Systems Engineering and Computer Science Graduate Program

Alberto Luiz Coimbra Institute for Graduate Studies and Research in Engineering

FEDERAL UNIVERSITY OF RIO DE JANEIRO

TECHNICAL REPORT

TR-PESC/Coppe/UFRJ- 800/2026

Data Governance in the Federal Public Administration: Diagnosis, Gaps, and Guidelines for a Structured and Communicated Program

Evidence from TCU Ruling No. 457/2026, analysis of IGOVSISP 2025 results, and Strategic Recommendations

Authors:

Viviane Cunha Farias[a,b] e Jano Moreira de Souza[a]

[a] Programa de Engenharia de Sistemas e Computação, COPPE, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Brazil

[b]Fundação Getúlio Vargas - FGV

Corresponding Authors: vfarias@cos.ufrj.br, jano@cos.ufrj.br

Abstract

This technical report analyzes the current scenario of data governance and management in the Federal Public Administration (FPA), in light of the evidence presented by the Federal Court of Accounts (TCU) in Ruling No. 457/2026 and the results of the Information Technology Governance Index of the 234 FPA agencies that are part of the Information Technology Resources Administration System (SISP), the IGOVSISP of 2025, focusing on the assessment of maturity in “data and information” and on the essential actions to support public policies based on evidence and reliable data. (Technical Report in Portuguese)

Keywords: data governance; public policy, maturity assessment, AI strategy

Publication Date: 06/12/2026

Programa de Engenharia de Sistemas e Computação

Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

RELATÓRIO TÉCNICO

RT-PESC/Coppe/UFRJ- 800/2026

Governança de Dados na Administração Pública Federal: Diagnóstico, Lacunas e Diretrizes para um Programa Estruturado

Evidências do Acórdão nº 457/2026 do TCU, análise dos resultados do IGOVSISP 2025 e Recomendações Estratégicas

Autores:

Viviane Cunha Farias[a,b] e Jano Moreira de Souza[a]

[a] Programa de Engenharia de Sistemas e Computação, COPPE, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Brasil

[b]Fundação Getúlio Vargas - FGV

Autores Correspondentes: vfarias@cos.ufrj.br, jano@cos.ufrj.br

Resumo

Este relatório técnico analisa o cenário atual da governança e da gestão de dados na Administração Pública Federal (APF), à luz das evidências apresentadas pelo Tribunal de Contas da União (TCU) no Acórdão nº 457/2026 e dos resultados do Índice de Governança de Tecnologia da Informação dos 234 órgãos da APF integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), o IGOVSISP de 20252, com o foco na avaliação da maturidade em “dados e informações” e nas ações essenciais para sustentar políticas públicas baseadas em evidências e em dados confiáveis. (Relatório Técnico em Português)

Palavras-chave: governança de dados; políticas públicas; avaliação de maturidade. estratégia de IA

Data de Publicação: 12/06/2026

Governança de Dados na Administração Pública Federal: Diagnóstico, Lacunas e Diretrizes para um Programa Estruturado

Evidências do Acórdão nº 457/2026 do TCU, análise dos resultados do IGOVSISP 2025 e Recomendações Estratégicas

Introdução

Este relatório técnico analisa o cenário atual da governança e da gestão de dados na Administração Pública Federal (APF), à luz das evidências apresentadas pelo Tribunal de Contas da União (TCU) no Acórdão nº 457/2026[1] e dos resultados do Índice de Governança de Tecnologia da Informação dos 234 órgãos da APF integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), o IGOVSISP de 2025[2], com o foco na avaliação da maturidade em "dados e informações"[2] e nas ações essenciais para sustentar políticas públicas baseadas em evidências e em dados confiáveis.

*A motivação deste relatório surgiu a partir dos resultados da auditoria conduzida pelo TCU, que avaliou a maturidade em governança de dados em cinco organizações públicas do Poder Executivo Federal — nas quais se observou "**um padrão recorrente caracterizado pela necessidade de evolução dos mecanismos e políticas institucionais formais de governança de dados, devido ao baixo nível de maturidade organizacional na maioria dos órgãos auditados ... que compromete a execução das políticas públicas**" (p. 19)[1].*

Este cenário é confirmado atualmente, em escopo mais amplo, pelos resultados da avaliação do IGOVSISP 2025 do Ministério da Gestão e da Inovação em Serviços Públicos (MGI)[2], que identificou, dentre outros achados, uma relevante dissociação entre iniciativas de dados e os objetivos estratégicos institucionais nos 234 órgãos da APF avaliados.

O desafio que orienta este estudo pode ser sintetizado da seguinte forma: como estruturar um Programa de Governança de Dados nos órgãos da Administração Pública Federal que seja estrategicamente orientado, sistemicamente integrado e capaz de responder às demandas apontadas pelo TCU de forma imediata, sustentável e evolutiva?

---

[1] TCU Acórdão 457/2026 - Plenário https://portal.tcu.gov.br/uploads/noticias/pdf/2026/03/04/457-2026.pdf . Acesso em maio de 2026.

[2] Autodiagnóstico SISP 2025 - https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/arquivos/relatorio_autodiagnostico_sisp_2025.pdf

Sumário

1. Governança de Dados na Administração Pública Federal

A Agenda 2030 das Nações Unidas[3], materializada nos 17 Objetivos de Desenvolvimento Sustentável (ODS), estabelece um marco político e normativo para o enfrentamento de desafios complexos, como desigualdades sociais, mudanças climáticas, pobreza e fragilidades institucionais. O alcance desses objetivos depende, de forma crescente, da capacidade dos Estados de produzir, governar, compartilhar e utilizar dados de maneira ética, segura e estratégica, especialmente em um contexto de transformação digital acelerada e de adoção crescente de Inteligência Artificial (IA) no setor público [brasil.un.org], [undp.org].

Nesse cenário, a governança de dados consolida-se como elemento estruturante para a formulação e a implementação de políticas públicas baseadas em dados, bem como para o monitoramento e a geração de evidências. A IA, por sua vez, amplia a capacidade analítica e operacional do Estado, permitindo a antecipação de cenários, a personalização de serviços e maior eficiência na APF. Contudo, tecnologias inovadoras somente produzem impactos positivos quando sustentadas por infraestruturas públicas digitais robustas e por arranjos institucionais e regulatórios adequados [4]. A ausência de uma governança de dados integrada compromete tanto a transformação digital quanto o alcance de resultados alinhados à Agenda 2030.

Organismos internacionais, como a OCDE, reconhecem que a IA pode contribuir significativamente para diversos ODS, especialmente nas áreas de saúde, educação, mercado de trabalho e redução das desigualdades [5][6]. Ainda assim, a literatura destaca riscos relevantes associados ao uso de IA no setor público quando os sistemas são treinados com dados de baixa qualidade ou submetidos a arranjos de governança inadequados. Esses riscos reforçam a governança de dados como condição prévia para uma IA confiável, ética e transparente [7].

Diante da crescente dependência de dados para a formulação de políticas públicas, a prestação de serviços digitais e a tomada de decisão estratégica, os órgãos da Administração Pública Federal (APF) enfrentam o desafio de estruturar práticas maduras de governança de dados [8]. A implementação bem-sucedida da Agenda 2030 no setor público pressupõe, portanto, a articulação entre a governança de dados, a adoção responsável de IA

---

[3] https://brasil.un.org/pt-br/sdgs Como as Nações Unidas apoiam os Objetivos de Desenvolvimento Sustentável no Brasil, Acesso em maio de 2026.

[4] Digital Public Infrastructure and Development: A World Bank Group Approach - Digital Transformation White Paper: Volume 1 , 2025. Acesso em abril 2026

[5] Governing with Artificial Intelligence | OECD , OECD, 2024. Acesso em maio de 2026

[6] Ferramenta de IA alinha planejamento estratégico de ministério aos ODS | United Nations Development Programme PNUD , 2025. Acesso em abril 2026

[7] AI-Report-Online.pdf Hello, World: Artificial intelligence and its use in the public sector, OCDE, 2019.

