (ii) fator de impacto e 80/20; (iii) análise de revistas que mais publicaram sobre o tema – Lei de Bradford; (iv) evolução do tema ano a ano – Obsolescência da literatura e Teoria Epidêmica de Goffman; (v) autores que mais publicaram *versus* autores que mais foram citados – Lei de Lotka e Lei do Elitismo; (vi) países que mais publicaram, frequência de palavras-chave e universidades que mais publicaram – Lei do

80/20; como sendo alguns dos princípios bibliométricos, ficando a critério do pesquisador quais demonstrações serão utilizadas.

Considerando o que [Lakatos & Marconi, 2003] afirmam sobre a escolha do método científico e sua aplicação dependerem da percepção do pesquisador sobre seu trabalho [Mariano & Rocha, 2017, Demo, 2000], os critérios bibliométricos selecionados para fins desta investigação foram: evolução do tema ano a ano; análise dos países que mais publicam sobre o tema; áreas que mais publicam; análise de revistas mais relevantes; e análise das universidades que mais publicaram.

Critério “Evolução do Tema Ano a Ano”

Dada a representatividade na pesquisa, as três bases de dados foram selecionadas dentre as bases outrora descritas para representar a temática conforme o recorte (2014–2024), ficando evidente a ascensão do número de pesquisas referente a “*access to information law*”. Observando os totais dos achados (Figura 2.3), em cada plataforma – WoS (62), Scopus Elsevier (49) e Google Acadêmico (2.600) – é evidente a ascensão do número de pesquisas referente a “*access to information law*” e o impacto da *Open Web* e parcerias entre plataformas [Clarivate, 2020].

Talvez, devido ao efeito agregador da plataforma Google Acadêmico, ela se destaca no total de achados, potencializando a construção de pesquisas, atividades de busca e referenciamento. A citação dos achados em vários formatos otimiza o trabalho dos pesquisadores.

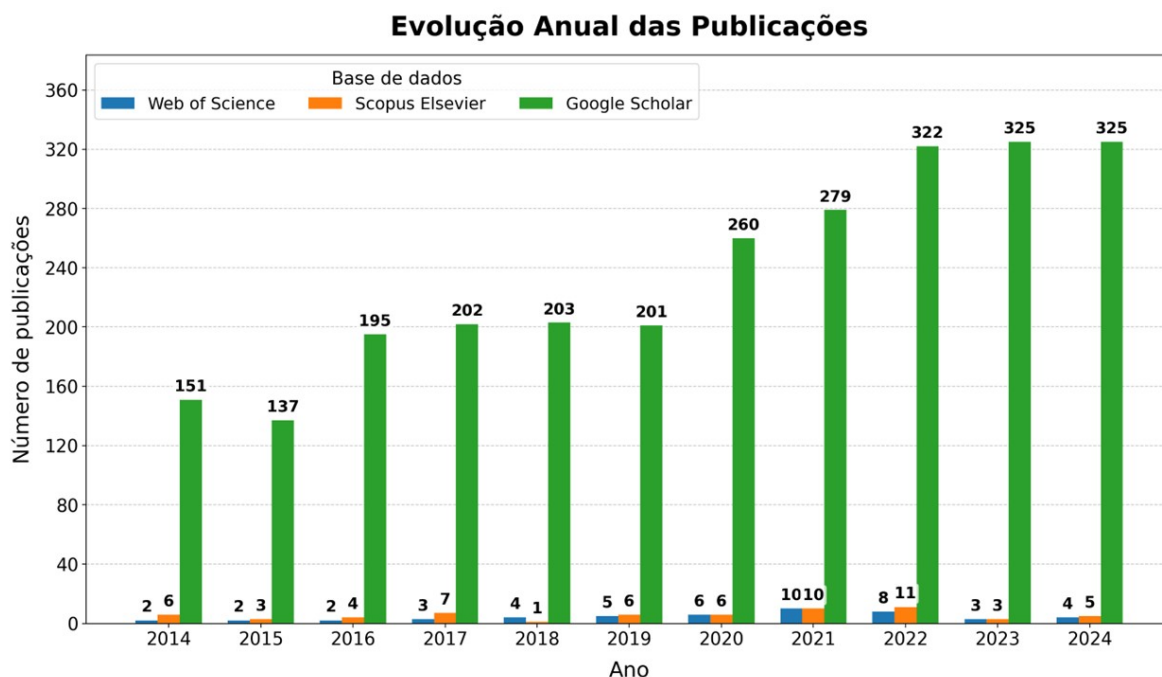


Figura 2.3: Evolução Anual das Pesquisas Sobre o Tema
 Fonte: Elaborada pelo autor, (2025)

Tais características indicam as plataformas como pontos de partida seguros e estruturados na construção de pesquisas, cabendo destacar a existência de diferenças no grau de cobertura dos bancos de dados em assuntos específicos [Harzing & Alakangas, 2016] e a necessidade de tratar as duplicidades.

Critério “Análise dos Países que Mais Publicam sobre o Tema”

O Brasil se destacou como o primeiro lugar no volume de publicações entre os países que mais publicaram sobre a temática de acesso à informação, com 41 dos 63 artigos, seguido pelo Canadá com 5 publicações; sendo o terceiro lugar do ranking dividido entre a Espanha e a Suíça com 4 publicações; e o quarto lugar com os Estados Unidos da América, que possui 3 publicações. Os demais países não foram contabilizados por conterem volume de publicações com valor ≤ 2 .

Critério “Áreas que Mais Publicam”

Analisando os achados nas bases **WoS** e Scopus Elsevier, fica evidente a representação das seguintes áreas: Ciências Sociais (53); Ciência da Informação e Biblioteconomia (17); Ciência da Computação (15); Lei do Governo (8); Administração Pública (6); Artes e Humanidades (6); Economia Empresarial (5); Ciências Ambientais e Ecologia (3); Negócios,

Gestão e Contabilidade (3); Economia, Econometria e Finanças (3); e Medicina (3). As demais áreas concentraram publicações com valor ≤ 2 e foram desconsideradas.

Critério “Análise de Revistas Mais Relevantes”

No ano de 2019, a **RICI** destacou-se com o maior número de publicações, conforme Figura 2.4.

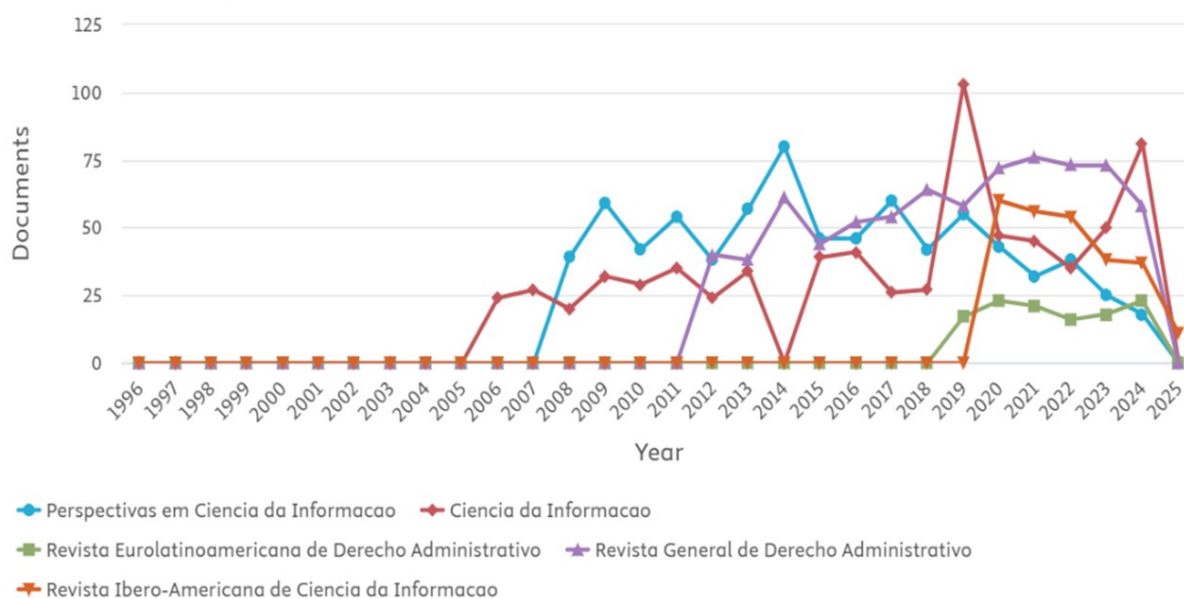


Figura 2.4: Análise das Revistas mais relevantes – Lei de Bradford [Scopus, 2025].

A **RICI** é publicada desde 2008, com periodicidade quadrimestral, pela Universidade de Brasília (**Universidade de Brasília (UnB)**), mais precisamente pela Faculdade de Ciência da Informação e seu Programa de Pós-Graduação em Ciência da Informação [Rodrigues & Abadal, 2014].

Critério “Análise das Universidades que Mais Publicaram”

Aprofundando nos achados da Scopus Elsevier, identificou-se 41 publicações de autoria de pesquisadores do Brasil (Figura 2.5). Destaca-se a produtividade da Universidade de Brasília (**UnB**), que lidera o ranking com nove publicações; seguida pela Universidade Estadual Paulista Júlio de Mesquita Júnior (Unesp) com seis publicações; a Universidade de São Paulo (USP) em terceiro com cinco publicações; e na quarta posição a Universidade Federal do Paraná (UFPR) com três publicações. As demais instituições de ensino superior encontradas apresentam histórico de publicações com valor ≤ 2 .

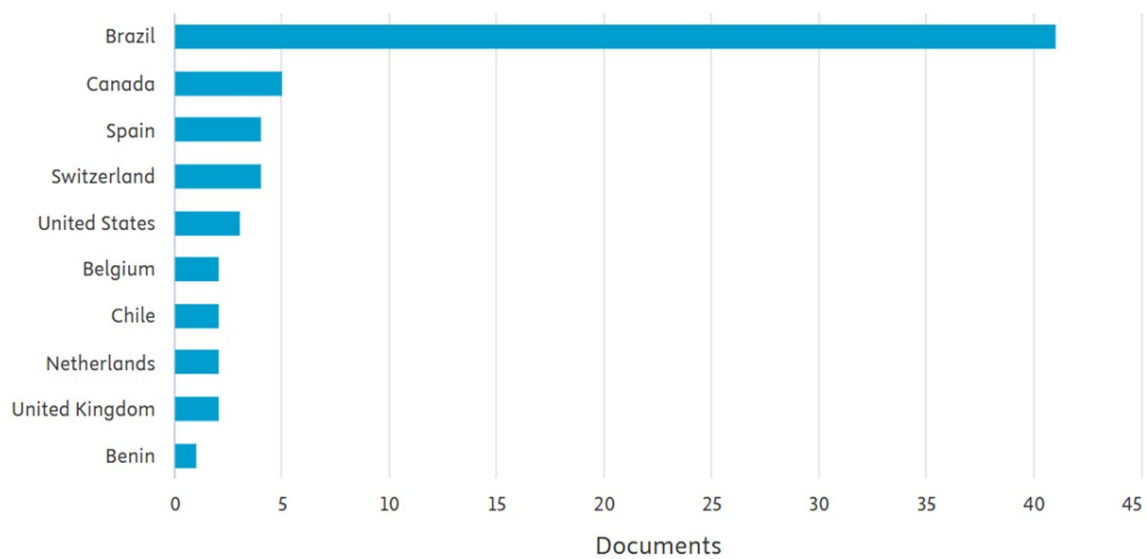


Figura 2.5: Análise das Universidades que mais publicam [Scopus, 2025].

Critério “Autores Mais Produtivos – Lei de Lotka”

A Lei de Alfred J. Lotka [Lotka, 1926] introduz e descreve a distribuição da produtividade científica entre autores em um campo de conhecimento, destacando que poucos autores produzem muitos artigos, enquanto a maioria contribui com apenas um ou dois [Bensman & Smolinsky, 2017].

Aprofundando no contexto de destaque das instituições de ensino superior, os trabalhos da UnB que versam sobre “*access to information law*” estão associados ao esforço de 19 pesquisadores. A primeira publicação data do ano de 2017; dos nove trabalhos encontrados, sete são artigos, um é capítulo de livro e um é componente de uma análise. Os documentos estão relacionados de forma transversal a várias áreas do conhecimento. Mesmo atuando de forma parceira e transversal, os pesquisadores da UnB seguem linhas e objetivos autônomos de pesquisa.

Cabem alguns destaques: [Paulino & Dutra, 2024] discorrem, em capítulo de livro, sobre “Direitos epistêmicos e direito à informação no Brasil e no México”; [Capuano, 2022] avaliou o nível de satisfação dos usuários ante o processo de implementação da LAI no Governo Federal brasileiro; [Ribeiro et al., 2022] tratou sobre compartilhamento de dados entre os órgãos do Sistema Brasileiro de Inteligência (SISBIN); [Rodrigues et al., 2021] discorreu sobre a iniciativa brasileira de alteração da Lei Federal nº 12.527/2011 no

período da pandemia; [Mota & Araújo Júnior, 2021] investigou as limitações do acesso às informações sobre contratação pública em saúde no Brasil, no período de 1990 a 2018.

Ainda, [Fernandez et al., 2021] analisou a atuação da Ouvidoria-Geral do **Sistema Único de Saúde (SUS)** no âmbito das políticas de saúde; [Eirão & Leite, 2020] realizou um estudo do acesso à informação pública no contexto dos países do Cone Sul e estudou a temática do acesso à informação pública a partir de uma análise do seu relacionamento com a democracia [Eirão & Leite, 2019] e a importância da disponibilização da informação pública de maneira livre, tendo o sigilo como exceção; [Fácio, 2023] pesquisou “A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre interseções entre **LGPD** e **LAI** no Brasil”.

2.2.3 Detalhamento, Modelo Integrador e Validação por Evidências (Etapa 3)

Detalhamento

A terceira e última etapa do **TEMAC** requer a apresentação de uma análise mais profunda para prover *insights* capazes de orientar a tomada de decisão quanto à seleção dos principais autores, identificação das principais abordagens e linhas de pesquisa. Para tanto, são necessários novos índices bibliométricos capazes de detectar os colégios invisíveis (co-citação, co-autoria, *coupling*, co-ocorrência e frequência de palavras-chave), sendo que as duas últimas visam manter a coerência com a Lei de Zipf [Guedes & Borschiver, 2007].

A construção do modelo integrador segue com o avanço característico da criação dos mapas bibliométricos para a visualização dos dados coletados, criados com o *software* **VOSviewer** – versão 1.6.20 [Van Eck & Waltman, 2010]. O *software* é um visualizador que permite o exame detalhado de dados pelo mapeamento *Visualization of Similarities (VOS)* para explorar as relações de co-citação, co-autoria, co-ocorrência, *coupling* e frequência de palavras-chave. Segundo [Berriel & Santos, 2020], as funcionalidades podem ser resumidas conforme descrito na Figura 2.6.

Tipo de análise	Insight	Vantagens	Desvantagens
Co-authorship	Que pesquisadores trabalham juntos?	Mostra evidência de colaboração e a estrutura social do campo.	Nem sempre colaboração é apresentada com a coautoria.
Co-occurrence	Que palavras chave vêm sendo mais usadas em cada período determinado de tempo?	Pode usar o conteúdo do artigo para análise.	Palavras aparecem em diferentes formas e com diferentes significados.
Citation	Onde isso é pesquisado?	Destaca com facilidade trabalhos importantes de determinada área.	Pode ocultar novas publicações por não serem consideradas importantes.
Bibliographic coupling	Quem são as organizações centrais e periféricas em um grupo de pesquisa emergente?	Pode encontrar novas áreas de pesquisa.	Exige um timeframe reduzido, selecionando apenas uma amostra do tempo.
Co-citation	Quais são os autores mais influentes na área da Dinâmica de Sistemas, e quais são citados juntos?	Conectar trabalhos, autores e periódicos com co-citação é uma medida confiável.	Não é ótimo para mapear “ <i>research fronts</i> ”, porque mapeia artigos citados.

Figura 2.6: Funcionalidades do VOSviewer® [Berriel & Santos, 2020].

A ferramenta foi escolhida devido à sua eficácia em análises bibliométricas, mapeamentos conceituais e afinidade com a técnica **TEMAC** [Mariano & Rocha, 2017], além de permitir o uso de formas distintas de mapas bibliométricos, cada uma evidenciando aspectos específicos e relevantes [van Eck & Waltman, 2010]. Segundo [Mariano & Rocha, 2017], por meio destes resultados pode-se obter o núcleo de autores indispensáveis, referências, abordagens e linhas de pesquisa.

Uma vez identificados os principais resultados da literatura, procede-se à análise de validade a partir da leitura dos resumos, visto que algumas vezes os resultados podem levar a falsas associações. Caso os resumos não sejam suficientes, faz-se necessária a leitura de todo o artigo; o pesquisador deve realizar uma catalogação pessoal dos trabalhos visando encontrar as similaridades apontadas nas análises bibliométricas anteriores (co-citação, co-autoria, *coupling*, co-ocorrência e frequência de palavras-chave).

Critério “Análise de Co-citação de Documentos”

Esta análise tem como objetivo estudar as conexões entre os autores frequentemente citados juntos, revelando relações e influências entre os seus trabalhos. Ou seja, visa identificar qual artigo cita outro artigo – ou quais autores dos artigos citam autores de artigos do autor –, identificando as conexões entre documentos que compartilham referências bibliográficas e permitindo identificar grupos de pesquisa e temas emergentes que estão sendo explorados conjuntamente (Figura 2.7).

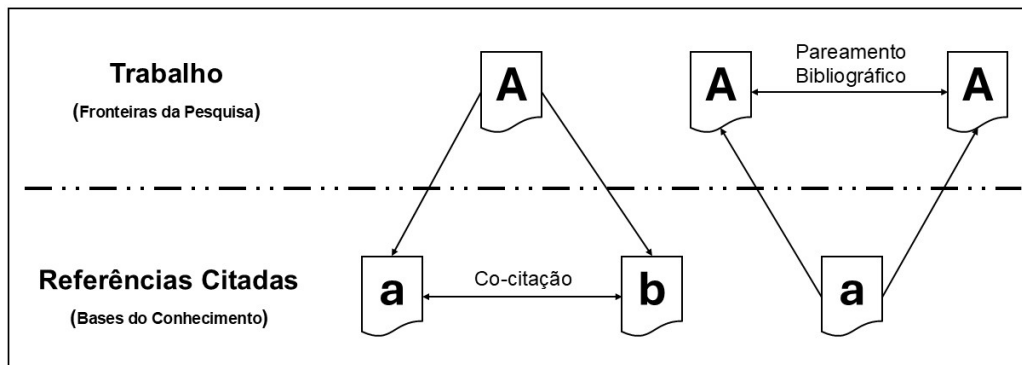


Figura 2.7: Técnica de Cocitação e Pareamento Bibliográfico [Zupic & Čater, 2014].

No **VOSviewer** restringiu-se a seleção dos autores aos com número de citações ≥ 15 , e a pesquisa retornou um total de 15 *clusters* na versão 1.6.20.

Os documentos mais citados são de autoria de [Hong et al., 2021], com 74 conexões (artigo que investiga os motivadores e inibidores da preocupação com a privacidade na Internet); [Fabris et al., 2022], com 62 citações (estudou os conjuntos de dados de justiça algorítmica: a história até agora); [Etemadi et al., 2021], com 58 citações (identificou e classificou as barreiras significativas que afetam a implementação da tecnologia *block-chain* como um componente-chave do gerenciamento de risco da cadeia de suprimentos cibernética – *Cyber Supply Chain Risk Management (CSCRM)*); [Rana et al., 2020], com 56 citações (Figura 2.8), que investigou os principais desafios para os serviços financeiros digitais nas economias emergentes: o contexto indiano; e [Wang et al., 2021], com 55 citações, que analisou os desafios de adoção da *Internet of Things (IoT)* e da *IA* para cidades inteligentes na China. Os demais documentos obtiveram total de citações ≤ 49 .

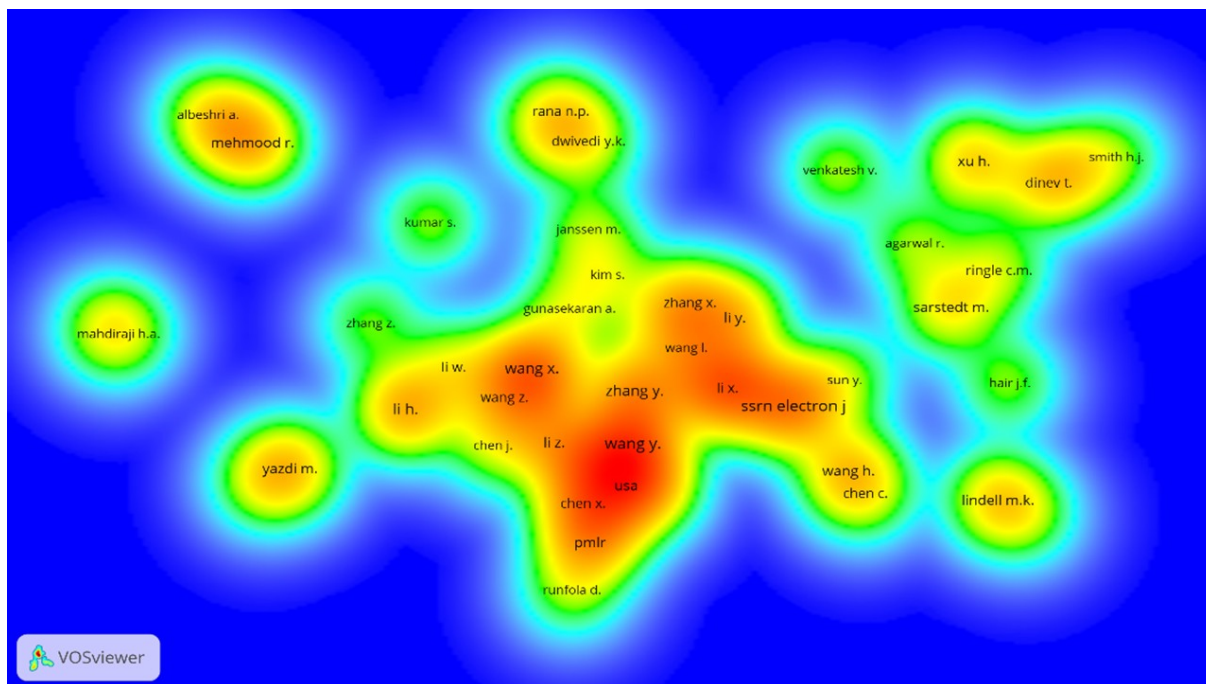


Figura 2.8: Mapa de Densidade de Cocitação de Obras [Van Eck & Waltman, 2010]

A análise de Co-citação de Autores (Figura 2.9) ocorre quando duas publicações são co-citadas se houver uma terceira publicação que cita ambas as publicações [Marshakova, 1981].

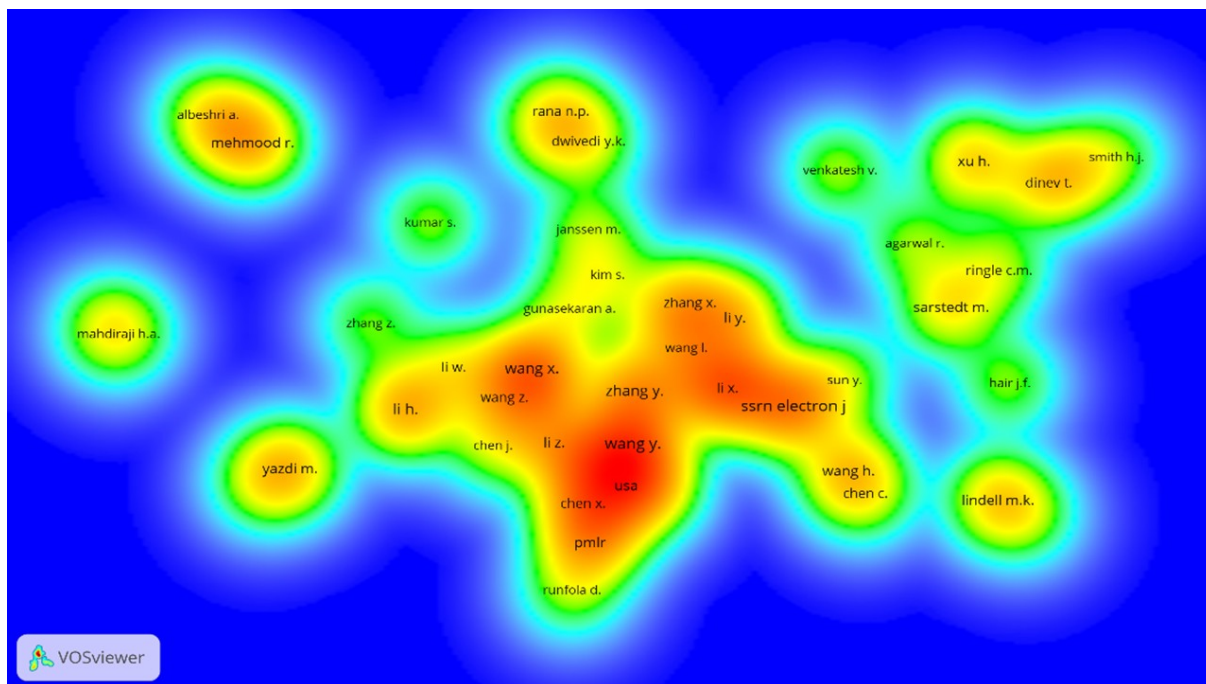


Figura 2.9: Mapa de Densidade de Cocitação de Autores [Van Eck & Waltman, 2010].

Quanto maior o número de publicações pelas quais duas publicações são co-citadas, mais forte é a relação de co-citação entre as duas publicações (3ª publicação mais recente).

Na análise de co-citação de autores, o mapa de calor de ocorrências de autores mais citados revelou o total de 13.572 autores co-citados; no gráfico estão representados os 53 que foram citados em quantidade ≥ 20 vezes, obtendo-se o total de 5 (cinco) *clusters*. Entre os autores classificados pelo número de artigos citados, destacam-se alguns principais dentro de cada *cluster*, conforme Tabela 2.1.

Tabela 2.1: Principais autores por *Clusters*. Elaborada pelo autor, (2025).

<i>Cluster</i>	Autores	Tema da Pesquisa	DOI
1º	HONG,2021	<i>Drivers</i> e inibidores da preocupação com a privacidade na Internet: perspectiva da teoria do desenvolvimento multi-dimensional	https://doi.org/10.1007/s10551-019-04237-1
2º	FABRIS,2022	Conjuntos de dados de justiça algorítmica: a história até agora	https://doi.org/10.1007/s10618-022-00854-z
3º	ETEMADI,2021	Uma modelagem ISM de barreiras para adoção de tecnologia de <i>blockchain</i> /razão distribuída em cadeias de suprimentos em direção à segurança cibernética	https://doi.org/10.3390/su13094672
4º	RANA,2020	Principais desafios para serviços financeiros digitais em economias emergentes: o contexto indiano	https://doi.org/10.1108/ITP-05-2018-0243
5º	WANG,2021	Analisando os desafios de adoção da IoT e da IA para cidades inteligentes na China	https://doi.org/10.3390/su131910983

Análise de *Coupling*

A análise de *coupling* ou forças de acoplamento [Batagelj & Cerinsek, 2013] é uma técnica que permite identificar semelhanças conceituais entre documentos por meio da comparação das suas referências; quanto maior o número de referências entre dois documentos, maior a similaridade entre eles. O acoplamento bibliográfico é o oposto de co-citação: duas publicações são acopladas bibliograficamente se houver uma terceira publicação que é

citada por ambas [Kessler, 1963] – em outras palavras, o acoplamento bibliográfico trata da sobreposição nas listas de referências de publicações (3ª publicação mais antiga).

O acoplamento bibliográfico entre autores [Zhao & Strotmann, 2008] é uma extensão do conceito de acoplamento bibliográfico [Kessler, 1963]; os autores analisaram a evolução estrutural de dois períodos de 5 anos (2001–2005 e 2006–2010), concluindo que dois autores com referências mais comuns são mais relacionados e têm interesses de pesquisa mais semelhantes [Gazni & Didegah, 2016]. Em contraste com a análise de co-citação, que requer sinais de força (número de citações), o acoplamento bibliográfico pode auxiliar na detecção de frentes de pesquisa mesmo com sinais fracos [Glänzel & Czerwon, 1996]. De acordo com a teoria normativa da citação, as citações são indicadores de influência cognitiva ou intelectual de um trabalho científico [Monteiro & Sant’Ana, 2023]. O acoplamento bibliográfico evidencia quem são os pesquisadores que compartilham bases comuns, formando redes que impulsionam a evolução do debate. A análise (Figura 2.10) demonstra a permanência de autores como [Hong et al., 2021], [Rana et al., 2020], na lista dos mais citados, e registra a ascensão de [Wang et al., 2021] no cenário.

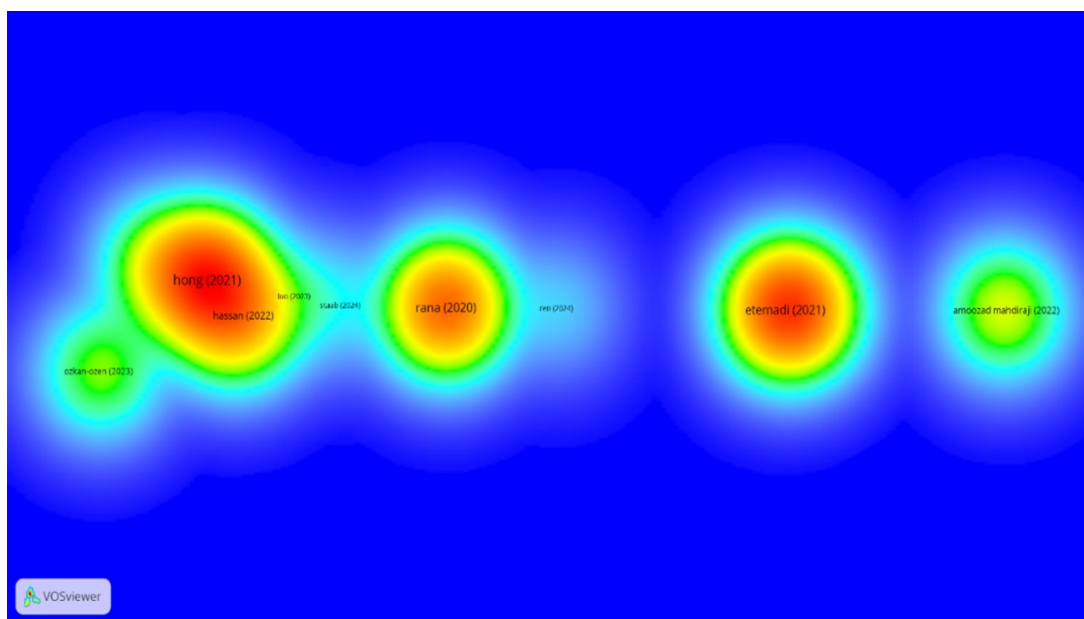


Figura 2.10: Mapa de Densidade de Análise de Acoplamento [Zupic & Čater, 2014].

Isso reforça que o estudo sobre a LAI e riscos no compartilhamento de dados se apoia tanto em literatura já consolidada (co-citação) quanto em autores emergentes que definem as novas frentes, especialmente em torno de análises centradas em riscos, *big data*, privacidade e governança digital.

Análise de Palavras-chave

A análise de palavras-chave permite o resumo de tópicos de estudo em uma área de pesquisa específica, gerando a exploração de pontos críticos e destacando direções dentro dessa área. O **VOSviewer** foi utilizado para representar graficamente todas as palavras-chave (*Author Keywords* e *Keywords Plus*).

Frequência de Palavras-chave

Dentre as 510 palavras-chave identificadas, listou-se as citadas em quantidade ≥ 2 vezes, obtendo-se o retorno de 52 achados, organizados em *clusters*. O mapa apresenta uma rede de *clusters* em torno da gestão de riscos, trazendo palavras-chave próprias e destacando padrões e tendências em cada um deles. Esses *clusters* demonstram que a literatura sobre riscos no contexto da LAI e do compartilhamento de dados é multidimensional: abrange legislação, políticas públicas, metodologias analíticas, sustentabilidade, tecnologias emergentes, segurança da informação e formação social.

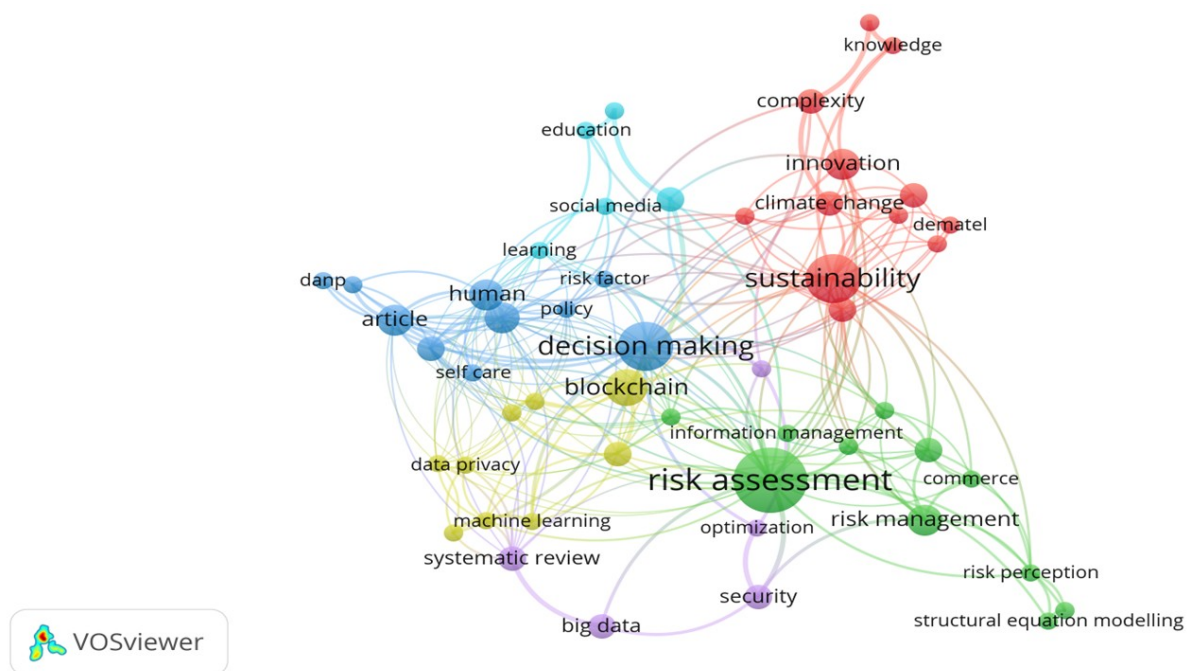


Figura 2.11: Espelho de pesquisa *Hierarchical Process Analysis “Risks”* [Zupic & Čater, 2014].

