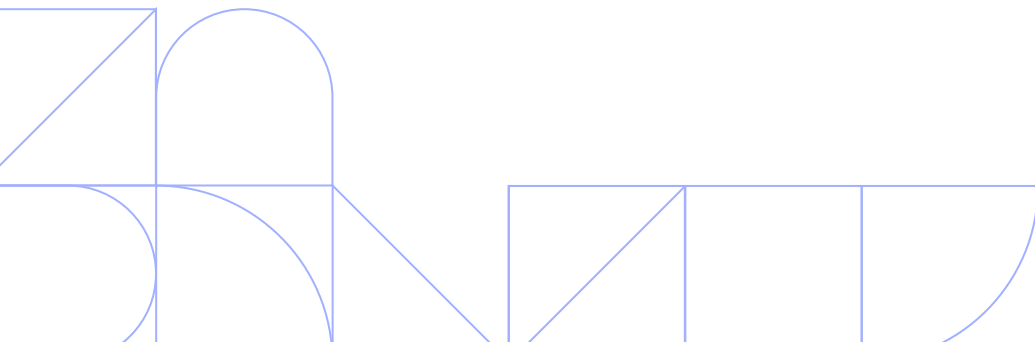




INFRAESTRUTURA NACIONAL DE DADOS:

Arquitetura Institucional para o Desenvolvimento Seguro e Integrado



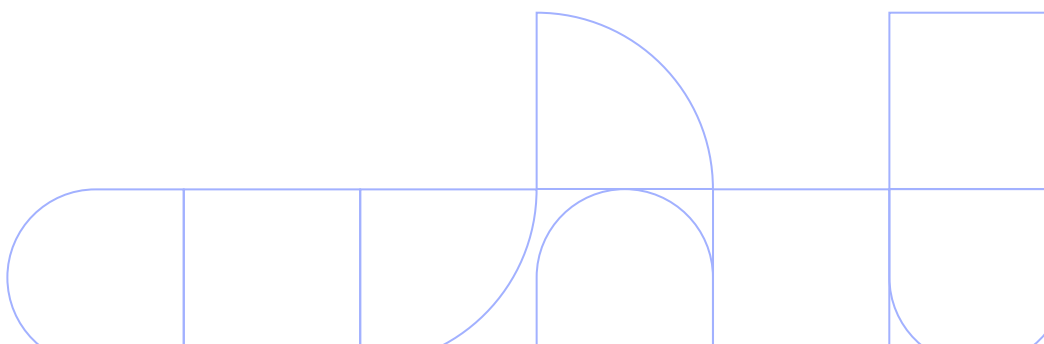




INFRAESTRUTURA NACIONAL DE DADOS:

Arquitetura Institucional para o
Desenvolvimento Seguro e Integrado

Brasília, junho de 2026





FICHA TÉCNICA

**Ministra de Estado da Gestão e da
Inovação em Serviços Públicos**

Esther Dweck

Secretário-Executivo

Cilair Rodrigues de Abreu

Secretário-Executivo Adjunto

Adauto Modesto Jr.

Secretário de Governo Digital

Rogério Souza Mascarenhas

**Secretária Adjunta
de Governo Digital**

Luanna Sant'Anna Roncaratti

**Diretor do Departamento de
Infraestrutura de Dados Públicos**

Marcos Moreira

Elaboração:

Consultor

Leonardo R. de Lima

Coordenação

Anna Carolina Venturini, Marina Luna,
Marcos Moreira, Daniela Nunes de
Menezes, Mariana Piccoli Lins Cavalcanti,
Ana Carolina Freitas de Andrade Saboia e
Bruno Carbonari Alves

Pessoas Entrevistadas

Marcos Moreira, Daniela Nunes de
Menezes, Renan Mendes Gaya Lopes dos
Santos, Eleidimar Odilia Isaque da Silva e
Leonardo Rodrigo Ferreira