[8] Governança de Dados — Governo Digital - Governança de Dados do Poder Executivo Federal, acesso em abril 2026.

e as infraestruturas públicas digitais, sustentadas por políticas públicas eficazes [9]. Trata-se menos de uma agenda tecnológica e mais de uma agenda institucional, ética e democrática, na qual dados e algoritmos devem servir ao desenvolvimento sustentável e ao fortalecimento do Estado.

No cenário nacional, a Infraestrutura Nacional de Dados (IND), estabelecida pelo Decreto nº 12.198/24, visa promover o uso estratégico dos dados em posse dos órgãos e entidades do Poder Executivo Federal[10].

Em estudo recente[11], o Gartner — consultoria internacional especializada em tecnologia da informação, reconhecida por fornecer análises e boas práticas em governança de dados — ressaltou que, no futuro próximo, agentes de IA ampliarão o avanço tecnológico ao automatizar decisões, o que exigirá uma governança de dados robusta e uma cultura organizacional preparada para garantir confiança e valor, inclusive em empresas públicas.

Entretanto, como ação imediata, os principais obstáculos à efetividade da governança de dados são predominantemente de natureza humana — como necessidade de definição de papéis e responsabilidades sobre o uso dos dados, percepção limitada de valor e falta de engajamento e interoperabilidade — o que explica por que instituições e entidades que focam apenas em processos e tecnologia tendem a falhar e não alcançar diferenciação por meio de uma estratégia de IA consistente e sustentável (GARTNER, 2026).

No contexto brasileiro da Administração Pública Federal (APF), o Tribunal de Contas da União (TCU) exerce papel central no controle externo, incluindo a fiscalização da governança e da gestão de dados[12]. Complementarmente, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Secretaria de Governo Digital (SGD), atua como principal instância orientadora para a institucionalização da governança de dados na APF[13].

O Decreto nº 12.198/2024[14] estabelece que a governança de dados é um elemento essencial da Estratégia Federal de Governo Digital 2024–2027 e deve ser contemplada nos Planos de Transformação Digital dos órgãos públicos. Nesse sentido, a Secretaria de Governo Digital do MGI promove a integração e a governança de dados entre os entes federativos, fortalecendo a interoperabilidade e a gestão estratégica da informação no setor público.

Anualmente, a SGD/MGI promove o Autodiagnóstico de Governança de Tecnologia aplicado a 234 órgãos da APF integrantes do Sistema de Administração dos Recursos de

---

[9] Belli et al., 2024 Governança de dados no setor público: dados abertos, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável . Acesso em abril, 2026

[10] [10] Decreto nº 12.198/2024 Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12198.htm Acesso em: 18 maio 2026

[11] GARTNER. 3 tips to tackle cultural inhibitors to Data Governance success. Stamford, CT: Gartner, 17 March 2026.

[12] https://www.gov.br/governodigital/pt-br/IND/governanca-de-dados - Papéis e responsabilidade em Governança de Dados na APF

[13] Governança de Dados — Governo Digital - Governança de Dados do Poder Executivo Federal

[14] Decreto nº 12.198/2024 Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027, https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12198.htm

Tecnologia da Informação (SISP)[15], com o objetivo de avaliar o nível de maturidade em temas diversos afetos à governança de TI e identificar capacidades relacionadas ao uso e à governança de dados [16].

Como resultado de recente auditoria, o TCU publicou os achados do Acórdão nº 457/2026[1] evidenciando que a governança de dados na APF ainda apresenta baixa maturidade, sobretudo em decorrência da ausência de políticas institucionais eficazes, claras e devidamente implementadas. Além disso, a falta de diretrizes estruturadas, aliada a fragilidades organizacionais e culturais, limita a qualidade, a gestão e o uso estratégico dos dados, comprometendo a capacidade do órgão ou entidade da APF de viabilizar iniciativas mais avançadas, especialmente as baseadas em inteligência artificial.

A proposta deste estudo, portanto, não se configura como mero aprimoramento normativo e objetiva uma contribuição ao estágio atual de maturidade dos órgãos do SISP, assegurando que a evolução tecnológica ocorra de forma coordenada, segura e orientada "*diretamente à capacidade dos órgãos e entidades de transformar dados brutos em informações úteis para a geração de valor público [1]*".

Parte-se do entendimento de que uma política de governança de dados pode assumir um papel central e um ponto de inflexão normativo e estratégico (Figura 1), apta a orientar programas institucionais, direcionar mudanças organizacionais e fomentar uma cultura orientada a dados no âmbito dos órgãos integrantes do SISP na APF. Uma política efetiva deve estabelecer, de forma clara, papéis, responsabilidades, estruturas de governança e práticas operacionais de tratamento de dados, a fim de promover diretrizes comuns para a coleta, o uso, a operação, o compartilhamento e a interoperabilidade de dados entre os órgãos do SISP.

A análise do TCU adotou a metodologia de referência DAMA-DMBOK2[17], que reconhece a Governança de Dados como dimensão central e integradora de todas as capacidades de gestão de dados. Com base nesse referencial, este relatório examina de forma holística a relação entre os achados do TCU e os indicadores de governança digital, dados e informação aferidos pelo IGOVSISP 2025 aplicado à 234 órgãos da APF pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), identificando convergências, lacunas estruturais e oportunidades de atuação sistêmica, inclusive com foco no uso dos dados para apoiar estratégias de inteligência artificial.

A metodologia **DAMA-DMBOK2** (usada como referencial metodológico pelo TCU para a condução da auditoria) reconhece a Governança de Dados como a dimensão central e orientadora de todas as demais capacidades de gestão de dados (por exemplo: qualidade

---

[15] O Sistema SISP foi instituído pelo Decreto nº 7.579/2011, que organiza, de forma sistêmica, o planejamento, coordenação, operação, controle e supervisão dos recursos de TI na APF. Ele abrange os órgãos e entidades da administração direta, autárquica e fundacional. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm

[16] Autodiagnóstico do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP 2025 https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp P

[17] DAMA INTERNATIONAL. DAMA-DMBOK: Data Management Body of Knowledge. 2. ed. Basking Ridge, NJ: Technics Publications, 2017. Disponível em: <https://www.dama.org>. Acesso em: 7 maio 2026.

da informação, conformidade com a LGPD, gestão de metadados, ciclo de vida da informação e promoção da cultura orientada a dados).

Por conceituação, a governança de dados distingue-se da gestão de dados ao concentrar-se no estabelecimento do nível decisório, normativo e de responsabilização que orienta o tratamento de dados no âmbito das instituições (no caso, os órgãos e entidades da APF integrantes do SISP). A gestão de dados, por sua vez, é operacional e refere-se às atividades técnicas necessárias à execução dessas diretrizes. Essa distinção é fundamental para assegurar o alinhamento estratégico, a clareza das responsabilidades e a efetividade institucional.

Como contribuição prática adicional, este trabalho propõe um modelo de Política de Governança de Dados sugerido aos órgãos do SISP, estruturado em princípios, diretrizes, papéis, instâncias decisórias e artefatos mínimos, alinhado às boas práticas internacionais, às recomendações do TCU e às exigências normativas brasileiras, em especial aquelas relacionadas à Estratégia de Governo Digital [18] e à proteção de dados pessoais[19].

2. Análise das evidências identificadas no Acórdão nº 457/2026 – do TCU

As evidências identificadas pelo Tribunal de Contas da União demonstram fragilidades estruturais persistentes na governança de dados da Administração Pública Federal, em especial "*a integração insuficiente entre bases e sistemas, a dependência de soluções legadas e a adoção de iniciativas de interoperabilidade de forma reativa e não estratégica*". Esse cenário resulta em elevados custos de manutenção, retrabalho, riscos à conformidade legal e limitações concretas à transformação digital e à execução de políticas públicas baseadas em dados.