O *cluster* verde – gestão de riscos e governança – pode ser visto como o *cluster* central, estruturando a pesquisa sobre avaliação de riscos, gestão de riscos e percepção de risco. É composto por palavras-chave como “commerce”, “information management”,

“investments”, “literature reviews”, “risk assessment”, “risk management”, “risk perception”, “structural equation modelling”, “sustainable development”, “technology acceptance” e “wellbeing”.

O *cluster* amarelo está centrado na privacidade, dados e tecnologias, destacando tecnologias emergentes e dilemas éticos e jurídicos do compartilhamento de dados. A presença de *“blockchain”, “data sharing” e “data privacy”* indica a ênfase em tecnologias de rastreabilidade e proteção, enquanto *“privacy” e “confidential information”* remetem diretamente às tensões entre transparência (LAI) e proteção de dados pessoais (LGPD).

O *cluster* azul-escuro – decisão e políticas – está concentrado na tomada de decisão (*“decision making”*), política e individual, associada a fatores de risco e a contextos humanos. Inclui métodos de apoio à decisão, como o *Decision-Making Trial and Evaluation Laboratory with Analytic Network Process (DANP)*, reforçando o elo entre análise multicritério, formulação de políticas e avaliação de riscos.

O *cluster* azul-claro – educação e aprendizagem em riscos – traz a perspectiva de formação e difusão de conhecimento em riscos, com foco em aprendizagem organizacional e impacto das redes sociais, indicando que a capacidade de aprendizagem é parte essencial da mitigação de riscos.

O *cluster* vermelho – sustentabilidade e inovação – reúne a literatura sobre inovação aplicada à sustentabilidade, apresentando metodologias de análise multicritério em sistemas sociais e a necessidade de conhecimento aplicado à gestão de riscos climáticos e de longo prazo, mostrando como a transparência e a governança de riscos se conectam diretamente a objetivos globais de sustentabilidade e inovação tecnológica.

Já o *cluster* roxo – modelagem e segurança da informação – é mais técnico, composto por palavras como *“big data”, “numerical model”, “optimization”, “security” e “systematic review”*. Destaca ferramentas de modelagem numérica, otimização e segurança da informação, trazendo uma base metodológica para suportar análises quantitativas de risco em grandes volumes de dados (*big data*) e reforçando a parte operacional e científica da governança de riscos.

Tendências por Palavras-chave

Embora a produção científica mantenha como núcleo central a avaliação de riscos e transparência, ao observar estudos recentes sobre a LAI, é possível inferir que temas emergentes têm sido incorporados, com tendência à combinação de métodos quantitativos robustos, inovações digitais (IA, *blockchain*, *big data*) e análises normativas e sociais, consolidando uma abordagem interdisciplinar e multicritério para riscos no compartilhamento de dados públicos.

Esses achados confirmam que os riscos do compartilhamento de dados públicos não se restringem ao aspecto normativo, mas se expandem para questões tecnológicas, sociais e de governança institucional, reforçando a necessidade de abordagens multicritério.

Modelo Integrador

Passada a análise documental, visando encontrar as similaridades apontadas nas análises bibliométricas, foram identificados os principais resultados da literatura. Após a identificação das principais abordagens históricas e linhas de pesquisa, foi proposto um modelo integrador que represente de forma visual os principais artigos identificados por relevância no processo de compartilhamento de dados derivados do atendimento a pedidos de acesso à informação. O Modelo Integrador está detalhado no Apêndice A.

Um modelo integrador pode ser definido como uma estrutura ou abordagem metodológica capaz de reunir, harmonizar e sintetizar resultados provenientes de diferentes métodos, fontes de dados, técnicas ou abordagens analíticas, de modo a produzir uma visão unificada, comparável e coerente para subsidiar decisões complexas [Santos et al., 2017a].

Para [Santos et al., 2017b], um modelo integrador representa uma abordagem metodológica que viabiliza a combinação de diferentes métodos ou resultados, criando sínteses robustas e permitindo comparações, agregações e generalizações entre domínios inicialmente incompatíveis. Já para [Krueger et al., 2012], os modelos integrados são necessários para cruzar fronteiras disciplinares, permitindo a síntese e a tradução mútua de resultados que usam diferentes escalas, unidades ou metodologias.

Após análise das referidas obras, foi possível identificar um grupo de pesquisas restrito tratando sobre a Lei Federal nº 12.527/2011 – LAI do Brasil – e outro grupo de registros que apresentaram abordagens pontuais sobre a execução da lei de acesso à informação em outros países. Essas comparações foram o alicerce para a formulação do resultado final por meio da categorização das principais descobertas. Tais resultados são condensados no modelo integrador [Pareja-Daza et al., 2024, Mariano et al., 2011, Mariano et al., 2012] e desdobrados no decorrer da investigação.

[Paulino & Dutra, 2024] fazem um comparativo da aplicação da legislação do México e do Brasil, avaliando o nível de satisfação dos usuários. Em sua pesquisa “Lei de acesso à informação e os ‘ventos de mudança’ estagnados na Zâmbia”, Sam Phiri (2016), argumenta que a abordagem local para facilitar o acesso à informação pública tem sido falha, pois seu foco é limitado, o que resultou na paralisação do processo. [Trautendorfer et al., 2025] apresentam o estudo “Da transparência de jure à transparência de fato: analisando a lacuna de conformidade à luz das leis de liberdade de informação”, baseado em 101.089 solicitações de informação enviadas a 7.188 órgãos públicos alemães entre 2011 e 2021.

Os dados provêm da plataforma *online* alemã de acesso à informação *FragDenStaat* – que pode ser traduzido como “Pergunte ao Estado” – hospedada por uma organização não governamental (**Organização Não Governamental (ONG)**).

A revisão da literatura destacou a ausência de pesquisas específicas que identificassem e analisassem a teoria e a prática vivenciada pelos servidores públicos das instituições do Executivo Federal, o que destaca a importância e relevância da investigação dos riscos derivados do processo de compartilhamento de dados relacionados à operação da **LAI** do Brasil, por meio da aplicação de métodos multicritério na hierarquização e análise dos riscos.

Validação por Evidências

Apresentada essa etapa, seguiu-se para a última das três fases da **TEMAC**: a validação final do modelo por meio de evidências, tais como: (i) pelo menos uma publicação de revisão sistemática (forte), opção aplicada na validação da pesquisa, conforme descrito a seguir; (ii) pelo menos uma publicação de estudo de caso com resultados apresentados (forte); (iii) estudos por mais de um centro ou grupo de pesquisa; e (iv) opiniões de autoridades respeitadas, baseadas em projetos implementados com sucesso, estudos descritivos ou relatórios de comitês de especialistas.

Os trabalhos de [Kempeneer et al., 2023] estudaram a relação e os impactos das leis governamentais de dados abertos e de acesso à informação, destacando que a legislação “moderna” de acesso à informação caminha lado a lado com uma “mudança de paradigma”: enquanto a divulgação “passiva” de informações governamentais a pedido individual costumava ser a pedra angular da legislação tradicional de acesso à informação, hoje em dia dá-se mais ênfase à legislação que promove a divulgação afirmativa (proativa) por iniciativa dos próprios governos e aos **Dados Abertos Governamentais (DAG)**, destacando a necessidade de informações governamentais legíveis por máquina para fomentar sua reutilização.

Em sua pesquisa, [Pinto Filho et al., 2021] traça um panorama da Lei 12.527/2011 a partir de uma revisão sistemática de literatura, destacando pesquisas voltadas à aplicação da lei na esfera do Poder Executivo Municipal, do Poder Executivo Federal, além de obras que discutiram a lei e sua contribuição para o país. Por fim, [Martín-Martín et al., 2018a] destacam que a “**LAI** tem sido pouco estudada e muito descumprida, sendo eminente a necessidade de investigá-la em contextos diversos e de aumentar o monitoramento para garantir que ela seja respeitada”.

2.3 Sociedade da Informação

Os seres humanos são os agentes que interagem entre si e com o ambiente onde estão, construindo sistemas sociais com fluxos complexos de trocas de informações [Westrum, 1993, Frey & Osborne, 2017a]. A manutenção destes fluxos é o processo de construção e transformação da sociedade da informação, fenômeno global que, segundo [Castells, 2004], tem algumas características [Werthein, 2000] e regras que exigem um maior volume de interações homem-máquina, em muitas das vezes agravado pelos riscos operacionais [De Almeida, 2024].

A sociedade da informação passa por uma fascinação e entusiasmo quase ingênuo e incontrolável, onde a suposta promessa de ganhos obtidos com algumas soluções é tida como suficiente, não se observando “a que preço” isso está sendo desenvolvido [Solove, 2006]. Neste momento de êxtase, as discrepâncias sociais são agravadas, destacando as diferenças entre os países ricos e industrializados e o restante do mundo.

Os relacionamentos sociais foram “energizados” por um fluxo de informações que não encontra mais obstáculos físicos ou de distância, e que trazem em si os seus próprios novos riscos. A perda do sentimento de controle sobre a própria vida e a perda da identidade são temas que continuam preocupantes e que ainda merecem estratégias eficientes de intervenção [Beniger, 2009].

Essa nova forma de pensar e viver a organização da sociedade da informação está sedimentada na evolução tecnológica recente [Helbing, 2013] e exige uma reestruturação sistêmica das instituições governamentais [Zuboff, 2023, Beniger, 2009], dos modelos de sistemas educacionais e, principalmente, das áreas de segurança, do mercado de trabalho e da requalificação dos trabalhadores, pois os novos costumes incluem outros riscos e desafios éticos [Frey & Osborne, 2017a].

A inovação tecnológica e a difusão e consumo de novas tecnologias lideradas ou patrocinadas pelo Estado potencializaram o processo de transformação digital e de coleta e processamento de dados [Brynjolfsson & McAfee, 2016], construindo novos caminhos e mecanismos capazes de transmitir informações em quantidade, volume e velocidade jamais imagináveis. Segundo [Mansell & Wehn, 1998], “há riscos de que as novas políticas e investimentos nas aplicações das **Tecnologia da Informação e Comunicação (TIC)** introduzam novas forças de exclusão”.

Segundo [Forester, 1985], entre as questões sociais discutidas estão crimes de computador, privacidade, o impacto da nova tecnologia nas mulheres, nas economias emergentes, as armas “inteligentes” e o futuro do trabalho em si. A virtualização das relações sociais, de compra, de interação do homem com as tecnologias e serviços digitais [Koh & Kim, 2004], causou alterações e marcas muito profundas, principalmente nas concepções de espaço e tempo [Ellis et al., 2005, Jones, 1997].

Em alguns casos, estes problemas modernos afetam diretamente a população com a perda da privacidade [Solove, 2006], enquanto que, em contraponto, outra parte da sociedade tem se mobilizado para modelar, construir e promover o “comportamento normal responsável”, inclusive por meio de legislação adequada para proteger os direitos do cidadão na era digital. A satisfação com os avanços e benefícios tecnológicos não deve impedir a identificação e a crítica de áreas de preocupação com a direção e o ritmo atual [Werthein, 2000].

A presente investigação foi idealizada neste momento de sociedade da informação, com trocas em escala de *big data*, e visa extrair *insights* relevantes sobre os riscos existentes no processo de compartilhamento de dados, ocorridos no contexto do Poder Executivo Federal, motivados pelos pedidos de acesso à informação com base na LAI.

2.4 Acesso à Informação

Não é de hoje que se discute o acesso à informação. A divulgação de informações do governo desempenha um papel central no desenvolvimento das sociedades, tendo a transparência, o controle e a participação social como pilares fundamentais para a construção de políticas públicas e a prestação de contas em democracias. Conforme a Classificação Global do Direito à Informação [Global Right to Information Rating, 2026], historicamente, a primeira legislação sobre liberdade de informação (*Freedom of Information (FOI)*) mais antiga foi publicada na Suécia, em 1766, [Kongl. Maj:t, 1766], havendo uma lacuna de 122 anos até a publicação da lei da Colômbia, em 1888.

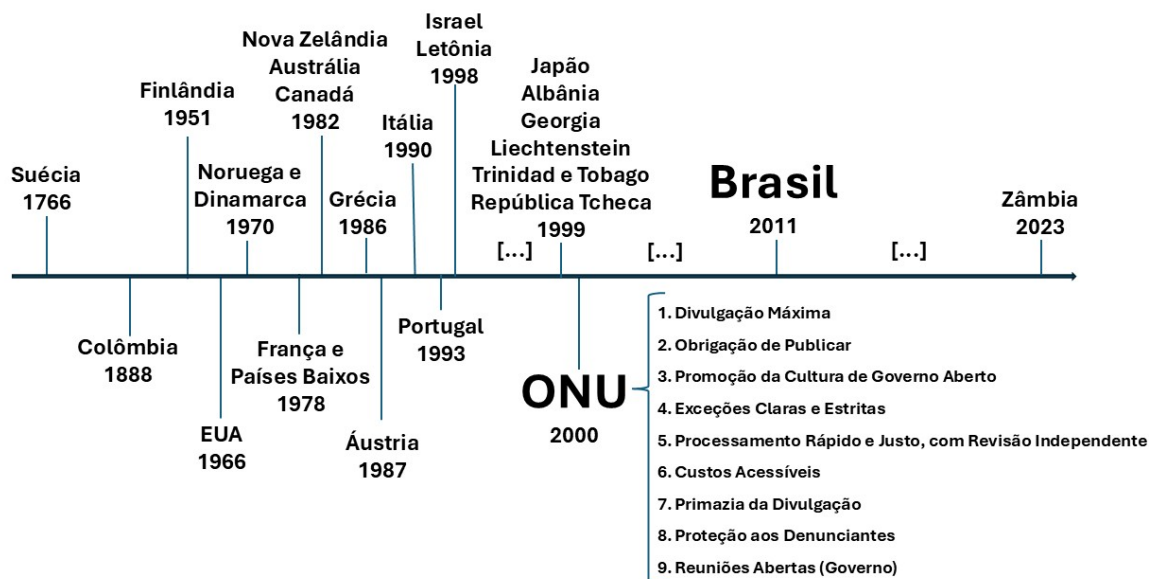


Figura 2.12: Histórico de Publicações das Leis de Liberdade de Informação.

Fonte: Elaborada pelo autor, (2025).

Na imagem é possível observar o relato de publicação de outros países; alguns estão ocultos para destacar as publicações do Relatório da **ONU** de 2000 e a lei brasileira. A partir dos anos de 1990, é visível o crescimento global do número de regulamentos para garantir o acesso à informação como um direito do cidadão [Relly, 2012].

Observando as últimas três décadas, é possível inferir que a legislação sobre liberdade de informação (**FOI**) deixou de ser um “luxo” legislativo desfrutado por algumas democracias avançadas para se tornar uma peça estrutural da democracia. Neste contexto, destaca-se o ano 2000 como um marco para as leis globais de acesso à informação.

A organização não governamental ARTIGO 19 [ARTICLE 19, 2016] publicou a obra “*The Public’s Right to Know: Principles on Freedom of Information Legislation*”, apresentando “nove princípios”, posteriormente endossados pela **ONU** [Commission on Human Rights & Hussain, 2000] e incorporados em seu relatório sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão, apresentado pela Comissão de Direitos Humanos em 18 de janeiro de 2000. Os “nove princípios” passaram a ser difundidos como referência, moldando uma nova geração de legislações de acesso à informação e afetando a forma como os governos concedem acesso às informações e a sociedade exerce suas garantias:

1. **Divulgação Máxima:** toda informação em poder do Estado é pública, salvo exceções restritas.

2. **Obrigaç o de Publicar:**  rg os p blicos devem divulgar informa  es ativamente, sem depender apenas de pedidos.
3. **Promo  o da Cultura de Governo Aberto:** a lei deve estimular pr ticas, treinamentos e campanhas para fortalecer a transpar ncia.
4. **Exce   es Claras e Estritas:** as restri   es de acesso precisam ser espec ficas, bem definidas e aplicadas de forma limitada.
5. **Processamento R pido e Justo, com Revis o Independente:** os pedidos devem ser respondidos prontamente e recusas devem poder ser revistas por inst ncia aut noma.
6. **Custos Acess veis:** as taxas n o podem ser impeditivas ao exerc cio do direito de acesso.
7. **Primazia da Divulga  o:** a lei de acesso deve prevalecer sobre normas de sigilo conflitantes.
8. **Prote  o aos Denunciantes:** indiv duos que revelam irregularidades de interesse p blico devem estar protegidos contra repres lias.
9. **Reuni  es Abertas:** as sess  es e encontros de  rg os p blicos devem ser abertos ao p blico, salvo justificativas legais excepcionais. Este item n o foi incorporado   legisla  o brasileira de acesso   informa  o.

A ado  o de leis de acesso   informa  o e transpar ncia   uma caracter stica de pa ses democr ticos, sendo um recurso fundamental para a constru  o de um governo transparente e democr tico – qualidades complementares da boa governan a, em contraposi  o aos pa ses com regimes totalit rios [Ingrams, 2018]. No Brasil o cen rio n o foi diferente [Campos, 2020].

A constitui  o do Estado Democr tico de Direito do Brasil, consolidada na Carta Magna de 1988, prev  o direito de acesso   informa  o. At  2011, exatos 245 anos ap s a lei sueca, o acesso   informa  o ainda era uma tem tica nebulosa, quando o pa s foi sentenciado pela Corte Interamericana de Direitos Humanos (2010), no caso “Gomes Lund e outros – Guerrilha do Araguaia *vs.* Brasil”, gerando uma exposi  o internacional negativa. Ap s tal exposi  o, o Brasil reagiu e publicou a Lei Federal n  12.527, de 18 de novembro de 2011 – LAI – regulamentada pelo Decreto Federal n  7.724, de 16 de maio de 2012, incorporando oito dos nove princ pios da transpar ncia [Commission on Human Rights & Hussain, 2000, Matozo & Baptistella, 2024], conforme Tabela 2.2.

Tabela 2.2: Aplicação dos Princípios de Transparência na **LAI** do Brasil. Elaborado pelo autor

Princípio (ONU)	Lei 12.527/2011	Decreto 7.724/2012
Máxima divulgação (publicidade como regra)	Art. 3º, I	Art. 2º <i>caput</i>
Obrigação de publicar (transparência ativa)	Art. 3º, II; art. 8º; art. 10 §3º–§4º (requisitos dos sítios)	Arts. 45, 63–64 (publicidade; entidades privadas)
Promoção de governo aberto / cultura de transparência e controle social	Art. 3º, IV e V	Art. 2º <i>caput</i>
Exceções claras e restritas (classificação e limites)	Cap. IV; Art. 21 par. único e arts. 23–31 (direitos humanos)	Arts. 25–38; 49–54 (Comissão Mista de Reavaliação de Informações (CMRI))
Processamento rápido com revisão independente	Art. 3º, III; arts. 10–11 (procedimento e prazos)	Arts. 15–21 (prazos, forma de resposta)
Prazos e revisão / recursos independentes	Arts. 15–18 e 35 (CMRI)	Arts. 21–24; 49–54 (procedimentos e CMRI)
Custos acessíveis (gratuidades com ressarcimento de cópias)	Art. 12	Art. 18
Primazia da divulgação (princípio pró-transparência)	Art. 3º, I (publicidade como regra; sigilo como exceção)	Art. 2º <i>caput</i>
Proteção a denunciantes	Art. 44 (inclui 126-A na Lei 8.112/1990)	–
Reuniões abertas	–	–

A **LAI** estimula a transparência e o controle social, mas também expõe os indivíduos a potenciais riscos de intrusão por meio do compartilhamento de dados. A gestão da Política Pública de transparência e acesso à informação no Brasil é executada pela **Secretaria**

Nacional de Acesso à Informação da Controladoria-Geral da União (SNAI/CGU), com ações relacionadas ao Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal, dentre elas a gestão da **Plataforma Integrada de Ouvidoria e Acesso à Informação (Fala.BR)** como canal digital centralizado para acolher os pedidos de acesso à informação da população.

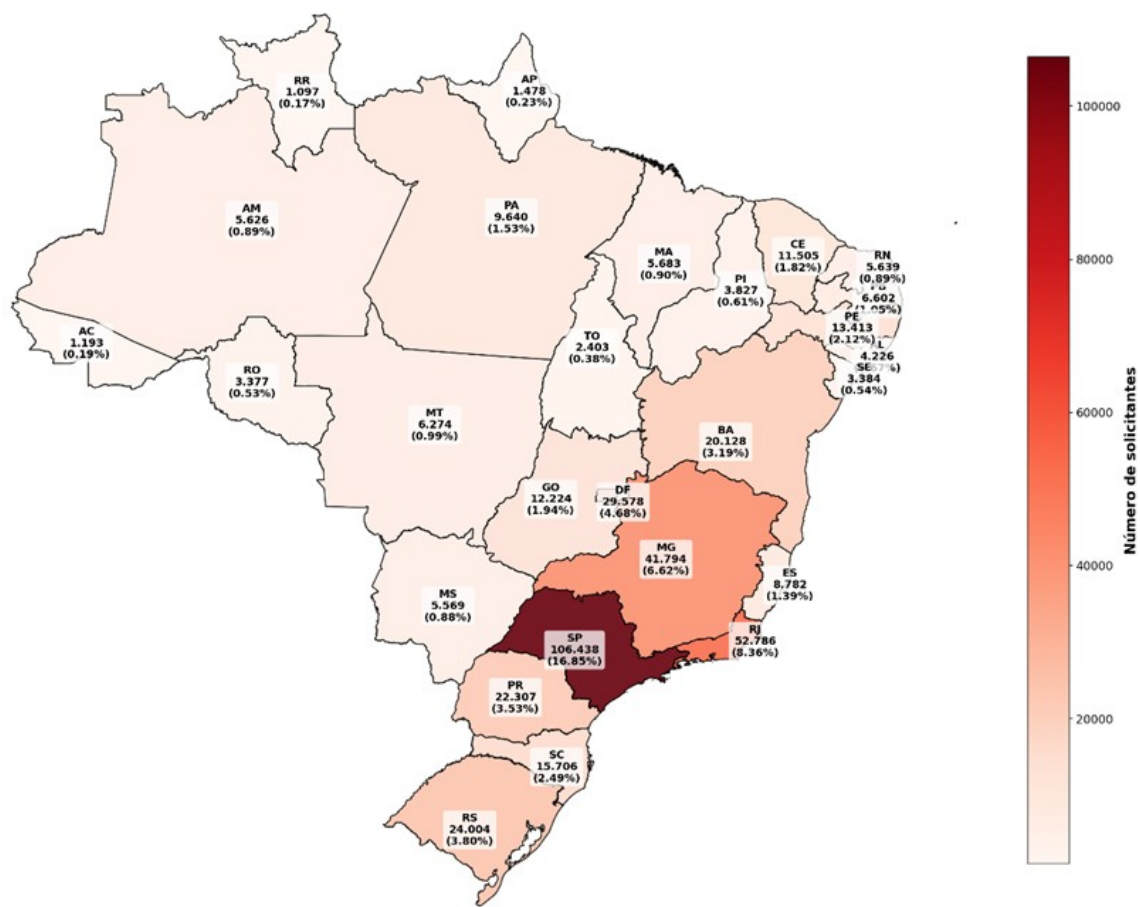
Segundo [Hazell & Worthy, 2010], é necessário monitorar: quanto uma lei de liberdade de informação é utilizada (volume de solicitações); quanto tempo os solicitantes devem esperar por uma resposta (atrasos); quanta informação é divulgada (proporção de solicitações que resultam em divulgação total ou parcial); quantos requerentes apelam; e quantos recursos são acatados. O Brasil segue este padrão de registro quantitativo dos pedidos de acesso à informação protocolados na plataforma; os números de pedidos da **LAI** no Brasil podem ser conferidos no Painel de Monitoramento da Lei de Acesso à Informação, disponibilizado pela **Controladoria-Geral da União (CGU)**, destacados na Figura 2.13.

Tipo de Resposta	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Acesso Concedido	82,28%	71,64%	69,16%	71,22%	67,58%	69,83%	67,84%	70,34%	58,90%	68,43%	72,50%	74,85%	74,01%	74,50%
Acesso Negado	8,80%	11,15%	11,07%	8,06%	10,10%	10,18%	11,49%	8,37%	7,06%	10,41%	7,16%	7,72%	8,36%	7,58%
Acesso Parcialmente Concedido	1,32%	3,96%	3,83%	7,53%	7,31%	7,08%	7,38%	6,41%	4,53%	7,21%	6,80%	5,97%	6,67%	7,05%
Informação Inexistente	3,01%	2,55%	2,09%	5,08%	6,40%	4,68%	5,30%	5,10%	3,20%	6,07%	5,56%	3,68%	3,30%	3,26%
Não se trata de célula de solicitação de informação	0,04%	4,57%	8,26%	3,33%	3,63%	3,16%	3,37%	4,40%	21,79%	3,84%	3,29%	3,19%	3,29%	3,04%
Órgão não tem competência para responder sobre o assunto	3,21%	4,34%	3,90%	2,83%	2,94%	3,15%	2,67%	3,07%	2,38%	2,31%	2,55%	2,40%	2,49%	2,33%
Pergunta Duplicada/Repetida	1,35%	1,79%	1,69%	1,94%	2,05%	1,92%	1,95%	2,32%	2,00%	1,72%	2,14%	2,20%	1,88%	2,25%

Figura 2.13: Tipos de Respostas a Pedidos de Acesso à Informação.

Fonte: Controladoria-Geral da União (CGU).

Conforme registros da **CGU**, desde a publicação da **LAI** no ano de 2011, o montante de 631.710 solicitantes responde pelos 1.476.733 pedidos recebidos, dos quais 1.476.675 já haviam sido respondidos, gerando uma média de 2,4 pedidos por pessoa. O solicitante brasileiro [Nasu et al., 2022] que usufrui dos seus direitos previstos na **LAI** tem um perfil próprio e se concentra em áreas específicas do território nacional, conforme especificado na Figura 2.14.



Os pedidos sem identificação de UF totalizam 207.182, o que equivale a aproximadamente 32,8% do total de solicitações registradas.

Figura 2.14: Distribuição de demandantes da LAI no Brasil.
Fonte: Elaborada pelo autor, (2025)

A maior parte dos usuários, responsáveis por 243.389 pedidos, compõem um grupo com faixa etária “não identificada”. A outra parcela dos solicitantes identificados (104.975) são os mais ativos e estão na faixa etária de 31 a 40 anos; outros 99.944 pedidos são dos usuários entre 21 e 30 anos; com 72.946 pedidos estão os de 41 a 50 anos; os de 51 a 60 anos tendo feito 54.875 pedidos; na sequência os com idade ≥ 60 , contabilizando 36.295; ficando a parcela da população ≤ 20 anos em última posição, detendo apenas 19.386 pedidos registrados.

A distribuição geográfica dos demandantes demonstra uma concentração nos estados de São Paulo (SP) com 106.438 pedidos (16,85%); Rio de Janeiro (RJ) com 52.786 pedidos (8,36%); Minas Gerais (MG) com 41.794 pedidos (6,62%); Distrito Federal (DF) com 29.578 pedidos (4,68%); Rio Grande do Sul (RS) com 24.004 pedidos (3,80%); e Paraná

(PR) com 22.307 pedidos (3,53%). Juntos, estes estados representam 43,84% do total de pedidos identificados.

Na construção da Figura 2.14 identificou-se que 207.182 pedidos ($\approx 32,8\%$) não apresentavam a identificação da **Unidade Federativa (UF)** de origem e, por este motivo, não foram incorporados. Outros dados estruturados sobre as decisões da **CGU** e da **CMRI** da **Presidência da República (PR)**, relativas aos recursos apresentados a essas instâncias no âmbito da **LAI**, podem ser consultados no *site* de “Busca de Precedentes da CGU”.

Outras ações são desenvolvidas pela **CGU** para governar os processos da **LAI**, tais como a Escala Brasil Transparente – Avaliação 360º, iniciativa que avalia aspectos das transparências passiva e ativa, verificando o cumprimento da **LAI** em todos os estados, no e nos 665 municípios com mais de 50 mil habitantes [Controladoria-Geral da União, 2026, Controladoria-Geral da União, 2021, Controladoria-Geral da União,].

2.5 Compartilhamento de Dados

Dada a complexidade do fluxo de compartilhamento e disponibilidade de grandes volumes de dados e a potencialização da capacidade de processamento da população, é possível perceber o crescimento de tecnologias e o interesse das instituições públicas e privadas na busca pela extração de *insights* estratégicos para fundamentar a tomada de decisão.

O aumento do consumo e da dependência tecnológica é uma característica marcante desta sociedade digital [Bell, 1973]. Para equilibrar e regular este processo, o Brasil desenvolveu várias ações, dentre as principais a Lei nº 13.709, de 14 de agosto de 2018 – **LGPD** – que conceitua o tratamento de dados como:

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

Inciso X, artigo 5º da LGPD (grifo do autor).

Neste recorte da legislação, é possível inferir que o compartilhamento de dados está contido no processo de tratamento de dados. De acordo com [Jussen-Lengersdorf et al., 2023], o compartilhamento de dados pode ser definido como “o processo de conceder a terceiros acesso a conjuntos de dados de outros”. Esses terceiros podem incluir empresas, indivíduos ou instituições públicas, e os dados compartilhados são frequentemente utilizados para desenvolver novas aplicações e serviços.

Nesta investigação, utilizou-se do Ciclo de Vida do Tratamento de Dados (Figura 2.15), proposto pela **Secretaria de Governo Digital (SGD)** e descrito no Guia de Boas Práticas

para Implementação da **LGPD** na Administração Pública Federal, que destaca o Ciclo de Vida do Tratamento de Dados Pessoais organizado em fases, alinhadas ao contexto de hiperconectividade da sociedade digital [Fassnacht et al., 2024].



Figura 2.15: Fases do Ciclo de Vida do Tratamento de Dados [gui, 2020].

Segundo o Manual da **Secretaria de Governo Digital do Ministério da Economia (SGD/ME)**, o ciclo de vida do tratamento de dados é organizado em 5 (cinco) fases e assume protagonismo estratégico no governo federal [Zahid et al., 2023, Shah et al., 2021, Koo et al., 2020].

A fase de compartilhamento de dados, objeto desta investigação, é um processo que requer ações técnicas e administrativas de governança de dados e práticas robustas de segurança da informação e controle dos riscos. Tais medidas são indispensáveis para mitigar os riscos associados, garantir a proteção dos direitos dos titulares, promover uma cultura de consumo consciente de dados e potencializar o uso responsável das informações produzidas ou custodiadas pelo governo, permitindo a tomada de decisão baseada em evidências [Mortenson et al., 2015].

O Sistema de Governança de Dados do Executivo Federal é alicerçado em um conjunto de normativos, tais como a **LAI**, a **LGPD**, a Lei de Governo Digital, o Decreto de compartilhamento de dados no âmbito da administração pública federal e tantos outros que, juntos, delimitam e definem orientações técnicas e responsabilidades específicas em relação à proteção de dados pessoais, compartilhamento de dados, transformação e governo digital.

A **LAI** demanda governança de dados, estimula a transparência e o controle social, mas também pode expor indivíduos a riscos de intrusão em sua esfera privada, em linha com a discussão clássica de [Prosser, 1960] sobre violações da privacidade.

Governança de dados – exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos.

Inciso XV, art. 2º do Decreto 10.046/2019.

Por relevância, é preciso entender que, quando falamos de dados, é necessário enxergar além das informações óbvias armazenadas em computadores e em arquivos físicos. É preciso ampliar o entendimento do que pode ser coletado no preenchimento de um formulário ou de anotações em blocos de reunião; mais precisamente, é necessário observar os “dados brutos” [McCloud et al., 2023], não processados, que por si só não significam muito, passam despercebidos e podem ser tidos como símbolos que representam propriedades de objetos, eventos e seu ambiente [Ackoff, 1989].

[Fricke, 2019] deixa explícito que “um dado é uma proposição”; [Floridi, 2013] descreve os dados como “a diferença entre duas variáveis não interpretadas, x e y ”, podendo ser interpretado em três níveis: como “falta de uniformidade no mundo real”, “falta de uniformidade entre sinais” e “falta de uniformidade entre símbolos”. [Setzer, 2006] afirma que os dados são uma sequência de símbolos quantificados que podem ser reproduzidos sem que se perceba a diferença com o original; para [Sellars, 1973], os dados são capazes de fornecer um status justificatório positivo à informação; já para [Le Coadic, 1996], dados são uma representação composta de informação codificada que pode ser colocada em processamento eletrônico; e para [Barros et al., 2023], eles são a matéria-prima da informação e podem ser interpretados e utilizados na formulação de políticas públicas e na tomada de decisões do governo.

Para fins desta investigação, adotou-se o conceito de dado descrito no Decreto nº 8.777, de 11 de maio de 2016:

Dado – sequência de símbolos ou valores, representados em qualquer meio, produzidos como resultado de um processo natural ou artificial.

Inciso I, art. 2º do Decreto nº 8.777/2016.

A importância dos dados compartilhados envolve a correta compreensão de que são a matéria-prima essencial e fundamental na criação de novos ciclos do conhecimento, oferecendo insumos para processos interativos do ciclo de construção da pesquisa acadêmica [Rodrigues et al., 2022, Curty & Aventurier, 2017].