Diretora Nacional do Projeto BRA/21/011

Wanessa Queiroz de Souza Oliveira

Coordenadora Nacional do Projeto BRA/21/011

Marcela Campos Martins

Equipe de apoio ao Projeto BRA/21/011

Fernanda Cléo, Jainara Martins
e Oziel Oliveira

O conteúdo deste material foi elaborado pelo consultor Leonardo R. de Lima no âmbito do **Projeto BRA 21/011 — Fortalecimento de capacidades para modernização e aprimoramento da gestão estatal da União**, firmado entre o Programa das Nações Unidas para Desenvolvimento (PNUD) e o Ministério da Gestão e da Inovação em Serviços Públicos (MGI). As visões e as conclusões apresentadas nesse documento não representam, necessariamente, a perspectiva do PNUD ou do MGI. Esta publicação contou com suporte editorial do PNUD no âmbito desse projeto.

SUMÁRIO

RESUMO EXECUTIVO	8
INTRODUÇÃO	13
PARTE I — GOVERNO DIGITAL E SETOR PÚBLICO ORIENTADO POR DADOS	17
1. DO GOVERNO ELETRÔNICO AO DIGITAL	17
2. TENDÊNCIAS GLOBAIS: POLÍTICAS PÚBLICAS ORIENTADAS POR DADOS	21
PARTE II — INFRAESTRUTURA NACIONAL DE DADOS (IND)	23
3. CONSTRUÇÃO DE UMA INFRAESTRUTURA PÚBLICA DE DADOS BRASILEIRA	23
3.1. Limites do Modelo Descentralizado de Gestão de Dados	23
3.2. Institucionalização da Infraestrutura Nacional de Dados no Brasil	25
4. GOVERNANÇA	28
4.1. Evolução do Marco Normativo: da Transparência à Governança Sistêmica	29
4.2. A Política de Governança de Dados: Objetivos e Inovações do Novo Marco	30
4.3. Operacionalização: O Programa de Governança de Dados (PGDADOS)	32
4.4. Monitoramento e Evolução: Modelo de Maturidade de Dados (MMD)	33
5. INTEROPERABILIDADE	35
5.1. O Modelo Brasileiro: Descentralizado e Interoperável	35
5.2. Conecta gov.br: A Plataforma Nacional de Integração de Dados	37
5.3. Registros de Referência: Fonte Única da Verdade	38
5.4. Impacto Socioeconômico e Valor Público	39
6. CATÁLOGO NACIONAL DE DADOS	41
6.1. Arranjos Institucionais e Papéis na Governança de Dados	43
6.2. Padrões de Metadados e Interoperabilidade Semântica	43

6.3. Monitoramento e Qualidade dos Metadados	44
6.4. Integração Sistêmica do Catálogo na Infraestrutura Nacional de Dados	45
7. PRIVACIDADE E SEGURANÇA	46
7.1. Programa de Privacidade e Segurança da Informação (PPSI)	46
7.2. Prevenção e Resposta a Incidentes	49
7.3. Capacitação e Cultura Organizacional	50
7.4. Monitoramento e Melhoria Contínua	51
8. INFORMAÇÕES GEOESPACIAIS	52
8.1. Articulação entre IND e Infraestrutura Nacional de Dados Espaciais (INDE)	52
8.2. Arranjo Institucional e Responsabilidades	53
9. INTELIGÊNCIA ARTIFICIAL	54
9.1. Núcleo de Inteligência Artificial	55
9.2. Observatório do Núcleo de IA	57
10. AMBIENTE TECNOLÓGICO	58
10.1. Data Centers	58
10.2. Nuvem	59
10.3. Conectividade e Infovia Brasília	60
11. DECISÃO BASEADA EM DADOS	62
12. ECOSSISTEMA DE DADOS	64
13. A INFRAESTRUTURA NACIONAL DE DADOS COMO CAPACIDADE ESTATAL	66
14. EXPERIÊNCIAS INTERNACIONAIS COMPARADAS	68
REFERÊNCIAS	75

RESUMO EXECUTIVO

A Infraestrutura Nacional de Dados (IND) consolida-se como o pilar estruturante da capacidade estatal brasileira na era digital. Definida como um arranjo integrado de normas, arquiteturas e ativos de informação, a IND busca substituir um modelo fragmentado de gestão da informação por um ambiente em que os dados possam ser compartilhados de forma responsável, evitando retrabalho, reduzindo custos e melhorando a prestação de serviços à população.