Recentemente, os resultados do IGOVSISP 2025 confirmam e aprofundam os achados o Acórdão nº 457/2026, resultante de auditoria do TCU em órgãos selecionados com base nos resultados do IGOVSISP 2023[20], demonstrando que, ainda em 2025, mais de 68% dos órgãos da APF integrantes do SISP se encontravam nos níveis iniciais de maturidade em governança de dados (N1 e N2), caracterizados pela inexistência ou informalidade de estruturas de governança, pela ausência de papéis definidos e pela fragilidade de mecanismos de coordenação, supervisão e monitoramento.

Entre as principais fragilidades identificadas estão a ausência de comitês de governança de dados, a indefinição de papéis e responsabilidades, a inexistência de escritórios de governança de dados, bem como a atuação fragmentada e descentralizada das

---

[18] Decreto nº 12.198/2024 Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027ital, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12198.htm Acesso em: 18 maio 2026

[19] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 18 maio 2026.

[20] Autodiagnóstico SISP **2023.** https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/arquivos/autodiagnostico_2023.pdf/@@download/file

iniciativas relacionadas ao ciclo de vida dos dados. De forma convergente, as recomendações do TCU enfatizam os pilares centrais do referencial metodológico DAMA-DMBOK2, destacando a governança de dados como eixo estruturante para a institucionalização organizacional e a promoção de uma cultura *data-driven*.

O TCU reforça que a interoperabilidade e o compartilhamento de dados ultrapassam a dimensão técnica, constituindo elementos centrais da estratégia organizacional e demandando políticas claras, definição de responsabilidades, controles, rastreabilidade e gestão de riscos ao longo de todo o ciclo de vida dos dados, em conformidade com os normativos aplicáveis, como a LGPD[21] e o Decreto nº 10.046/2019[22].

De maneira geral, as recomendações do Acórdão do TCU propõem uma trajetória de evolução da governança de dados para os órgãos auditados que serve de referência aos demais órgãos do SISP, conforme o nível de maturidade institucional[23] identificado, indicando que:

- em níveis iniciais (**N1**) e básicos (**N2**), o foco deve ser a **estruturação** organizacional e a normatização;
- no nível intermediário (**N3**), a prioridade recai sobre processos, **controles** e qualidade dos dados;
- em níveis aprimorado (**N4**) e avançado (**N5**), a ênfase concentra-se na integração e **interoperabilidade**, na geração de **valor** e na sustentabilidade das iniciativas de dados.

Nesse contexto, o TCU recomenda prioritariamente a institucionalização formal da governança de dados, por meio de atos normativos que estabeleçam arranjos organizacionais perenes, legitimados pela alta administração e alinhados à estratégia institucional dos órgãos da APF.

O TCU também destaca que é inadequada a subordinação da governança de dados exclusivamente à área de TI, ao apontar (de forma reiterada no relatório) a :

> *"inexistência de unidade [...] separadamente da área de TI"* e fragilidades na *"institucionalização de políticas, procedimentos, comitês, papéis e rotinas essenciais"*,

... reforçando o caráter organizacional, estratégico e transversal do tema.

---

[21] Lei Geral de Proteção de Dados Pessoais – http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm - Acesso em: 18 maio 2026.

[22] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm Acesso em: 18 maio 2026

[23] níveis de maturidade em governança de dados: N1 "Inexpressivo", N2 "Iniciando", N3 "Intermediário", N4 "Aprimorado, N5 "avançado"

A governança de dados deve ser tratada como função corporativa e estratégica, cabendo à TI o papel de habilitadora técnica (custódia e implementação), e não de instância decisória (DAMA-DMBOK, Cap. 3)[24].

Na atribuição de coordenação da governança de dados na APF, para auxiliar os órgãos do SISP na estruturação de seus respectivos Programas de Governança de Dados, o MGI elaborou o "*Guia de Implementação dos Programas de Governança de Dados do Poder Executivo Federal" (PGDADOS)*[25], que constitui o principal referencial governamental para a institucionalização da governança de dados na APF.

O guia prevê que um Programa de Governança de Dados seja implementado em três fases: com uma *Política Interna de Governança de Dados*, seguida de uma *Estratégia de Dados* e de um *Plano de Implementação*.

Essas fases implementam o previsto na minuta de decreto, ainda em fase pré-decisória, que institui a Política de Governança de Dados no Governo Federal, em fase de consulta pública e em consonância com o arcabouço normativo vigente, incluindo a Lei nº 13.709/2018 (LGPD)[22], a Lei nº 14.129/2021 (Lei do Governo Digital)[26] e o Decreto nº 10.046/2019[23].

Este cenário revela uma lacuna relevante entre a orientação normativa pretendida e a necessidade prática e imediata de implementação e adequação pelos órgãos do SISP, em atendimento às recomendações do TCU.

O modelo de Política Integrada, proposto na Seção 5 deste relatório, objetiva apoiar, de forma imediata, a institucionalização da governança de dados como instrumento estratégico nos órgãos do SISP, promovendo a integração organizacional, a sustentabilidade das iniciativas e a geração de valor público. Dessa forma, a política de governança de dados proposta não é acessória a uma estratégia de IA nos órgãos da APF, mas tem o potencial de atuar como condição habilitadora da visão orientada a dados.

3. Análise dos Resultados do IGOVSISP 2025 sobre Temas Habilitadores para o uso de IA

Os resultados do IGovSISP 2025, analisados em correlação com os achados da auditoria do Tribunal de Contas da União (TCU)[27]evidenciam oportunidades estruturais de melhoria na maturidade da governança de dados dos órgãos do SISP. A articulação entre evidências quantitativas do IGovSISP 2025 e constatações do controle externo revela padrões sistêmicos de baixa institucionalização, com impactos diretos na transparência, na efetividade

[24] DAMA-DMBOK, Cap. 3. https://dama.org/learning-resources/dama-data-management-body-of-knowledge-dmbok/

[25] Guia de Implementação do Programa de Governança de Dados (PGDADOS), versão 1.2, outubro de 2025 guia_politica-interna-de-governanca-de-dados-_v1-2.pdf

[26] Lei do Governo Digital - https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm - Acesso em maio de 2026.

[27] TCU Acórdão 457/2026 - Plenário https://portal.tcu.gov.br/uploads/noticias/pdf/2026/03/04/457-2026.pdf . Acesso em maio de 2026.

das políticas públicas e na capacidade de inovação do Estado, principalmente em relação à estratégia de uso de IA na APF.

Este relatório concentrou-se em temas-chave representados por indicadores específicos do IGOVSISP 2025[28], que permitem avaliar se a Governança de Dados se encontra formalmente institucionalizada por meio de políticas comunicadas e efetivamente implementadas, capazes de alinhar a gestão e uso de dados aos objetivos estratégicos organizacionais.

Nesse sentido, foram selecionados e examinados, de forma integrada, os indicadores de Gestão Orientada a Dados (G310DI) e de Alinhamento com Objetivos Estratégicos (G361DI), bem como a existência de uma Estrutura Organizacional para uma Governança de Dados Assertiva (G322DI) e de Princípios e Políticas de Dados formalizados (G321DI). Adicionalmente, analisa-se em que medida os processos decisórios são orientados por evidências, a partir do indicador de Tomada de Decisão Baseada em Dados (G307DI), e em que medida são apoiados por uma Estratégia Institucional de Inteligência Artificial (G337DI) voltada à antecipação de cenários e ao fortalecimento da capacidade analítica do Estado.

A síntese analítica entre os resultados do IGOVSISP 2025 e os achados do TCU evidencia riscos institucionais associados à ausência ou à baixa maturidade da governança de dados, bem como seus potenciais impactos sobre a transparência governamental, a efetividade das políticas públicas e a capacidade de inovação no setor público, apresentados nas análises parciais (1 a 3) e sintetizados na conclusão da Figura 1.

[28] Auto Diagnóstico IGOVSISP 2025 - https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/arquivos/autodiagnostico_2025.pdf/@@download/file

Figura 1 – Características dos Programas de Governança de Dados em quadrantes - Representação gráfica da evolução da gestão de dados e do alinhamento estratégico rumo ao uso estratégico de IA

ANÁLISE 1 – A GOVERNANÇA DE DADOS ESTÁ INSTITUCIONALIZADA POR MEIO DE POLÍTICAS COMUNICADAS?