O Brasil é um país que tem uma alta taxa de concessão de acesso aos seus dados [Lemieux et al., 2015], mas ainda carece de boas práticas de compartilhamento, de ações

técnicas e administrativas em consonância com as dimensões de privacidade, para assegurar que o direito à informação pública não se converta em vulnerabilidade para o cidadão, mas sim em um instrumento de democracia seguro [Candela et al., 2015].

2.6 Riscos

Dada a sua natureza e a transversalidade do tratamento de dados, todas as atividades contêm riscos associados e demandam ações de governança [Wang et al., 2021], independentemente da área do conhecimento, podendo ser riscos cibernéticos [Konzen et al., 2012], riscos de privacidade [Zottmann et al., 2023] ou riscos de segurança da informação [Bezerra, 2024].

A Estratégia Federal de Governo Digital do Brasil, no ciclo de 2024–2027 e em consonância com a LAI, promove a digitalização dos serviços governamentais, prioriza processos de trabalho digitais e corrobora com o esforço nacional de orientar e direcionar a população para o uso e consumo das plataformas digitais do governo; esta estratégia é global e requer governança dos riscos próprios.

A cultura orientada por dados está associada ao conceito de valores, crenças e suposições que orientam uma instituição na maneira como ela deve proceder para ter sucesso [Chatterjee et al., 2024]. As capacidades inovadoras orientadas por dados foram aprimoradas pelas aplicações de tecnologia avançada da TIC, fortes capacidades analíticas, gerenciamento eficaz de dados e mecanismos de governança [Ransbotham & Kiron, 2017, Wang et al., 2018].

O Governo Federal é o maior agente nacional de tratamento de dados da população brasileira, responsável por grandes volumes de compartilhamento de dados. Quando consideradas bases governamentais de dados como a Conta Plataforma digital de serviços públicos do Governo Federal (Gov.BR), que alcançou ≈ 166 milhões de usuários em 2025 [Ministério da Gestão e da Inovação em Serviços Públicos, 2025]; o Cadastro Nacional de Eleitores (Tribunal Superior Eleitoral (TSE)), com dados de biometria de 158,6 milhões de pessoas, aproximadamente 86% do eleitorado; o Cadastro Único (CadÚnico), com $\approx 94,6$ milhões de pessoas; e o Censo da Educação Básica (INEP/MEC), com $\approx 4,9$ milhões de estudantes por ano – dentre várias outras – confirma-se a posição favorecida da Administração Pública brasileira como uma das maiores entidades controladoras de dados pessoais do país, mesmo ante entidades privadas como bancos, financeiras de crédito, entidades educacionais, instituições de saúde e telecom.

Tais plataformas de compartilhamento e tratamento de dados do Governo Federal compõem um grupo de alvos prioritários para crimes e incidentes cibernéticos em situações de acesso e compartilhamento indevido de dados. Este processo potencializa o compar-

tilhamento dos dados motivados pela LAI, assim como os riscos relativos à privacidade e à governança de dados, podendo comprometer os requisitos de segurança da informação – disponibilidade, integridade, confidencialidade e autenticidade – das informações produzidas e custodiadas pelo governo.

Em consulta realizada em 15 de abril de 2025 sobre os registros de incidentes cibernéticos [Craig et al., 2014] ocorridos no recorte temporal de 2021 a 2025, identificou-se que o Centro de Tratamento e Resposta a Incidentes Cibernéticos Centro de Tratamento e Resposta a Incidentes Cibernéticos (CTRIC) registrou o total de 52.485 casos (ocorrências de vulnerabilidades – 27.432 + incidentes cibernéticos – 25.053), distribuídos em: Vulnerabilidade de Criptografia (13.061); Vazamento de Dados (13.027); Abuso de Sítio Web (9.606); Vulnerabilidade DRDoS (9.153); *Software* Vulnerável (5.574); *Scan* (2.943); *Phishing* (2.114); Página Falsa (2.005); Abuso no Serviço de *e-mail* – SMTP (1.070); e *Ransomware* (38). Cabe ressaltar que, nos termos da Portaria Ministerial nº 91, de 26 de julho de 2017, o [CTIR GOV, 2025] registra apenas os incidentes ocorridos no setor público, não havendo registros relacionados ao setor privado nesses dados.

As vulnerabilidades destacadas [CTIR GOV, 2025] afetam a confiança da sociedade na capacidade de autogovernança institucional do Estado, colocando a integridade da população em recorrente situação de risco. O [Project Management Institute, 2004] define risco como um evento ou condição incerta que, se ocorrer, tem um efeito positivo ou negativo nos objetivos do projeto, sem, no entanto, definir incerteza no .

Segundo [Olsson, 2002], o risco é caracterizado pela incerteza de resultados futuros – só há risco quando há incerteza, mas pode haver incerteza sem risco. Para [Morgan & Henrion, 1990], é preciso distinguir risco de incerteza: os riscos são eventos sobre os quais podemos refletir em termos de serem factíveis de ocorrer, enquanto a incerteza é o domínio do imprevisível. De acordo com [Head, 2009], o risco representa um acontecimento futuro que tanto pode ser positivo quanto negativo, existindo três características que o descrevem: o sentido (positivo ou negativo), o grau de probabilidade e a magnitude das suas consequências.

A norma ABNT NBR ISO 31000:2018 apresenta uma perspectiva onde o risco pode ser compreendido como “um efeito de incerteza com potencial para causar um desvio nos objetivos em relação ao esperado ou planejado”. Risco é uma situação ou evento em que algo de valor humano (incluindo os próprios humanos) está em jogo e cujo resultado é incerto [Rosa et al., 2003, Aven & Renn, 2019].

A Instrução Normativa Conjunta do Ministério do Planejamento e da Controladoria-Geral da União nº 1, de 2016 (INC MP/CGU nº 1/2016), que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, destaca risco como sendo a “possibilidade de ocorrência de um evento que venha a ter impacto

no cumprimento dos objetivos”, e determina que os riscos sejam medidos em termos de impacto e de probabilidade.

Por não haver um consenso na literatura acerca da padronização da tipologia de riscos, Whitfield (2003) afirma que as instituições devem adotar as tipologias que melhor as representem. Desta forma, para a delimitação das tipologias de riscos desta pesquisa, aplicou-se a referência descrita no artigo 18 da **INC MP/CGU nº 1/2016**:

Art. 18. Os órgãos e entidades, ao efetuarem o mapeamento e avaliação dos riscos, deverão considerar, entre outras possíveis, as seguintes tipologias de riscos: a) riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas; b) riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional; c) riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade; e d) riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

INC MP/CGU nº 1/2016.

Estas tipologias descritas na **INC MP/CGU nº 1/2016** e o conceito de riscos descrito na **ABNT NBR ISO 31000:2018** compõem a estrutura metodológica aplicada na pesquisa.

2.7 Processo de Tomada de Decisão

Os riscos institucionais precisam ser governados e, na última década, tem ocorrido um direcionamento e adoção de ações de governança de risco pelo Estado. Identificar, compreender, avaliar, gerir e comunicar sobre riscos ou problemas deles derivados exige que os gestores de dados dos órgãos públicos adquiram novas competências digitais [Aven & Renn, 2019]. [Renn et al., 2022] destaca que os riscos sistêmicos são caracterizados pela sua alta complexidade, múltiplas incertezas, grandes ambiguidades e efeitos transgressivos sobre outros sistemas fora do sistema de origem, envolvendo muitos elementos interativos cujos efeitos emergentes ainda são pouco compreendidos [Aven & Renn, 2019], o que sobrecarrega as instituições.

Os riscos associados ao compartilhamento de dados entre órgãos públicos são um exemplo de riscos sistêmicos, o que justifica a necessidade de adoção de processos e metodologias capazes de identificá-los e direcionar os gestores de riscos na definição de estratégias de governança e mitigação de forma estratégica. Cada risco identificado deverá ser convertido

em ação prática de governança, fundamentada em tomadas de decisão práticas [Garuti & Spencer, 2007].

Esse cenário de alto risco vivido pelos gestores de dados governamentais exige a aquisição de competências digitais para a aplicação de metodologias sistemáticas, capazes de entregar análises estratégicas confiáveis que vão além de identificar e classificar os riscos, permitindo também tomar decisões quanto à alocação de recursos e priorização segundo fatores de risco como gravidade e impacto. Nisto aplica-se o uso da *Failure Mode and Effects Analysis* (FMEA) na tomada de decisão sobre riscos [Wang et al., 2009], associada a modelos multicritério de hierarquização como a *Analytic Hierarchy Process* (AHP) de Thomas L. Saaty [Saaty, 1977].

Somos tomadores de decisão [Saaty, 2009] mesmo que muitas das nossas decisões sejam reflexos automáticos ou intuitivos [Plassmann et al., 2005]. Este conjunto de processos cognitivos que envolvem percepção, interpretação, imaginação, memória, raciocínio e linguagem é único quando comparado a outros animais. Estruturar uma decisão é o primeiro passo que uma mente pensante dá para organizar e representar qualquer problema; em particular um problema de decisão que precise de ação – precisamos de estruturas geométricas para representar nossa compreensão abstrata das influências entre os elementos do mundo real e suas conexões e interações [Garuti & Spencer, 2007].

Em geral, um problema começa com alguma insatisfação com uma situação em curso ou, segundo [Altshuller, 1998], “um problema é uma contradição na mente”. Nossas mentes são condicionadas e guiadas por sentimentos de satisfação ou insatisfação que são preenchidos em diferentes graus, como [Maslow, 1943] demonstrou em sua hierarquia de necessidades. Para lidar com um problema, tenta-se identificar os elementos que se relacionam a ele, suas conexões e interações, a(s) causa(s) que dão origem ao problema e possíveis formas de solução; para fazer isso, temos que estruturar o problema [Frey & Osborne, 2017b]. Em geral, existem dois tipos de estruturas usadas para representar problemas: hierarquias e redes.

As estruturas devem satisfazer no mínimo dois requisitos: que sejam lógicas na identificação e no agrupamento de coisas semelhantes e que as relacionem com precisão de acordo com o fluxo de influência existente entre elas [Saaty, 2009]; a estrutura hierárquica de decisão pode ser formalmente organizada e definida em termos matemáticos [Saaty, 1977, Saaty & Vargas, 1980, Saaty, 1986, Saaty, 1990].

A prática da tomada de decisões está ligada à avaliação das alternativas, todas satisfazendo um conjunto de objetivos pretendidos [Saaty, 1990]. Muitas vezes é mais difícil lidar com a estruturação do problema, pois isso envolve um grau consideravelmente maior de abstração do que a própria solução; precisamos de uma forma de ideação inventiva [Ross, 2006] para estruturar um problema.

Nesta pesquisa adotou-se duas ferramentas para a estruturação do processo de tomada de decisão: a **FMEA** [Enang et al., 2022], uma estrutura de decisão operacional orientada à análise, identificação e priorização de riscos, que organiza informação sobre falhas, mede criticidade e força uma decisão de tratamento e priorização, focada na identificação de “o que tratar primeiro”, não em “qual alternativa maximiza objetivos estratégicos” – o que pode não representar uma aplicação prática [Wang et al., 2009]; e, por este motivo, utilizou-se também a metodologia **AHP** de Thomas L. Saaty [Saaty, 1977], uma metodologia que tem por objetivo a escolha de alternativas considerando diferentes critérios e subcritérios qualitativos e quantitativos, sendo um dos aspectos mais importantes da **AHP** a sua capacidade de estruturar problemas complexos, multipessoais, multicritérios e multiperíodos hierarquicamente [Saaty, 1990].

2.8 Análise de Modos e Efeitos de Falha (FMEA)

A **ABNT**, na norma NBR 5462 (1994) [ABNT, 1994], adota a sigla originária do inglês **FMEA** (*Failure Mode and Effects Analysis*) ou, em tradução livre, Análise de Modos e Efeitos de Falhas, definida como técnica analítica utilizada por um time como uma maneira de garantir que, até a extensão possível, os modos potenciais de falha e suas causas e mecanismos associados tenham sido considerados e localizados.

Observa-se que a norma NBR 5462/1994 utiliza o termo “pane” para expressar falha, especifica que a **FMEA** é um método qualitativo de análise de confiabilidade que envolve o estudo dos modos de falha que podem existir para cada item analisado, e define falha como sendo o “término da capacidade de um item desempenhar a função requerida”.

Originalmente conhecida como FMECA – *Procedures for Performing a Failure Mode, Effects and Criticality Analysis* –, a **FMEA** está associada como padrão para as operações militares norte-americanas desde 1949 [U.S. Department of Defense, 1980], tendo como objetivo a avaliação da confiabilidade para determinar os efeitos nos sistemas e falhas em equipamentos. As falhas identificadas foram classificadas de acordo com seus impactos nos sucessos das missões e com a segurança pessoal e de equipamentos.

O conceito de falha é fortemente dependente do contexto – um evento que provoca uma diminuição parcial ou total da função do produto e de suas metas de desempenho. Por fim, uma falha é definida como a falta de capacidade de um item em desempenhar a função para a qual foi projetado, podendo ser considerada um risco. Pritchard (2001) descreve o risco como sendo composto por três elementos fundamentais: o evento (E), a ocorrência (O) e a gravidade (G). O evento é a descrição do risco que pode ocorrer; uma vez definido, sua probabilidade de ocorrência pode ser estimada por meio de cálculos

estatísticos e da teoria da probabilidade; já a severidade reflete o impacto da ocorrência do risco sobre os objetivos do projeto.

Segundo [Carvalho et al., 2019], a análise é direcionada por perguntas como: De que maneiras um componente pode falhar? Quais tipos de falhas são observados? Quais partes do sistema são afetadas? Quais são os efeitos da falha sobre o sistema? Qual a importância da falha? Como prever a ocorrência das falhas? Nesta pesquisa optou-se pelo sistema de pontuação em escalas de 1 a 10, conforme descritos nas Tabelas 2.3, 2.4 e 2.5.

Tabela 2.3: Escala de Ocorrência de uma Falha. Adaptado de [Ben-Daya & Raouf, 1996] e [Wang et al., 2009].

Pont.	Descrição Qualitativa	Descrição Quantitativa
1	Bastante remota; muito improvável – até pessoas experientes no fluxo não se recordam da última ocorrência.	Chance quase zero de ocorrer (0,1%).
2	Improvável – as pessoas mais experientes se recordam, com dificuldade, de uma vez em que ocorreu.	Chance menor que 1% de ocorrer.
3	Chance pequena de ocorrer – pessoas mais experientes lembram, com dificuldade, de poucas vezes.	Chance de 1 a 3% de ocorrer.
4	Alguma chance de ocorrer – pessoas mais experientes no fluxo apontam poucos casos.	Chance de 3 a 5% de ocorrer.
5	Poucas ocorrências – todos envolvidos no fluxo se lembram de poucos casos.	Chance de 5 a 8% de ocorrer.
6	Número considerável de ocorrências – pessoas mais experientes apontam alguns casos.	Chance de 8 a 15% de ocorrer.
7	Ocorre com alguma frequência – todos envolvidos no fluxo lembram de alguns casos.	Chance de 15 a 25% de ocorrer.
8	Ocorre com alguma frequência – todos envolvidos no fluxo lembram de alguns casos.	Chance de 25 a 35% de ocorrer.
9	Ocorre muito provavelmente – todos envolvidos no fluxo se lembram de muitos casos.	Chance de 35 a 50% de ocorrer.
10	Ocorre quase certamente (diversas vezes) – todos da instituição conseguem apontar muitos casos.	Chance maior de 50% de ocorrer.

Tabela 2.4: Escala de Gravidade (Severidade). Adaptado de [Wang et al., 2009].

Pont.	Efeito	Gravidade do efeito
1	Nenhum	Sem efeito
2	Muito pequeno	Sistema operável com interferência mínima
3	Menor	Sistema operável com alguma degradação de desempenho
4	Muito baixo	Sistema operável com degradação significativa de desempenho
5	Baixo	Sistema inoperante sem danos
6	Moderado	Sistema inoperante com danos menores
7	Alto	Sistema inoperante com danos no equipamento
8	Muito alto	Sistema inoperante com falha destrutiva sem comprometer a segurança
9	Perigoso com aviso	Classificação muito alta quando um modo de falha potencial afeta a operação segura do sistema com aviso
10	Perigoso sem aviso	Classificação muito alta quando um modo de falha potencial afeta a operação segura do sistema sem aviso

Tabela 2.5: Escala de Detecção de uma Falha. Adaptado de [Wang et al., 2009].

Pont.	Detecção	Probabilidade de detecção pelo controle de projeto
1	Quase certo	O controle de projeto detectará a causa/mecanismo potencial e o modo de falha subsequente
2	Muito alto	Há grande probabilidade de que o controle de projeto detecte a causa/mecanismo potencial e o modo de falha subsequente
3	Alto	Grande probabilidade de o controle de projeto detectar a causa/mecanismo potencial e o modo de falha subsequente
4	Moderadamente alto	Chance moderadamente alta de que o controle de projeto detecte a causa/mecanismo potencial e o modo de falha subsequente
5	Moderado	Chance moderada de que o controle de projeto detecte a causa/mecanismo potencial e o modo de falha subsequente
6	Baixo	Pouca chance de o controle de projeto detectar a causa/mecanismo potencial e o modo de falha subsequente
7	Muito baixo	Muito baixa probabilidade de o controle de projeto detectar a causa/mecanismo potencial e o modo de falha subsequente
8	Remoto	Chance remota de que o controle do projeto detecte a causa/mecanismo potencial e o modo de falha subsequente
9	Muito remoto	Chance muito remota de que o controle de projeto detecte a causa/mecanismo potencial e o modo de falha subsequente
10	Incerteza absoluta	O controle de projeto não consegue detectar a causa/mecanismo potencial e o modo de falha subsequente

O objetivo da **FMEA** é a priorização dos modos de falha. Com a aplicação do modelo, tomou-se conhecimento dos modos de falha do processo de compartilhamento de dados, permitindo a tomada de decisão estratégica sobre providências técnicas e administrativas a serem executadas. Os fatores de risco – ocorrência (O), gravidade (G) e detecção (D) – devem ser pontuados conforme escalas de 1 a 10 com base nos contextos descritos nas Tabelas 2.3, 2.4 e 2.5. O **Número de Prioridade de Riscos (NPR)** é o produto final, derivado da multiplicação dos fatores de risco, conforme a equação a seguir:

$$\text{NPR} = O \times G \times D \quad (2.1)$$

O **NPR** é uma informação estratégica que auxilia no processo de tomada de decisão e alocação de recursos para a gestão adequada dos riscos; quanto maior o **NPR** de um modo

de falha, maior deve ser a atenção e o emprego de recursos para a governança do risco. Ao identificar o **NPR**, está sendo executado, na prática, um processo de hierarquização de riscos.

Padrões como as normas **ABNT** **ISSO/IEC** 31010:2012 (TC56) e 60812:2018 indicam explicitamente que os modos de falha podem ser ranqueados para suportar decisões de tratamento, situando a **FMEA** como técnica sistemática de priorização dentro de processos de gestão e avaliação de riscos. No entanto, resultados imprecisos podem ser gerados devido às condições incertas sob as quais a avaliação de riscos utilizando a **FMEA** é realizada [Enang et al., 2022]. Para amenizar as incertezas e a imprecisão do processo de avaliação, optou-se pela aplicação da metodologia de tomada de decisão multicritério **AHP** de Thomas L. Saaty [Saaty, 1977, Saaty & Vargas, 1980, Saaty & Vargas, 1984, Saaty, 1986, Saaty, 1990, Saaty, 1995, Saaty & Shih, 2009, Saaty, 2008, Saaty, 2009].

2.9 Análise Hierárquica de Processo (AHP)

A tomada de decisão multicritério refere-se à triagem, priorização, classificação ou seleção de um conjunto de alternativas sob critérios geralmente independentes, incomensuráveis ou conflitantes. A característica central dos métodos multicritérios de hierarquização está em procurar a solução mais adequada para as diversas alternativas disponíveis, priorizando a utilização otimizada dos recursos disponíveis; esta técnica considera um conjunto de critérios de avaliação e opções alternativas dentre as quais a melhor decisão deve ser tomada.

Uma hierarquia é uma forma poderosa de classificação usada pela mente para ordenar informações obtidas a partir da experiência ou do próprio pensamento, a fim de compreender a complexidade do mundo ao nosso redor, de acordo com a ordem e a distribuição das influências que levam à obtenção de certos resultados [Saaty, 2009]. Neste contexto, o pesquisador e professor Thomas Lorie Saaty [Saaty, 1977] propôs o método **AHP** e descreve que na tomada de decisão o nível de consenso predefinido deve ser alcançado, destacando a avaliação do grau de discordância (Figura 2.16).

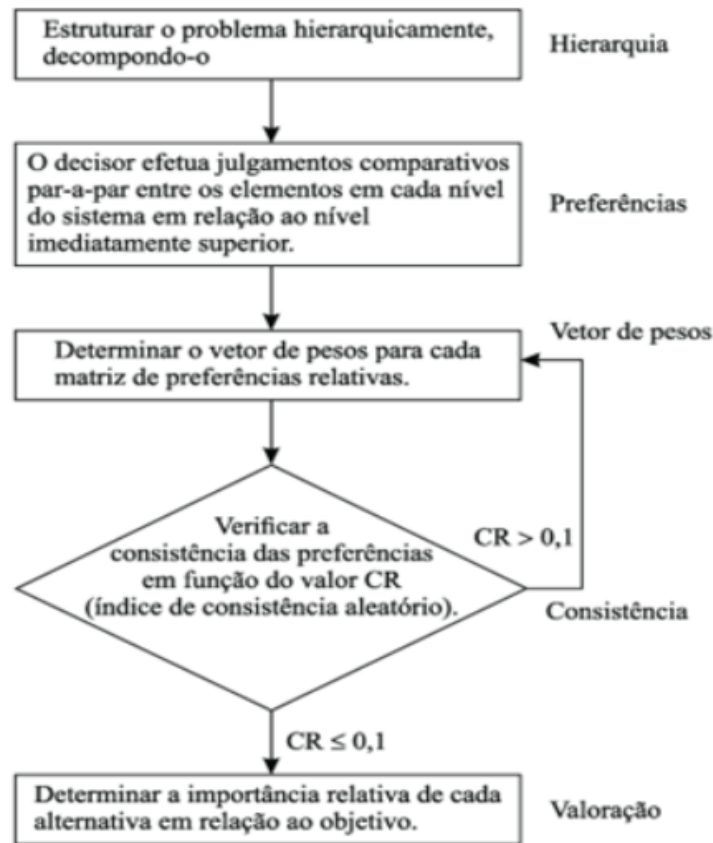


Figura 2.16: Fluxo de aplicação da AHP [Santos & Cruz, 2013].

A **AHP** de [Saaty & Vargas, 1980] consolidou-se como uma das ferramentas multicritério mais aplicadas no processo de tomada de decisão, auxiliando os tomadores de decisão a comparar opções e encontrar o melhor caminho, utilizando dados quantitativos e fatores qualitativos.

[Marins et al., 2009] sugerem estruturar o problema em três níveis [Saaty & Vargas, 1980, Saaty, 1990]: no nível mais alto da hierarquia, estabelece-se o problema de análise de decisão a ser apoiado pela **AHP**; nos níveis intermediários, são posicionados os critérios, os quais podem ou não ser desdobrados em subcritérios; e, no nível mais baixo, estão as alternativas a serem consideradas para a tomada de decisão.

2.9.1 Estruturação do Problema

A **AHP** ajuda a determinar a importância relativa de um conjunto de atividades ou critérios. As alternativas são ranqueadas por ordem de prioridade com base em um conjunto de critérios pré-definidos organizados em uma matriz de decisão. [Marins et al., 2009] sugerem estruturar o problema estudado da seguinte forma: no nível mais alto da hierarquia, estabelece-se o problema de análise de decisão a ser apoiado pela **AHP**; no

nível mais baixo, estão as alternativas a serem consideradas; nos níveis intermediários, são posicionados os critérios, os quais podem ou não ser desdobrados em subcritérios, conforme a Figura 2.17.

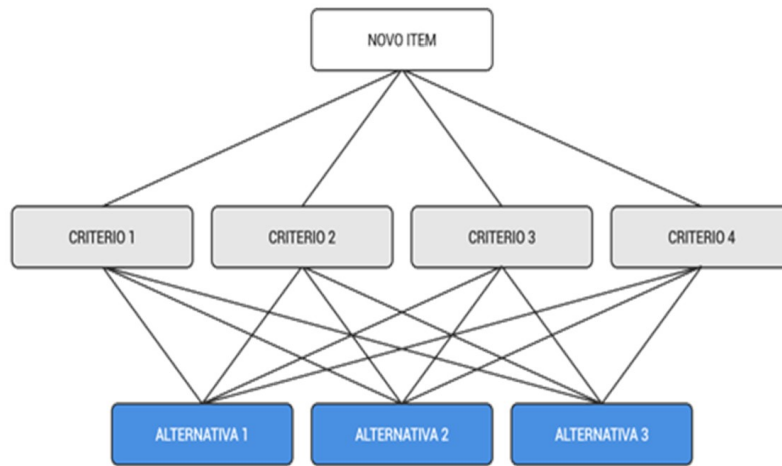


Figura 2.17: Estrutura de Decisão Hierárquica [Santos & Cruz, 2013].

Esta organização visa facilitar a compreensão dos critérios determinantes da pesquisa. A estrutura de decisão hierárquica desta pesquisa (Figura 3.1) utiliza as tipologias de riscos descritas na INC MP/CGU nº 1/2016 como critérios e utiliza um grupo de riscos extraídos da literatura e selecionados por especialistas, compondo as 12 (doze) alternativas.

2.9.2 Definição das Prioridades

Segundo [Saaty, 2009], a tomada de decisão requer a criação de uma estrutura organizada, representando a abstração de um problema; tal estrutura permite a visualização e compreensão da relevância dos elementos no modelo estudado. Um dos aspectos mais importantes dessa abordagem é a sua capacidade de estruturar problemas complexos, multipessoais, multicritérios e multiperíodos hierarquicamente [Saaty, 1990].

A escala proposta por [Saaty, 2008] é amplamente utilizada, indo de 1 a 9, com 1 significando a indiferença de importância de um critério em relação ao outro e 9 significando a extrema importância de um critério sobre outro, com estágios intermediários de importância entre esses níveis, conforme Figura 2.18.

PESOS	DEFINIÇÃO	AVALIAÇÃO
1	Importância igual	A e B contribuem igualmente para o objetivo
3	Importância moderada	Evidência / experiência favorece levemente A sobre B
5	Importância forte (grande / essencial)	Evidência favorece claramente A sobre B
7	Importância muito forte	A é fortemente favorecido; diferença é evidente na prática.
9	Importância extrema (absoluta)	Evidência favorece A com grau máximo de convicção
2, 4, 6, 8	Valores intermediários	Usados quando a preferência fica “entre” dois níveis adjacentes
Recíprocos	Se A tem valor x sobre B, então B tem valor 1/x sobre A	

Figura 2.18: Escala de prioridades de Thomas L. Saaty [Saaty, 2008]

Para se fazer uso da escala de prioridades, é preciso compreender que um julgamento ou comparação é a representação numérica da relação entre dois elementos que possuem o mesmo “pai”. Grandzol (2005) descreve que, por meio de julgamentos de comparações aos pares em cada nível da hierarquia, baseadas na escala de prioridades da **AHP**, os participantes desenvolvem pesos relativos para diferenciar a importância e as prioridades dos critérios.

O grupo de todos esses julgamentos pode ser representado por uma matriz quadrada (Figura 2.19), na qual os elementos são comparados com eles mesmos; cada julgamento representa a dominância de um elemento da coluna à esquerda sobre um elemento na linha do topo [Saaty & Shih, 2009].

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1j} \\ 1/a_{12} & 1 & a_{23} & \dots & a_{2j} \\ 1/a_{13} & 1/a_{23} & 1 & \dots & a_{3j} \\ \dots & \dots & \dots & 1 & \dots \\ 1/a_{1j} & 1/a_{2j} & 1/a_{3j} & \dots & 1 \end{pmatrix}$$

Figura 2.19: Matriz de julgamento par-a-par [Santos & Cruz, 2013].

Esta escala gera um peso para cada critério de avaliação de acordo com as comparações em pares do tomador de decisão. Quanto maior o peso, mais importantes são os critérios correspondentes. As posições da diagonal serão sempre “1”, afinal, um elemento é igualmente importante a ele mesmo ($n = n$); apenas metade das comparações precisa ser feita, porque a outra metade constitui-se das comparações recíprocas na matriz de comparações, que são os valores recíprocos já comparados.

Para preencher os outros elementos da matriz fora da diagonal, fazem-se os julgamentos e determina-se a intensidade de importância de acordo com a tabela de comparações da AHP [Saaty & Vargas, 1984], que apresenta a escala de comparações empregadas no método. Também é evidente na literatura que, na maioria dos casos, especialistas e profissionais são incapazes de definir pesos para os critérios devido à falta de dados ou conhecimento [Mahmoud et al., 2015, Chen et al., 2015].

2.9.3 Avaliação da Consistência Lógica

Feita a matriz de comparação entre os critérios (julgamento), é preciso calcular a razão de coerência (RC); para tal, é fundamental obter o resultado do autovalor máximo (λ_{max}), do índice de coerência (CI), do índice randômico (Índice de Consistência Aleatória (RI)) e da razão de coerência (CR). A RC deve ser inferior a 10%; caso contrário, será necessário realizar um novo julgamento. O Vetor de Eigen (λ_{max}), também conhecido como número principal de Eigen ou autovalor, é necessário para verificar se os dados da matriz de prioridades são consistentes; quanto mais próximo estiver o valor de λ_{max} de n , maior será a consistência dos juízos.

Para identificar a consistência dos dados, é necessário calcular o Índice de Consistência (CI), dado pela Equação 2.2, onde n é igual à quantidade de critérios descrita na Estrutura de Decisão Hierárquica e tem como base do cálculo o número principal de Eigen (λ_{max}):

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (2.2)$$

[Saaty & Shih, 2009] especificam que, encontrado o Índice de Consistência (CI), é recomendado o cálculo da Razão de Consistência (CR); o valor final deve ser $\leq 0,1$, caso contrário a matriz de prioridades está inconsistente e deve ser refeita. O cálculo é feito pela Equação 2.3:

$$CR = \frac{CI}{RI} \leq 0,1 \approx 10\% \quad (2.3)$$

Como os especialistas são humanos, Saaty, (1992), afirma que a AHP prevê que pode haver inconsistência; então o processo permite uma inconsistência de no máximo 10% para que os resultados possuam credibilidade. O cálculo do CR está diretamente ligado

ao valor do **RI**. O valor do **RI** (Figura 2.20), tem como base o número de critérios avaliados, conforme proposto por [Saaty, 2008].

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Figura 2.20: Índice de Consistência Aleatória (RI) [Saaty, 1977, Saaty, 2008].

As estruturas geométricas representam a compreensão abstrata das influências entre os elementos do mundo real e suas conexões e interações [Garuti & Spencer, 2007]. Mas nem toda tomada de decisão envolve pensamento, pois muitas de nossas decisões são reflexos automáticos ou intuitivos [Plassmann et al., 2005]. Partindo do entendimento apresentado por [Demo, 2000], fica evidente que a inteligência na tomada de decisão está na habilidade de lidar com a ambivalência, onde aprender é sobretudo saber pensar, para além da lógica retilínea e evidente, porque nem o conhecimento é reto ou linear [Bauman, 1999].

2.10 Algoritmo Mini-Max

Pesquisas que utilizam diferentes métodos de análise, como a **FMEA** e o **AHP**, expressam seus resultados em escalas e unidades distintas, o que dificulta a comparação direta e a priorização dos valores dos itens avaliados. Para superar esse desafio, recorre-se à aplicação de técnicas de normalização.

O artigo clássico “*Zur Theorie der Gesellschaftsspiele*”, publicado por [Von Neumann, 1928], apresenta o modelo do algoritmo Minimax, voltado para ambientes de decisão estratégica em jogos de soma zero, nos quais o objetivo de um jogador é maximizar

seu ganho minimizando a máxima perda possível frente a um adversário racional. O modelo compartilha o conceito de análise de extremos (mínimos e máximos); porém, suas aplicações e fundamentos teóricos são claramente distintos, sendo o Algoritmo Minimax Estatístico uma ferramenta fundamental para a integração metodológica em análises multicritério.

Este procedimento funciona naturalmente como modelo de normalização, sendo reconhecido na literatura como recurso para integração de múltiplos métodos de decisão, ao possibilitar a harmonização dos *outputs* convertendo os resultados heterogêneos [Von Neumann, 1928], expressos em unidades ou escalas diversas, para uma métrica comum, reescalando os resultados para um intervalo de $[0, 1]$ ou $[1, 10]$.

Capítulo 3

Metodologia

De acordo com [Prodanov & Freitas, 2013], esta pesquisa caracteriza-se como aplicada quanto à natureza; quanto aos objetivos, é exploratória [Piovesan & Temporini, 1995]. No que se refere aos procedimentos técnicos, o estudo articula pesquisa bibliográfica a partir de publicações em bases de dados [Russo et al., 2006] e pesquisa documental com agentes públicos do Executivo Federal. Quanto à abordagem do problema, adota-se uma estratégia predominantemente quantitativa, com suporte qualitativo na etapa de seleção, validação e interpretação dos riscos.

A pesquisa mapeou e analisou a produção científica no período de 2014 a 2024. Para isso, combinou-se a análise do estado da arte, desenvolvido por meio de revisão bibliométrica baseada na Teoria do Enfoque Meta Analítico Consolidado - TEMAC [Mariano & Rocha, 2017] com o levantamento do estado da prática, estruturado a partir de documentos normativos nacionais e internacionais [Garousi et al., 2019]. Com o apoio de ferramentas como o o *software* **VOSviewer** – versão 1.6.20 [Van Eck & Waltman, 2010], foi possível obter a representação gráfica de dados.

Para identificar, priorizar e hierarquizar os riscos envolvidos no processo analisado, optou-se por ferramentas consagradas, como FMEA e AHP [Saaty & Shih, 2009] que mostrou-se adequada para lidar com a complexidade do cenário investigado, permitindo hierarquizar riscos de modo consistente e replicável.