Fundamentos e Modelo Internacional – Governo Digital e Infraestrutura Pública Digital

No plano internacional, organismos como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) definem governo digital como a integração estratégica das tecnologias digitais aos processos de modernização do Estado, com vistas à geração de valor público, ao fortalecimento da governança e ao uso sistemático de evidências na formulação de políticas públicas. Esse entendimento representa uma mudança estrutural em relação a abordagens centradas exclusivamente na informatização de processos, ao reposicionar o digital como componente da capacidade estatal.

Avaliações comparadas indicam que essa transformação tem sido acompanhada pela adoção de estratégias nacionais transversais, voltadas à integração de sistemas, dados e processos em escala governamental. Nesse contexto, o governo digital deixa de ser compreendido como um conjunto de serviços online e passa a operar como instrumento estruturante da ação pública, capaz de sustentar interoperabilidade, coordenação interinstitucional e reutilização de ativos digitais em múltiplas políticas públicas.

Esse enquadramento converge com o reconhecimento dos dados como infraestrutura pública essencial. Instituições como a OCDE, o Banco Mundial e o Programa das Nações Unidas para o Desenvolvimento (PNUD) passaram a tratar dados, sistemas de identificação digital, plataformas de pagamento e mecanismos de compartilhamento de informações como componentes críticos para o funcionamento do Estado contemporâneo. Essa abordagem, frequentemente denominada Infraestrutura Pública Digital (*Digital Public Infrastructure – DPI*), refere-se a sistemas compartilhados, seguros e interoperáveis, concebidos como camadas comuns reutilizáveis, capazes de reduzir custos de transação e ampliar a capacidade de coordenação estatal.

Evolução da Política de Dados no Brasil e a Institucionalização da IND

A trajetória brasileira de modernização administrativa baseada no uso estratégico das tecnologias digitais teve início nos anos 2000, com a informatização de processos, a ampliação da oferta de serviços pela internet e a padronização técnica de funções administrativas. Ao longo da década de 2010, essa agenda evoluiu para incorporar princípios de transparência, participação social e abertura de dados, impulsionada por marcos como a Lei de Acesso à Informação, a criação da Infraestrutura Nacional de Dados Abertos e do Portal Brasileiro de Dados Abertos.

A partir de 2016, com a instituição da Política e da Estratégia de Governança Digital, consolidou-se a transição para o paradigma de Governo Digital, que reposiciona os serviços públicos a partir da perspectiva do usuário e prioriza a simplificação e a integração. Paralelamente, o Estado brasileiro acumulou extensas infraestruturas setoriais de dados, ampliando sua capacidade de produção e armazenamento de informações, ainda que organizadas sob lógicas predominantemente verticais.

Um marco decisivo ocorreu em 2019, com a edição do Decreto nº 10.046, que instituiu a governança do compartilhamento de dados como política pública estruturada, definiu responsabilidades institucionais e estabeleceu o Cadastro Base do Cidadão como referência para identificação unívoca, em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD). Essa evolução convergiu com o enquadramento internacional das Infraestruturas Públicas Digitais e, em 2024, o Brasil formalizou sua adesão a essa agenda, criando as condições institucionais para a consolidação da IND como política pública integrada no âmbito da Estratégia de Governo Digital 2024–2027.

Nesse contexto, a IND passou a ser concebida como uma infraestrutura que combina componentes técnicos — como plataformas de interoperabilidade, catálogos de metadados, serviços de integração e ambientes computacionais — com mecanismos de governança, definição de responsabilidades institucionais e desenvolvimento de capacidades organizacionais. Esse arranjo preserva a custódia descentralizada dos dados, ao mesmo tempo em que fortalece a coordenação transversal entre órgãos e níveis de governo, orientando-se por princípios como a coleta única de informações (*once-only*), a definição de fontes únicas de verdade e o reuso seguro e legítimo dos dados para fins públicos.