Com base no diagnóstico do IGOVSISP 2025, a análise dos indicadores **G322DI (Estrutura Organizacional para Governança de Dados)** e **G321DI (Princípios e Políticas de Dados Comunicados)** demonstra que a governança de dados na APF permanece majoritariamente em estágio pré-institucional.

No indicador **G322DI (Estrutura Organizacional para Governança de Dados)**, mais de **68%** dos órgãos do SISP concentram-se nos níveis **A1 e A2**[29], caracterizados pela inexistência ou informalidade das estruturas de governança, pela ausência de papéis e responsabilidades definidos e pela fragilidade dos mecanismos de coordenação, supervisão e monitoramento.

Em estágio intermediário, **21,79%** dos órgãos ainda no **Nível A3** relatam políticas e *frameworks* em elaboração, mas sem mecanismos estruturados de monitoramento contínuo — com risco de estagnação ou regressão.

Somente menos de **10%** dos órgãos, já nos **Níveis A4 e A5**, refletem efetiva institucionalização, melhoria contínua e maturidade elevada na governança de dados, formalizada em políticas internas apoiadas pela alta gestão.

No indicador **G321DI (Princípios e Políticas de Dados)**, observa-se um padrão semelhante: a maior parte dos órgãos permanece nos níveis iniciais (**A1** e **A2**), com princípios e políticas de dados inexistentes ou frágeis e comunicação institucional incipiente.

Apenas um grupo reduzido alcança níveis avançados (**A4** e **A5**), nos quais as políticas estão formalizadas, amplamente comunicadas e integradas aos processos institucionais.

A análise conjunta dos resultados do **G322DI** e do **G321DI** indica que o avanço na maturidade da governança de dados não decorre simplesmente da existência de princípios e políticas, mas, principalmente, da maneira como esses elementos são difundidos, comunicados e efetivamente integrados à estratégia institucional e às boas práticas operacionais de gestão de órgãos do SISP.

Nesse sentido, **a comunicação institucional emerge como vetor central de maturidade, responsável por transformar políticas formais em prática organizacional** efetiva que impulsione a governança de dados no setor público.

[29] 5 níveis de maturidade: N1 “Inexpressivo”, N2 “Iniciado”,N3 “Emergente”, N4“Desenvolvido” e N5 “Otimizado”, IGOVSISP

ANÁLISE 2 – A GESTÃO DE DADOS ESTÁ ALINHADA AOS OBJETIVOS ESTRATÉGICOS?

A análise conjunta dos indicadores **G310DI (Gestão Orientada a Dados)** e **G361DI (Alinhamento com Objetivos Estratégicos)** evidencia que o principal desafio dos órgãos do SISP, quanto à eficácia da governança de dados, não é tecnológico, mas estratégico.

No tema **G310DI (Gestão Orientada a Dados)**, **83,34%** dos órgãos concentram-se nos níveis **A2 e A3**, indicando reconhecimento do valor dos dados e uso parcial ou emergente, porém ainda sem gestão plenamente consolidada.

Em contraste, no tema **G361DI (Alinhamento com Objetivos Estratégicos)**, **66,24%** dos órgãos permanecem nos níveis **A1** e **A2**, nos quais o alinhamento entre dados e estratégia é inexistente, inicial ou fragmentado.

Destaca-se que **48,72%** dos órgãos situam-se especificamente no **Nível A2** de alinhamento, o que evidencia que, na maioria dos casos, os dados ainda não orientam o planejamento estratégico , nem estão vinculados de forma consistente a metas e indicadores institucionais.

Apenas **8,98%** dos órgãos atingem níveis avançados (**A4** e **A5**) em gestão orientada a dados, percentual que corresponde diretamente aos níveis mais elevados de alinhamento estratégico (**8,55%**), nos quais os dados sustentam planejamento baseado em evidências, inovação e proatividade institucional.

A leitura integrada dos resultados do **G310DI** e do **G361DI** revela uma relação estrutural e causal: ***o alinhamento estratégico não antecede a maturidade em gestão orientada a dados, mas dela decorre***.

Para avançar nos dois temas de forma coordenada – a **Gestão Orientada a Dados (G310DI)** e o **Alinhamento com Objetivos Estratégicos (G361DI)** – os órgãos do SISP precisam tratar os dados como meio estruturante, integrado às diretrizes de governança corporativa. Uma forma efetiva é explicitar a **estratégia de dados** no planejamento institucional vinculando indicadores de dados às metas organizacionais.

ANÁLISE 3 – O PROCESSO DECISÓRIO É BASEADO EM DADOS E VIABILIZA O USO ESTRATÉGICO DE IA?

Os indicadores **G307DI (Tomada de Decisão Baseada em Dados)** e **G337DI (Estratégia de Inteligência Artificial)** revelam um avanço assimétrico.

No tema **G307DI (Tomada de Decisão Baseada em Dados)**, **79,06%** dos órgãos concentram-se nos níveis **A2** e **A3**, o que reflete o uso crescente de indicadores, métricas de desempenho e ferramentas de *Business Intelligence* (BI), com a substituição gradual de decisões baseadas exclusivamente na intuição.

Por outro lado, no indicador **Estratégia de Inteligência Artificial (G337DI)**, verifica-se que **85,04%** dos órgãos permanecem nos níveis **A1 e A2**, caracterizados por iniciativas pontuais ou experimentais, pela ausência de diretrizes formais e por uma governança incipiente ou inexistente.

Esse descompasso evidencia que, embora os órgãos tenham desenvolvido capacidade inicial de decisão baseada em dados (incluindo *Business Intelligence* BI), ainda não dispõem das condições institucionais necessárias para escalar esse uso por meio de IA de forma ética, segura e estratégica.

Os resultados indicam que o ponto de inflexão entre a maturidade intermediária em decisão baseada em dados e a adoção estruturada de IA depende diretamente da existência de uma **política de governança de dados estratégica, comunicada e efetivamente implementada**, que atuará como elemento estruturante para transformar o uso pontual de dados em prática institucional confiável, escalável e legitimada.

Em síntese, considerando especificamente as Análises 1, 2 e 3 deste relatório, a correlação entre IGovSISP 2025 e os achados do TCU demonstra, com base empírica, que a evolução da governança de dados nos órgãos do SISP depende menos de iniciativas técnicas isoladas e mais da institucionalização por meio de políticas claras, integradas e orientadas à estratégia e visão dos órgãos do SISP.

4. Ações imediatas, lacunas e diretrizes para um Programa de Governança de Dados estruturado

A abordagem proposta neste relatório — *Política de Governança de Dados*, *Estratégia de Dados* e *Plano de Implementação* em um único instrumento — mostra-se necessária para enfrentar o descompasso entre a orientação normativa do *Guia de Implementação dos Programas de Governança de Dados do Poder Executivo Federal* (PGDADOS) [30] (ainda em fase

[30] Guia de Implementação do Programa de Governança de Dados (PGDADOS), versão 1.2, outubro de 2025 guia_politica-interna-de-governanca-de-dados-_v1-2.pdf

de elaboração da Política de Governança de Dados no Governo Federal) e a capacidade prática de implementação imediata pelos órgãos do SISP.

Atualmente, o MGI elaborou diretrizes para a Parte 1 - Políticas Internas de Governança de Dados, o que não é suficiente para operacionalizar a governança de dados de forma efetiva e imediata, com os três instrumentos principais (Política, Estratégia e Plano de Implementação). A Parte 2 - *Passo a Passo para formular uma Estratégia de Dados* (previsto); e Parte 3 - *Criação dos Planos de Implementação* (previsto) estão previstos. Diante deste desafio, este relatório apresenta a contribuição para contemplar as 3 partes e para a adoção de ações imediatas e escaláveis pelos órgãos do SISP.