Conforme [Wazlawick, 2009] e [Prodanov & Freitas, 2013], o método da pesquisa consiste em uma sequência estruturada de etapas que evidenciam como os objetivos do estudo foram atingidos no processo metodológico desenvolvido. Desta forma, este capítulo descreve sistematicamente todas as etapas do processo metodológico seguidas para o alcance dos objetivos desta pesquisa, cada etapa está detalhada na Figura 3.1.

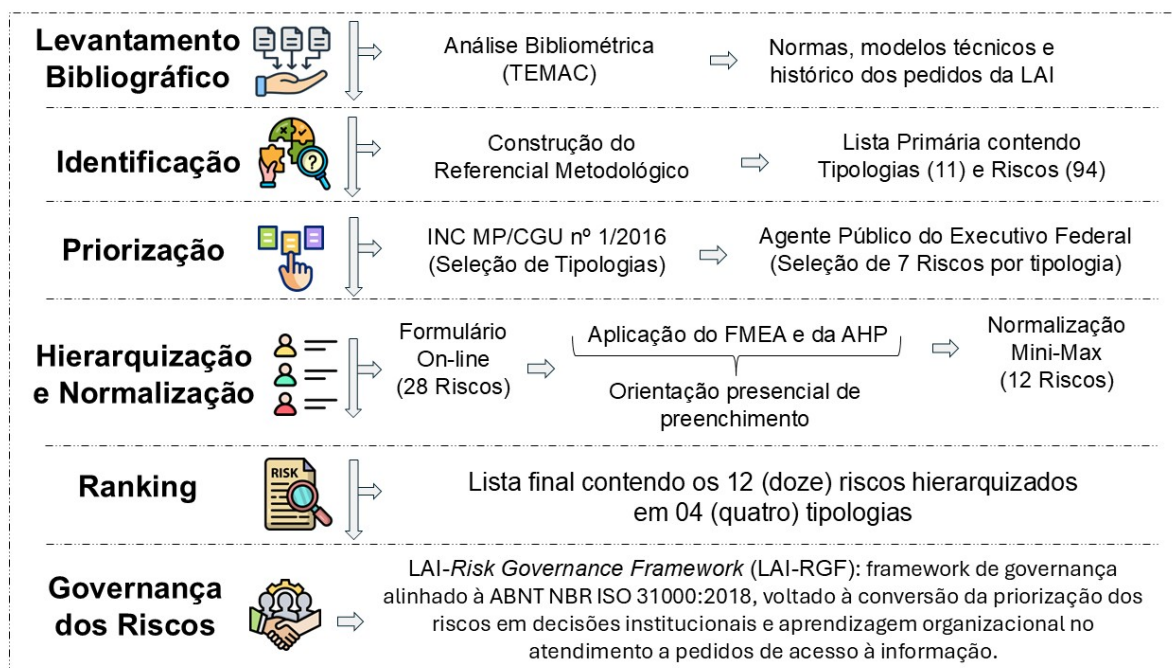


Figura 3.1: Fluxo metodológico adotado na pesquisa.

Fonte: Elaborada pelo autor, (2025)

Na execução destas etapas houve a participação de agentes públicos, cujos perfis estão descritos no texto e destacados na Figura 4.1. As etapas foram detalhadas a seguir. O processo sintetizado na Figura 3.1 está organizado em seis etapas relacionadas com a construção da estrutura de riscos utilizada na pesquisa: (i) levantamento bibliográfico; (ii) identificação; (iii) priorização; (iv) hierarquização e normalização – FMEA e AHP com o Mini-max; (v) *ranking*; e (vi) governança – com a proposição de um *framework* de governança alinhado à ABNT NBR ISO 31000:2018 como um modelo replicável, com aplicação prática utilizando o *ranking* dos riscos identificados.

3.1 Levantamento Bibliográfico

Estudos mostram que existem diferenças no grau de cobertura dos bancos de dados em assuntos específicos [Martín-Martín et al., 2018b, Baas et al., 2020b, Clarivate, 2020, GONZÁLEZ-VALIENTE & LÓPEZ-MESA, 2022, Harzing & Alakangas, 2016]; por este motivo, para estruturar a construção do referencial metodológico da investigação, objetivando o levantamento sistêmico do arcabouço teórico de publicações relevantes ao tema e a agregação de conhecimento ao estudo em desenvolvimento, partiu-se de uma análise da literatura por meio da TEMAC [Mariano & Rocha, 2017].

A estratégia de busca dos dados foi organizada em análise bibliométrica, análise do arcabouço normativo e dos registros históricos de pedidos de acesso à informação da

CGU. Os achados da análise compuseram a base e estrutura acadêmica de referências da pesquisa, autores, palavras-chave e tendências da literatura, inclusive direcionando sobre as referências fundamentais do arcabouço normativo brasileiro afeto à temática estudada. Já no processo de coleta dos dados históricos de pedidos de acesso à informação, os dados foram coletados em 09/03/2025 do Painel da **LAI**, disponibilizado e administrado pela **CGU**. Ao término desta fase, obteve-se o referencial teórico utilizado nesta pesquisa.

3.2 Fase de Identificação

Construído o referencial teórico estrutural da investigação, utilizou-se da **TEMAC**, conforme detalhado na Seção 2.2, e do *software* **VOSviewer** (v. 1.6.20) [Van Eck & Waltman, 2010], para a criação dos mapas bibliométricos evidenciando aspectos específicos e relevantes relacionados com os resultados das Leis da Bibliometria [van Eck & Waltman, 2010].

Para tabular os dados, criar tabelas, gráficos, medir a frequência de palavras-chave e tratar arquivos .CSV, utilizou-se de programação em linguagem Python, *softwares* de **IA** e recursos do PowerPoint e do Excel – do pacote Office – para gerar as matrizes **FMEA** e **AHP** respondidas pelos agentes públicos, e do Google Forms para a criação e disponibilização do questionário *on-line*.

3.3 Fase de Priorização

Foram empregados recursos distintos para a seleção das tipologias e dos riscos. As tipologias foram priorizadas observando a **INC MP/CGU nº 1/2016**; já para a seleção dos riscos mais aderentes ao processo estudado, optou-se pela participação de especialistas [Dror et al., 2021], conforme sintetizado na Figura 3.2.

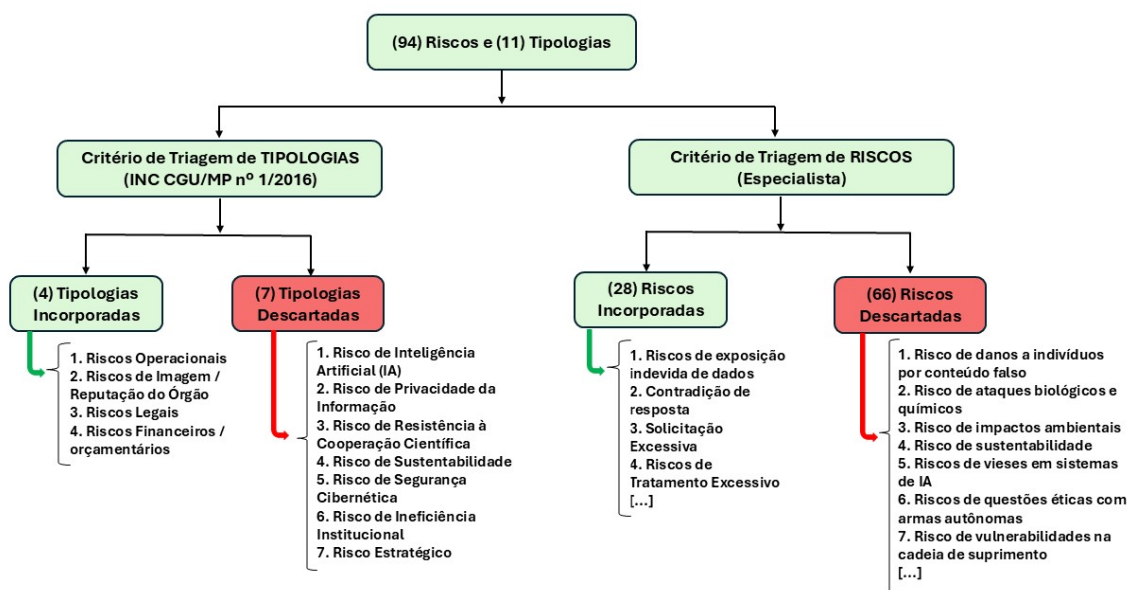


Figura 3.2: Processo de priorização
Fonte: Elaborada pelo autor, (2025)

Partindo do referencial teórico construído (Capítulo 2), com base nas literaturas selecionadas, prosseguiu-se para a construção da lista primária dos riscos; concluída esta fase, identificou-se o total de 11 (onze) tipologias e 94 (noventa e quatro) riscos (Figura 3.2).

Uma vez que a investigação foi feita no contexto do Executivo Federal, optou-se pelo uso e aplicação da **INC MP/CGU nº 1/2016** como parâmetro de seleção das tipologias de riscos mais aderentes. Desta forma, foram selecionadas 4 (quatro) tipologias de riscos: riscos operacionais, riscos de imagem/reputação, riscos legais e riscos financeiros/orçamentários; as demais foram desconsideradas para esta pesquisa.

A seleção dos riscos foi realizada por dois agentes públicos com mais de dez anos de experiência em ouvidoria pública e com atendimento a pedidos de acesso à informação, ocupantes de cargos de operação e gestão do Serviço de Informação ao Cidadão (SIC). De forma presencial e individual, os agentes tiveram acesso à lista primária contendo os riscos identificados.

Eles os organizaram considerando sua experiência profissional com a temática [Vanderhoeven et al., 2017], a relevância e associação de cada risco com o processo de compartilhamento de dados motivados pela LAI estudado, e selecionaram os riscos observando a probabilidade de ocorrência deles no ambiente público. Ao término das análises, obteve-se a lista final de riscos para cada uma das quatro tipologias previstas conforme a **INC MP/CGU nº 1/2016**, totalizando uma base de riscos (Apêndice B).

3.4 Hierarquização e Normalização

Partindo da base de 28 riscos, foi estruturado um formulário *on-line* (Apêndice B) e disponibilizado aos agentes públicos no período de 15 a 20 de setembro de 2025. O preenchimento foi voluntário e a hierarquização dos riscos foi realizada de maneira crescente, sendo o risco colocado na primeira linha com a maior probabilidade de ocorrência e na última linha com a menor probabilidade de ocorrência. Os dados de identificação não foram coletados de forma obrigatória e o perfil dos respondentes selecionados está detalhado na Figura 4.1.

A literatura metodológica enfatiza que questões mal formuladas podem confundir os respondentes [Kimble, 1994], prejudicando a confiabilidade das respostas obtidas. Sendo assim, o texto do formulário foi ajustado e redigido com a aplicação de linguagem cidadã [Oliveira et al., 2021a, Oliveira et al., 2021b, Shumskaya, 2019], seguindo as diretrizes do Governo Federal do Brasil, com destaque para o art. 5º, inciso XIV, da Lei Federal nº 13.460, de 26 de junho de 2017 [BRASIL, 2017], e da Lei Federal nº 14.129, de 29 de março de 2021 [BRASIL, 2021], que propõe o uso de linguagem simples, clara e compreensível a qualquer cidadão.

A critério do pesquisador [Mariano & Rocha, 2017, Lakatos & Marconi, 2003, Demo, 2000], foram selecionados os três riscos principais de cada uma das quatro categorias, formando a base de 12 (doze) riscos utilizada na construção da matriz de FMEA, com o objetivo da identificação do NPR, e na AHP (*Analytic Hierarchy Process*), para identificar os Peso Local (PL) e os Peso Global (PG) das alternativas.

Os respondentes foram orientados presencialmente sobre o objetivo acadêmico da coleta e a forma tecnicamente adequada de preencher as matrizes de FMEA, até a obtenção do NPR, e de AHP, até a obtenção dos valores de PG e PL, em conformidade com as regras definidas [Saaty, 1977]. Todos os participantes contribuíram de forma voluntária e sem compensação de qualquer natureza.

Considerando a replicação do modelo e a auditoria dos valores obtidos nos cálculos, optou-se por não utilizar *softwares* externos: as matrizes FMEA (Figura 3.3) e AHP (Figura 3.4) de cada agente foram respondidas utilizando formulário Excel de autoria do pesquisador, contendo as fórmulas necessárias para a identificação dos valores desejados e de possíveis erros de fórmula ou arredondamento.

Modo de Falha	Causas de Falha	Efeitos de Falha	Ocorrência	Deteção	Gravidade	NPR	Ações para Reduzir a Ocorrência de Falhas						
Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	9	9	9	729	Treinar servidores para decisões baseadas em análise de risco						
Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	7	9	9	567	Implementar conferência dupla nas respostas						
Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	6	7	10	420	Capacitar quanto à LGPD e reforçar consentimentos						
Modo de Falha	Causas de Falha	Efeitos de Falha	Ocorrência	Deteção	Gravidade	NPR	Ações para Reduzir a Ocorrência de Falhas						
Baixa qualidade de sen	Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	8	9	10	720	Treinar servidores para decisões baseadas em análise de risco					
Quebra de sigilo	Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	7	8	9	504	Implementar conferência dupla nas respostas					
Contradição de resposta	Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	6	7	10	420	Capacitar quanto à LGPD e reforçar consentimentos					
Vazamento de dados por técnica	Baixa qualidade de se	Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	8	9	9	648	Treinar servidores para decisões baseadas em análise de risco				
Despesas judiciais	Quebra de sigilo	Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	6	8	9	432	Implementar conferência dupla nas respostas				
Segurança da informação	Contradição de resp	Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	8	8	9	576	Capacitar quanto à LGPD e reforçar consentimentos				
Software infectado	Vazamento de dados po	Baixa qualidade de se	Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	8	8	9	576	Treinar servidores para decisões baseadas em análise de risco			
Custo da Transparência	Despesas judiciais	Quebra de sigilo	Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	7	7	9	441	Implementar conferência dupla nas respostas			
Fraude e descaminho	Segurança da inform	Contradição de resp	Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	8	8	8	512	Capacitar quanto à LGPD e reforçar consentimentos			
Software infectado	Vazamento de dados por técnica	Baixa qualidade de s	Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	7	9	9	567	Treinar servidores para decisões baseadas em análise de risco			
Custo da Transparência	Despesas judiciais	Quebra de sigilo	Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	8	8	9	576	Implementar conferência dupla nas respostas			
Fraude e descaminho	Segurança da inform	Contradição de resp	Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	8	8	8	512	Capacitar quanto à LGPD e reforçar consentimentos			
Software infectado	Vazamento de dados p	Baixa qualidade de serviço	Desatenção, falta de revisão	Informações erradas ou incompletas	6	9	9	486	Aplicar checklist e revisão em duplo controle				
Custo da Transparência	Despesas judiciais	Quebra de sigilo	Erro de classificação da informação	Comprometimento da segurança institucional	5	5	10	250	Reforçar classificações e procedimentos de restrição				
Fraude e descaminho	Segurança da inform	Contradição de resposta	Falta de controle e análise de demandas	Desconfiança no serviço	3	9	9	243	Adotar ferramentas de controle e histórico de respostas				
Software infectado	Vazamento de dados por falha técnica	Problemas em sistemas e configurações	Divulgação não autorizada de dados	Acesso e disponibilização não autorizada de informações sigilosas	5	5	9	225	Realizar auditorias periódicas em sistemas de TI				
Despesas judiciais	Segurança da inform	Judicialização por negativas legítimas	Custos jurídicos e imagem negativa	Custos jurídicos e imagem negativa	4	7	7	196	Estabelecer estratégias de defesa preventiva				
Custo da Transparência	Segurança da informação	Falta de procedimentos adequados	Comprometimento de dados	Comprometimento de dados	3	5	10	150	Aprimorar controles de acesso e criptografia de dados				
Fraude e descaminho	Software infectado	Execução de aplicativos ou macros contaminados	Acesso e disponibilização não autorizada de informações sigilosas	Acesso e disponibilização não autorizada de informações sigilosas	2	8	9	144	Implementar plano de gerenciamento de crises de imagem				
Custo da Transparência	Solicitações complexas e volumosas	Aumento de custos operacionais	Aumento de custos operacionais	Aumento de custos operacionais	1	9	10	90	Otimizar processos de atendimento para reduzir volume				
Fraude e descaminho	Acesso a dados pessoais e financeiros	Uso de informações divulgadas para realizar golpes de phishing, transferências indevidas ou obtenção de vantagem econômica	Uso de informações divulgadas para realizar golpes de phishing, transferências indevidas ou obtenção de vantagem econômica	Uso de informações divulgadas para realizar golpes de phishing, transferências indevidas ou obtenção de vantagem econômica	1	6	7	42	Planejar investimentos com base em análise de risco				

Figura 3.3: Matriz FMEA
Fonte: Elaborada pelo autor, (2025)

Partindo da lista composta por 12 (doze) riscos, montou-se a matriz de **FMEA**, preenchida no período de outubro e novembro de 2025, com o objetivo da identificação do **NPR**. Após o preenchimento individual e análise das 5 (cinco) matrizes, obteve-se o valor de **NPR** por respondente; com o propósito de materializar a percepção dos agentes públicos e construir uma estrutura única da percepção do grupo sobre os riscos [Saulino et al., 2017], aplicou-se a média simples dos valores finais de **NPR**, hierarquizando as alternativas de risco (Figura 4.2). Os resultados obtidos neste processo estão destacados e podem ser consultados na Seção 4.2.

Conforme a base metodológica construída no Capítulo 2, todos os padrões e indicadores de aplicação da **AHP**, definidos por [Saaty, 1977], foram observados na construção do arquivo utilizado na pesquisa. As tipologias descritas na **INC MP/CGU nº 1/2016** foram utilizadas como critérios, enquanto a mesma lista prioritária de 12 (doze) riscos utilizada na confecção da **FMEA** foi aplicada como alternativas vinculadas aos critérios, conforme representado na Figura 3.4.

Quadro resumo contendo os valores derivados da análise do respondente 01											
Altern.	Descritivo dos Critérios	C1		C2		C3		C4		C5	
		P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global
A1	contradição de resposta	0,110	0,060	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A2											
A3											
Quadro resumo contendo os valores derivados da análise do respondente 02											
Altern.	Descritivo dos Critérios	C1		C2		C3		C4		C5	
		P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global
A1	contradição de resposta	0,100	0,053	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A2	exposição indevida de dados										
A3	transparência excessiva										
A4	vazamento de dados por falha técnica										
A5	software infectado										
A6	baixa qualidade do serviço										
A7	segurança da informação										
A8	quebra de sigilo										
A9	violação de direitos										
A10	despesas judiciais										
A11	fraude e descaminho										
A12	custo da transparência										
Quadro resumo contendo os valores derivados da análise do respondente 03											
Altern.	Descritivo dos Critérios	C1		C2		C3		C4		C5	
		P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global
A1	contradição de resposta	0,091	0,060	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A2	exposição indevida de dados										
A3	transparência excessiva										
A4	vazamento de dados por falha técnica										
A5	software infectado										
A6	baixa qualidade do serviço										
A7	segurança da informação										
A8	quebra de sigilo										
A9	violação de direitos										
A10	despesas judiciais										
A11	fraude e descaminho										
A12	custo da transparência										
Quadro resumo contendo os valores derivados da análise do respondente 04											
Altern.	Descritivo dos Critérios	C1		C2		C3		C4		C5	
		P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global	P. Local	P. Global
A1	contradição de resposta	0,077	0,049	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A2	exposição indevida de dados	0,308	0,194	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A3	transparência excessiva	0,615	0,389	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
A4	vazamento de dados por falha técnica	0,000	0,000	0,077	0,009	0,000	0,000	0,000	0,000	0,000	0,000
A5	software infectado	0,000	0,000	0,231	0,026	0,000	0,000	0,000	0,000	0,000	0,000
A6	baixa qualidade do serviço	0,000	0,000	0,692	0,079	0,000	0,000	0,000	0,000	0,000	0,000
A7	segurança da informação	0,000	0,000	0,000	0,000	0,143	0,029	0,000	0,000	0,000	0,000
A8	quebra de sigilo	0,000	0,000	0,000	0,000	0,286	0,059	0,000	0,000	0,000	0,000
A9	violação de direitos	0,000	0,000	0,000	0,000	0,571	0,117	0,000	0,000	0,000	0,000
A10	despesas judiciais	0,000	0,000	0,000	0,000	0,000	0,000	0,100	0,005	0,000	0,000
A11	fraude e descaminho	0,000	0,000	0,000	0,000	0,000	0,000	0,300	0,015	0,000	0,000
A12	custo da transparência	0,000	0,000	0,000	0,000	0,000	0,000	0,600	0,029	0,000	0,000
Auditoria: soma dos Pesos Locais deve ser 1 (100%) por critério											
		1	0,632	1	0,115	1	0,205	1	0,049		
		↓		↓		↓		↓		↓	
		63,190%		11,480%		20,480%		4,850%		100%	

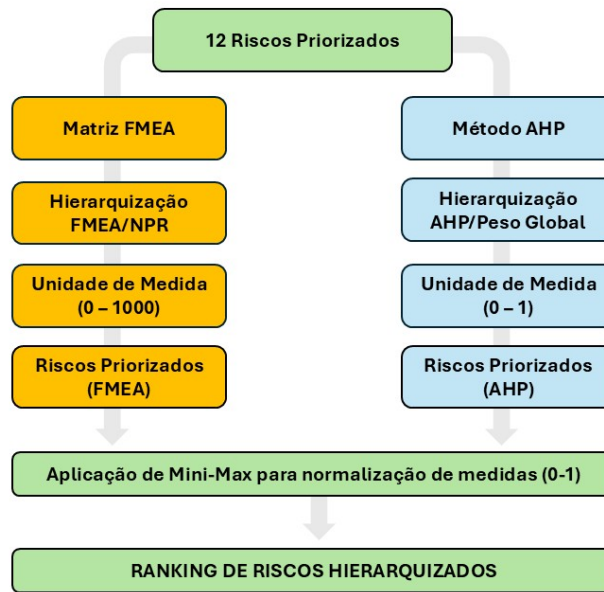


Figura 3.5: Fluxo de Normalização dos Valores dos Riscos.
Fonte: Elaborada pelo autor, (2025)

Considerando que a **FMEA** produz **NPR** em escala (0–1000) e a **AHP** gera **PG** em escala (0–1), utilizou-se do processo de normalização dos valores para padronizar os resultados [Von Neumann, 1928], em uma escala comum entre (0–1). A geração de uma escala comum dos valores obtidos com a **FMEA** (**NPR**) e da **AHP** (**PG**) permite comparação e integração coerente entre as priorizações obtidas pelos dois métodos; este processo confere consistência estatística e escalabilidade, consolidando-o como um modelo viável de avaliação e priorização de riscos [Carmo et al., 2013]. A padronização e fusão dos valores de **NPR** da **FMEA** e **PG** da **AHP**, colocando-os em uma única escala, cria uma base comum de comparação, garantindo a não interferência entre métodos – onde cada um gera seu resultado de forma independente – e ambos são analisados para a tomada de decisão [Aguarón et al., 2023].

3.5 Ranking de Riscos

Após a aplicação de normalização dos valores do **NPR** obtidos com a **FMEA** e dos **PG** das alternativas identificados na **AHP-AIJ**, gerou-se o *ranking* dos riscos prioritários relacionados com o processo de compartilhamento de dados motivados pela **LAI**. Os resultados obtidos estão especificados nas Figuras 4.10 e 4.11, e detalhados na Seção 4.4.

3.6 Governança dos Riscos

À luz da **ABNT** NBR ISO 31000:2018, a gestão de riscos é compreendida como um processo estruturado, iterativo e integrado à governança e à tomada de decisão organizacional. Nesse processo, o tratamento dos riscos corresponde à seleção e à implementação de opções destinadas a modificar o risco, a partir de informações produzidas nas etapas anteriores de identificação, análise e avaliação.

Nessa perspectiva, o **LAI-RGF** foi fundamentado e estruturado como um *framework* de governança orientado por riscos, concebido para atuar no contexto do atendimento a pedidos de acesso à informação, convertendo a priorização dos riscos mapeados em decisões institucionais, medidas de tratamento e aprendizagem organizacional. O uso organizacional de uma categorização dos riscos institucionais em níveis – inaceitável, alto, limitado e mínimo – pode oferecer uma matriz analítica útil para utilizar o *framework* na hierarquização dos riscos institucionais relacionados com o compartilhamento de dados sob a base da **LAI**.

Com base nessa arquitetura conceitual, o **LAI-RGF** foi estruturado em quatro fases encadeadas, tomando a operação da **LAI** como parâmetro organizador: Triagem → Atendimento → Pós-resposta → Lições Aprendidas. O diagrama apresentado na Figura 4.13, sintetiza essa organização em quatro fases e evidencia seu encadeamento funcional no ciclo de atendimento da **LAI**. Uma das formas de operacionalização do **LAI-RGF** consiste na sua tradução em um plano de implementação estruturado no modelo 5W2H [Santos Neto et al., 2016], que o converte em artefato simples, intuitivo e aplicável em diferentes contextos institucionais; o modelo está detalhado na Tabela 4.1 do capítulo seguinte.

Dessa forma, o **LAI-RGF** possui natureza híbrida, pois dialoga com resultados oriundos da identificação, análise e avaliação de riscos; contudo, sua aplicação operacional predominante se realiza na fase de tratamento dos riscos, por transformar a priorização obtida na avaliação em respostas institucionais, medidas de mitigação, padronização decisória e aprendizagem organizacional. É precisamente essa conversão do risco em providência administrativa que permite situar o *framework*, de forma predominante, na fase de tratamento dos riscos, tornando-o compatível com a lógica da **ABNT** NBR ISO 31000:2018 e com as exigências do processo decisório no âmbito da **LAI**.

Outros normativos e modelos foram observados no processo de idealização e construção do *framework*, permitindo que tenha um sólido fundamento de *compliance* com a **LAI**; com as normas de riscos **ABNT** NBR ISO 31010:2018 e 31010:2012; assim como alguns modelos de documentos disponibilizados pela **CGU**; sendo também aderente a modelos internacionais como o Código de Práticas de Governança Cibernética [Financial Reporting Council, 2024], publicado no Reino Unido; o Regulamento (UE) 2024/1689 do Parlamento Europeu sobre Inteligência Artificial [European Union, 2024], que propõe uma abordagem

baseada em risco e impõe restrições ao uso de sistemas de IA em contextos sensíveis; o NIST CSF de 2025 [National Institute of Standards and Technology, 2026]; o NIST SP 800-61r3, versão 2.0 de 2025 (Rev. 3) [Nelson et al., 2025]; e o NIST SP 800-53, Revisão 5.2.0, de 2025 [Joint Task Force, 2020], que discorre sobre controles de segurança e privacidade para sistemas de informação.

Assim, o detalhamento prático da aplicação do LAI-RGF (Figura 4.13) no serviço público, apresentado na Seção 4.5 do capítulo seguinte, consolida o *framework* como instrumento aderente à ABNT NBR ISO 31000:2018, na medida em que traduz os riscos prioritários do processo estudado em parâmetros operacionais de tratamento, acompanhamento e decisão institucional. Ao articular a priorização dos riscos com ações, responsáveis, recursos, momentos de execução e mecanismos de monitoramento, o modelo oferece aos gestores públicos um referencial estruturado para qualificar a análise das situações concretas, orientar a alocação de recursos institucionais e apoiar decisões mais proporcionais, rastreáveis e consistentes no atendimento a pedidos de acesso à informação.

Capítulo 4

Resultados e Discussão

Este capítulo apresenta os principais resultados obtidos a partir da aplicação da metodologia abordada no capítulo anterior, detalhando os resultados derivados da aplicação da **FMEA** e da **AHP**, os processos estatísticos de análise de matrizes par-a-par e técnicas de explicabilidade e, por fim, as aplicações práticas no processo de governança dos riscos de compartilhamento de dados.

4.1 Perfil dos Participantes

A análise do perfil demográfico dos respondentes (agentes públicos) revela um grupo homogêneo, com predominância de idade entre 40 e 44 anos (60%), do sexo masculino (60%), com renda familiar acima de 10 salários-mínimos (60%), tempo de serviço público superior a 10 anos (80%) e estado civil casado(a) (60%). Em conjunto, os dados indicam uma amostra composta majoritariamente por agentes públicos com elevada experiência institucional, o que reforça a pertinência dos julgamentos emitidos na etapa de priorização dos riscos Figura 4.1.

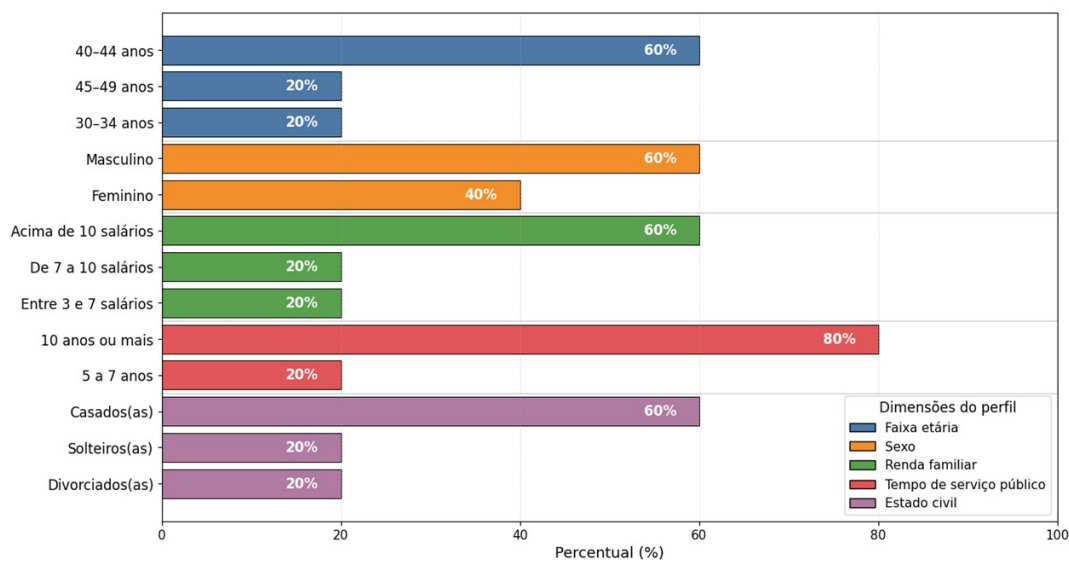


Figura 4.1: Dados Demográficos dos Respondentes
Fonte: Elaborada pelo autor, (2026)

A combinação de uma amostra intencional de especialistas com um instrumento cuidadosamente elaborado resulta em dados mais robustos e confiáveis. Essa sinergia entre perfil dos participantes e rigor instrumental reflete as recomendações da literatura para pesquisas aplicadas em contextos organizacionais. Segundo [Meyer & Booker, 2001], ao envolver agentes públicos, a pesquisa ganha em precisão, profundidade e relevância prática.

Uma vez que os dados deste estudo apresentam uma função de teste e demonstração, não de generalização estatística, priorizou-se a qualificação dos avaliadores, não o volume amostral [Saaty & Vargas, 2012, Benabdellah et al., 2019, Marins et al., 2009].

4.2 Análise Sistemática dos Modos de Falha e seus Efeitos (FMEA)

A etapa de aplicação da técnica **FMEA** no processo de priorização dos riscos foi conduzida a partir da identificação dos modos de falha [Asgari Dastjerdi et al., 2017] de suas causas, efeitos e ações de tratamento, individualmente por cinco agentes públicos.

Para assegurar uniformidade de entendimento quanto aos critérios de avaliação, os respondentes foram orientados presencialmente antes do preenchimento da matriz, recebendo esclarecimentos sobre a lógica da ferramenta e sobre como proceder com a atribuição dos escores de ocorrência, severidade e detecção.

Esse cuidado metodológico foi aplicado com o objetivo de reduzir ambiguidades de interpretação e aumentar a consistência do julgamento individual, o que é compatível com as recomendações da literatura sobre a **FMEA**, gerando valores de **NPR** das alternativas analisadas (modo de falha), agrupados na Figura 4.2.

Modo de Falha	NPR_R1	NPR_R2	NPR_R3	NPR_R4	NPR_R5
Transparência excessiva	729	720	648	576	567
Exposição indevida	567	504	432	441	576
Violação de direitos fundamentais	400	420	432	486	512
Baixa qualidade de serviço	378	420	441	480	486
Quebra de sigilo	192	200	240	243	250
Contradição de resposta	180	192	210	225	243
Vazamento de dados por falha técnica	210	180	175	210	225
Despesas judiciais	150	162	175	192	196
Segurança da informação	120	126	135	144	150
Software infectado	112	120	126	128	144
Custo da transparência	70	75	81	84	90
Fraude e descaminho	30	37	35	38	35

Figura 4.2: Valores Individuais de NPR por Respondentes
Fonte: Elaborada pelo autor, (2026)

Segundo [Murphy, 2000], a combinação de funções de crença leva a um paradoxo: quanto maior o conflito entre as evidências, maior a “certeza” na combinação; usar um valor médio reduz esse efeito. A adoção dessa regra de agregação atendeu a três requisitos relevantes para a pesquisa: a transparência dos cálculos; a padronização para garantir a reprodução do processo de obtenção dos valores de **NPR**; e a comparação direta entre as alternativas. A consolidação dos resultados em tabela única (Figura 4.4) e sua posterior representação gráfica (Figura 4.3) permitiram visualizar tanto a dispersão entre os respondentes quanto a tendência central dos julgamentos.