Estrutura e Eixos da IND

A IND organiza-se como um arranjo integrado de capacidades institucionais, técnicas e normativas, estruturado em eixos que operam de forma complementar e interdependente. Esses eixos não constituem iniciativas isoladas, mas componentes de uma arquitetura comum voltada à governança, à integração e ao uso estratégico dos dados públicos em escala governamental. Em conjunto, eles sustentam a transformação de dados dispersos em ativos públicos reutilizáveis, seguros e orientados à produção de valor público.

A IND estrutura-se em oito eixos principais:

- **Governança**, responsável por estabelecer regras, responsabilidades institucionais, instâncias decisórias e mecanismos de monitoramento para a gestão do ciclo de vida dos dados no setor público;
- **Interoperabilidade**, voltada à integração estruturada de sistemas governamentais, viabilizando o compartilhamento seguro e padronizado de dados, com preservação da custódia descentralizada;
- **Catálogo Nacional de Dados**, que assegura a visibilidade, a organização e a previsibilidade sobre os ativos informacionais do Estado, apoiando o compartilhamento, o reuso e a abertura de dados;
- **Privacidade e Segurança**, dedicado à proteção de dados pessoais, à segurança da informação e à resiliência dos sistemas públicos, em consonância com padrões nacionais e internacionais;
- **Informações Geoespaciais**, que integra a dimensão territorial aos dados administrativos, fortalecendo o planejamento, a coordenação e a avaliação de políticas públicas;
- **Inteligência Artificial**, que organiza a adoção coordenada de soluções de IA no setor público, conectando demanda governamental, infraestrutura compartilhada, fomento e capacitação;
- **Ambiente Tecnológico**, que provê a base técnica para a operação integrada e segura dos sistemas governamentais, incluindo diretrizes de computação em nuvem, padrões de serviço e gestão de riscos tecnológicos;
- **Decisão Baseada em Dados**, que materializa o uso efetivo dos dados nos processos decisórios, operacionais e de prestação de serviços, convertendo integração e governança em aplicações concretas voltadas ao cidadão.

Essa estrutura permite que a IND opere simultaneamente como infraestrutura transversal do Estado e como base adaptável para aplicações setoriais e temáticas, assegurando coerência institucional, escalabilidade e sustentabilidade no uso de dados públicos.

Resultados Observáveis e Efeitos sobre a Capacidade Estatal

A implementação da IND produziu resultados observáveis em três níveis — entregas institucionais, mudanças funcionais e efeitos sistêmicos sobre a capacidade estatal.

No plano das entregas institucionais, a IND consolidou um conjunto articulado de instrumentos que estruturaram a governança e a integração dos dados públicos. Esse arranjo incluiu a institucionalização da Política de Governança de Dados, com adoção obrigatória do Programa de Governança de Dados (PGDADOS) nos órgãos federais; a definição de Registros de Referência como fontes oficiais e autoritativas; e a incorporação do Modelo de Maturidade de Dados (MMD) como mecanismo permanente de avaliação institucional.

Em paralelo, a consolidação do Conecta Gov.br como plataforma nacional de interoperabilidade, baseada em APIs com controle de acesso, rastreabilidade e preservação da custódia descentralizada, estabeleceu as bases técnicas para o compartilhamento estruturado de dados em escala governamental.

Esse esforço foi complementado pela estruturação do Catálogo Nacional de Dados como instrumento de governança e transparência, que, até dezembro de 2025, reunia 15.605 conjuntos de dados, 103.498 recursos descritos e 286 organizações públicas, com 74% das cerca de 9 mil bases federais previstas já abertas.

No campo da proteção da informação, a implementação do Programa de Privacidade e Segurança da Informação (PPSI), associada à criação do Centro Integrado de Segurança Cibernética (CISC Gov.br) e do Centro de Excelência em Privacidade e Segurança (CEPS Gov.br), consolidou frameworks nacionais comuns de segurança e proteção de dados.

Adicionalmente, a estruturação do Núcleo de Inteligência Artificial, com portfólio de 50 projetos previstos até 2026, e a adoção de uma estratégia de infraestrutura compartilhada para IA — apoiada por investimentos de aproximadamente R\$ 6,5 bilhões no âmbito do Plano Brasileiro de Inteligência Artificial e pela capacitação prevista de 115 mil servidores públicos — ampliaram as capacidades institucionais para a adoção coordenada de tecnologias emergentes.