Fundamentado no referencial DAMA-DMBOK, o modelo proposto incorpora pilares essenciais, como alinhamento estratégico, interoperabilidade, qualidade de dados, segurança da informação, gestão de riscos e conformidade, garantindo a adaptação à diversidade de contextos institucionais dos órgãos do SISP, à luz do contexto observado pelo TCU.

A Unidade de Auditoria Especializada em Tecnologia da Informação do TCU incluiu, no planejamento 2023–2024, a meta de mapear o nível de maturidade em governança de dados de 100% das organizações integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), estabelecendo como objetivo estratégico tornar a atuação da APF orientada a dados confiáveis. Tal direcionamento confere caráter prioritário à adoção estruturada de Programas de Governança de Dados, independentemente da consolidação normativa definitiva.

A *Tabela 1* apresenta as ações imediatas para apoiar o Plano de Implementação que contemple as recomendações do TCU.

Tabela 1 - Ações imediatas e efeito esperado do controle identificado pelo TCU

Achado do TCU	Descrição Sintética do Achado	Controle Institucional na Política	Referência no Acórdão 457/2026	Estratégia de Comunicação na Política	Ação imediata e Efeito Esperado do Controle
Ausência de instância deliberativa específica para dados	Inexistência ou fragilidade de comitês de governança de dados, com decisões dispersas, consultivas ou diluídas em instâncias amplas	Instituição de **Comitê de Dados** como instância deliberativa estratégica	9.1.1, 9.1.4	Política (diretrizes)	Centralização da tomada de decisão estratégica; alinhamento entre dados, estratégia, segurança e privacidade; redução de decisões ad hoc
Gestão fragmentada e falta de integração entre dados e segurança da informação	Gestão de riscos fragmentada entre segurança da informação, privacidade de dados e governança	Atuação do Comitê de Segurança da Informação articulada ao Comitê de Dados e ao Encarregado de Dados Pessoais	9.1.2.8, 9.1.5.17	Política (diretrizes)	Proteção integrada dos ativos de informação ao longo do ciclo de vida, contemplando governança de dados, segurança da informação e privacidade
Conformidade parcial com LGPD	Privacidade fora do processo decisório e decisões sobre dados pessoais sem instância clara	Atuação deliberativa do Encarregado de Dados Pessoais (DPO) no ciclo de vida de dados pessoais de acordo com a finalidade pretendida	9.1.1.6, 9.1.5.17	Política (diretrizes)	Incorporação sistemática dos requisitos de privacidade às decisões institucionais, processo de autorização formalizado atendendo aos requisitos de privacidade e base legal
Cultura de dados incipiente	Uso limitado e reativo dos dados na tomada de decisão	Promoção *data-driven* pelo EGD em todas as instâncias relacionadas ao ciclo de vida de dados	9.1.1.4, 9.1.4.6	Política (diretrizes)	Decisão baseada em dados e uso estratégico e responsável dos dados como ativo institucional
Baixa atuação da Alta Direção na governança de dados	Governança tratada como tema técnico, sem responsabilização da alta gestão	Comitê de Dados assessorando a Alta Direção, alinhamento estratégico como pilar da política	9.1.1	Política (diretrizes)	Reforço do patrocínio institucional; integração da governança de dados à governança corporativa
Inexistência de unidade institucional dedicada à governança de dados	Governança absorvida pela TI ou inexistente, sem coordenação corporativa	Criação do Escritório de Governança de Dados (EGD)	9.1.1.3	Política (diretrizes))	Implantação de capacidade institucional permanente para coordenar, normatizar e supervisionar a governança de dados
Fragmentação das práticas de governança	Ações isoladas, não coordenadas e sem visão corporativa	Coordenação centralizada pelo EGD em atendimento às deliberações do Comitê de Dados	9.1.1	Estratégia (objetivos planejados)	Alinhamento estratégico, gestão de riscos, valor institucional, coerência, padronização institucional e alinhamento das boas práticas
Risco elevado na atuação de terceiros e de aprisionamento tecnológico	Ausência de exigência formal de conformidade de parceiros, ausência de estratégia de gestão do conhecimento	Exigência de documentação e evidências de conformidade de terceiros, absorção e formalização do conhecimento	9.1.4.10, 9.1.2.7	Estratégia (objetivos planejados)	Mitigação de riscos legais, tecnológicos, contratuais e reputacionais
Indefinição de responsabilidades sobre os dados	Ausência de *accountability* sobre dados e de responsáveis claros pela decisão, uso e riscos associados aos dados	Definição formal do papel de Proprietário de Dados (*Data Owner*), com representatividade por demanda no Comitê de Dados	9.1.1.2, 9.1.4.3, 9.1.5.4	Estratégia (objetivos planejados)	*Clara accountability institucional* sobre dados, riscos, acessos e compartilhamento. Deliberação sobre acordos de compartilhamento de dados
Compartilhamento de dados informal e sem governança clara	Cessões informais sem avaliação de risco, finalidade ou autorização	Autorização de cessão pelo Data Owner com acordos formalizados	9.1.5.3	Estratégia (objetivos planejados)	Compartilhamento orientado por visão e valor institucional, propósito, risco e conformidade.
Viés tecnológico e confusão entre responsabilidades técnicas (TI) e decisórias	Decisões de governança absorvidas pela TI e uso de soluções tecnológicas em desalinhamento com	Separação entre Curador e Custodiante de Dados. Observância às deliberações	9.1.4.4, 9.1.5.5, 9.1.4.3	Estratégia (objetivos planejados)	Associar a Governança de Dados à estratégia institucional. Clareza de papéis; governança orientando a tecnologia, e não o inverso

	visão institucional para extração de valor dos dados	do Comitê de Dados e coordenação do EGD			
Ausência de inventário e catálogo dados corporativos	Baixa visibilidade dos ativos de dados e dificuldades de interoperabilidade	Catálogo de Dados corporativo gerido pelo EGD	9.1.3.8, 9.1.5.8	Plano de Implementação (ações)	Identificação, reutilização e compartilhamento seguro de dados de interesse institucional. Estabelecimento de indicadores, cronograma e atividades
Metadados incompletos ou inexistentes	Fragilidade na rastreabilidade, interpretação e integração dos dados	Procedimentos de catalogação, metadados, dados mestre e de referência, monitoramento da qualidade dos dados	9.1.3.8, 9.1.4.7	Plano de Implementação (ações)	Consistência semântica, linhagem e mapeamento do fluxo de dados, interoperabilidade e governança do ciclo de vida Inventário de ativos, cronograma e atividades
Fragilidade na gestão funcional do dado	Falta de responsável pelo conteúdo, qualidade e significado do dado	Instituição do papel de Curador de Dados (Data Steward) por domínios de dados	9.1.4.7, 9.1.5.10	Plano de Implementação (ações)	Garantia de qualidade, metadados, linhagem, consistência e uso adequado. Monitoramento da qualidade dos dados e linhagem
Baixa maturidade na gestão do ciclo de vida dos dados	Dados mantidos indefinidamente ou descartados sem critérios	Gestão do ciclo de vida por Curadores, orientados pelo EGD	9.1.4.8	Plano de Implementação (ações)	Conformidade regulatória, eficiência e redução de riscos, otimização de infraestrutura (inclusive gestão de nuvem) Elaboração de normas e procedimentos internos
Fragilidades técnicas em disponibilidade e integridade	Controles operacionais inconsistentes. Adoção inadequada de soluções e plataformas tecnológicas	Responsabilidade técnica do Custodiante de Dados e alinhamento institucional de soluções de tecnologia	9.1.4.3	Plano de Implementação (ações)	Maior planejamento, maior ROI, maior confiabilidade operacional e auditabilidade. Monitoramento e operacionalização das soluções de tecnologia com avaliação do ROI (DataOps e FinOps)
Ausência de mecanismos de monitoramento e avaliação da implementação	Inexistência de modelos, indicadores e metodologias de acompanhamento	Recomendações de aprimoramento e registro das ações corretivas adotadas	9.1.4.3	Plano de Implementação (ações)	Relatórios anuais, avaliação da maturidade de dados, revisões bienais, acompanhamento periódico de indicadores , dentre outros.