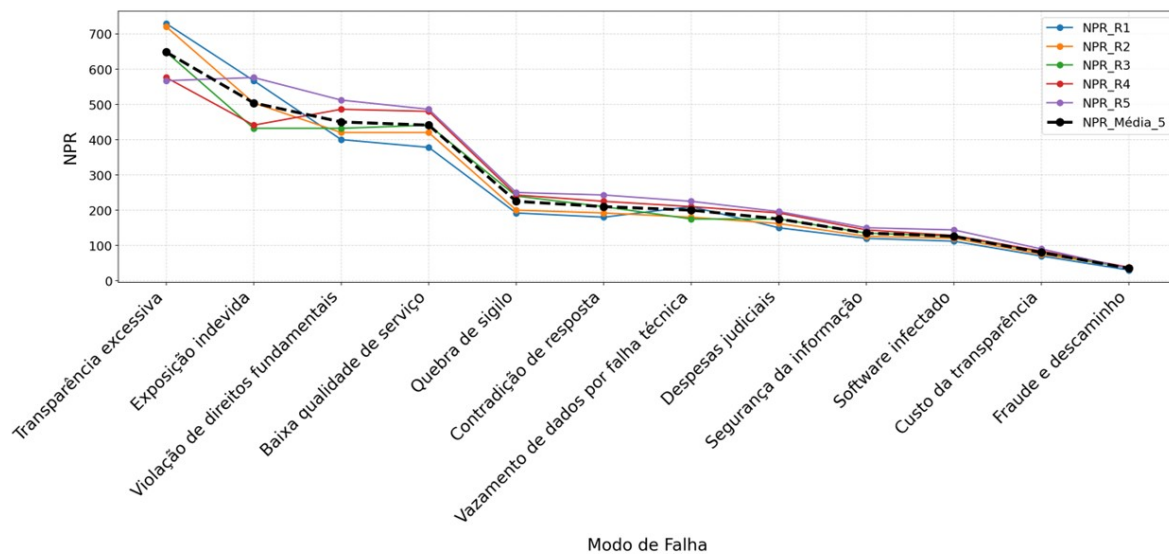


Figura 4.3: Média do Valor de NPR
Fonte: Elaborada pelo autor, (2026)

A Figura 4.3 detalha a percepção gráfica dos valores de **NPR** obtidos. Conforme os valores de **NPR**, obteve-se o *ranking* de importância dos riscos, destacando-se a “Transparência Excessiva” com o maior **NPR** médio (648), seguida por “Exposição Indevida” (504), “Violação de Direitos Fundamentais” (450) e “Baixa Qualidade de Serviço” (441). Em um segundo patamar aparecem Quebra de Sigilo (225), Contradição de Resposta (210) e Vazamento de Dados por Falha Técnica (200). Já os menores valores foram observados em Despesas Judiciais (175), Segurança da Informação (135), *Software* Infectado (126), Custo da Transparência (80) e Fraude e Descaminho (35).

O **NPR** evidencia os riscos que devem ser priorizados (Figura 4.4), justificando ações imediatas e estruturantes para a tomada de decisão institucional, conforme o nível de apetite a risco da instituição.

Ranking	Alternativa	Descrição	Critério	NPR
1 ^a	A3	transparência excessiva	C1	648
2 ^a	A2	exposição indevida de dados	C1	504
3 ^a	A9	violação de direitos	C3	450
4 ^a	A6	baixa qualidade do serviço	C2	441
5 ^a	A8	quebra de sigilo	C3	225
6 ^a	A1	contradição de resposta	C1	210
7 ^a	A4	vazamento de dados por falha técnica	C2	200
8 ^a	A10	despesas judiciais	C4	175
9 ^a	A7	segurança da informação	C3	135
10 ^a	A5	software infectado	C2	126
11 ^a	A12	custo da transparência	C4	80
12 ^a	A11	fraude e descaminho	C4	35

Figura 4.4: Média do Valor de NPR
Fonte: Elaborada pelo autor, (2026)

Os principais riscos identificados demonstram o alinhamento da pesquisa com o contexto atual vivido pela sociedade da informação nos processos de geração, consumo e compartilhamento de dados, bem como a sensibilidade social e a construção jurídica para garantias da privacidade e proteção de dados pessoais. A priorização final mostra que os riscos mais críticos se concentram em dimensões diretamente ligadas à exposição indevida de informações, à violação de direitos e à perda de qualidade decisória no tratamento dos pedidos.

Em termos gerenciais, isso significa que o problema não está apenas no eventual vazamento técnico de dados, mas, sobretudo, na combinação entre interpretação binária inadequada, falhas humanas de resposta e insuficiência de controles institucionais. O gráfico evidencia que as quatro primeiras alternativas concentram os maiores níveis de criticidade, formando um bloco de riscos prioritários claramente destacado em relação às demais. Essa ordenação permitiu selecionar o **NPR** final de cada alternativa e, a partir dele, estabelecer a hierarquia de priorização para fins de análise e discussão dos riscos mais relevantes no contexto investigado. A **FMEA** não apenas ordenou os riscos, mas também ofereceu uma base racional para a definição de ações corretivas e preventivas, direcionando a atenção institucional para os modos de falha de maior impacto potencial. Os mesmos riscos foram organizados (Figura 4.5) e analisados com a aplicação da **AHP**.

4.3 Análise Hierárquica de Processos (AHP)

4.3.1 Estruturação do Problema

Para a análise estruturada dos riscos, seguiu-se o padrão de organização em três níveis [Saaty & Vargas, 1980, Saaty, 1990]. Inicialmente, definiu-se o objetivo geral como a identificação e hierarquização dos riscos derivados do compartilhamento de dados fundamentados na LAI, conforme Figura 4.5.

Os critérios escolhidos são as tipologias dos riscos descritas na INC MP/CGU nº 1/2016, a saber: (C1) riscos operacionais, (C2) riscos de imagem/reputação do órgão, (C3) riscos legais e (C4) riscos financeiros/orçamentários. As alternativas são as 12 (doze) prioritárias conforme identificado na análise FMEA anterior; os riscos prioritários foram ajustados e convertidos em alternativas, a saber:

- (A1) Contradição de Resposta;
- (A2) Exposição Indevida de Dados;
- (A3) Transparência Excessiva;
- (A4) Vazamento de Dados por Falha Técnica;
- (A5) *Software* Infectado;
- (A6) Baixa Qualidade do Serviço;
- (A7) Segurança da Informação;
- (A8) Quebra de Sigilo;
- (A9) Violação de Direitos;
- (A10) Despesas Judiciais;
- (A11) Fraude e Descaminho;
- (A12) Custo da Transparência.

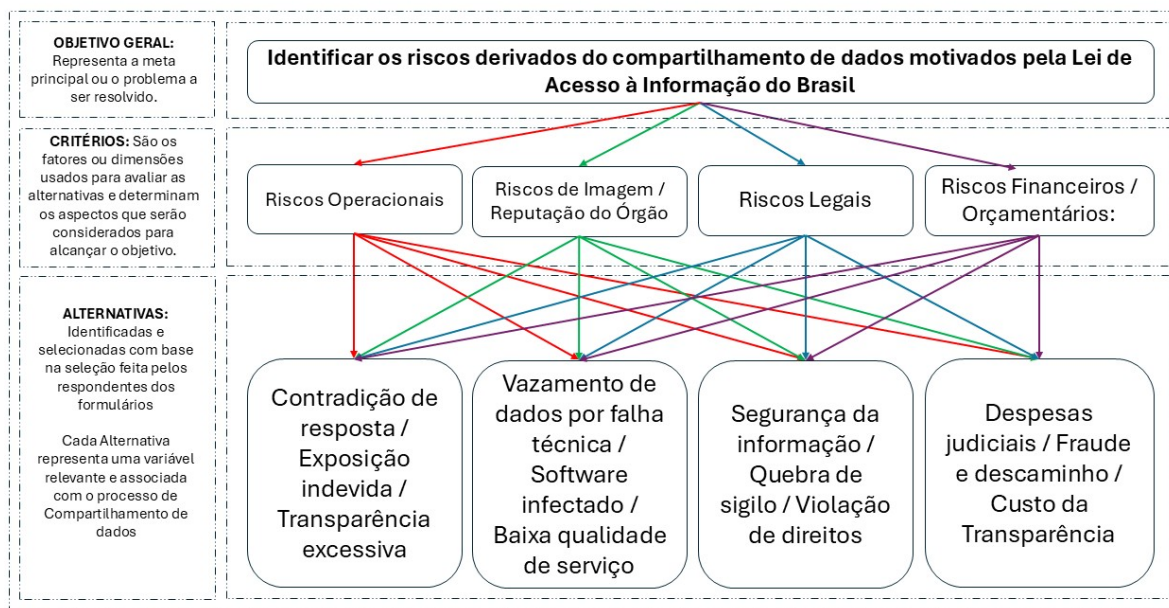


Figura 4.5: Estrutura de Decisão Hierárquica
Fonte: Elaborada pelo autor, (2026)

A Figura 4.5 representa a estrutura de decisão hierárquica, um mapa de relações que explana sobre como cada critério tende a se relacionar com cada uma das alternativas.

4.3.2 Definição das Prioridades

Os cálculos da matriz de julgamento par-a-par [Saaty, 2008] identificaram a importância local e global dos critérios e das alternativas, observando o princípio da reciprocidade e a necessidade de consistência da análise, utilizando a escala de prioridades de Saaty [Saaty, 1977, Saaty, 2008], respondendo às duas perguntas: qual dos dois elementos é mais importante com respeito a um critério de nível superior? E com que intensidade? A figura a seguir apresenta o registro do ranqueamento individual das alternativas, conforme a percepção dos respondentes.

Os **PL** de uma alternativa refletem apenas sua relevância isolada dentro de um critério específico, não sendo suficiente para ranqueá-la no conjunto das alternativas. Enquanto os **PG**, destacados na Figura 4.6, representam a relevância e o respectivo impacto da alternativa em todo o modelo analisado, considerando simultaneamente: a importância relativa da alternativa dentro de seu critério (**PL**); e a importância do próprio critério no contexto geral da decisão (peso do critério).

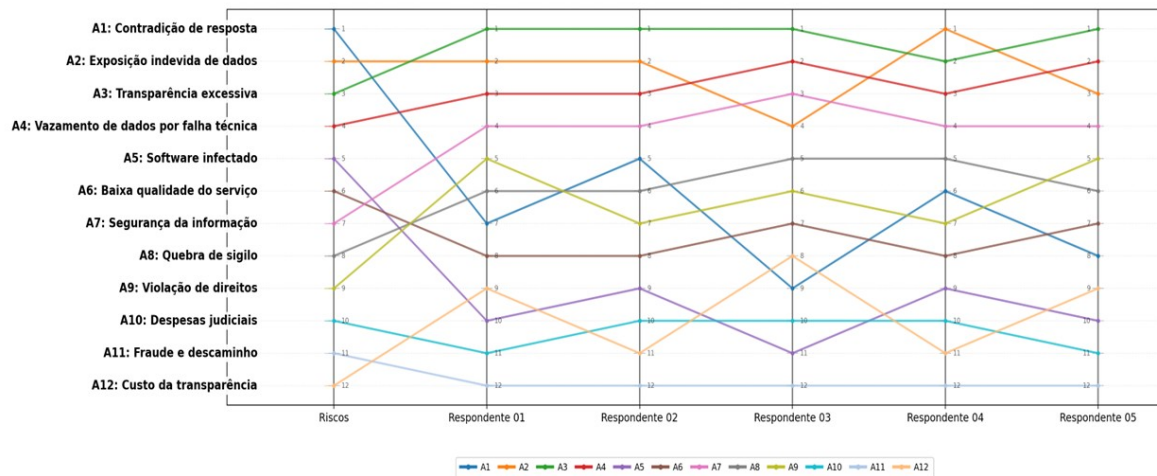


Figura 4.6: Ranqueamento de Riscos por Respondentes
 Fonte: Elaborada pelo autor, (2026)

A coluna inicial (riscos) é o ponto de partida das trajetórias dos riscos; cada linha do gráfico representa um risco específico, que varia conforme a percepção dos respondentes, representados nos eixos verticais. Quanto mais próximo de 1 o valor, maior é a prioridade percebida do risco; e quanto mais próximo de 12, menor a prioridade – destacando os pesos relativos e o valor de prioridade de cada item a partir da sua contribuição com o objetivo principal, evidenciando “quem pesa mais” e “quanto mais um critério pesa em relação aos outros”.

Transparência Excessiva (A3) aparece como 1º lugar para 80% dos respondentes; junto com Exposição Indevida de Dados (A2), formam a dupla de alta prioridade da análise, com variações pequenas de posição, indicando forte convergência na percepção e análise dos respondentes.

Outras alternativas oscilaram mais no *ranking* geral, destacando que a mesma alternativa é vista de maneiras diferentes pelos respondentes, o que pode estar associado a três fatores: (i) formação e função organizacional dos respondentes – o perfil jurídico de *compliance* tende a maximizar riscos de exposição indevida e violação de direitos; o perfil de **TIC** tende a perceber e enfatizar falhas técnicas; e o perfil de gestão tende a priorizar o risco reputacional e o custo político da transparência; (ii) os respondentes alternam as posições dos riscos conforme sua percepção, formação e experiência profissional; e (iii) as experiências recentes de incidentes, auditorias, demandas judiciais e pressão midiá-

tica, que tornam um tipo de risco mais “evidente” para um avaliador do que para outro [Tversky & Kahneman, 1981].

Individualmente, os critérios analisados ficaram com pesos globais bem definidos: em primeiro lugar aparecem os “Riscos Operacionais” com 59,11% de relevância; seguido dos “Riscos Legais” com 23,03%; dos “Riscos de Imagem/Reputação do Órgão” com 12,16%; e dos “Riscos Financeiros/Orçamentários” com 5,70%.

A alta relevância dos Riscos Operacionais destaca que os incidentes organizacionais não derivam de um único erro isolado, mas são produto da convergência de falhas sequenciadas que se alinham em um contexto de condições latentes no sistema de governança, no desenho de um processo, na definição de padrões de segurança institucional, na cultura organizacional relacionada ao tratamento de dados, e assim por diante. Quando os “furos” de várias camadas de defesa se alinham e abrem uma trajetória de oportunidade favorável para a ocorrência do evento danoso [Reason, 2000a, Reason, 2000b, Wiegmann et al., 2022].

4.3.3 Avaliação da Consistência Lógica

Encontrar os valores de consistência lógica do modelo significa que, para cada matriz par-a-par (critérios e alternativas), deve-se calcular o Índice de Consistência (CI); na sequência, é recomendado o cálculo da Razão de Consistência (RC). [Saaty, 1995] afirma que o método AHP prevê a possibilidade de inconsistência de no máximo 10% para que os resultados possuam credibilidade [Duleba & Szádoczy, 2022].

O cálculo deverá obter o resultado do autovalor máximo (λ_{max}) da matriz – Vetor de Eigen – necessário para verificar se os dados da matriz de prioridades são consistentes; quanto mais próximo estiver o valor de λ_{max} de n , maior será a consistência da análise. O cálculo do CR está diretamente ligado ao valor do RI, que tem como base o número de critérios avaliados conforme proposto por [Saaty, 2008], conforme Figura 4.7.

Respondente	N	RI	$\lambda_{\text{máx}}$	CI	CR	Status	C1	C2	C3	C4	Auditoria
1	4	0,90	4,190	0,063	0,070	Consistente	54,80%	12,28%	25,31%	7,61%	100%
2	4	0,90	4,000	0,000	0,000	Consistente	53,33%	13,33%	26,67%	6,67%	100%
3	4	0,90	4,037	0,012	0,014	Consistente	58,96%	12,73%	23,22%	5,08%	100%
4	4	0,90	4,147	0,049	0,054	Consistente	66,08%	10,28%	19,20%	4,44%	100%
5	4	0,90	4,078	0,026	0,029	Consistente	63,19%	11,48%	20,48%	4,85%	100%

Figura 4.7: Consistência Lógica dos Critérios

Fonte: Elaborada pelo autor, (2026)

Os valores obtidos destacam a consistência do modelo analisado. A matriz de comparação dos critérios apresentou CI satisfatório com valor máximo de (0,063), representando alto grau de coerência dos julgamentos e consistência [Saaty, 2008]. Após calculados de forma individual, aplicou-se o modelo de PG e PL das alternativas, que se mostraram igualmente consistentes.

4.3.4 Matriz AHP Consolidada (AHP-AIJ)

[Forman & Peniwati, 1998] afirmam que o AHP é frequentemente utilizado em ambientes de grupo, onde os membros se envolvem em discussões para alcançar um consenso ou expressar suas próprias preferências.

Há uma infinidade de outras técnicas para alcançar um consenso de grupo [Dyer & Forman, 1992, Aull-Hyde et al., 2006], mas os dois procedimentos mais aceitos dentro do AHP [Ossadnik et al., 2016] são: a AHP-AIJ, para os casos em que os respondentes devem decidir em conjunto; e a Agregação de Prioridades Individuais (API), aplicável nos casos em que indivíduos manifestam suas preferências com seus próprios sistemas de valores de forma individualizada.

Após os cálculos e análise da consistência lógica dos critérios e alternativas das matrizes individuais dos 5 (cinco) respondentes (Figura 4.1), utilizou-se da média geométrica [Forman & Peniwati, 1998] para obter os valores que representam o julgamento do grupo

– *Aggregate Individual Judgments (AHP-AIJ)* –, resultando em uma única matriz **AHP** agregada.

Partindo da matriz **AHP-AIJ**, seguiu-se com os cálculos conforme as regras e definições de [Saaty & Vargas, 1980, Saaty, 1990]. Os critérios foram hierarquizados, os valores individuais de **PL** e **PG** das alternativas foram calculados e a análise de consistência lógica foi executada, gerando os valores detalhados na Figura 4.8.

Ranking global (12 alternativas) — pesos locais e globais (AIJ)					
Ranking	Alternativa	Descrição	Critério	Peso_Local_AIJ	Peso_Global_AIJ
1 ^a	A3	transparência excessiva	C1	0,6466	0,3858
2 ^a	A2	exposição indevida de dados	C1	0,2627	0,1567
3 ^a	A9	violação de direitos	C3	0,5852	0,1334
4 ^a	A6	baixa qualidade do serviço	C2	0,5882	0,0702
5 ^a	A8	quebra de sigilo	C3	0,2754	0,0628
6 ^a	A1	contradição de resposta	C1	0,0907	0,0541
7 ^a	A12	custo da transparência	C4	0,7288	0,0408
8 ^a	A5	software infectado	C2	0,3084	0,0368
9 ^a	A7	segurança da informação	C3	0,1394	0,0318
10 ^a	A4	vazamento de dados por falha técnica	C2	0,1034	0,0123
11 ^a	A11	fraude e descaminho	C4	0,1980	0,0111
12 ^a	A10	despesas judiciais	C4	0,0731	0,0041

Figura 4.8: Pesos Locais e Pesos Globais das Alternativas (AHP-AIJ).

Fonte: Elaborada pelo autor, (2026)

A hierarquização proporcionada pelo **AHP (PG)** não destaca apenas os riscos mais críticos, mas também oferece uma base sólida para a tomada de decisão estratégica na priorização de ações de governança, tornando possível direcionar recursos e esforços adequados para as áreas de maior potencial de impacto organizacional e institucional, identificados pelo valor do **PG-AHP-AIJ** (Figura 4.9).

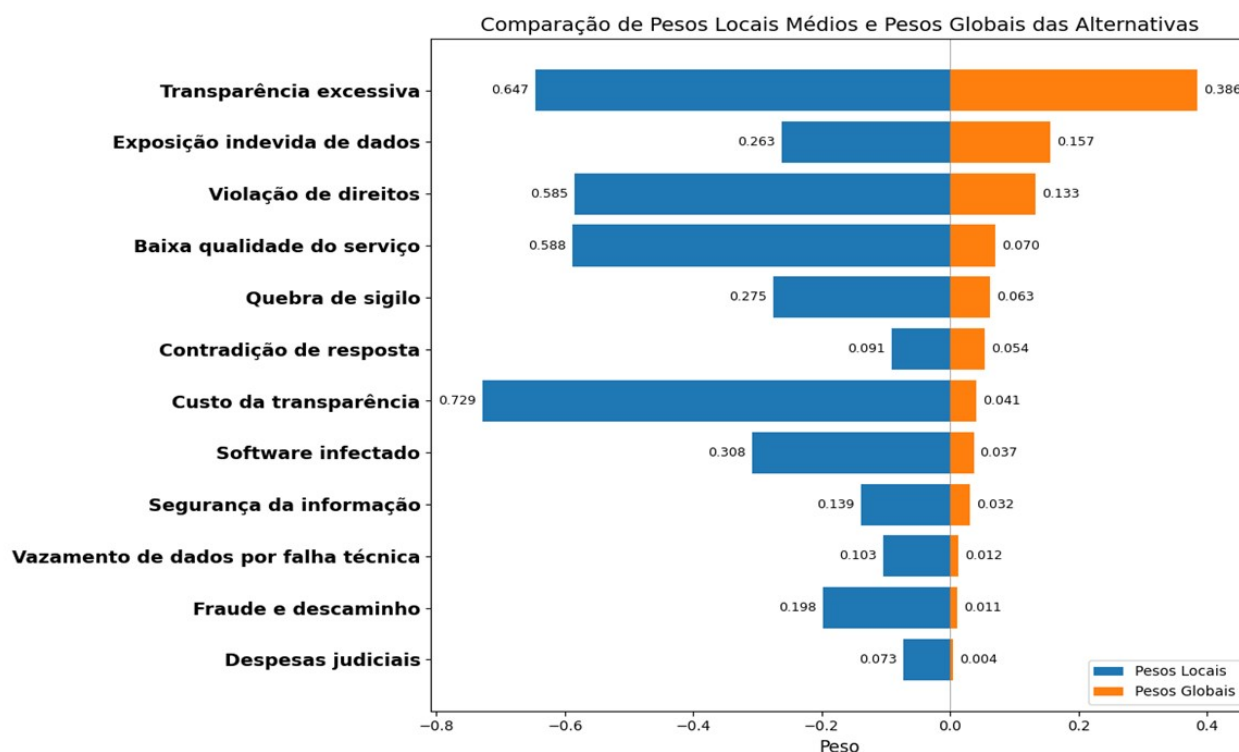


Figura 4.9: Ranking Global (Alternativas)

Fonte: Elaborada pelo autor, (2026)

Transparência Excessiva (A3), com **PG** de 38,58% e **PL** de 64,66%, e Exposição Indevida (A2), com **PG** de 15,67% e **PL** de 26,27%, aparecem como dominantes na lista de prioridades e podem representar “furos alinhados” no processo de compartilhamento de dados, tendo como desfecho natural o dano para a sociedade na Violação de Direitos (A9), com **PG** de 13,34% e **PL** de 58,52%, reforçados pela Baixa Qualidade do Serviço (A6), com **PG** de 7,02% e **PL** de 58,82%.

Uma vez que estas quatro alternativas concentram 74,62% de relevância no modelo avaliado, percebe-se que não se trata de um agrupamento de riscos pequenos e aleatórios, mas de uma provável fragilidade, destacando o *gap* institucional entre normas e a capacidade real de execução e manutenção do direito de acesso à informação nos órgãos. Isso alerta sobre a necessidade de priorização e centralização de recursos em ações de gestão e incorporação de controles de riscos no processo de atendimento às demandas da LAI [Michener et al., 2018a, Michener et al., 2018b, Trautendorfer et al., 2025].

Os valores de **PG** da AHP-AIJ obtidos apresentam coesão com os valores de **NPR** hierarquizados pela FMEA, conforme detalhamento na Figura 4.10.

4.4 Modelo de Normalização – FMEA e AHP-AIJ

4.4.1 Normalização e Ranqueamento

Os cálculos da **FMEA** para composição do **NPR** são gerados em escala de valores entre $[0-1000]$, enquanto os valores obtidos com a matriz **AHP-AIJ** na definição dos **PG** são definidos em escala numérica entre $[0-1]$. Para superar esse desafio, recorre-se à aplicação de técnicas de normalização, como o Min-Max estatístico [Von Neumann, 1928], reescalando todos os valores em um intervalo comum de $[0-1]$, conforme descrito na Figura 4.10.

Alternativa	AHP (Peso Global)	AHP Normalizado (0-1)	FMEA (NPR)	FMEA Normalizado (0-1)
Exposição Indevida de Dados	0.1567	0.3998	504	0.7651
Contradição de Resposta	0.0541	0.1310	210	0.2855
Transparência Excessiva	0.3858	1.0000	648	1.0000
Baixa Qualidade do Serviço	0.0702	0.1732	441	0.6623
Vazamento de Dados por Falha Técnica	0.0123	0.0215	200	0.2692
Software Infectado	0.0368	0.0857	126	0.1485
Quebra de Sigilo	0.0628	0.1538	225	0.3100
Violação de Direitos	0.1334	0.3387	450	0.6770
Segurança da Informação	0.0318	0.0726	135	0.1631
Custo da Transparência	0.0408	0.0961	80	0.0734
Despesas Judiciais	0.0041	0.0000	175	0.2284
Fraude e Descaminho	0.0111	0.0183	35	0.0000

Figura 4.10: Valores Normalizados de FMEA e AHP

Fonte: Elaborada pelo autor, (2026)

É possível perceber a convergência plena em “Transparência Excessiva” (A3), que atinge o valor máximo em ambas as abordagens, destacando esse evento como o principal risco sistêmico do compartilhamento de dados no processo de atendimento a pedidos de acesso à informação fundamentados na **LAI**.

Tal resultado pode representar a existência de tensões institucionais entre divulgação e proteção de informações, destacando o papel e o impacto direto da **LGPD** no processo estudado, podendo ser causado por interpretações extensivas, pressão externa e ingerência no tratamento de dados, além da ausência de critérios robustos de exclusão e/ou anonimização de dados, que podem levar à divulgação inadequada de conteúdos sensíveis.

Tal hipótese se consolida ao observar os três riscos priorizados na sequência: “Exposição Indevida de Dados” (A2), “Violação de Direitos” (A9) e “Baixa Qualidade do

Serviço” (A6). Juntos, os quatro formam o bloco prioritário de riscos do processo estudado, concentrando $\approx 74,62\%$ de relevância e importância no modelo avaliado. Este último (A6) apresenta maior valor de intensidade relativa na **FMEA** [0,6623] do que no **AHP** [0,1732], podendo sugerir maior sensibilidade aos riscos com impacto operacional imediato e maior recorrência percebida no processo; enquanto o **AHP**, ao sintetizar julgamentos multicritério, reorienta a prioridade para riscos com maior efeito sistêmico e regulatório.

Em pesquisas que utilizam diferentes métodos de análise, como a **FMEA** e o **AHP**, os resultados são expressos em unidades distintas, o que pode dificultar a comparação direta e a priorização dos itens avaliados. Visando prover a análise conjunta de padrões de convergência e divergência entre os valores normalizados de **PG** referentes às alternativas da matriz **AHP-AIJ** e de **NPR** obtidos pela aplicação da **FMEA**, gerou-se a Figura 4.11.

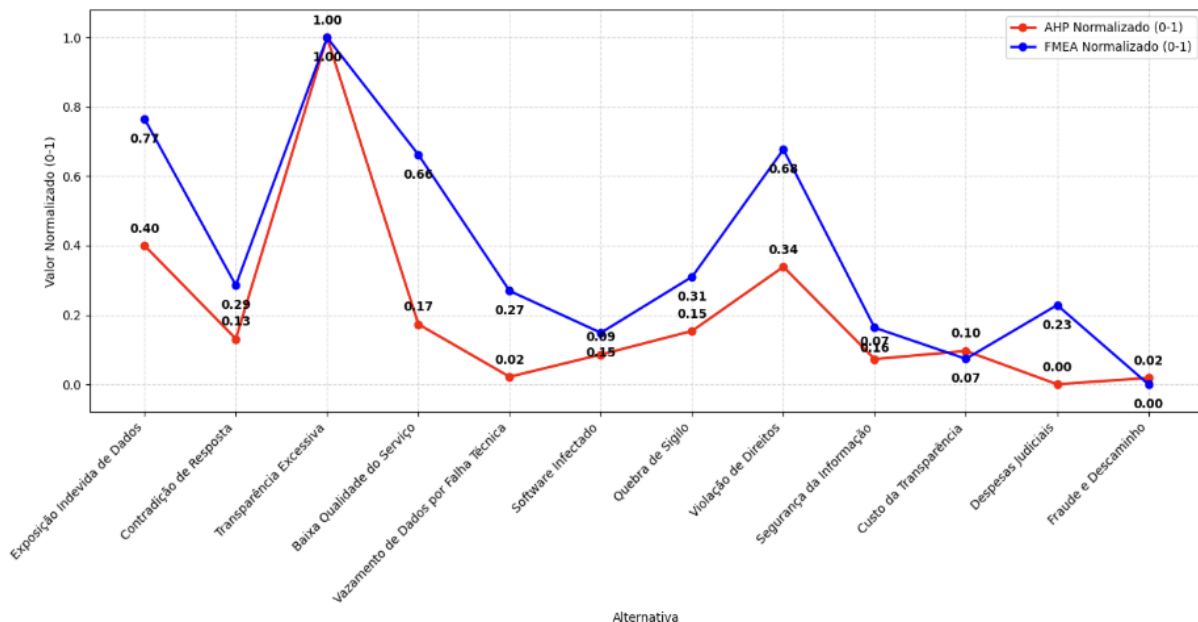


Figura 4.11: Comparativo dos Valores Normalizados

Fonte: Elaborada pelo autor, (2026)

Este grupo prioritário de riscos (A2, A3, A9 e A6) é operacionalmente muito mais próximo do ato administrativo de responder a um pedido de acesso à informação, podendo ser considerado como riscos estruturais do processo estudado; eles são mais propensos a gerar “furos” nas barreiras de defesa, causando o alinhamento negativo de oportunidades e gerando uma trajetória direta e favorável para a ocorrência de evento danoso [Reason, 2000a, Reason, 2000b, Wiegmann et al., 2022].

Se o órgão classifica mal, revisa mal, interpreta a **LAI** de forma binária ou entrega dados e informações além do necessário e legalmente cabido, já caracteriza o incidente

institucional; as consequências são percebidas de forma direta, imediata e estrutural na operação institucional.

Já o risco de “Fraude e Descaminho” (A11) ficou no piso mais baixo da priorização, tendo sido destacado para a cauda da distribuição pelos dois modelos, reforçando a convergência metodológica da investigação no uso da **FMEA** e do **AHP**. Neste caso, é possível inferir que o risco (A11) foi percebido como menos direto, menos imediato e menos estrutural que os outros riscos ligados ao compartilhamento de dados fundamentados na **LAI**, uma vez que ele depende de uma cadeia mais longa de eventos: a informação precisa ser compartilhada, depois apropriada por terceiro malicioso, depois combinada com outros dados ou usada oportunisticamente, para só então produzir dano – ou seja, trata-se de um risco indireto e mediado.

Cabe destacar que a baixa prioridade relativa não significa irrelevância absoluta e não quer dizer que o risco de “Fraude e Descaminho” seja inexistente ou desprezível. Significa que, comparativamente ao grupo prioritário, ele foi percebido como menos urgente do que os riscos que incidem de forma imediata e direta sobre o processo decisório e sobre fatores de conformidade da resposta com a **LAI**, direitos fundamentais, privacidade e tantos outros.

Ante o exposto, é possível inferir que o processo decisório analisado está fortemente condicionado por riscos que combinam transversalmente fatores de ordem normativa, operacional e orçamentária, confirmando que a governança de dados no âmbito da **LAI** é uma temática carente de modelos e padronização de processos de trabalho. Sendo assim, ante a lacuna identificada, a hierarquização obtida orienta diretamente as etapas de priorização de mitigação e subsidia a construção do **LAI-RGF**, permitindo ações proporcionais ao impacto percebido pelos especialistas.

4.5 *Framework* de Gestão de Riscos

Segundo a **ABNT** NBR ISO 31000:2018, a gestão de riscos é concebida como um processo estruturado, iterativo e integrado à governança e à tomada de decisão organizacional, detalhado na Figura 4.12.

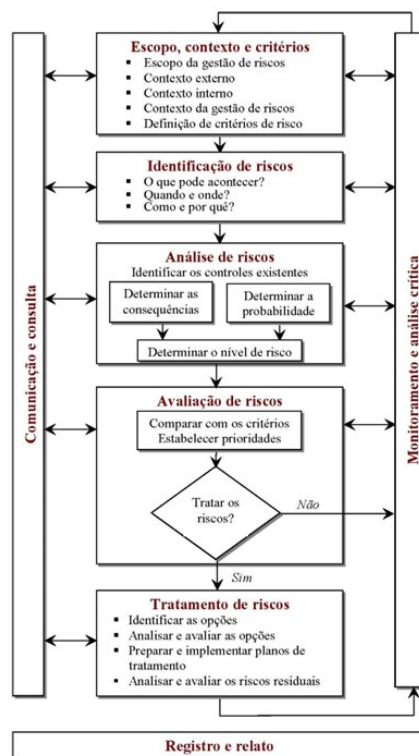


Figura 4.12: Processo de Gestão de Riscos ABNT NBR ISO 31000:2018.

Fonte: Elaborada pelo autor, (2026)

A norma estabelece que o processo de gestão de riscos compreende, de modo articulado: a definição do escopo, contexto e critérios; a avaliação de riscos, composta por identificação, análise e avaliação; o tratamento de riscos; além de atividades permanentes de comunicação e consulta, monitoramento e análise crítica, bem como registro e relato. Do ponto de vista conceitual, a análise de riscos aprofunda a compreensão da natureza do risco, estima seu nível e considera o papel dos controles já existentes [Glette-Iversen et al., 2023a, Parviainen et al., 2021].

Já a avaliação de riscos compara os resultados produzidos na análise com os critérios de risco definidos no contexto da organização, com a finalidade de estabelecer prioridades e verificar a necessidade de tratamento.

Estudos sobre gestão de riscos com base na ISO 31000 observam que a fase de avaliação constitui o espaço em que a organização confronta evidências, critérios, valores e alternativas de ação, especialmente em contextos complexos ou dinâmicos de tomada de decisão. [Parviainen et al., 2021] e [Glette-Iversen et al., 2023b] destacam que a avaliação compreende a comparação e priorização de alternativas de tratamento de riscos com base nos resultados da análise. A tomada de decisão informada pelo risco [Apostolakis, 2004] segue a lógica em que a informação gerada pelas avaliações de risco serve como insumo

para o processo decisório institucional, devendo ser considerada em conjunto com uma gama de recursos, *frameworks* e normas desenvolvidos para orientar esse processo.

À luz da ISO 31000, o tratamento de riscos corresponde à seleção e implementação de opções para modificar o risco; nesse sentido, o **LAI-RGF** foi idealizado para ser intuitivo e aplicado como recurso de suporte nesta fase. Ele pode ser incorporado à **Estrutura de Gestão de Riscos (EGR)** de qualquer organização pública ou privada que esteja sujeita aos termos da **LAI** no Brasil, trazendo benefícios consideráveis.