Essas entregas institucionais viabilizaram mudanças funcionais mensuráveis no funcionamento da administração pública. A integração efetiva de sistemas governamentais em escala nacional permitiu a aplicação operacional do princípio do *once-only*, reduzindo duplicidades cadastrais, exigências redundantes e retrabalho administrativo.

O reuso sistemático de dados entre órgãos e políticas públicas ampliou a visibilidade e a previsibilidade sobre os ativos informacionais do Estado e sustentou a incorporação do uso de dados aos processos decisórios e operacionais.

No ecossistema do Gov.br, esse movimento materializou-se em aplicações de alta capilaridade, como mecanismos de recomendação de serviços, notificações personalizadas e a Caixa Postal Digital.

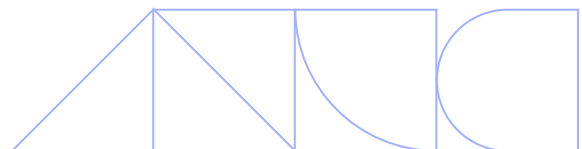
No campo da interoperabilidade, o Conecta Gov.br registrou aproximadamente 2,25 bilhões de transações de dados desde 2020, evidenciando a operação contínua e em larga escala da integração entre sistemas públicos.

De forma complementar, o uso efetivo do Catálogo Nacional de Dados é demonstrado por mais de 100 mil usuários registrados e 82 reúsos documentados, indicando localização e reaproveitamento ativo dos dados catalogados.

Como efeitos sistêmicos, a integração de dados consolidou-se como capacidade estatal permanente, traduzindo-se em ganhos estruturais de eficiência administrativa, previsibilidade institucional e qualidade dos serviços públicos.

Entre 2020 e 2025, a interoperabilidade viabilizada pela IND gerou economia administrativa acumulada estimada em R\$ 12,98 bilhões, associada à eliminação de redundâncias, à automação de fluxos informacionais e à redução de retrabalho, dos quais R\$ 9,52 bilhões desde a criação formal da IND em 2024.

No conjunto, tais resultados evidenciam a conversão de capacidades antes dispersas em um arranjo sistêmico de coordenação governamental, com fortalecimento da gestão da informação, integração entre governança, privacidade, segurança e tecnologias, redução do ônus informacional sobre cidadãos e setor público e aumento da confiabilidade e da resiliência informacional do Estado, caracterizando a transição efetiva para um modelo de Estado orientado por dados.



INTRODUÇÃO

A Infraestrutura Nacional de Dados (IND) parte da identificação da necessidade de tratar dados como base permanente para a coordenação de políticas públicas, para a integração de serviços e para a produção de respostas estatais em contextos de elevada complexidade social, econômica e territorial.

Ao reconhecer os dados como infraestrutura, o Estado assume que a transformação digital não se esgota na digitalização de processos ou na ampliação de canais eletrônicos de atendimento. Ela exige uma base informacional capaz de conectar políticas, territórios e instituições, permitindo que informações produzidas em diferentes áreas possam ser utilizadas de forma legítima, segura e coordenada em múltiplas frentes da ação pública.

Essa compreensão resulta de um processo acumulativo. Ao longo da última década, o Brasil ampliou o uso de registros administrativos, cadastros e sistemas digitais em áreas como saúde, educação, assistência social, trabalho, tributação e planejamento territorial. Esses avanços fortaleceram capacidades setoriais, mas também tornaram mais visível um limite estrutural: políticas públicas cada vez mais interdependentes continuavam apoiadas em bases de dados organizadas de forma fragmentada, com padrões distintos e baixo grau de articulação entre sistemas.

Nesse contexto, a integração de dados deixou de ser apenas uma questão técnica e passou a ser compreendida como problema de coordenação institucional. Tornou-se claro que a capacidade do Estado de operar políticas complexas, responder a crises, monitorar resultados e focalizar intervenções depende não apenas da existência de dados, mas da forma como esses dados circulam, são governados e são convertidos em conhecimento para a ação pública.