5. Proposta: Uma proposta de Política Integrada (política + estratégia + plano de implementação) para apoiar o Programa de Governança de Dados na APF

Os resultados das análises supracitadas demonstram que o Poder Executivo Federal já avançou de forma consistente no uso de dados para subsidiar decisões. Entretanto, esse avanço não será sustentável nem escalável sem a consolidação da Governança de Dados institucionalmente comunicada, capaz de maximizar o valor público gerado pelos dados e orientar a adoção ética, segura e estratégica da IA (conforme representado na Figura 1).

Mesmo para as organizações que já elaboraram políticas, é necessário e decisivo comunicar e integrar, de maneira sistêmica, o ciclo de vida dos dados aos princípios, valores e diretrizes, de modo que a rotina traga a transformação digital de forma consistente. Sem estratégia de comunicação institucional, a governança de dados tende a permanecer nos estágios iniciais, a depender de esforços individuais, sem escalar nem se sustentar no tempo.

O modelo de Política Integrada proposto neste estudo desempenha uma função estruturante ao formalizar e comunicar os papéis e responsabilidades dos produtores (*Supplier*) e dos consumidores (*Consumer*) de dados, estabelecidos ao longo de todo o ciclo de vida da informação. Ao definir quem responde pela criação, manutenção, atualização e qualidade dos dados mestres e de referência, a política viabiliza o reconhecimento desses dados (ativos estratégicos e fontes oficiais para IA), reduzindo duplicidades, inconsistências e conflitos semânticos. Tal definição constitui condição necessária para o estabelecimento de acordos formais de compartilhamento de dados (*Data Sharing Agreements*), nos quais o fornecedor e o recebedor assumem compromissos claros quanto à qualidade, disponibilidade, uso adequado e aderência às finalidades institucionais.

É importante prever um arranjo institucional com autoridade decisória clara e responsabilização distribuída, distinguindo entre governança, operação tecnológica, segurança da informação e proteção de dados pessoais. A criação de um Comitê ou Instância Estratégica de Governança de Dados para atuar como instância deliberativa superior, responsável por decisões estratégicas sobre compartilhamento, interoperabilidade e priorização de ativos de dados, integra-se estrategicamente ao *executivo de dados* ou *ao líder do escritório de governança de dados (EGD), que,* por atribuição, concentra capacidades executivas relacionadas a padrões, metadados, arquitetura corporativa e difusão da cultura orientada a dados.

No nível funcional, a política proposta explicita os papéis de Curador de Negócio ou Proprietário de Dados (*Data Owner*), Curador de Dados (*Data Steward*) e Custodiante Técnico dos Dados *(Technical Data Steward)*, fortalecendo a qualidade, a segurança e a conformidade normativa. A integração do Encarregado de Dados Pessoais (DPO) às instâncias decisórias assegura que a proteção de dados pessoais esteja incorporada ao núcleo da governança institucional.

Adicionalmente, como parte de um modelo de implementação, a política estabelece protocolos de interoperabilidade que integram as dimensões técnicas, semânticas e organizacionais. Protocolos técnicos (como APIs e padrões de integração), semânticos (vocabulários controlados e modelos de dados comuns) e organizacionais (fluxos decisórios,

instâncias de coordenação e mecanismos de governança) são essenciais para transformar o compartilhamento de dados em prática rotineira, confiável e sustentável. À medida que a maturidade institucional se amplia, a interoperabilidade deixa de ser um objetivo em si e passa a se consolidar como resultado natural do fortalecimento da governança de dados.

6. Modelo de Política

O modelo proposto contempla o marco normativo nacional — representado pelo Decreto que institui a Política Nacional de Governança de Dados e pelas diretrizes da Cartilha GovDados — Volume 3 —, bem como as boas práticas internacionalmente consolidadas do DAMA-DMBOK, com o objetivo de favorecer a institucionalização de um programa de governança de dados estruturado, alinhado à estratégia, orientado a decisões e ações imediatas para os órgãos do SISP.

IMPORTANTE: Este modelo deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas , bem como observar a aderência aos processos internos, a fim de construir uma política adequada à sua realidade.
Para usar este modelo, basta substituir o texto por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplo [em vermelho]

POLÍTICA DE GOVERNANÇA DE DADOS

I. CONTEXTUALIZAÇÃO E COMUNICAÇÃO

[*Esta seção apresenta uma visão estruturada levando em consideração a natureza e a finalidade do órgão do SISP e como deve organizar, controlar e utilizar seus dados de forma estratégica, segura e eficiente, usando a governança de dados como base para decisões melhores, inovação e geração de valor público, que reconhece os dados como ativos institucionais estratégicos e integra a governança de dados à governança corporativa*]

Exemplo:

A **Governança de Dados do [Órgão/Entidade]** é constituída por um conjunto de processos, políticas, regras, estruturas organizacionais, padrões e práticas que orientam, monitoram e gerenciam as **atividades de tratamento de dados** de interesse institucional, essenciais à geração de valor, à inovação e à eficiência diante de desafios tecnológicos emergentes e da crescente complexidade dos ecossistemas digitais.

Nesse contexto, será alinhada aos objetivos estratégicos, à missão, à visão e aos **valores institucionais** do [Órgão/Entidade]. Suas diretrizes e melhores práticas têm o propósito de garantir suporte eficiente e eficaz ao processo decisório baseado em dados, com transparência e confiabilidade, assegurando um diferencial competitivo e foco na geração sustentável de **valor**.

Para os fins desta *Política*, considera-se **ciclo de vida de dados** o conjunto de **atividades de tratamento de dados** desde a coleta até o descarte, incluindo produção, aquisição, uso, acesso, reprodução, transmissão, processamento, armazenamento, eliminação, modificação, compartilhamento, integração e extração de dados de interesse institucional, conduzidas conforme os princípios e diretrizes institucionais e aplicadas de forma integrada às atividades do [Órgão/Entidade].

[Acrescente aqui os objetivos para a Política de Governança de Dados que julgar necessário, adaptável ao contexto do órgão]

II. DESTINATÁRIOS, ESCOPO E ABRANGÊNCIA

[*Esta seção* apresenta a governança de dados como responsabilidade distribuída entre servidores, colaboradores, parceiros e terceiros, abrangendo todos que lidam com dados da instituição, internos ou externos, desde que desempenhem algum papel no tratamento desses dados. Liste os agentes públicos e colaboradores necessários e indique quaisquer exclusões ou exceções fora do escopo]

Esta *Política* se destina aos [.....], a todos que atuam em nome do [Órgão/Entidade], em atividades de tratamento de dados.

III. FINALIDADE OU OBJETIVOS DA POLÍTICA

[Esta seção sugere um referencial para nortear os órgãos do SISP na definição de pilares que comuniquem quais objetivos estratégicos e resultados institucionais a política busca alcançar].

Exemplo:

> Esta *Política de Governança de Dados* ("*Política*" ou "*PGD*") dispõe sobre o **uso**, a **interoperabilidade** e o **compartilhamento** de dados de interesse **do [Órgão/Entidade]** e tem por objetivo estabelecer as diretrizes, conceitos e melhores práticas a serem aplicados às operações que envolvam **atividades de tratamento de dados**, que estejam sob sua responsabilidade ou no âmbito de suas atividades.
>
> A presente *Política* tem por **objetivos**:
>
> - [Acrescente aqui outros objetivos relacionados ao escopo da Política que julguem necessários, exemplos:]
> - Promover o uso legal, ético, seguro e eficiente de dados e apresentar as principais instâncias em governança de dados no âmbito do [Órgão/Entidade];
> - Ressaltar a importância da adoção de boas práticas em governança e gestão de dados que assegurem a qualidade, a segurança e a proteção dos dados, considerados ativos estratégicos do [Órgão/Entidade], de forma a usufruir da evolução tecnológica emergente, fortalecendo a tomada de decisão baseada em dados e processos de inovação sustentável;
> - Garantir à [Órgão/Entidade] mecanismos para a conformidade com leis e regulações nacionais e internacionais que lhe sejam aplicáveis, incluindo a Lei 13.709/2018 ("LGPD").