Ao adotar o **LAI-RGF** (Figura 4.13), implementa-se um mecanismo democrático que oferece uma trilha única, escalonável e replicável para os gestores equilibrarem-se entre o direito de acesso à informação da população e a tomada de decisão orientada pelos riscos do processo estudado.

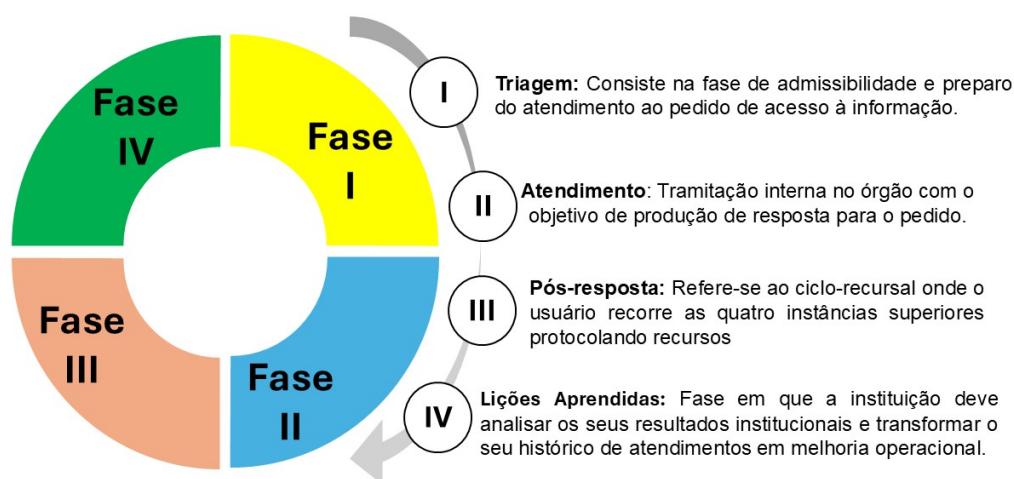


Figura 4.13: *Framework* de Gestão de Riscos de Compartilhamento da LAI.

Fonte: Elaborada pelo autor, (2026)

Ao organizar o processo de atendimento a demandas da **LAI**, as atividades previstas em cada fase do **LAI-RGF** correspondem às ações por meio das quais o órgão público conduz o atendimento aos pedidos de acesso à informação, tomando os riscos como variável relevante de observação, ponderação e controle no processo decisório. Nessa lógica, os riscos não constituem um fim em si mesmos, mas um elemento orientador da ação institucional.

O *framework* direciona a Administração Pública para que avance da lógica decisória estritamente binária e centrada em deferir ou indeferir o acesso aos grupos de dados solicitados, para uma lógica alargada, fundamentada no direcionamento de risco, mais compatível com a perspectiva da ISO 31000 de utilização da gestão de riscos como suporte

à qualificação da decisão organizacional, ajudando os agentes públicos a avançarem da condição de “gerentes de incêndio” nos órgãos para se tornarem uma equipe de governança de riscos.

O **LAI-RGF** foi idealizado e estruturado em quatro fases, tomando a operação da legislação como parâmetro estruturante: Triagem → Atendimento → Pós-resposta → Lições Aprendidas, descritas a seguir.

Na fase de **Triagem**, os pedidos recebidos via plataforma **Fala.BR** são examinados quanto à sua admissibilidade e aderência aos requisitos da **LAI**, definindo se estão conformes ou desconformes com a legislação, e são definidos os trâmites de encaminhamento do processo.

Na fase de **Atendimento**, ocorre a tramitação interna no órgão com o objetivo de produzir a resposta ao solicitante; conforme orientações da **CGU**, uma vez identificado que se trata de pedido de informação sob competência do órgão ou entidade, a resposta deve ser elaborada e posteriormente registrada no **Fala.BR**.

A fase de **Pós-resposta** é quando o processo evolui para o ciclo recursal: recursos de primeira instância são apreciados por autoridade hierarquicamente superior àquela que originou a decisão inicial; os recursos de segunda instância são direcionados à autoridade máxima do órgão; em terceira instância, a apreciação é realizada pela **CGU**; e, quando alcançam a quarta instância, os recursos passam à **CMRI**, responsável por atuar como última instância administrativa recursal nas negativas de acesso à informação.

Por fim, a fase de **Lições Aprendidas** é destinada à análise do histórico de atendimentos e à sua transformação em melhoria operacional, com vistas ao aperfeiçoamento dos controles internos e externos, ao fomento da transparência e controle social, e ao aprimoramento da governança dos riscos associados ao compartilhamento de dados públicos. Nessa configuração, o *framework* passa a oferecer uma trilha concreta para gestores e proprietários de riscos, permitindo governar o ciclo de atendimento aos pedidos de acesso à informação com práticas de governança previstas na **ABNT NBR ISO 31000:2018**.

O **LAI-RGF** é um recurso com aplicação operacional predominante centrada na fase de tratamento dos riscos, por transformar a priorização obtida na avaliação em medidas concretas de resposta, mitigação, padronização decisória e aprendizagem institucional no processo de atendimento da **LAI**.

Embora dialogue com resultados oriundos da identificação, análise e avaliação de riscos, no **LAI-RGF** os riscos funcionam como variável orientadora da ação administrativa; por isso, o *framework* se realiza predominantemente na fase de tratamento dos riscos, uma vez que organiza as providências concretas a serem adotadas pelo órgão no atendimento aos pedidos de acesso à informação. É precisamente essa conversão do risco em providência administrativa que permite situá-lo, de forma predominante, na fase de tratamento dos

riscos (ISO 31000:2018).

Esse processo cria retroalimentação institucional, melhora o controle social e pode ser conduzido por um plano de gestão de riscos que incorpore o **LAI-RGF** como recurso complementar.

Uma das formas de implementação deste recurso é o 5W2H [Santos Neto et al., 2016], uma matriz idealizada para ser flexível e aplicável em diferentes contextos e projetos de sistemas computacionais [Klock et al., 2016]; por este motivo, o modelo ilustrativo de orientação do usuário que segue está organizado na estrutura 5W2H, traduzindo o **LAI-RGF** em um artefato simples de ser operado e implementado nas entidades públicas e privadas.

O plano de implementação proposto e detalhado no Tabela 4.1 não esgota as possibilidades de uso do modelo, mas demonstra como a priorização dos riscos pode ser convertida em providências administrativas concretas e em aprendizagem organizacional no setor público.

Tabela 4.1: Plano de Implementação do **LAI-RGF**. Elaborada pelo autor, 2025.

Elemento	Plano de Implementação
What (O quê?)	Implementar o LAI-RGF como ferramenta de decisão para o tratamento de riscos no ciclo de pedidos de acesso à informação, estruturado em quatro fases: Triagem → Atendimento → Pós-resposta → Lições Aprendidas.
Why (Por quê?)	Transformar a base legal (LAI) e as boas práticas de gestão de riscos (ISO 31000) em decisão rastreável e proporcional ao risco (divulgação/indeferimento total ou parcial), institucionalizando <i>accountability</i> e maturidade democrática.
Who (Quem?)	Gestores e proprietários de riscos no órgão; SIC para a operação no Fala.BR ; instâncias recursais internas e, quando aplicável, CGU e CMRI . A EGR deve estar alinhada à estratégia institucional.
Where (Onde?)	No órgão/entidade sujeito à LAI , com operação do fluxo na plataforma Fala.BR , observando a base legal brasileira e os normativos complementares indicados para cada fase.
When (Quando?)	Atendimento: prazo de 20 dias + 10 (prorrogação justificada). Pós-resposta/Recursos: cadeia 1ª instância → 2ª instância → CGU → CMRI . As demais fases seguem o ciclo operacional descrito (Triagem antes do atendimento; Lições Aprendidas ao final).
How (Como?)	(1) Mapear o processo de atendimento a pedidos LAI ; (2) Identificar riscos; (3) Classificar por tipologia mínima (operacionais, reputação, legais, financeiros/orçamentários) conforme INC MP/CGU nº 1/2016 ; (4) Selecionar e excluir riscos não relacionados; (5) Avaliar e priorizar com FMEA (NPR) ou AHP (PG) ; (6) Construir a EGR e o Plano de Gestão de Riscos; (7) Operar por fase: Triagem (é pedido LAI ? competência? transparência ativa); Atendimento (trâmite e resposta via Fala.BR); Pós-resposta (gestão de recursos); Lições Aprendidas (melhoria contínua).
How Much (Quanto?)	Deverá ser calculado caso a caso, considerando o contexto e a maturidade institucional no atendimento a pedidos de acesso à informação e na gestão de riscos.

As ações sugeridas no plano permitem que outras estratégias sejam somadas ao **LAI-RGF**, ou que ele mesmo seja uma ação complementar do Plano de Gestão dos Riscos Institucionais, oferecendo uma trilha concreta, replicável e alinhada às melhores práticas internacionais para os gestores de entidades públicas.

O *framework* não foi concebido como uma ferramenta voltada para a descoberta de riscos institucionais inéditos, nem como instrumento primário de cálculo autônomo de

probabilidade e impacto desses riscos. O **LAI-RGF** é uma ferramenta de suporte à tomada de decisão no contexto do compartilhamento de dados regulado pela **LAI**, organizada em quatro fases encadeadas com a finalidade de tornar o fluxo auditável, replicável e rastreável, com base nos riscos institucionais já identificados, classificados e priorizados.

Em vez de compreender os riscos priorizados na pesquisa (Figura 3.2), como eventos isolados obtidos por **FMEA/NPR** e **AHP/PG** (Figura 4.9), a proposta analítica do *framework* (Figura 4.13) permite visualizá-los conforme o momento institucional em que tendem a surgir, se intensificar, se materializar ou retroalimentar o sistema ao longo das fases de operação do **LAI-RGF**. A Figura 4.14 apresenta a distribuição da probabilidade de ocorrência dos riscos priorizados ao longo das quatro fases do **LAI-RGF**.

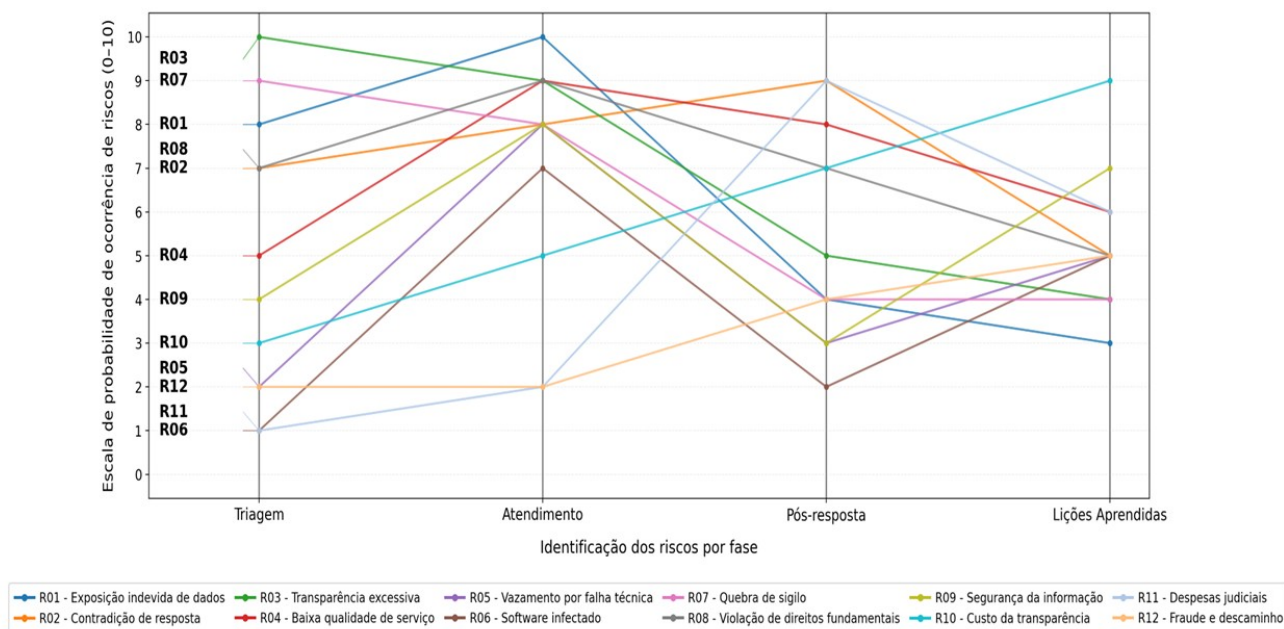


Figura 4.14: Ocorrência dos Risco Prioritários no LAI-RGF.

Fonte: Elaborada pelo autor, (2026)

No eixo horizontal estão representadas as fases do *framework*, enquanto o eixo vertical adota uma escala de 0 a 10, na qual valores mais elevados indicam maior possibilidade de ocorrência do risco na respectiva fase do processo analisado. Cada linha do gráfico corresponde a um risco priorizado, permitindo visualizar, de forma comparativa, em que momento do ciclo de atendimento ao pedido de acesso à informação determinado risco tende a se manifestar com maior intensidade.

Desse modo, o gráfico não apenas evidencia a variação do comportamento dos riscos entre as fases, mas também auxilia a identificar pontos de maior criticidade, favorecendo a compreensão de onde os gestores públicos devem concentrar maior atenção, controles e recursos institucionais. Trata-se, portanto, de uma representação visual que contribui para interpretar a dinâmica dos riscos no processo estudado e reforça a aplicação do *framework* como ferramenta de apoio à tomada de decisão orientada por riscos.

Observando a Figura 4.14, é possível perceber que os riscos prioritários (Figura 4.11) estão concentrados nas Fases I e II, ou seja, nas fases em que o órgão interpreta o pedido, classifica a informação, define limites de acesso, produz a resposta e operacionaliza o compartilhamento. Já as Fases III e IV funcionam como espaços de revelação ampliada, retroalimentação e correção institucional. Isso explica por que riscos como Transparência Excessiva (A3), Exposição Indevida de Dados (A2), Violação de Direitos Fundamentais (A9) e Baixa Qualidade do Serviço (A6) concentram 74,62% de relevância no modelo avaliado, assumindo maior centralidade do que riscos mais periféricos como Fraude e Descaminho (A11), que representa 1,11% de relevância no modelo avaliado.

Na **Fase I** – de Triagem – concentram-se especialmente os riscos de Transparência Excessiva (A3), Quebra de Sigilo (A8), Contradição de Resposta (A1), Exposição Indevida de Dados (A2) e, em parte, Violação de Direitos Fundamentais (A9). Essa é a fase em que o órgão decide se o pedido é admissível, qual é seu escopo, qual unidade é competente, que tipo de informação está sendo demandada e quais limites jurídicos e técnicos devem balizar a futura resposta.

A **Fase II** – de Atendimento – é o núcleo operacional do risco no *framework*. É nela que os dados são tratados, localizados, extraídos, manipulados, consolidados, revisados, eventualmente anonimizados e, na sequência, encaminhados para compor a resposta ao pedido. Por isso, essa fase concentra a maior densidade de riscos prioritários, especialmente Exposição Indevida de Dados (A2), Baixa Qualidade do Serviço (A6), Vazamento de Dados por Falha Técnica (A4), Segurança da Informação (A7), *Software* Infectado (A5), Violação de Direitos Fundamentais (A9), Quebra de Sigilo (A8), Contradição de Resposta (A1) e a própria Transparência Excessiva (A3), quando esta se concretiza na entrega de conteúdo além do juridicamente cabível.

Na **Fase III** – de Pós-resposta – os riscos assumem uma feição mais evidente de consequência, contestação e amplificação institucional. Nessa etapa, ganham destaque Despesas Judiciais (A10), Contradição de Resposta (A1), Violação de Direitos Fundamentais (A9), Baixa Qualidade do Serviço (A6), Custo da Transparência (A12) e, de forma mais residual, Fraude e Descaminho (A11). A justificativa é simples: é no pós-resposta que os efeitos das falhas anteriores aparecem de forma mais visível, seja na forma de recursos administrativos, contestações, judicialização, dano reputacional, necessidade de retrabalho

ou uso indevido das informações já divulgadas.

A **Fase IV** – de Lições Aprendidas – não é propriamente uma fase de origem dos riscos, mas uma etapa de absorção institucional, correção e maturação da governança. Aqui, todos os riscos devem ser reprocessados como insumo de melhoria, mas alguns ganham especial relevância como indicadores de falha sistêmica: Baixa Qualidade do Serviço (A6), Contradição de Resposta (A1), Segurança da Informação (A7), *Software* Infectado (A5), Vazamento de Dados por Falha Técnica (A4), Despesas Judiciais (A10), Custo da Transparência (A12) e Fraude e Descaminho (A11). A lógica dessa fase é menos reativa e mais estratégica.

Sob perspectiva analítica, o gráfico também demonstra que os riscos não têm comportamento homogêneo nas fases do *framework*, mas assumem comportamentos distintos conforme a natureza das atividades desenvolvidas, os agentes públicos envolvidos, os volumes de dados a serem tratados e a complexidade da demanda em cada etapa. Em termos práticos, isso significa que determinados riscos se mostram mais críticos em momentos específicos do processo, o que reforça a necessidade de adoção de controles, cautelas e decisões proporcionais ao contexto operacional de cada fase.

Desta forma, a representação gráfica auxilia na conscientização da necessidade de considerar os riscos como variável sensível no processo de tomada de decisão relacionada com o compartilhamento de dados no atendimento a pedidos de acesso à informação segundo a **LAI**, e que a gestão dos riscos nesse âmbito não deve ser tratada de forma genérica ou estática, mas sim de maneira processual, situada e orientada pelas características de cada fase do atendimento.

Ao destacar as oscilações de probabilidade de ocorrência dos riscos, o gráfico oferece suporte à leitura do **LAI-RGF** como instrumento de governança aderente à lógica da **ABNT** NBR ISO 31000:2018; não apenas ilustra os resultados obtidos, mas também reforça a viabilidade de uso do *framework* como ferramenta de apoio à tomada de decisão e à alocação mais qualificada de recursos institucionais no setor público.

Nesse sentido, a figura cumpre função interpretativa relevante para a dissertação, pois evidencia visualmente onde os riscos priorizados tendem a se concentrar com maior intensidade e, por consequência, onde a atuação institucional deve ser mais atenta.

Se a instituição identifica recorrência de respostas contraditórias, judicialização, falhas de revisão, exposição indevida de dados ou incidentes de segurança, isso precisa ser convertido em aprendizagem organizacional: revisão de fluxos, atualização de critérios, capacitação, melhoria dos controles, padronização decisória, definição de trilhas de auditoria e reforço dos mecanismos de proteção da informação.

O problema central do compartilhamento de dados sob a **LAI** não está apenas em ameaças externas ou usos ilícitos posteriores da informação, mas, sobretudo, nas falhas

primárias de governança que antecedem o ato de compartilhar. Em outras palavras, o risco mais crítico não é, em primeiro lugar, o que o terceiro faz com o dado; é o que a própria administração deixa de fazer antes de disponibilizá-lo. Essa conclusão reforça a utilidade do **LAI-RGF** como modelo analítico e gerencial, pois ele permite posicionar o risco no processo e orientar a tomada de decisão sobre medidas de controle de modo mais cirúrgico.

Os riscos mais altos não recaíram, em sua maioria, sobre consequências externas tardias, mas sobre falhas primárias de governança, classificação, revisão, proteção da informação e qualidade da decisão administrativa. Em termos práticos, o problema mais sensível não está apenas nas atividades ou processos que terceiros podem realizar depois que o dado sai do órgão, mas no modo como o próprio órgão prepara, trata, revisa e entrega a informação. Esse achado é coerente com os resultados dos métodos multicritério e de priorização.

Capítulo 5

Considerações Finais

5.1 Objetivos e Resultados Obtidos na Pesquisa

Esta investigação teve como objetivo geral analisar os principais riscos do compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação, com vistas a fundamentar e estruturar um *framework* de governança, alinhado à ABNT NBR ISO 31000:2018, capaz de converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional no setor público. Esse objetivo foi alcançado a partir do percurso metodológico apresentado no Capítulo 3, e dos resultados discutidos no Capítulo 4, os quais permitiram construir uma trajetória analítica que partiu do mapeamento da literatura e culminou na estruturação do LAI-RGF.

O primeiro objetivo específico, voltado a mapear a literatura acadêmica e normativa sobre os riscos relacionados ao compartilhamento de dados públicos no contexto da LAI, foi alcançado por meio da pesquisa bibliométrica e documental realizada na etapa inicial do estudo. Essa fase permitiu reunir referências acadêmicas, normativas e institucionais relevantes, compondo a base conceitual e regulatória necessária à compreensão do fenômeno investigado e à delimitação do problema de pesquisa.

O segundo objetivo específico, destinado a identificar e organizar, por tipologia, os principais riscos associados ao compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação, foi alcançado com base na análise da literatura, no exame dos referenciais normativos adotados e na participação de especialistas. A partir desse procedimento, foi possível consolidar um conjunto de riscos organizados em tipologias, favorecendo maior clareza analítica e aderência ao contexto institucional estudado.

O terceiro objetivo específico, referente à hierarquização dos principais riscos associados ao compartilhamento de dados públicos no processo de atendimento a pedidos de acesso à informação, foi alcançado mediante a aplicação integrada de técnicas de priorização. O emprego combinado da FMEA, da AHP-AIJ e da normalização Mini-Max permitiu

ordenar os riscos segundo seu grau de criticidade, produzindo um *ranking* fundamentado em julgamentos especializados e em critérios analíticos compatíveis com os propósitos da pesquisa.

O quarto objetivo específico, voltado a fundamentar e estruturar um *framework* de governança, alinhado à ABNT NBR ISO 31000:2018, capaz de converter a priorização dos riscos em decisões institucionais, medidas de tratamento e aprendizagem organizacional no setor público, foi alcançado com a construção do LAI-RGF e de seu respectivo plano de implementação. A estruturação do *framework* representou a principal contribuição aplicada da dissertação, ao transformar a priorização dos riscos em uma proposta de governança orientada para a ação institucional, organizada em fases e concebida para apoiar a condução do atendimento a pedidos de acesso à informação sob parâmetros de rastreabilidade, proporcionalidade, controle e melhoria contínua.

Em síntese, os resultados obtidos demonstram que a pesquisa atingiu os objetivos propostos ao percorrer, de forma articulada, as etapas de mapeamento da literatura, identificação e organização tipológica dos riscos, hierarquização multicritério e estruturação de um *framework* de governança alinhado à ABNT NBR ISO 31000:2018. Com isso, a dissertação oferece não apenas uma leitura analítica dos principais riscos do compartilhamento de dados públicos no contexto da LAI, mas também uma proposta aplicada de governança voltada à conversão da priorização dos riscos em decisão institucional, tratamento e aprendizagem organizacional no setor público.

5.2 Limitações da Pesquisa

Decorrida a investigação, destacam-se como aspectos limitadores: o cenário de estudo ter sido circunscrito ao contexto do Poder Executivo Federal; e a utilização de um quantitativo reduzido de respondentes [Saaty & Vargas, 2012, Benabdellah et al., 2019], o que pode restringir a generalização dos resultados quando aplicados a outro contexto institucional ou a outras áreas de governo.

A utilização da FMEA juntamente com a AHP como ferramentas da estrutura metodológica da pesquisa mostrou-se suficiente para o êxito no objetivo desejado; porém, a inclusão de modelos de preferências multicritério – para aprofundar a etapa de priorização e tornar explícitas as escolhas e pesos entre os critérios – como, por exemplo, o método PROMETHEE (I, II e variantes), poderia ampliar a robustez analítica do modelo.

O viés cognitivo pode ser encontrado nos resultados obtidos na FMEA e no AHP; sendo assim, a reaplicação dos formulários em momentos diferentes para verificar consistência, associada à comparação entre especialistas de diferentes áreas, pode ser uma

estratégia para equilibrar vieses, aumentar a confiabilidade e reduzir a incidência de qualquer distorção entre os respondentes.

5.3 Sugestões para Trabalhos Futuros

As atividades listadas a seguir podem ser consideradas como trabalhos futuros decorrentes desta pesquisa. Tais proposições visam não somente ampliar o escopo e a robustez do presente trabalho, mas potencializar e expandir sua aderência aos critérios de excelência e inovação exigidos para a obtenção do título de mestre em Computação Aplicada oferecido pelo [Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília \(PPCA/UnB\)](#).

1. **Ampliar a coleta de dados** para identificar e extrair mais *insights* sobre a política pública brasileira de transparência e acesso à informação, assim como sobre os possíveis impactos da [LAI](#) na estrutura de tomada de decisão do Brasil e no comportamento da sociedade como um todo. Estudos estes a serem fundamentados nos casos disponibilizados pela [SNAI/CGU](#).
2. **Aplicação de novos métodos:** a literatura aponta lacunas [[Ciani et al., 2019](#)] nos estudos sobre riscos de compartilhamento de dados na esfera federal, sendo necessário fomentar pesquisas integrando outros métodos de análise e captação da percepção do estado da prática, como a substituição do [NPR/FMEA](#) pelo modelo *Action Priority* (AP/[FMEA](#)).
3. **Análise de perspectivas dos usuários e cidadãos:** estender o estudo para capturar e comparar percepções de diferentes perfis de servidores públicos, gestores e cidadãos usuários do serviço público, promovendo uma visão mais ampla e fidedigna dos riscos e qualificando ainda mais as recomendações para a aplicação do modelo em políticas públicas.
4. **Implementação e expansão do modelo:** implementar o modelo proposto nesta pesquisa e analisar todos os departamentos de um órgão. A Hierarquia de Desempenho de Especialistas (HEP) [[Dror, 2016](#)] destaca que especialistas de áreas distintas podem perceber riscos de formas muito divergentes e que receber contexto adicional pode alterar a forma de observar riscos.

Referências

- [nis,] Technical report. 7
- [gui, 2020] (2020). Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). GOV.BR. x, 33
- [ABNT, 1994] ABNT (1994). *ABNT NBR 5462: confiabilidade e manutenibilidade (terminologia)*. Associação Brasileira de Normas Técnicas, Rio de Janeiro. 39
- [Ackoff, 1989] Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, 16(1), 3–9. 34
- [Adeyeye, 2024] Adeyeye, K. (2024). Controlling the ‘elephant in the room’: A new protocol for sharing data from home performance monitoring systems. *Technology in Society*, 76, 102478. 2
- [Aguarón et al., 2023] Aguarón, J., Escobar, M. T., & Moreno-Jiménez, J. M. (2023). Reducing Incompatibility in a Local AHP-Group Decision Making Context. *Annals of Operations Research*, 326(1), 1–26. 58
- [Altshuller, 1998] Altshuller, G. S. (1998). *Forty Principles*. Technical Innovation Center, 1st english edition. 1^a ed. russa, 1974. 38
- [Apostolakis, 2004] Apostolakis, G. E. (2004). How Useful Is Quantitative Risk Assessment? *Risk Analysis*, 24(3), 515–520. 76
- [ARTICLE 19, 2016] ARTICLE 19 (2016). The Public’s Right to Know: Principles on Right to Information Legislation. https://www.article19.org/data/files/RTI_Principles_Updated_EN.pdf. Originally developed in 1999 and updated in 2015. 27
- [Asgari Dastjerdi et al., 2017] Asgari Dastjerdi, H., Khorasani, E., Yarmohammadian, M. H., & Ahmadzade, M. S. (2017). Evaluating the Application of Failure Mode and Effects Analysis Technique in Hospital Wards: A Systematic Review. *Journal of Injury and Violence Research*, 9(1), 51–60. 62
- [Aull-Hyde et al., 2006] Aull-Hyde, R., Erdogan, S., & Duke, J. M. (2006). An Experiment on the Consistency of Aggregated Comparison Matrices in AHP. *European Journal of Operational Research*, 171(1), 290–295. 70
- [Aven & Renn, 2019] Aven, T. & Renn, O. (2019). Algumas questões fundamentais relacionadas à governança de riscos e diferentes tipos de riscos. *Journal of Risk Research*, 23(9), 1121–1134. 36, 37

- [Aytac et al., 2025] Aytac, S., Tran, C. Y., & Frye, N. (2025). Lei de Lotka da produtividade científica em todas as disciplinas de pesquisa: Uma revisão. *Science & Technology Libraries*, (pp. 1–13). 8, 10
- [Baas et al., 2020a] Baas, J., Schotten, M., Plume, A., Côté, G., & Karimi, R. (2020a). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies*, 1(1), 377–386. 9
- [Baas et al., 2020b] Baas, J., Schotten, M., Plume, A. M., Côté, G., & Karimi, R. (2020b). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies*, 1(1), 377–386. 9, 52
- [Barros et al., 2023] Barros, M. J., Melo, P., & Guevara, A. (2023). How management information systems might add value to the decision-making process in organizations. 34
- [Batagelj & Cerinsek, 2013] Batagelj, V. & Cerinsek, M. (2013). On bibliographic networks. *Scientometrics*, 96, 845–864. 19
- [Bauman, 1999] Bauman, Z. (1999). *Modernidade e ambivalência*. Jorge Zahar Editor. 49
- [Beardsley et al., 2020] Beardsley, M., Martínez-Moreno, J., Santos, P., & Hernández-Leo, D. (2020). Apoio aos alunos na tomada de decisões informadas sobre o compartilhamento de dados: da compreensão ao consentimento. In *Proceedings of the IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 175–179). Tartu, Estônia. 2
- [Bell, 1973] Bell, D. (1973). *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Basic Books. 32
- [Ben-Daya & Raouf, 1996] Ben-Daya, M. & Raouf, A. (1996). Um modelo revisado de análise de modos e efeitos de falhas. *International Journal of Quality & Reliability Management*, 13(1), 43–47. xii, 41
- [Benabdellah et al., 2019] Benabdellah, A. C., Benghabrit, A., & Bouhaddou, I. (2019). A survey of clustering algorithms for an industrial context. *Procedia Computer Science*, 148, 291–302. 62, 86
- [Beniger, 2009] Beniger, J. R. (2009). *The control revolution: Technological and economic origins of the information society*. Harvard University Press. 25
- [Bensman & Smolinsky, 2017] Bensman, S. J. & Smolinsky, L. J. (2017). Lotka’s Inverse Square Law of Scientific Productivity: Its Methods and Statistics. *Journal of the Association for Information Science and Technology*, 68(7), 1786–1791. 14
- [Berriel & Santos, 2020] Berriel, P. & Santos, M. (2020). Bibliometria com o VOSviewer. x, 15, 16
- [Bezerra, 2024] Bezerra, J. A. S. (2024). A importância da gestão do risco cibernético: um estudo de [...]. TCC – Escola Superior de Guerra. 35

- [BRASIL, 2017] BRASIL (2017). Lei n.º 13.460, de 26 de junho de 2017. dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Presidência da República. 55
- [BRASIL, 2021] BRASIL (2021). Lei n.º 14.129, de 26 de março de 2021. dispõe sobre princípios, regras e instrumentos para o Governo Digital. Presidência da República. 55
- [Brynjolfsson & McAfee, 2016] Brynjolfsson, E. & McAfee, A. (2016). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton & Company, reprint edition. 25
- [Bygrave, 2017] Bygrave, L. A. (2017). Proteção de dados desde a concepção e por padrão: decifrando os requisitos legislativos da UE. *Oslo Law Review*, 4(2), 105–120. 2
- [Campos, 2020] Campos, J. M. d. S. (2020). Lei de Acesso à Informação: Direito Comparado entre Brasil e Estados Unidos. *Revista Acadêmica da Faculdade de Direito do Recife*, 91(2), 25–48. DOI não localizado. 28
- [Candela et al., 2015] Candela, L., Castelli, D., Manghi, P., & Tani, A. (2015). Data journals: a survey. *Journal of the Association for Information Science and Technology*, 66(9), 1747–1762. 35
- [Capuano, 2022] Capuano, E. A. (2022). Lei de Acesso à Informação no Brasil: o que os dados de implementação revelam. *Ciência da Informação*, 51(3). 14
- [Carmo et al., 2013] Carmo, D. K. d. S., Marins, F. A. S., Salomon, V. A. P., & Mello, C. H. P. (2013). On the Aggregation of Individual Priorities in Incomplete Hierarchies. In *Proceedings of the International Symposium on the Analytic Hierarchy Process*. 58
- [Carvalho et al., 2019] Carvalho, A. L., Andrade, L., Mendes, H. T. C., Alves, M. A., & Pinheiro, P. V. (2019). Análise de modos e efeitos de falhas: abordagem extensionista aplicada a uma pequena empresa. *Conecte-se! Revista Interdisciplinar de Extensão*, 3(5), 86–100. DOI não localizado. 40
- [Castells, 2004] Castells, M. (2004). *The network society: a cross-cultural perspective*. Edward Elgar Publishing. 25
- [Cavoukian, 2010] Cavoukian, A. (2010). Privacidade por design: o workshop definitivo. *Identity in the Information Society (IDIS)*, 3, 247–251. 2
- [Chatterjee et al., 2024] Chatterjee, S., Chaudhuri, R., & Vrontis, D. (2024). A cultura orientada por dados impacta a inovação e o desempenho de uma empresa? uma análise empírica. *Annals of Operations Research*, 333, 601–626. 35
- [Chen et al., 2015] Chen, S., Liu, J., Wang, H., & Augusto, J. C. (2015). A group decision making model for partially ordered preference under uncertainty. *Information Fusion*, 25, 32–41. 48
- [Ciani et al., 2019] Ciani, L., Guidi, G., & Patrizi, G. (2019). A critical comparison of alternative risk priority numbers in failure modes, effects, and criticality analysis. *IEEE Access*. 87