O Brasil tem se posicionado de forma consistente na vanguarda das políticas, marcos normativos e soluções tecnológicas voltadas à gestão e ao uso estratégico de dados no setor público. Ao longo das últimas duas décadas, o país avançou simultaneamente na consolidação de um arcabouço robusto de gestão e proteção de dados, na digitalização em larga escala dos serviços públicos e no fortalecimento da comunicação entre sistemas governamentais.

Os resultados dessa trajetória têm sido reconhecidos no cenário internacional. No índice global de maturidade em governo digital (GovTech Index), elaborado pelo Banco Mundial, o Brasil ocupa a quarta colocação entre os países avaliados, refletindo o grau de institucionalização de suas políticas de governo digital, a escala da oferta de serviços digitais e o uso estratégico de tecnologias para a modernização do setor público (BANCO MUNDIAL, 2025).

Esse movimento nacional ocorre em paralelo a um reposicionamento do debate internacional sobre transformação digital. Em diferentes países, experiências de identidade digital, interoperabilidade de sistemas e plataformas públicas passaram a ser compreendidas como partes de um mesmo arranjo: as chamadas Infraestruturas Públicas Digitais (*Digital Public Infrastructure – DPI*), que tratam dados, interoperabilidade e confiança digital como camadas estruturantes da capacidade estatal e do desenvolvimento sustentável. Esse enquadramento reforça a ideia de que a construção de Estados digitais eficazes depende de infraestruturas compartilhadas, reutilizáveis e orientadas ao interesse público.

É nesse ambiente que a IND é consolidada como política pública integrada, articulando novas soluções e instrumentos existentes sob um desenho institucional orientado à coordenação sistêmica dos fluxos de dados no setor público. A IND não substitui sistemas setoriais nem centraliza bases de dados, mas organiza as condições para que esses sistemas operem como parte de um mesmo ecossistema estatal, com padrões comuns, responsabilidades definidas e mecanismos permanentes de interoperabilidade, proteção e uso analítico da informação.

Essa arquitetura se estrutura em oito eixos que operam de forma integrada:

- Governança, que organiza responsabilidades e coordenação institucional;
- Interoperabilidade, que permite a circulação padronizada de informações entre sistemas;
- Catálogo Nacional de Dados, que torna visíveis e utilizáveis os ativos informacionais do Estado;
- Privacidade e Segurança, que asseguram salvaguardas e proteção de direitos;
- Informações Geoespaciais, que conectam políticas públicas à dimensão territorial;
- Inteligência Artificial, que estrutura o uso institucional de soluções algorítmicas baseadas em dados governados;
- Ambiente Tecnológico, que sustenta a operação em escala;
- Decisão Baseada em Dados, que transforma integração informacional em capacidade efetiva de gestão, monitoramento e avaliação de políticas.

Esses eixos traduzem a etapa presente de institucionalização da IND, sem prejuízo de sua ampliação progressiva à medida que novas capacidades e arranjos venham a ser incorporados ao ecossistema de dados governamentais. Eles não operam de forma isolada e a força da IND reside precisamente nessa integração: cada componente reforça os demais, criando um sistema no qual a circulação de dados é tecnicamente viável, institucionalmente legítima e orientada a resultados de política pública.

Este documento analisa a IND como elemento da estratégia brasileira de fortalecimento das capacidades estatais na era digital. Partindo de seus fundamentos conceituais e de sua trajetória de institucionalização, o relatório descreve a organização da IND em eixos estruturantes, seus principais instrumentos operacionais e sua aplicação em ecossistemas de políticas públicas, com atenção especial aos mecanismos de governança, interoperabilidade, segurança e uso analítico.

A metodologia adotada baseou-se em um estudo de caso aprofundado da Infraestrutura Nacional de Dados, combinado com revisão bibliográfica especializada. A revisão incluiu documentos internacionais de referência no debate sobre desenvolvimento digital, governança de dados e capacidades estatais, produzidos por organismos multilaterais e instituições reconhecidas no campo da economia digital e da administração pública. No plano nacional, foram analisados documentos oficiais do governo federal, incluindo estratégias, planos, normas, leis, decretos, portarias e demais atos normativos relacionados à política de dados, governo digital, privacidade e segurança da informação.