IV. DOCUMENTOS DE REFERÊNCIA

[Esta seção assegura a integração a políticas de segurança da informação, privacidade e gestão de riscos, de acordo com normativos vigentes nos órgãos]

[Acrescente aqui outros documentos de referência da Política de Governança de Dados que julgue necessários]

V. PRINCÍPIOS E DIRETRIZES

[Esta seção apresenta a base interpretativa da política e estabelece os pilares conceituais, que asseguram que os dados sejam usados de forma estratégica, segura, responsável e eficiente em toda a atuação do órgão do SISP]

São **princípios** da Política de Governança de Dados do *[Órgão/Entidade]* :

- [Acrescente aqui os princípios norteadores principais, exemplos:
- I – **Alinhamento Estratégico**: a valorização dos dados de interesse institucional como **ativos estratégicos** do [Órgão/Entidade], aliada ao compromisso com as atividades de tratamento de dados de forma proativa e eficaz, como parte essencial para o alcance dos propósitos definidos na **missão**, **visão** e **valores** do [Órgão/Entidade];
- II – **Gestão de Riscos e Conformidade**: o compromisso com a observância aos requisitos de privacidade, aos princípios éticos, à conformidade institucional e regulatória. Envolve a gestão dos **riscos** relacionados ao tratamento de dados e a avaliação dos **impactos** e resultados decorrentes;
- III – **Segurança da Informação**: a garantia da **segurança** dos dados ao longo de todo o ciclo de vida, por meio de medidas que assegurem sua disponibilidade, **integridade** e confidencialidade, em infraestruturas adequadas ao tratamento seguro e eficaz das informações;
- IV – **Qualidade de Dados**: a condução de ações voltadas à avaliação e à **melhoria contínua** da qualidade dos dados de interesse, fortalecendo a confiança no uso das informações e nos resultados gerados por soluções inovadoras e tecnologias emergentes aplicadas à gestão e análise de dados;
- V – **Interoperabilidade**: a promoção do compartilhamento, reuso e **integração coordenada** de dados previamente tratados, governados e de qualidade, com vistas a otimizar processos internos e fomentar a adoção de soluções centradas em dados de interesse corporativo.
- VII – **Eficiência Operacional**: a promoção da **gestão eficiente e estratégica** das atividades de tratamento de dados, desde a coleta até o descarte, com vistas à otimização de recursos, à melhoria dos processos institucionais e ao fortalecimento da confiabilidade nas informações utilizadas.

VI. ESTRUTURAÇÃO

[Esta seção apresenta a metodologia ou o framework DAMA-DMBOK. que organiza a governança de dados em componentes interdependentes, que devem ser geridos de forma integrada por diretrizes institucionais, definindo instâncias, papéis e responsabilidades]

A estruturação da Governança de Dados no [Órgão/Entidade] baseia-se, mas não se limita, na metodologia DAMA-DMBOK (sigla em inglês para *Data Management Body of Knowledge*[31]). A metodologia define componentes interdependentes que devem ser gerenciados de forma integrada por diretrizes de Governança de Dados, representadas pelos seguintes pilares: Arquitetura de Dados; Modelagem de Dados; Armazenamento e Operações de Dados; Segurança de Dados; Integração e

[31] DAMA INTERNATIONAL. *DAMA-DMBOK: Data Management Body of Knowledge*. 2. ed. Revised Basking Ridge, NJ: Technics Publications, 2024. ISBN 978-1-63462-236-3. Acesso em: 3 set. 2025

Interoperabilidade de Dados; Gestão de Documentos e Conteúdo; Gestão de Dados Mestre e de Referência, Inteligência de Dados; Gestão de Metadados; e Gestão da Qualidade dos Dados.

VII. ESTRATÉGIA DE DADOS

[Esta seção apresenta a interoperabilidade e o compartilhamento de dados tratados como instrumentos estratégicos de geração de valor, inovação, eficiência e conformidade, com responsabilidades claras, acordos formais e atuação colaborativa entre as Divisões/Departamentos/Unidades do órgão do SISP]

Esta *Política* estabelece diretrizes para que seus destinatários entendam e, no que for pertinente, definam **processos internos**, adotem **boas práticas**, e cumpram exigências legais e normativas que versam sobre a **gestão do ciclo de vida de dados**, sob responsabilidade do **[Órgão/Entidade].**

Será instrumento orientador da estratégia de dados do [Órgão/Entidade], no que se refere a ações para garantir a **interoperabilidade e** o **compartilhamento** seguro dos ativos de dados, que apoiem os objetivos institucionais do **[Órgão/Entidade]**.

Compartilhamento[2] de dados é o processo de disponibilizar dados entre diferentes partes interessadas, no uso de aplicações, análises e sistemas, de forma segura, controlada e orientada por um propósito claramente definido. Envolve acordos formais (no termo em inglês, *Data Sharing Agreements*[32]), que estabelecem os termos, as responsabilidades e os requisitos de qualidade, segurança e conformidade para o uso dos dados.

Interoperabilidade[2] é a capacidade de **compartilhar**, integrar e **utilizar** dados de forma consistente, segura e eficiente entre diferentes aplicações, análises e sistemas para gerar valor institucional, promovendo resultados e *insights* estratégicos com controle, conformidade e segurança. Além disso, a interoperabilidade de dados contribui para a **eficiência operacional** ao reduzir custos de manutenção, minimizar esforços de integração e otimizar processos — especialmente aqueles apoiados por decisões automatizadas, com base no uso de dados de interesse corporativo.

No contexto de **compartilhamento** e **interoperabilidade** de dados, os **[Órgãos/Entidades]** podem atuar indistintamente como entidades **Cedentes** (Fornecedores ou, no termo em inglês, *Suppliers*[2]) ou

[32] DAMA-DMBOK2 (Data Management Body of Knowledge, 2ª edição) - Implementation Guidelines - Data Sharing Agreements

Recebedores de Dados (Consumidores ou, no termo em inglês, *Consumers*[2]), assumindo responsabilidades em cada papel.

Os **Cedentes** devem garantir que os dados compartilhados estejam íntegros, identificados e em conformidade com os princípios regulatórios, éticos e requisitos de qualidade, segurança e governança institucionais.

Os **Recebedores** devem assegurar que os dados recebidos sejam utilizados de forma segura, transparente e alinhada aos objetivos institucionais e finalidades de uso, respeitando os direitos dos titulares e os acordos estabelecidos.

Os acordos de compartilhamento e interoperabilidade serão formalizados entre **Cedentes** e **Recebedores** de dados.

São atitudes básicas que orientam a **interoperabilidade** e o **compartilhamento de dados** no [Órgão/Entidade]:

- [Acrescente as ações que promovam a interoperabilidade e o compartilhamento de dados, exemplos:]
- Promover a disponibilização de fontes de dados , **padronizadas**, **íntegras, precisas** e **reutilizáveis**, com foco no compartilhamento e no reaproveitamento de recursos de infraestrutura de comunicação, armazenamento e processamento de dados.
- Incentivar a atuação integrada entre **[Órgão/Entidade]**, em atividades, serviços e processos decisórios centrados em dados, com garantia de transparência, rastreabilidade, governança, segurança e conformidade regulatória.

VIII. PLANO DE IMPLEMENTAÇÃO E RESPONSABILIDADES

[Esta seção define os papéis e as responsabilidades para o tratamento de dados].

Os **controles** de **Governança de Dados** devem ser **adaptáveis** à estratégia e ao domínio de uso dos dados, ao desenvolvimento tecnológico e às mudanças constantes nos ambientes operacionais e regulatórios nos quais o [Órgão/Entidade] está inserido [33].

[Exemplos de papéis, áreas e responsabilidades]:

- Comitê de Dados ou Instância Estratégica de Governança de Dados

Representa a **instância deliberativa** para aprovar conceitos e diretrizes específicos sobre atividades de tratamento de dados no [Órgão/Entidade] e deliberar sobre outros assuntos afins ao tema.