- [Clarivate, 2020] Clarivate (2020). Google scholar and Web of Science. Web of Science Group. 11, 52
- [Commission on Human Rights & Hussain, 2000] Commission on Human Rights & Hussain, A. (2000). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Submitted in Accordance with Commission Resolution 1999/36*. Thematic Report E/CN.4/2000/63, UN Commission on Human Rights. Accessed: 2026-04-25. 27, 28
- [Controladoria-Geral da União,] Controladoria-Geral da União. Manual do Usuário. Manual institucional destinado a orientar o uso do Fala.BR em pedidos de acesso à informação. 32
- [Controladoria-Geral da União, 2021] Controladoria-Geral da União (2021). CGU divulga resultado da 2ª edição da Escala Brasil Transparente – Avaliação 360°. Notícia institucional sobre a divulgação dos resultados da 2ª edição da Escala Brasil Transparente – Avaliação 360°. 32
- [Controladoria-Geral da União, 2026] Controladoria-Geral da União (2026). Mapa Brasil Transparente. Sistema temporariamente fora do ar para atualizações. Previsão de retorno: junho de 2026. 32
- [Craig et al., 2014] Craig, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. 36
- [CTIR GOV, 2025] CTIR GOV (2025). CTIR Gov em números. GOV.BR. 36
- [Curty & Aventurier, 2017] Curty, R. G. & Aventurier, P. (2017). O paradigma da publicação de dados e suas diferentes abordagens. In *Anais do XVIII Encontro Nacional de Pesquisa em Ciência da Informação* Marília: UNESP. 34
- [De Almeida, 2024] De Almeida, V. A. R. (2024). Maturidade na gestão do risco operacional: Uma análise do setor da produção e distribuição de água de organizações ISO 9001 em Portugal. Master's thesis, Iscte-Instituto Universitário de Lisboa. 25
- [Demo, 2000] Demo, P. (2000). Ambivalências da sociedade da informação. *Ciência da Informação*, 29(2), 37–42. 11, 49, 55
- [Dror, 2016] Dror, I. E. (2016). A Hierarchy of Expert Performance. *Journal of Applied Research in Memory and Cognition*, 5(2), 121–127. 87
- [Dror et al., 2021] Dror, I. E., Scherr, K. C., Mohammed, L. A., MacLean, C. L., & Cunningham, L. (2021). Biasability and Reliability of Expert Forensic Document Examiners. *Forensic Science International*, 318, 110610. 53
- [Duleba & Szádoczki, 2022] Duleba, S. & Szádoczki, Z. (2022). Comparing Aggregation Methods in Large-Scale Group AHP: Time for the Shift to Distance-Based Aggregation. *Expert Systems with Applications*, 196, 116667. 69
- [Dyer & Forman, 1992] Dyer, R. F. & Forman, E. H. (1992). Group Decision Support with the Analytic Hierarchy Process. *Decision Support Systems*, 8(2), 99–124. 70

- [Eirão & Leite, 2019] Eirão, T. G. & Leite, F. C. L. (2019). Acceso a la información pública y democracia: algunas anotaciones. *Biblios Journal of Librarianship and Information Science*, (75), 35–45. 15
- [Eirão & Leite, 2020] Eirão, T. G. & Leite, F. C. L. (2020). Divulgar, solicitar e restringir: os verbos conjugados no acesso à informação pública nos países do Cone Sul. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, 18(00), e020002. 15
- [Ellis et al., 2005] Ellis, D., Oldridge, R., & Vasconcelos, A. (2005). Community and virtual community. *Annual Review of Information Science and Technology*, 38. 25
- [Enang et al., 2022] Enang, I., Shemami, N., Avakh Darestani, S., & Shamami, M. (2022). Failure mode and effects analysis: a decision-making risk prioritisation approach. *International Journal of Productivity and Quality Management*, 1, 1. 39, 44
- [Etemadi et al., 2021] Etemadi, N., Van Gelder, P., & Strozzi, F. (2021). An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity. *Sustainability*, 13(9). 17
- [European Union, 2024] European Union (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 1689. 7, 59
- [Fabris et al., 2022] Fabris, A., Messina, S., Silvello, G., & Susto, G. A. (2022). Algorithmic Fairness Datasets: The Story So Far. *Data Mining and Knowledge Discovery*, 36, 2074–2152. 17
- [Fassnacht et al., 2024] Fassnacht, M. et al. (2024). Práticas de compartilhamento de dados: a interação entre dados, estruturas organizacionais e dinâmica de rede. *Electronic Markets*, 34. 33
- [Fernandez et al., 2021] Fernandez, M. V., Cavalcanti, P., Sá, D., & Viegas, J. (2021). Ouvidoria como instrumento de participação, controle e avaliação de políticas públicas de saúde no brasil. *Physis: Revista de Saúde Coletiva*, 31(4), e310403. 15
- [Financial Reporting Council, 2024] Financial Reporting Council (2024). UK Corporate Governance Code 2024. Financial Reporting Council. 7, 59
- [Floridi, 2013] Floridi, L. (2013). *The Philosophy of Information*. Oxford University Press. 34
- [Forester, 1985] Forester, T., Ed. (1985). *The Information Technology Revolution*. MIT Press. 25
- [Forman & Peniwati, 1998] Forman, E. & Peniwati, K. (1998). Aggregating Individual Judgments and Priorities with the Analytic Hierarchy Process. *European Journal of Operational Research*, 108(1), 165–169. 70

- [Frey & Osborne, 2017a] Frey, C. B. & Osborne, M. A. (2017a). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, 114, 254–280. 25
- [Frey & Osborne, 2017b] Frey, C. B. & Osborne, M. A. (2017b). The Future of Employment: How Susceptible Are Jobs to Computerisation? *Technological Forecasting and Social Change*, 114, 254–280. 38
- [Fricke, 2019] Fricke, M. (2019). The knowledge pyramid: the DIKW hierarchy. *Knowledge Organization*, 46(1), 33–46. 34
- [Fácio, 2023] Fácio, R. (2023). A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre lei geral de proteção de dados e lei de acesso à informação no brasil. *Revista Eurolatinoamericana de Derecho Administrativo*, 10, e247. 15
- [Garousi et al., 2019] Garousi, V., Felderer, M., & Mantyla, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106, 101–121. 6, 51
- [Garousi & Mantyla, 2016] Garousi, V. & Mantyla, M. V. (2016). When and what to automate in software testing? A multivocal literature review. *Information and Software Technology*, 76, 92–117. 6
- [Garuti & Spencer, 2007] Garuti, C. & Spencer, I. (2007). Parallels between the analytic hierarchy and network processes (AHP/ANP) and fractal geometry. *Mathematical and Computer Modelling*, 46(7–8), 926–934. 38, 49
- [Gazni & Didegah, 2016] Gazni, A. & Didegah, F. (2016). The Relationship Between Authors’ Bibliographic Coupling and Citation Exchange: Analyzing Disciplinary Differences. *Scientometrics*, 107(2), 609–626. 20
- [Glänzel & Czerwon, 1996] Glänzel, W. & Czerwon, H.-J. (1996). A New Methodological Approach to Bibliographic Coupling and Its Application to the National, Regional and Institutional Level. *Scientometrics*, 37(2), 195–221. 20
- [Glette-Iversen et al., 2023a] Glette-Iversen, I., Flage, R., & Aven, T. (2023a). Extending and Improving Current Frameworks for Risk Management and Decision-Making: A New Approach for Incorporating Dynamic Aspects of Risk and Uncertainty. *Safety Science*, 168, 106317. 76
- [Glette-Iversen et al., 2023b] Glette-Iversen, I., Flage, R., & Aven, T. (2023b). Extending and Improving Current Frameworks for Risk Management and Decision-Making: A New Approach for Incorporating Dynamic Aspects of Risk and Uncertainty. *Safety Science*, 168, 106317. 76
- [Global Right to Information Rating, 2026] Global Right to Information Rating (2026). Methodology. 26

- [GONZÁLEZ-VALIENTE & LÓPEZ-MESA, 2022] GONZÁLEZ-VALIENTE, C. L. & LÓPEZ-MESA, E. K. (2022). Estrutura intelectual da biblioteconomia e ciência da informação na iberoamérica usando análise de co-citação de periódicos: um estudo comparativo baseado em scopus e web of science. *Transinformação*, 34, e210036. 9, 52
- [Guedes & Borschiver, 2007] Guedes, V. L. S. & Borschiver, S. (2007). Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento. In *Anais do VI CIFORM*: Universidade Federal da Bahia. 8, 10, 15
- [Harzing & Alakangas, 2016] Harzing, A. W. & Alakangas, S. (2016). Google Acadêmico, Scopus e Web of Science: uma comparação longitudinal e interdisciplinar. *Scientometrics*, 106, 787–804. 9, 12, 52
- [Hazell & Worthy, 2010] Hazell, R. & Worthy, B. (2010). Assessing the performance of freedom of information. *Government Information Quarterly*, 27(4), 352–359. 30
- [Head, 2009] Head, G. (2009). *Risk management: why and how*. International Risk Management Institute (IRMI). 36
- [Helbing, 2013] Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, 497, 51–59. 25
- [Hong et al., 2021] Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, 168(3), 539–564. 17, 20
- [Ingrams, 2018] Ingrams, A. (2018). Democratic Transition and Transparency Reform: An fsQCA Analysis of Access to Information Laws in Twenty-Three Countries. *Government Information Quarterly*, 35(3), 428–436. 28
- [Joint Task Force, 2020] Joint Task Force (2020). *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Rev. 5, National Institute of Standards and Technology. Includes updates as of 10 Dec. 2020. 60
- [Jones, 1997] Jones, Q. (1997). Comunidades virtuais, assentamentos virtuais e ciberarqueologia: um esboço teórico. *Journal of Computer-Mediated Communication*, 3(3), JCMC331. 25
- [Jussen-Lengersdorf et al., 2023] Jussen-Lengersdorf, I. et al. (2023). Data sharing fundamentals: definition and characteristics. In *Proceedings of the 56th Hawaii International Conference on System Sciences*. 32
- [Kempeneer et al., 2023] Kempeneer, S., Pirannejad, A., & Wolswinkel, J. (2023). Open Government Data from a Legal Perspective: An AI-Driven Systematic Literature Review. *Government Information Quarterly*, 40(3), 101823. 24
- [Kessler, 1963] Kessler, M. M. (1963). Bibliographic coupling between scientific papers. *American Documentation*, 14(1), 10–25. 20

- [Kimble, 1994] Kimble, J. (1994). Answering the Critics of Plain Language. *The Scribes Journal of Legal Writing*, 5, 51–85. Published in volume 5, 1994–1995. DOI não localizado. 55
- [Klock et al., 2016] Klock, A. C. T., Gasparini, I., & Pimenta, M. S. (2016). 5W2H Framework: A Guide to Design, Develop and Evaluate the User-Centered Gamification. In *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems, IHC '16*: Association for Computing Machinery. 79
- [Koh & Kim, 2004] Koh, J. & Kim, Y.-G. (2004). Knowledge sharing in virtual communities: An e-business perspective. *Expert Systems with Applications*, 26(2), 155–166. 25
- [Kongl. Maj:t, 1766] Kongl. Maj:t (1766). Kongl. Maj:ts Nådige Förordning, Angående Skrif- och Tryck-friheten. Swedish Freedom of the Press Act of 1766. Source text reproduced in *The History of Copyright: A Critical Overview With Source Texts in Five Languages*, by Karl-Erik Tallmo. 26
- [Konzen et al., 2012] Konzen, M. P., Fontoura, L. M., & Nunes, R. C. (2012). Gestão de riscos de segurança da informação baseada na norma ISO/IEC 27005 usando padrões de segurança. In *Anais do IX Simpósio de Excelência em Gestão e Tecnologia (IX SEGeT)* Resende. 35
- [Koo et al., 2020] Koo, J., Kang, G., & Kim, Y.-G. (2020). Segurança e privacidade no ciclo de vida do Big Data: Uma pesquisa e desafios em aberto. *Sustainability*, 12(24), 10571. 33
- [Krueger et al., 2012] Krueger, T., Page, T., Hubacek, K., Smith, L., & Hiscock, K. (2012). The role of expert opinion in environmental modelling. *Environmental Modelling & Software*, 36, 4–18. 23
- [Kwilinski & Kardas, 2024] Kwilinski, A. & Kardas, M. (2024). O papel do princípio de Pareto na gestão da qualidade na Indústria 4.0: uma análise bibliométrica abrangente. *Virtual Economics*, 7(3), 7–24. 8, 10
- [Lakatos & Marconi, 2003] Lakatos, E. M. & Marconi, M. A. (2003). *Fundamentos de metodologia científica*. São Paulo: Atlas, 5 edition. 11, 55
- [Landström, 2024] Landström, K. (2024). Sobre o extrativismo epistêmico e a Ética do compartilhamento de dados. *Philosophy of the Social Sciences*, 54(5), 387–411. 2
- [Le Coadic, 1996] Le Coadic, Y.-F. (1996). *La science de l'information*. Presses Universitaires de France, 3 edition. 34
- [Lemieux et al., 2015] Lemieux, V., Trapnell, S., Worker, J., & Excell, C. (2015). Transparency and open government: Reporting on the disclosure of information. *JeDEM - eJournal of eDemocracy and Open Government*, 7, 75–93. 34
- [Lotka, 1926] Lotka, A. J. (1926). The Frequency Distribution of Scientific Productivity. *Journal of the Washington Academy of Sciences*, 16(12), 317–323. DOI not located. 14

- [Mahmoud et al., 2015] Mahmoud, S. H., Alazba, A. A., Adamowski, J., et al. (2015). Métodos de SIG para coleta e armazenamento sustentáveis de águas pluviais utilizando sensoramento remoto para dados de cobertura do solo. *Environmental Monitoring and Assessment*, 187, 598. 48
- [Mansell & Wehn, 1998] Mansell, R. & Wehn, U., Eds. (1998). *Knowledge societies: Information technology for sustainable development*. Oxford University Press. 25
- [Mariano et al., 2012] Mariano, A. M., Blanco Granado, R., Mariano Filho, A., & Garrido-Grande Caballero, M. (2012). Contribución de los Enfoques Teóricos en la Creación de un Modelo de Desempeño de las Alianzas Estratégica Internacionales. In *Congresso Internacional de Administração – Gestão Estratégica: Empreendedorismo e Sustentabilidade*. Conference paper. DOI not located. 23
- [Mariano et al., 2011] Mariano, A. M., García Cruz, R., & Arenas Gaitán, J. (2011). Alianzas Estratégicas Internacionales: Contribuciones de las Líneas de Investigación en la Formación de un Modelo Integrador. *Revista ADMpg Gestão Estratégica*, 4(1), 55–61. DOI not located. 23
- [Mariano & Rocha, 2017] Mariano, A. M. & Rocha, M. S. (2017). Revisão da literatura: apresentação de uma abordagem integradora. In *Proceedings of the 18th AEDEM International Conference* (pp. 427–442). x, 8, 9, 10, 11, 16, 51, 52, 55
- [Marins et al., 2009] Marins, C. S., Souza, D. O., & Barros, M. S. (2009). O uso do método de análise hierárquica (AHP) na tomada de decisões gerenciais – um estudo de caso. In *Anais do XLI Simpósio Brasileiro de Pesquisa Operacional (SBPO)* (pp. 1778–1788). Porto Seguro, BA. 45, 62
- [Marshakova, 1981] Marshakova, I. V. (1981). Citation networks in information science. *Scientometrics*, 3, 13–25. 18
- [Martín-Martín et al., 2018a] Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & Delgado López-Cózar, E. (2018a). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, 12(4), 1160–1177. 1, 24
- [Martín-Martín et al., 2018b] Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & Delgado López-Cózar, E. (2018b). Google scholar, web of science, and scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, 12(4), 1160–1177. 9, 52
- [Maslow, 1943] Maslow, A. H. (1943). Uma teoria da motivação humana. *Psychological Review*, 50(4), 370–396. 38
- [Matey et al., 2025] Matey, S. V., Raut, D. N., Pansare, R. B., & Kant, R. (2025). Uma estrutura híbrida para priorizar as métricas de desempenho para a adoção da tecnologia Blockchain nas indústrias de produção. *Journal of Modelling in Management*, 20(3), 701–731. 1

- [Matozo & Baptistella, 2024] Matozo, H. C. F. & Baptistella, R. (2024). O direito de acesso à informação pública: uma análise histórica nacional e comparativa frente a outros Estados. *Revista Foco*, 17(8), 1–26. Article e5765. 28
- [McCloud et al., 2023] McCloud, R. F., Bekalu, M. A., Vaughan, T., Maranta, L., Peck, E., & Viswanath, K. (2023). Evidence for decision-making: The importance of systematic data collection as an essential component of responsive feedback. *Global Health, Science and Practice*, 11(Suppl 2). 34
- [Meyer & Booker, 2001] Meyer, M. A. & Booker, J. M. (2001). *Eliciting and Analyzing Expert Judgment: A Practical Guide*. Number 7 in ASA-SIAM Series on Statistics and Applied Probability. Society for Industrial and Applied Mathematics. 62
- [Michener et al., 2018a] Michener, G., Contreras, E., & Niskier, I. (2018a). From Opacity to Transparency? Evaluating Access to Information in Brazil Five Years Later. *Revista de Administração Pública*, 52(4), 610–629. 72
- [Michener et al., 2018b] Michener, G., Contreras, E., & Niskier, I. (2018b). From Opacity to Transparency? Evaluating Access to Information in Brazil Five Years Later. *Revista de Administração Pública*, 52(4), 610–629. 72
- [Ministério da Gestão e da Inovação em Serviços Públicos, 2025] Ministério da Gestão e da Inovação em Serviços Públicos (2025). GOV.BR: número de contas ouro supera o de bronze pela primeira vez. GOV.BR. 35
- [Monteiro & Sant’Ana, 2023] Monteiro, E. C. d. S. d. A. & Sant’Ana, R. C. G. (2023). Desafios no compartilhamento de dados: anomia relacionada aos direitos autorais. *Perspectivas em Ciência da Informação*, 28, e41032. 20
- [Morgan & Henrion, 1990] Morgan, M. G. & Henrion, M. (1990). *Uncertainty: A guide to dealing with uncertainty in quantitative risk and policy analysis*. Cambridge: Cambridge University Press, 6 edition. 36
- [Mortenson et al., 2015] Mortenson, M. J., Doherty, N. F., & Robinson, S. (2015). Operational research from Taylorism to Terabytes: A research agenda for the analytics age. *European Journal of Operational Research*, 241(3), 583–595. 33
- [Mota & Araújo Júnior, 2021] Mota, V. d. A. & Araújo Júnior, R. H. d. (2021). Limitações do acesso à informação sobre contratação pública em saúde no Brasil à luz da Lei de Acesso à Informação: uma revisão integrativa da literatura. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, 19(00), e021011. 15
- [Murphy, 2000] Murphy, C. K. (2000). Combining Belief Functions When Evidence Conflicts. *Decision Support Systems*, 29(1), 1–9. 63
- [Nasu et al., 2022] Nasu, V., Borges, Y., & Silva, B. (2022). Perfil dos solicitantes dos pedidos de acesso à informação: análise com os dados da plataforma Fala.BR de 2012 a 2021. *Revista da CGU*, 14, 33–49. 30

- [National Institute of Standards and Technology, 2026] National Institute of Standards and Technology (2026). Cybersecurity Framework. Página oficial do NIST Cybersecurity Framework, incluindo o CSF 2.0 Resource Center. 7, 60
- [Nelson et al., 2025] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3)*. Technical report, National Institute of Standards and Technology. 7, 60
- [Nisonger, 2008] Nisonger, T. (2008). The “80/20 rule” and core journals. *The Serials Librarian*, 55, 62–84. 8, 10
- [Oliveira et al., 2021a] Oliveira, R., Cappelli, C., & Oliveira, J. (2021a). Diretrizes para o Design de Visualização da Informação: Estendendo a Linguagem Cidadã. In *Anais do IX Workshop de Computação Aplicada em Governo Eletrônico* (pp. 259–266). Porto Alegre: Sociedade Brasileira de Computação. 55
- [Oliveira et al., 2021b] Oliveira, R., Cappelli, C., & Oliveira, J. (2021b). Diretrizes para o design de visualização da informação: Estendendo a linguagem cidadã. In *Anais do IX Workshop de Computação Aplicada em Governo Eletrônico* (pp. 259–266). Porto Alegre: SBC. 55
- [Olsson, 2002] Olsson, R. (2002). Risk and risk-generating events. In *Risk and Governance* (pp. 3–24). Palgrave/Springer. 36
- [Ossadnik et al., 2016] Ossadnik, W., Schinke, S., & Kaspar, R. H. (2016). Group Aggregation Techniques for Analytic Hierarchy Process and Analytic Network Process: A Comparative Analysis. *Group Decision and Negotiation*, 25, 421–457. 57, 70
- [Pareja-Daza et al., 2024] Pareja-Daza, C., Orlandini-Gonzalez, I., & Mariano, A. M. (2024). Modelos de negócio y emprendimiento digital: Un análisis bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (pp. 423–435). 23
- [Parviainen et al., 2021] Parviainen, T., Goerlandt, F., Helle, I., Haapasaari, P., & Kuikka, S. (2021). Implementing Bayesian Networks for ISO 31000:2018-Based Maritime Oil Spill Risk Management: State-of-Art, Implementation Benefits and Challenges, and Future Research Directions. *Journal of Environmental Management*, 278, 111520. 76
- [Passas, 2024] Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia*, 4, 1014–1025. 8
- [Paulino & Dutra, 2024] Paulino, F. O. & Dutra, L. P. (2024). Direitos epistêmicos e direito à informação no Brasil e no México. In M. Aslama Horowitz & others (Eds.), *Direitos epistêmicos na era da disrupção digital*. Cham: Palgrave Macmillan. 14, 23
- [Pinto Filho et al., 2021] Pinto Filho, J., Finger, A. B., & Pinto, I. M. B. S. (2021). Acesso à Informação: traçando um panorama da Lei 12.527/2011 a partir de uma revisão sistemática de literatura. *Revista Gestão e Desenvolvimento*, 18(3), 131–156. 24

- [Piovesan & Temporini, 1995] Piovesan, A. & Temporini, R. (1995). Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública. *Revista de Saúde Pública*, 29. 51
- [Plassmann et al., 2005] Plassmann, H., Kenning, P., Deppe, M., Kugel, H., & Schwindt, W. (2005). *Neural correlates of the affect heuristic during brand choice*. Technical Report Working Paper Experimental 0509004, University Library of Munich. 2, 38, 49
- [Prodanov & Freitas, 2013] Prodanov, C. C. & Freitas, E. C. d. (2013). *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico*. Feevale. 51
- [Project Management Institute, 2004] Project Management Institute (2004). *A guide to the Project Management Body of Knowledge (PMBOK Guide)*. Newtown Square, PA: Project Management Institute, 3 edition. ISBN 1-930699-45-X. 36
- [Prosser, 1960] Prosser, W. L. (1960). Privacy. *California Law Review*, 48(3), 383–423. 2, 34
- [Rana et al., 2020] Rana, N. P., Luthra, S., & Rao, H. R. (2020). Key Challenges to Digital Financial Services in Emerging Economies: The Indian Context. *Information Technology & People*, 33(1), 198–229. 17, 20
- [Ransbotham & Kiron, 2017] Ransbotham, S. & Kiron, D. (2017). Analytics as a source of business innovation. *MIT Sloan Management Review*, 58(3). 35
- [Reason, 2000a] Reason, J. (2000a). Human error: models and management. *BMJ*, 320(7237), 768–770. 69, 74
- [Reason, 2000b] Reason, J. (2000b). Human Error: Models and Management. *BMJ*, 320(7237), 768–770. 69, 74
- [Relly, 2012] Relly, J. (2012). Freedom of information laws and global diffusion testing rogers’s model. *Journalism Mass Communication Quarterly*, 89, 431–457. 27
- [Renn et al., 2022] Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R. W., & Schweizer, P.-J. (2022). Systemic Risks from Different Perspectives. *Risk Analysis*, 42(9), 1902–1920. 37
- [Ribeiro et al., 2022] Ribeiro, C., Albuquerque, R., & Nunes, R. (2022). Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do sistema brasileiro de inteligência. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, E49, 169–183. 14
- [Rodrigues et al., 2022] Rodrigues, D. G. A., Anjos, R. L., & Dias, G. A. (2022). Tipologia dos dados científicos das teses brasileiras da Ciência da Informação: Investigando a sua natureza e origem. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*, 27(1), 1–25. 34
- [Rodrigues et al., 2021] Rodrigues, G. M., Geraldles, E., & Kaya, G. T. (2021). Impactos da pandemia da Covid-19 nas Leis de Acesso à Informação no Brasil e no mundo. *Revista Ibero-Americana de Ciência da Informação*, 14(2), 420–439. 14

- [Rodrigues et al., 2024] Rodrigues, N. S., Mariano, A. M., & Ralha, C. G. (2024). Revisão bibliográfica com desambiguação do nome do autor e abordagem meta-analítica consolidada. *International Journal on Digital Libraries*, 25, 765–785. 8, 10
- [Rodrigues & Abadal, 2014] Rodrigues, R. & Abadal, E. (2014). Ibero-american journals in scopus and web of science. *Learned Publishing*, 27, 56–62. 13
- [Rosa et al., 2003] Rosa, E. A., Renn, O., & McCright, A. M. (2003). The risk society revisited: social theory and risk governance. In *The handbook of risk and governance*. Sage. 36
- [Ross, 2006] Ross, V. E. (2006). A model of inventive ideation. *Thinking Skills and Creativity*, 1(2), 120–129. 38
- [Russo et al., 2006] Russo, G. M., Van Aduard de Macedo-Soares, T. D. L., & Villas, M. V. (2006). Importância da hierarquização das revistas científicas: resultados de uma investigação empírica no Brasil e proposta de um método de pesquisa bibliográfica. 51
- [Saaty, 1977] Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology*, 15(3), 234–281. x, 38, 39, 44, 49, 55, 56, 67
- [Saaty, 1986] Saaty, T. L. (1986). A note on the AHP and expected value theory. *European Journal of Operational Research*. 38, 44
- [Saaty, 1990] Saaty, T. L. (1990). How to make a decision: The Analytic Hierarchy Process. *European Journal of Operational Research*, 48(1), 9–26. 38, 39, 44, 45, 46, 66, 71
- [Saaty, 1995] Saaty, T. L. (1995). Transport Planning with Multiple Criteria: The Analytic Hierarchy Process Applications and Progress Review. *Journal of Advanced Transportation*, 29(1), 81–126. 44, 69
- [Saaty, 2008] Saaty, T. L. (2008). Medição relativa e sua generalização na tomada de decisão: porque comparações pareadas são centrais na matemática para a medição de fatores intangíveis. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 102, 251–318. x, 44, 46, 47, 49, 67, 69, 70
- [Saaty, 2009] Saaty, T. L. (2009). Structures in decision making: on the subjective geometry of hierarchies and networks. *European Journal of Operational Research*, 199(3), 867–872. 38, 44, 46
- [Saaty & Shih, 2009] Saaty, T. L. & Shih, H.-S. (2009). Structures in Decision Making: On the Subjective Geometry of Hierarchies and Networks. *European Journal of Operational Research*, 199(3), 867–872. 44, 47, 48, 51
- [Saaty & Vargas, 1980] Saaty, T. L. & Vargas, L. G. (1980). Hierarchical analysis of behavior in competition: prediction in chess. *Behavioral Science*, 25(3), 180–191. 38, 44, 45, 66, 71
- [Saaty & Vargas, 1984] Saaty, T. L. & Vargas, L. G. (1984). Inconsistency and Rank Preservation. *Journal of Mathematical Psychology*, 28(2), 205–214. 44, 48

- [Saaty & Vargas, 2012] Saaty, T. L. & Vargas, L. G. (2012). *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. New York: Springer, 2 edition. 62, 86
- [Santos et al., 2017a] Santos, J. L. G., Erdmann, A. L., Meirelles, B. H. S., Lanzoni, G. M. M. L., Cunha, V. P., & Ross, R. (2017a). Integração entre dados quantitativos e qualitativos em uma pesquisa de métodos mistos. *Texto & Contexto-Enfermagem*, 26(3), e1590016. 23
- [Santos et al., 2017b] Santos, J. L. G. d., Erdmann, A. L., Meirelles, B. H. S., Lanzoni, G. M. d. M., Cunha, V. P. d., & Ross, R. (2017b). Integração entre dados quantitativos e qualitativos em uma pesquisa de métodos mistos. *Texto & Contexto - Enfermagem*, 26(3), e1590016. 23
- [Santos & Cruz, 2013] Santos, L. F. & Cruz, R. B. C. (2013). O uso do método AHP na tomada de decisão para seleção de sistemas de lajes de edifícios comerciais. *Engenharia Estudo e Pesquisa*, 13(1), 39–52. x, 45, 46, 47
- [Santos Neto et al., 2016] Santos Neto, A. F. d., Moreira, Á. R. d. C., Pinheiro, B. E., Gomes, J. d. S., Otal, L. d. O., & Fragoso, M. N. (2016). Quadro 5W2H: uma ferramenta para definição do problema de projeto e de suas variáveis. *Humanas Sociais & Aplicadas*, 6(16), 23–30. 59, 79
- [Saulino et al., 2017] Saulino, M. F., Patel, T., & Fisher, S. P. (2017). The application of failure modes and effects analysis methodology to intrathecal drug delivery for pain management. *Neuromodulation: journal of the International Neuromodulation Society*, 20(2), 177–186. 56
- [Scopus, 2025] Scopus (2025). Scopus: A Comprehensive Abstract and Citation Database for Impact Makers. x, 13, 14
- [Sellars, 1973] Sellars, W. (1973). Philosophy and the scientific image of man: Some reflections. *The Journal of Philosophy*, 70(18), 612–624. 34
- [Setzer, 2006] Setzer, V. W. (2006). Data, Information, Knowledge and Competence. Original: Apr. 2001; revised and enlarged version 3.1: Feb. 2006. 34
- [Shah et al., 2021] Shah, S. I. H., Peristeras, V., & Magnisalis, I. (2021). DaLiF: uma estrutura de ciclo de vida de dados para governos orientados por dados. *Journal of Big Data*, 8, 89. 33
- [Shintaku et al., 2015] Shintaku, M., Duque, C., & Suaiden, E. J. (2015). Análise da adesão às tendências da Ciência pelos repositórios institucionais brasileiros. *InCID: Revista de Ciência da Informação e Documentação*, 6(2), 148–169. 9
- [Shumskaya, 2019] Shumskaya, D. (2019). Linguagem clara: uma questão de cidadania corporativa para as instituições financeiras? Master's thesis, Escola Superior de Comunicação Social. 55

- [Sinha et al., 2015] Sinha, A., Shen, Z., Song, Y., Ma, H., Eide, D., Hsu, B., & Wang, K. (2015). An Overview of Microsoft Academic Service (MAS) and Applications. In *Proceedings of the 24th International Conference on World Wide Web, WWW '15 Companion* (pp. 243–246). New York, NY, USA: Association for Computing Machinery. 9
- [Solove, 2006] Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. 25, 26
- [Trautendorfer et al., 2025] Trautendorfer, J., Hohensinn, L., & Hilgers, D. (2025). Da transparência de jure à transparência de facto: analisando a lacuna de conformidade à luz das leis de liberdade de informação. *Regulation and Governance*, 1(1), 253–283. 1, 23, 72
- [Trbojevic, 2005] Trbojevic, V. M. (2005). Risk criteria in eu. *Archives of Transport*, 17(3–4), 209–220. Presented at the European Safety and Reliability Conference, ESREL 2005, Gdynia–Sopot–Gdansk, Poland, 27–30 June 2005. DOI not located. 3
- [Tversky & Kahneman, 1981] Tversky, A. & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 211(4481), 453–458. 69
- [UK Government, 2025] UK Government (2025). First international AI safety report to inform discussions at AI Action Summit. GOV.UK. 7
- [United Nations, 2023] United Nations (2023). Governing AI for humanity: interim report of the High-Level Advisory Body on Artificial Intelligence. United Nations. 7
- [Urbizagástegui Alvarado, 2002] Urbizagástegui Alvarado, R. (2002). A Lei de Lotka na bibliometria brasileira. *Ciência da Informação*, 31(2), 14–20. 8
- [U.S. Department of Defense, 1980] U.S. Department of Defense (1980). Procedures for performing a failure mode, effects, and criticality analysis (MIL-STD-1629A). U.S. Department of Defense. 39
- [van Eck & Waltman, 2010] van Eck, N. J. & Waltman, L. (2010). Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping. *Scientometrics*, 84(2), 523–538. 16, 53
- [Van Eck & Waltman, 2010] Van Eck, N. J. & Waltman, L. (2010). VOSviewer: um programa de computador para mapeamento bibliométrico. *Scientometrics*, 84, 523–538. x, 15, 18, 51, 53
- [Vanderhoeven et al., 2017] Vanderhoeven, S. et al. (2017). Além dos protocolos: melhorando a confiabilidade da análise de risco baseada em especialistas que sustenta as políticas de espécies invasoras. *Biological Invasions*, 19, 2507–2517. 54
- [Von Neumann, 1928] Von Neumann, J. (1928). Zur Theorie der Gesellschaftsspiele. *Mathematische Annalen*, 100, 295–320. 49, 50, 57, 58, 73
- [Wang et al., 2020] Wang, K., Shen, Z., Huang, C., Wu, C.-H., Dong, Y., & Kanakia, A. (2020). Microsoft Academic Graph: When Experts Are Not Enough. *Quantitative Science Studies*, 1(1), 396–413. 9

- [Wang et al., 2019] Wang, K., Shen, Z., Huang, C., Wu, C.-H., Eide, D., Dong, Y., Qian, J., Kanakia, A., Chen, A., & Rogahn, R. (2019). A Review of Microsoft Academic Services for Science of Science Studies. *Frontiers in Big Data*, 2, 45. 9
- [Wang et al., 2021] Wang, K., Zhao, Y., Gangadhari, R. K., & Li, Z. (2021). Analyzing the Adoption Challenges of the Internet of Things (IoT) and Artificial Intelligence (AI) for Smart Cities in China. *Sustainability*, 13(19). 17, 20, 35
- [Wang et al., 2018] Wang, Y., Kung, L., & Byrd, T. A. (2018). Big Data Analytics: Understanding Its Capabilities and Potential Benefits for Healthcare Organizations. *Technological Forecasting and Social Change*, 126, 3–13. 35
- [Wang et al., 2009] Wang, Y. M., Chin, K. S., Poon, G. K. K., & Yang, J. B. (2009). Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean. *Expert Systems with Applications*, 36(2), 1195–1207. xii, 38, 39, 41, 42, 43
- [Wazlawick, 2009] Wazlawick, R. S. (2009). *Metodologia de pesquisa para ciência da computação*. Campus/Elsevier, 6 edition. 51
- [Werthein, 2000] Werthein, J. (2000). A sociedade da informação e seus desafios. *Ciência da informação*, 29, 71–77. 25, 26
- [Westrum, 1993] Westrum, R. (1993). Culturas com a imaginação requerida. In J. A. Wise, V. D. Hopkin, & P. Stager (Eds.), *Verificação e Validação de Sistemas Complexos: Questões de Fatores Humanos*, volume 110 of *Série NATO ASI*. Berlin, Heidelberg: Springer. 25
- [Wiegmann et al., 2022] Wiegmann, D. A., Wood, L. J., Cohen, T. N., & Shappell, S. A. (2022). Understanding the “Swiss Cheese Model” and Its application to patient safety. *Journal of Patient Safety*, 18(2), 119–123. 69, 74
- [Zahid et al., 2023] Zahid, R. et al. (2023). Ciclo de vida de gerenciamento seguro de dados para ecossistemas de big data governamentais: perspectiva de design e desenvolvimento. *Systems*, 11(8), 380. 33
- [Zhao & Strotmann, 2008] Zhao, D. & Strotmann, A. (2008). Evolution of Research Activities and Intellectual Influences in Information Science 1996–2005: Introducing Author Bibliographic-Coupling Analysis. *Journal of the American Society for Information Science and Technology*, 59(13), 2070–2086. 20
- [Zottmann et al., 2023] Zottmann, C. E. M., Nunes, R. R., Georg, M. A. C., Alves, R. S., & Silva, M. A. (2023). Proposta de metodologia para avaliação de riscos de privacidade para órgãos do Poder Judiciário no Brasil. In *Encontro de Administração da Justiça (EnAJUS)* Brasília. 35
- [Zuboff, 2023] Zuboff, S. (2023). The age of surveillance capitalism (cap. 27). In *Social Theory Re-Wired*. Routledge. 25
- [Zupic & Čater, 2014] Zupic, I. & Čater, T. (2014). Métodos bibliométricos em gestão e organização. *Organizational Research Methods*, 18(3), 429–472. x, 17, 20, 21

Apêndice A

Modelo Integrador da Teoria do Enfoque Meta Analítico (TEMAC)

Tabela A.1: Modelo Integrador da Teoria do Enfoque Meta Analítico (TEMAC).