O estudo de caso da IND foi desenvolvido a partir da articulação entre a literatura oficial e entrevistas semiestruturadas realizadas com dirigentes e gestores diretamente envolvidos na concepção, implementação e operação da infraestrutura. Foram entrevistados o Sr. Marcos Moreira, Diretor-Geral da Infraestrutura Nacional de Dados; a Sra. Daniela Nunes de Menezes, Coordenadora-Geral de Governança de Dados; o Sr. Renan Mendes Gaya Lopes dos Santos, Diretor do Departamento de Estruturação de Dados para Públicos Digitais; a Sra. Eleidimar Odilia Isaque da Silva, Diretora do Departamento de Serviços Públicos Digitais; e o Sr. Leonardo Rodrigo Ferreira, Diretor da Diretoria de Privacidade e Segurança da Informação.

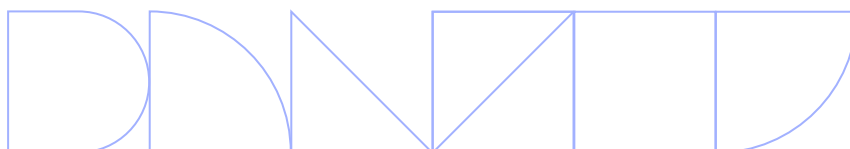
As entrevistas foram organizadas de forma individualizada, tomando como referência os eixos estruturantes da IND e as responsabilidades institucionais de cada área. O método de análise concentrou-se na identificação do ciclo de políticas públicas associado à Infraestrutura Nacional de Dados, abrangendo as etapas de definição do problema, formulação da política, implementação, monitoramento, avaliação e apoio à tomada de decisão. A partir desse enquadramento analítico, foram aprofundados, de maneira orientada, temas específicos considerados relevantes para a compreensão do funcionamento da IND, de seus desafios institucionais e de seus mecanismos de coordenação interorganizacional.

Adicionalmente, as entrevistas permitiram incorporar experiências internas relacionadas tanto ao processo de elaboração dos instrumentos da IND quanto à consolidação progressiva da infraestrutura como política pública transversal. As contribuições dos técnicos da Secretaria de Governo Digital (SDG) e das equipes da Infraestrutura Nacional de Dados foram fundamentais para contextualizar decisões institucionais, esclarecer arranjos operacionais e qualificar a análise sobre a aplicação prática da IND no ecossistema de políticas públicas federais.

Com base na combinação das duas abordagens metodológicas — revisão bibliográfica e estudo de caso —, o relatório estrutura-se em duas partes, subdivididas em 13 capítulos. A primeira parte dedica-se à conceituação e à contextualização das políticas públicas relacionadas a dados e à transformação digital do Estado, com base na literatura nacional e internacional, incluindo a exposição de experiências internacionais análogas à Infraestrutura Nacional de Dados identificadas ao longo da pesquisa.

A segunda parte concentra-se na experiência brasileira com a IND. Nessa seção, apresenta-se o histórico de identificação do problema público, o processo de idealização, implementação e consolidação da infraestrutura, bem como os instrumentos institucionais prévios que foram fundamentais para sua criação. Em seguida, o documento examina o estado da arte da IND, aprofundando suas contribuições a partir da análise detalhada de cada um de seus eixos estruturantes, com um capítulo dedicado a cada componente da infraestrutura.

Por fim, o capítulo final, a partir da consolidação analítica dos conteúdos apresentados ao longo do relatório, sistematiza a experiência da Infraestrutura Nacional de Dados como elemento central no processo de consolidação e ampliação das capacidades estatais digitais no Brasil. O capítulo examina de que maneira a IND contribui para o aumento da eficiência administrativa, para o fortalecimento dos processos decisórios baseados em dados e para a melhoria da oferta e da qualidade dos serviços públicos, situando essa experiência no contexto mais amplo da transformação digital do Estado brasileiro.