[33] Cartilha de Governança de Dados Poder Executivo Federal - https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhaGovDadosvol3.pdf

Cabe ao **Comitê de Dados**:

a) [Acrescente as atribuições do Comitê de Dados, exemplos:]
b) Deliberar, orientar e, quando aplicável, priorizar os investimentos em ações que suportem as diretrizes de governança de dados, inclusive no que se refere a infraestruturas e plataformas para armazenamento, processamento, interoperabilidade e compartilhamento de dados.

- Executivo de Dados ou Líder do Escritório de Governança de Dados

Cabe à Equipe do Executivo de Dados ou do **Escritório de Governança de Dados**, a partir das estratégias alinhadas junto ao **Comitê de Dados**, a coordenação, monitoramente e supervisão das práticas de governança de dados corporativa, o que inclui, mas não se limita a:

a) [Acrescente as atribuições do Executivo de Dados, exemplos:]
b) coordenar a implantação, normatização e a operacionalização da **Governança de Dados** no [Órgão/Entidade], de forma alinhada aos objetivos estratégicos;
c) promover o inventário de dados corporativo e a atuação colaborativa, adequada e integrada dos **Proprietários** (ou, no termo em inglês, *Data Owner*[3]), **Curadores** e **Custodiantes de Dados** das **Unidades [Órgão/Entidade],** em benefício da Governança de Dados corporativa;
d) orientar a gestão de dados corporativa, os processos de **interoperabilidade**, uso e **compartilhamento** de dados entre **Recebedores** e **Cedentes**, inclusive por meio da definição de padrões, requisitos e mecanismos que assegurem a qualidade, a segurança e a proteção dos dados, observando o desenvolvimento tecnológico emergente e a legislação aplicável;
e) divulgar e promover a **cultura** de transformação digital do [Órgão/Entidade] **centrada em dados** (*data-driven*);
f) disponibilizar e manter o **Catálogo de Dados do [Órgão/Entidade]** com as informações sobre as bases de dados, projetos e ativos de dados que representem interesse e valor corporativo;
g) promover, orientar e dispor de **procedimentos para catalogação de dados corporativos**, gestão de **dados mestre**[5] e **de referência**[5] e sobre normas e processos necessários a operacionalização da interoperabilidade e compartilhamento de dados no [Órgão/Entidade].

Proprietário de Dados (*Data Owner*)

Considera-se **Proprietário de Dados** (no termo em inglês, *Data Owner*[34]), a Liderança da **Unidade do [Órgão/Entidade]** responsável por um conjunto específico de dados e pela finalidade das atividades de tratamento, com poderes para definir diretrizes específicas, classificar, autorizar acessos, avaliar riscos, garantir conformidade e aprovar decisões

[34] DAMA-DMBOK2 (Data Management Body of Knowledge, 2ª edição) Data Governance – Types of Data Stewards

estratégicas relacionadas ao ciclo de vida dos dados sob sua responsabilidade.

Cabe aos **Proprietários de Dados**:

a) [Acrescente as atribuições do Proprietário de Dados, exemplos:]

b) assegurar que o uso, a qualidade, a segurança e o compartilhamento dos dados estejam alinhados às políticas institucionais do [Órgão/Entidade] , à legislação vigente (incluindo a LGPD) e aos requisitos de negócio, governança e auditoria.

c) indicar, no âmbito de sua área, os respectivos **Curadores** e **Custodiantes de Dados** que serão os pontos focais/responsáveis pela atenção a esta *Política* e às *Normas de Procedimentos* a ela correlatas.

d) atuar como **Cedente de Dados** e autorizar a cessão de dados sob sua responsabilidade, em atendimento aos solicitado pelos **Recebedores de Dados**, conforme **acordos** de **compartilhamento** e **interoperabilidade**.

Curador de Dados OU Curador corporativo

Os **Curadores de Dados** (no termo em inglês, *Data Steward*[4]) são representantes das áreas corporativas, em exercício de suas atividades em **Unidades do [Órgão/Entidade]**, reportam-se ao **Proprietário de Dados** e são responsáveis pela **gestão e uso** das bases de dados e/ou ativos de informação relacionados às atividades de tratamento de dados sob sua responsabilidade.

Cabe aos **Curadores de Dados**:

a) [Acrescente as atribuições do Curador de Dados, exemplos:]

b) seguir as diretrizes desta *Política* e garantir que os dados sob a sua responsabilidade atendam aos requisitos de governança de dados, especialmente os relativos à gestão dos metadados, segurança, qualidade e privacidade.

c) zelar pela proteção dos dados pessoais sob sua curadoria, nos termos da legislação e observadas as diretrizes internas e normativas e as orientações do **Encarregado de Dados Pessoais** do [Órgão/Entidade] ;

d) assegurar a gestão, manutenção e atualização contínua dos metadados — incluindo linhagem, integrações e descrições de negócio — de modo a garantir consistência semântica, correta interpretação, interoperabilidade e uso adequado dos dados sob sua curadoria

e) atualizar o **Catálogo de Dados do [Órgão/Entidade]** com as informações sobre as bases de dados e ativos sob sua responsabilidade.

Custodiante de Dados ou Curador de Dados

Os **Custodiantes de Dados** (no termo em inglês *Technical Data Steward*[35]) são representantes das **áreas de tecnologia**, em exercício de suas atividades no **[Órgão/Entidade]** ou em benefício delas, responsáveis por zelar pela gestão técnica, disponibilidade, integridade, operação e administração da infraestrutura e processos de tecnologia relacionados às bases de dados que estejam sob a sua custódia.

Cabe aos **Custodiantes de Dados**:

a) [Acrescente as atribuições do Custodiante de Dados, exemplos:]
b) gerenciar, controlar e operacionalizar as demandas tecnológicas que suportam as atividades de tratamento de dados, conforme requisitos definidos pelo **Curador de Dados**, em conformidade com esta *Política* .
c) atualizar o **Catálogo de Dados do [Órgão/Entidade]** com os metadados, informações técnicas e operacionais das bases de dados e ativos sob sua responsabilidade.

IX. GLOSSÁRIO, TERMOS E DEFINIÇÕES

[O Glossário funciona como uma base conceitual e normativa que sustenta toda a Política de Governança de Dados para definir os termos-chave, siglas ou conceitos que serão utilizados na política.
Recomenda-se utilizar como referência as definições apresentadas no Art. 5 da LGPD e no DAMA-DMBOK[36]].
Exemplo:

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

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

[35] DAMA-DMBOK2 (Data Management Body of Knowledge, 2ª edição) Data Governance – Types of Data Stewards
[36] DAMA-DMBOK2 (Data Management Body of Knowledge, 2ª edição) – *Reference and Master Data*

Referências

- [1]TCU Acórdão 457/2026 - Plenário https://portal.tcu.gov.br/uploads/noticias/pdf/2026/03/04/457-2026.pdf . Acesso em maio de 2026.
- [1]Autodiagnóstico SISP 2025 - https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/arquivos/relatorio_autodiagnostico_sisp_2025.pdf
- Nações Unidas. *Agenda 2030 e Objetivos de Desenvolvimento Sustentável* [brasil.un.org]
- PNUD. *Indicadores e governança para a Agenda 2030* [undp.org]
- Índice de Maturidade em Governança em Tecnologia da Informação do Sistema de Administração dos Recursos de Tecnologia da Informação – iGOVSISP 2025: Estatísticas do questionário 943362 ,
- DAMA-DMBOK2 (Data Management Body of Knowledge, 2ª edição)
- World Bank. *Digital Public Infrastructure and Development* [documents1...ldbank.org]
- OECD. *Governing with Artificial Intelligence*; *OECD AI Principles* [oecd.org], [oecd.org]
- FGV/UNU-EGOV. *Governança de dados no setor público* [repositorio.fgv.br]
- ITS Rio. *Infraestruturas Públicas Digitais no Brasil* [itsrio.org]