Autor(es)	País/ Ano	Título	Métodos	Objetivos	Principais Resultados	DOI
Mabillard et al.	Bélgica (2025)	Barreiras à Liberdade de Informação: Perspectivas de uma Experiência na Bélgica	<i>Field experiment</i> em 581 municípios belgas	Analisar barreiras na implementação da FOI	Muitos casos de não-conformidade; novo <i>framework</i> de análise.	doi.org/10.1080/01900692.2024.2378329
Esposito et al.	Bélgica (2024)	Rumo a uma estrutura de ciência cidadã para avaliação de políticas públicas sobre FOI na Bélgica	<i>Participatory citizen science</i>	Desenvolver <i>framework</i> de avaliação da FOI	Maiores municípios respondem melhor; método participativo efetivo.	doi.org/10.1177/13563890241270195
Trautendorfer et al.	Alemanha (2025)	Da transparência de jure à transparência de fato: lacuna de conformidade nas leis de liberdade de informação	Análise comparativa de leis e conformidade	Explorar diferença entre normas FOI e aplicação prática	Destaca dinâmica entre variações legais e cumprimento real.	doi.org/10.1111/rego.12615
Wasike, B.	EUA (2020)	FOI em transição: análise comparativa entre os governos Obama e Trump	Análise comparativa entre administrações	Avaliar desempenho do FOIA nos EUA	Legado institucional explica desempenho melhor que ações de política.	doi.org/10.1016/j.giq.2019.101443
Wagner, A. J.	EUA (2022)	Informações populares: análise do uso e comportamento da Lei de Liberdade de Informação	Estudo exploratório com amostra nacional	Compreender quem usa a FOI e como	Mapeia perfis de usuários e comportamento de uso da FOI .	doi.org/10.1016/j.giq.2022.101677
Spáč et al.	Eslováquia (2025)	Liberdade de informação e volume de dados solicitados: estudo experimental	Estudo de aplicação prática	Investigar aplicação da FOI em país pós-comunista da UE	Foco prático em volume e uso das leis de FOI .	doi.org/10.1016/j.giq.2025.102030
Žuffová, M.	Reino Unido (2021)	Explorando o papel das leis de liberdade de informação no jornalismo de fiscalização	Estudo qualitativo de interações mídia-Estado	Explorar limites do FOIA para monitoramento da mídia	Identifica obstáculos à atuação da mídia.	doi.org/10.1177/19401612211006702
Mueller, H. E.	(2019)	Avaliação das Leis de FOI : Objetivos, Abordagens e Considerações Práticas	Revisão conceitual e recomendações metodológicas	Orientar design de avaliações robustas de leis de FOI	Fornece <i>framework</i> para avaliação abrangente das leis.	doi.org/10.1080/01900692.2019.1575663
De Coninck, I.; Förste, L.	Holanda/Alemanha (2019)	Transparência no Governo Local: estudo de caso em Hamburgo e Antuérpia	Estudo comparativo de políticas de informação	Mostrar limites para o efeito de transparência	Examina meios para implementar políticas de transparência no governo local.	doi.org/10.26481/marble.2014.v4.200
Hawkins et al.	Reino Unido (2023)	A lei dos retornos decrescentes? O desafio de usar a FOI para pesquisas em políticas de saúde	Revisão crítica	Investigar se leis de FOI cumprem transparência e responsabilização	Discute desafios práticos e “retornos decrescentes” na implementação.	doi.org/10.1080/09581596.2023.2220134

Apêndice B

Formulário On-line para Hierarquização Utilizando a Análise de Modos e Efeitos de Falha (FMEA)

PESQUISA: HIERARQUIZAÇÃO DOS RISCOS DO COMPARTILHAMENTO DE DADOS PELA LAI.

Este questionário é parte componente da dissertação de mestrado da linha de pesquisa centrada em riscos do Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília (PPGCA/UnB), orientado pelo Prof. Dr. João Gabriel de Moraes Sousa. A pesquisa tem como tema "Ter de acesso à Informação (LAI): Uma análise multidimensional sobre os principais riscos do compartilhamento de dados". A seguir você encontrará quatro questionários, contendo até 10 (dez) descrições de riscos, a saber: (i) riscos operacionais; (ii) riscos de imagem/reputação do órgão; (iii) riscos legais e (iv) riscos financeiros/orçamentários. Estas categorias e conceitos derivam da Instrução Normativa Conjunta da Controladoria Geral da União e o Ministério do Planejamento, Orçamento e Gestão (INC MP/CGU nº 1/2016).

Considerando a rotina de atendimento de pedidos de acesso à informação motivados pela LAI, ordene os riscos, considerando a probabilidade da sua ocorrência durante o processo de atendimento a pedido de acesso à informação, motivado pela Lei de Acesso à Informação (LAI). O risco que ficar na primeira linha deve ser o que tiver a maior probabilidade de ocorrer e na última linha o que tiver a menor probabilidade de ocorrer durante o processo.

As perguntas marcadas com asterisco (*) são obrigatórias; a sua participação é voluntária; o questionário deve ser hierarquizado conforme o seu entendimento e percepção individual; todas as respostas coletadas serão tratadas como confidenciais; nenhuma anexo a finalidades acadêmicas e o tratamento dos dados pessoais será realizado conforme inciso IV, do art. 7º da Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados (LGPD). O tempo médio de dedicação para o preenchimento total do questionário é de aproximadamente 10 minutos, caso seja necessário, entre em contato pelo e-mail - jmedulati@gmail.com.

Desde já eu agradeço a sua contribuição para a minha pesquisa e desenvolvimento da ciência. Mostrando Jorge Rocha.

1. Esta lista apresenta os riscos Operacionais - Eles são eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. **Fonte:** Alínea 'a', art. 18, da INC MP/CGU nº 1/2016.

Ordene os riscos, considerando a probabilidade da sua ocorrência durante o processo de atendimento a pedido de acesso à informação, motivado pela Lei de Acesso à Informação (LAI). O primeiro deve ter maior chance de ocorrência que os outros seguintes, o último tem menor probabilidade de ocorrer. *

Links inseguros: Risco de invasão cibernética por clicar (selecionar) links ou sites, enviados por usuários no corpo dos seus pedidos de acesso à informação. Links ou sites não verificados pelo órgão podem ser a porta para uma invasão da rede corporativa, motivado pelo roubo e uso indevido de credenciais e sequestro institucional.
Uso de inteligência artificial (IA): Risco de compartilhamento de dados restritos (pessoais, pessoais sensíveis) com plataformas de IA, como o GPT, para sintetizar, revisar ou criar respostas para atender pedidos de acesso à informação.
Limitação de recursos tecnológicos: Risco de geração de recursos por envio incompleto de informações para solicitante, por não ter ferramentas para anexar arquivos que ultrapassem 30MB ou quantidade maior que 10 arquivos por manifestação.
Exposição indevida: Risco de envio de resposta para usuário errado causando vazamento de dados. O problema pode ser causado pela não observação dos dados do solicitante enquanto responde vários pedidos na plataforma.
Transparência excessiva: Compartilhamento de dados e informações restritos por tomar decisão escolhendo de forma binária (sim ou não o acesso ao solicitante), sem considerar outros fatores como riscos, legislações, categorização dos dados, estratégia institucional, dentre outros.
Deverio de finalidade: Risco de classificar e atender de usuário ou de órgãos com demanda que originalmente não seja pedido de acesso à informação, como se fosse um pedido fundamentado na LAI.
Contradição de resposta: Risco de responder de forma divergente e contraditória as demandas diferentes do mesmo usuário ou demanda semelhante de usuários distintos por não ter recursos de controle e análise de demandas.

2. Esta lista apresenta os riscos de imagem/reputação do órgão - Eles são eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional. **Fonte:** Alínea 'b', art. 18, da INC MP/CGU nº 1/2016.

Ordene os riscos, considerando a probabilidade da sua ocorrência durante o processo de atendimento a pedido de acesso à informação, motivado pela Lei de Acesso à Informação (LAI). O primeiro deve ter maior chance de ocorrência que os outros seguintes, o último tem menor probabilidade de ocorrer. *

Software infectado: Risco de Software malicioso (vírus) enviado por fornecedores nas ferramentas utilizadas no órgão que acaba sendo distribuído para usuários da LAI que fazem pedidos ao órgão.
Vazamento de dados por falha técnica: Falhas em sistemas de TI ou configurações convencionais que resultam no envio equivocado (vazamento) de informações para terceiros.
Pressão social: Riscos de pedidos reiterados de temática restrita, causando pressão nas redes ou mídia sociais podem forçar o órgão a liberar inadvertidamente dados sigilosos ou sensíveis.
Falta de rastreabilidade: Ausência de fatores de identificação e verificação de registros de acesso a algum documento ou arquivo enviado para um solicitante.
Virtualização dos dados: É o processo de extrair dados de várias fontes e tipos, preparando-os para apresentá-los em um formato unificado, e digital, pronto para consumo da sociedade.
Baixa qualidade de serviço: Envio de arquivos errados, desatualizados, incompletos ou fora de prazo para solicitantes.
Solicitação excessiva: Solicitação excessiva e sem justificativa de complementos forçando a identificação do solicitante anônimo.

3. Esta lista apresenta os riscos Legais - Eles são eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade. **Fonte:** Alínea 'c', art. 18, da INC MP/CGU nº 1/2016.

Ordene os riscos, considerando a probabilidade da sua ocorrência durante o processo de atendimento a pedido de acesso à informação, motivado pela Lei de Acesso à Informação (LAI). O primeiro deve ter maior chance de ocorrência que os outros seguintes, o último tem menor probabilidade de ocorrer. *

Segurança da informação: Riscos de descumprimento ou inexistência de procedimentos para assegurar disponibilidade, integridade, confidencialidade e autenticidade dos dados produzidos ou controlados pelo órgão e compartilhados com usuário da LAI.
Negligência institucional: Risco de inconformidade por não aplicar as ações técnicas e administrativas vigentes (criptografia, treinamento institucional, normatização, gestão de vulnerabilidades e atualização de software/firmware), resultando em riscos elevados de interceptação de dados e informações de usuários do serviço público.
Exposição irregular: Risco de compartilhamento e publicação indevida de dados e informações que deveriam ser restritas, causando riscos à segurança institucional e riscos associados à proteção inadequada de direitos autorais.
Tratamento excessivo: Risco compartilhamento de dados e informações ultrapassando o mínimo necessário e justificado, aumentando os riscos de exposição e acesso por terceiros não autorizados.
Extratratamento apátrides: Risco de extração e tratamento excessivos de dados, ferindo barreiras éticas, emitindo opiniões pessoais na composição de respostas à demanda de usuários da LAI.
Cadeia de sigilo: Riscos de publicação e coleta de dados pessoais de usuários do serviço público por ausência de procedimentos robustos para gerenciar riscos associados a fornecedores e parceiros do órgão, possibilidade de acesso indevido a sistemas ou informações sensíveis.
Violação de direitos: Risco de compartilhamento de dados pessoais sem o devido consentimento ou sem seguir os princípios de finalidade, necessidade e proporcionalidade.

4. Esta lista apresenta os riscos Financeiros / Orçamentários - Eles são eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações. **Fonte:** Alínea 'd', art. 18, da INC MP/CGU nº 1/2016.

Ordene os riscos, considerando a probabilidade da sua ocorrência durante o processo de atendimento a pedido de acesso à informação, motivado pela Lei de Acesso à Informação (LAI). O primeiro deve ter maior chance de ocorrência que os outros seguintes, o último tem menor probabilidade de ocorrer. *

Investimento emergencial: Risco de investimentos em caráter de emergência para atender demandas de usuários. Quando sistemas legados não suportam a separação ou anonimização de dados pessoais, há necessidade urgente de investimento em pessoal, licenças específicas, digitalização de arquivos físicos de documentos, manutenção e análises de backups e a aplicação de criptografia, o que pode acabar comprometendo prioridades orçamentárias.
Despesa judicial: Risco de judicialização em decorrência de negativas legítimas de acesso à informação. Pedidos desanexados, desproporcional ou potencialmente abusivos com risco de potencial dano a terceiros e aparente má-fé do solicitante.
Fraude financeira: Risco de ataque cibernético por Phishing e fraude financeira para os servidores e parceiros do órgão, causada por acesso a conteúdo digital com engenharia social (com o envio de links maliciosos e infectados com vírus) no teor do pedido de acesso à informação, dando acesso indevido da rede institucional a terceiros não credenciados e mal intencionados.
Violação de direitos autorais: Risco gerado pelo uso de obra, imagem, conteúdo em geral e/ou software protegido sem a devida credencial ou licença adequada, no processo de geração de resposta para usuário da LAI.
Custo da Transparência: Riscos de solicitações recorrentes, com alto nível de complexidade ou que demandem análise de grandes volumes de arquivos, podem exigir horas extras de servidores, aquisição de software específico ou contratação de consultorias externas para triagem, anonimização e formatação dos dados, elevando substancialmente os custos orçamentários do órgão.
Fraude e descumprimento: Riscos de Subtração, destruição ou ocultação de informações com procedimento com a alteração ou ocultação de documentos ou dados públicos de forma indevida para favorecer ou prejudicar usuário da LAI.
Dano ao erário: Riscos de cálculo com estimativa inadequada (além ou aquém) dos valores financeiros relativos à despesa institucional com fornecimento de cópia de documento impresso para atender demanda de usuário, conforme previsto da LAI.

5. Faixa etária? *

- ☐ 18 a 20 anos
- ☐ 21 a 24 anos
- ☐ 25 a 29 anos
- ☐ 30 a 34 anos
- ☐ 35 a 39 anos
- ☐ 40 a 44 anos
- ☐ 45 a 49 anos
- ☐ 50 a 54 anos
- ☐ 55 a 59 anos
- ☐ 60 a 64 anos
- ☐ 65 a 69 anos
- ☐ 70 anos ou mais

6. Autoidentificação de identidade de gênero *

- ☐ Homem
- ☐ Mulher
- ☐ Pessoa não binária
- ☐ Prefiro me autodescrever (informar no próximo campo)

7. Campo para autodescrição de gênero (caso tenha marcado na anterior que prefere se autodescrever).

Insira sua resposta

8. Tempo de serviço público *

- ☐ ≤ 2 anos
- ☐ > 2 e 5 anos
- ☐ > 5 e 7 anos
- ☐ > 7 e 10 anos
- ☐ ≥ 10 anos

10. Faixa de renda familiar *

- ☐ Até 1 salário
- ☐ Entre 1 e 3 salários
- ☐ Entre 3 e 7 salários
- ☐ Entre 7 e 10 salários
- ☐ Acima de 10 salários

9. Estado civil *

- ☐ Solteiro(a)
- ☐ Casado(a)
- ☐ Viúvo(a)
- ☐ Divorciado(a)
- ☐ Outro
- ☐ Prefiro não informar

11. Deixe seu e-mail caso queira receber os resultados dessa pesquisa.

Insira sua resposta

Figura B.1: Formulário on-line para hierarquização utilizando a Análise de Modos e Efeitos de Falha (FMEA)

Apêndice C

**Lista de tipologia conforme INC
MP/CGU nº 1/2016 e riscos
priorizados por especialistas**

Tabela C.1: Lista de tipologia conforme **INC MP/CGU nº 1/2016** e riscos priorizados por especialistas.

Tipologia	Risco	Conceito básico (simplificado)
Operacional	Exposição Indevida de Dados	Enviar informação para o solicitante errado e vaziar dado (erro humano/processo/sistema).
	Limitação de Recursos Tecnológicos	Infra/sistemas insuficientes para atender, proteger e responder pedidos (capacidade, licenças, rede, <i>storage</i>).
	Contradição de Resposta	Responder diferente para pedidos iguais/parecidos por falta de padronização e base de conhecimento.
	Desvio de Finalidade	Usar dados do pedido LAI para outro propósito (fere o princípio da finalidade).
	Links Inseguros	Compartilhar URL fraca (sem HTTPS/externa/ <i>link rot</i>) e abrir porta para <i>phishing</i> /exposição.
	Uso de IA	Usar IA em triagem/anonimização sem explicabilidade/controle, gerando viés ou reidentificação.
	Transparência Excessiva	Decisão binária sem ponderar exceções, LGPD , classificação e risco.
Imagem / Reputação	Virtualização dos Dados	Camada que junta bases e pode “mascarar” controles de acesso, expondo dado sem querer.
	Solicitação Excessiva	Pico de pedidos satura o time/sistema e gera atraso, erro e indisponibilidade (DoS administrativo).
	Vazamento por Falha Técnica	Vulnerabilidade/configuração/bug/ <i>hardware/software</i> expõe dados (acidente ou ataque).
	Falta de Rastreabilidade	Sem trilha de auditoria: não prova quem acessou/alterou/divulgou; perde governança.
	Pressão Social	Mídia/rede social força decisão ruim e pode levar à liberação indevida de dado sigiloso/sensível.
	<i>Software</i> Infectado	<i>Malware</i> em <i>apps</i> /macros exfiltra dados ou corrompe respostas (cadeia de contaminação).
	Baixa Qualidade do Serviço	Resposta errada/desatualizada/incompleta/fora do prazo; derruba credibilidade e efetividade da LAI .
Legal	Violação de Direitos Fundamentais	Tratar/compartilhar dado pessoal sem base e sem princípios (finalidade, necessidade, proporcionalidade).
	Segurança da Informação	Falha/ausência de políticas e controles (CIA+A): aumenta chance de perda, indisponibilidade e vazamento.
	Exposição Irregular de Info Restrita	Divulgar informação legalmente restrita (segurança, sigilo, segredo, PI/direitos autorais).
	Tratamento Excessivo	Coletar/reter/divulgar mais do que o necessário (quebra minimização; “escopo inchado”).
	Negligência Institucional	Demora/desatenção percebida no atendimento; erosão de confiança e questionamento de transparência.
	Quebra de Sigilo	Divulgar dado sigiloso/pessoal a terceiro não autorizado (violação de confidencialidade).
	Extratativismo Epistêmico	Uso privado assimétrico de conhecimento público sem retorno social, gerando contestação de legitimidade.
Financeiro / Orçamentário	Violação de Direitos Autorais	Publicar material protegido sem autorização; risco de multa/-litígio.
	Investimento Emergencial	Gasto não planejado para cumprir LAI (infra, pessoal, <i>software</i> , digitalização, criptografia, etc.).
	Custo da Transparência	Pedidos complexos geram custo direto/indireto (horas, ferramentas, consultoria, retrabalho).
	Fraude Financeira	Info divulgada vira insumo para golpe (<i>phishing</i> , transferências indevidas) e gera passivo/indenização.
	Dano ao Erário	Multas, litígios e retrabalho por falhas LAI/LGPD oneram orçamento.
	Fraude e Descaminho	Dado público usado para contrabando/sonegação/desvio; afeta arrecadação e integridade fiscal.
	Despesas Judiciais	Judicialização (inclusive por pedidos abusivos) gera custas, advocacia e risco de condenação.

Apêndice D

Análise de Modos e Efeitos de Falha (FMEA) utilizando o Formulário on-line para hierarquização

Modo de Falha	 Causas de Falha	Efeitos de Falha	Ocorrência	Deteção	Gravidade	NPR	Ações para Reduzir a Ocorrência de Falhas
Transparência excessiva	Avaliação binária inadequada	Exposição de dados estratégicos	9	8	9	648	Treinar servidores para decisões baseadas em análise de risco
Exposição indevida	Erro humano ao responder múltiplos pedidos	Vazamento de dados sensíveis	7	8	9	504	Implementar conferência dupla nas respostas
Violação de direitos Fundamentais	Desrespeito a princípios da LGPD	Danos a titulares e sanções legais	9	5	10	450	Capacitar quanto à LGPD e reforçar consentimentos
Baixa qualidade de serviço	Desatenção, falta de revisão	Informações erradas ou incompletas	7	9	7	441	Aplicar checklist e revisão em duplo controle
Quebra de sigilo	Erro de classificação da informação	Comprometimento da segurança institucional	5	5	9	225	Reforçar classificações e procedimentos de restrição
Contradição de resposta	Falta de controle e análise de demandas	Desconfiança no serviço	5	6	7	210	Adotar ferramentas de controle e histórico de respostas
Vazamento de dados por falha técnica	Problemas em sistemas e configurações	Divulgação não autorizada de dados	5	5	8	200	Realizar auditorias periódicas em sistemas de TI
Despesas judiciais	Judicialização por negativas legítimas	Custos jurídicos e imagem negativa	5	5	7	175	Estabelecer estratégias de defesa preventiva
Segurança da informação	Falta de procedimentos adequados	Comprometimento de dados	3	5	9	135	Aprimorar controles de acesso e criptografia de dados
Software Infectado	Execução de aplicativos ou macros contaminados	Acesso e disponibilização não autorizada de informações sigilosas	7	2	9	126	Implementar plano de gerenciamento de crises de imagem
Custo da Transparência	Solicitações complexas e volumosas	Aumento de custos operacionais	2	5	8	80	Otimizar processos de atendimento para reduzir volume
Fraude e descaminho	Acesso à dados pessoais e financeiros	Uso de informações divulgadas para realizar golpes de <i>phishing</i> , transferências indevidas ou obtenção de vantagem econômica ilícita	5	1	7	35	Planejar investimentos com base em análise de risco

Figura D.1: Análise de Modos e Efeitos de Falha (FMEA) utilizando o Formulário on-line para hierarquização.

Apêndice E

Processo de Execução da Análise Hierárquica de Processos (AHP) de cada Respondente (Peso Local e Peso Global)

E.1 Respondente 01

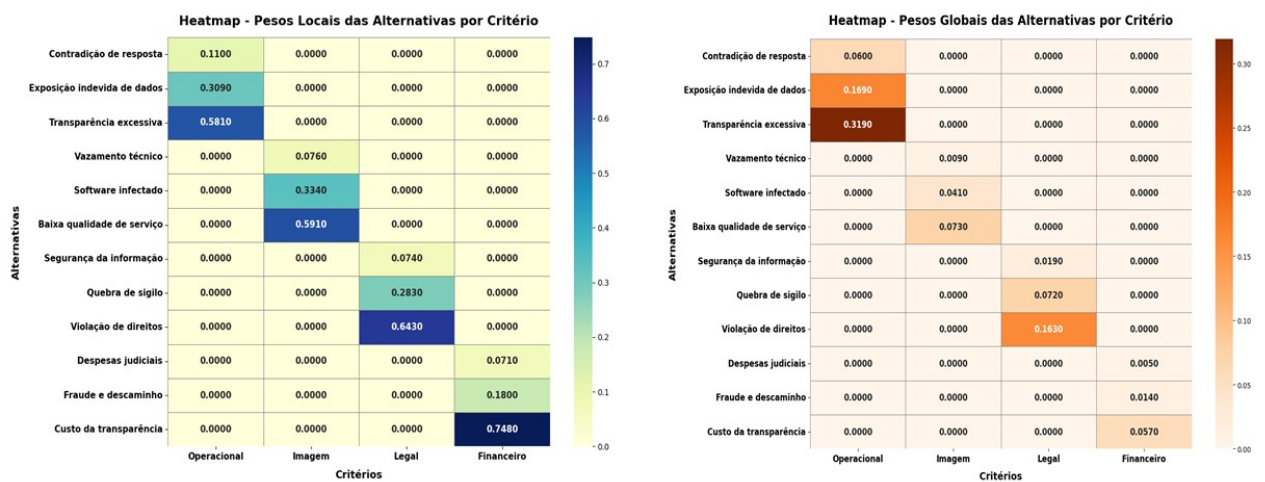


Figura E.1: Heatmap - pesos globais e locais das alternativas por critério para o respondente 01.

E.2 Respondente 02

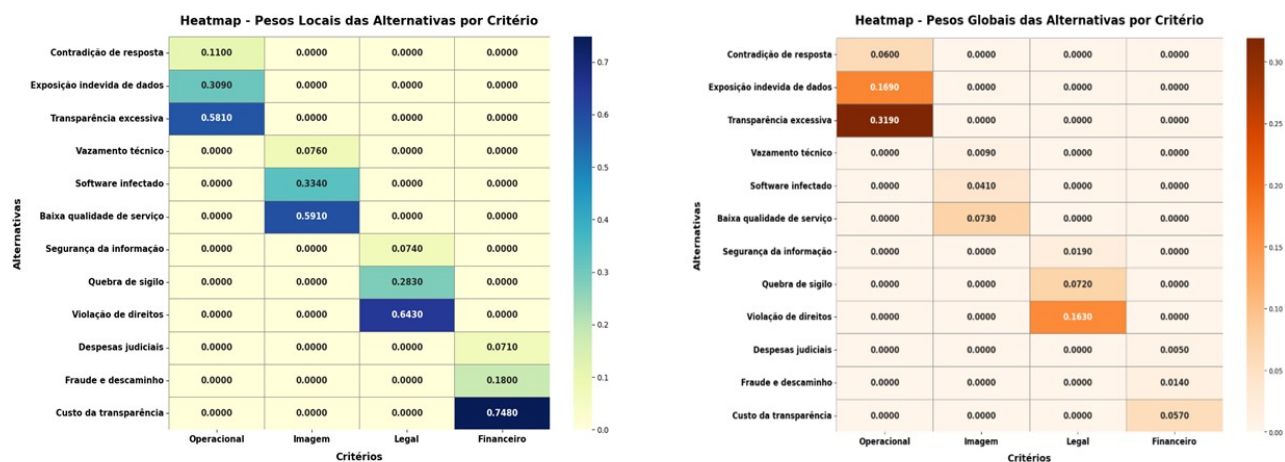


Figura E.2: Heatmap - pesos globais e locais das alternativas por critério para o respondente 02.

E.3 Respondente 03

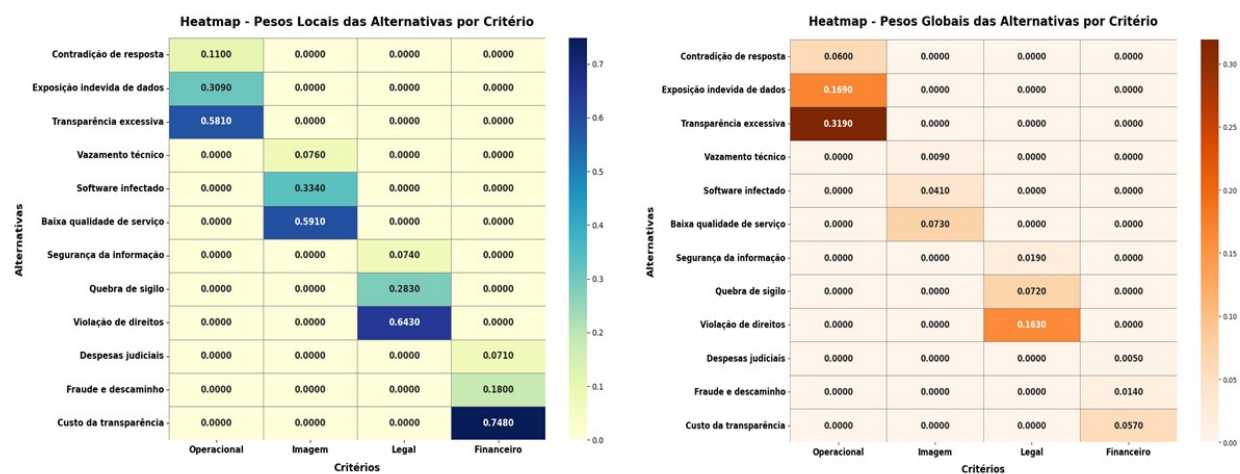


Figura E.3: Heatmap - pesos globais e locais das alternativas por critério para o respondente 03.

E.4 Respondente 04

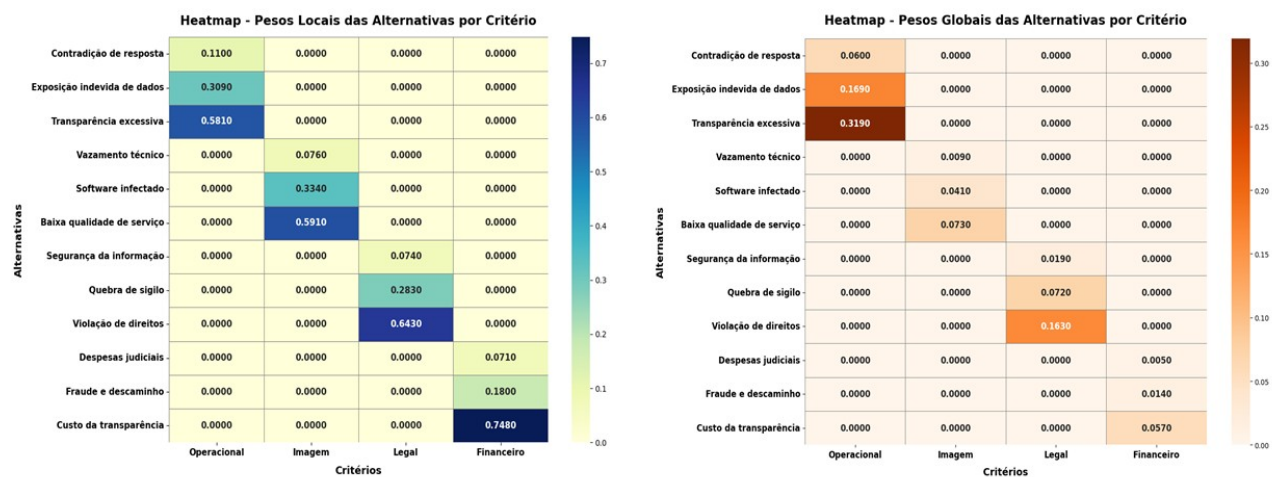


Figura E.4: Heatmap - pesos globais e locais das alternativas por critério para o respondente 04.

E.5 Respondente 05

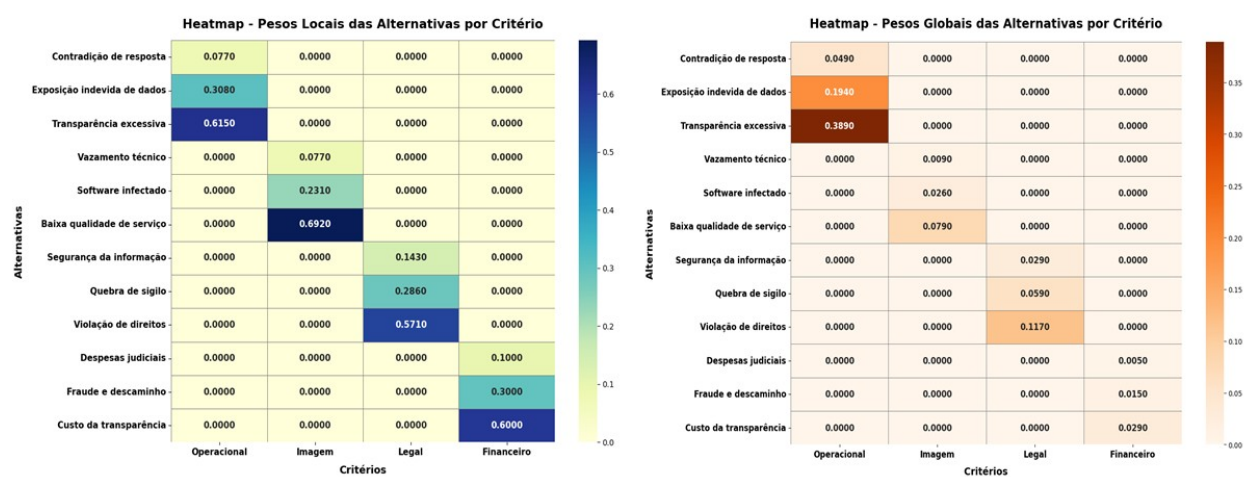


Figura E.5: Heatmap - pesos globais e locais das alternativas por critério para o respondente 05.