PARTE I – GOVERNO DIGITAL E SETOR PÚBLICO ORIENTADO POR DADOS

1. DO GOVERNO ELETRÔNICO AO DIGITAL

A transformação digital do setor público tem evoluído de iniciativas focadas na informatização de processos administrativos para abordagens mais amplas, integradas e orientadas por dados. Enquanto o chamado governo eletrônico (*e-government*) concentrou-se inicialmente na oferta de serviços por meios digitais, o conceito de governo digital incorporou o uso estratégico de tecnologias e dados como elementos estruturantes da ação estatal.

Nesse paradigma, o digital não é tratado como um componente acessório, mas como parte integrante da formulação, implementação e avaliação de políticas públicas. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define governo digital como o uso de tecnologias digitais integrado às estratégias de modernização do Estado, com o objetivo de gerar valor público, melhorar serviços, fortalecer a governança e apoiar a formulação de políticas baseadas em evidências (OCDE, 2014).

Essa mudança de enfoque tem sido acompanhada pela adoção de estratégias nacionais transversais, que buscam integrar sistemas, dados e processos em escala governamental, substituindo abordagens fragmentadas e setoriais (ONU, 2022). Nesse contexto, os dados passam a ocupar posição central, não apenas como subproduto da atividade administrativa, mas como insumo essencial para a tomada de decisão, a integração institucional e a prestação de serviços públicos.

A consolidação do governo digital, portanto, depende da capacidade dos Estados de estruturar ambientes nos quais os dados possam trafegar de forma segura, padronizada e interoperável, sustentando políticas públicas mais coordenadas e serviços mais eficientes.

O reconhecimento dos dados como infraestrutura pública representa uma inflexão conceitual relevante nas políticas de transformação digital. Organismos multilaterais passaram a tratar dados, sistemas de identificação digital, plataformas de pagamentos e mecanismos de compartilhamento de informações como componentes de uma infraestrutura essencial para o funcionamento do Estado e da economia digital (BANCO MUNDIAL, 2021; PNUD, 2023).

Essa abordagem, frequentemente denominada Infraestrutura Pública Digital (*Digital Public Infrastructure – DPI*), refere-se a sistemas digitais compartilhados, seguros e interoperáveis, que permitem a oferta de serviços públicos e privados em escala, promovendo inclusão, eficiência e inovação (BANCO MUNDIAL, 2021). Diferentemente de soluções isoladas, a DPI busca criar camadas comuns reutilizáveis por múltiplos serviços e políticas públicas.

Nesse enquadramento, os dados assumem papel análogo ao de infraestruturas físicas tradicionais, como redes de transporte ou energia, ao possibilitar conexões, reduzir custos de transação e viabilizar novas formas de organização institucional. A qualidade, disponibilidade e governança dos dados passam a influenciar diretamente a capacidade do Estado de executar políticas, responder a crises e planejar ações de longo prazo (PNUD, 2023).

Tratar dados como infraestrutura implica reconhecer que sua gestão não pode ser delegada exclusivamente a áreas técnicas, mas deve integrar a agenda estratégica do governo, envolvendo decisões sobre padrões, governança, financiamento, segurança e sustentabilidade institucional.

A OCDE reforça esse entendimento ao destacar que governos mais eficazes são aqueles capazes de tratar dados, interoperabilidade e coordenação digital como capacidades estruturais do Estado, e não como iniciativas setoriais de tecnologia da informação. De acordo com o *Government at a Glance 2025*, a consolidação de arranjos integrados de governança de dados e de infraestruturas digitais compartilhadas está associada a ganhos de eficiência administrativa, melhoria na prestação de serviços públicos e fortalecimento da confiança institucional, especialmente em contextos de elevada complexidade governamental (OCDE, 2025).

O desenvolvimento do governo digital pressupõe a adoção de uma arquitetura institucional baseada em componentes compartilhados e princípios de integração, que reorganizam a forma como o Estado produz, compartilha e utiliza dados e serviços. A noção de Governo como Plataforma (GaaP) constitui um dos pilares conceituais do governo digital. Nessa perspectiva, o Estado fornece componentes compartilhados — como dados, interfaces de programação (APIs), cadastros-base e serviços transversais — que podem ser reutilizados por diferentes órgãos e por atores externos, como empresas, universidades e organizações da sociedade civil (OCDE, 2020). Esse modelo favorece uma abordagem integrada de governo (*whole-of-government*), ao reduzir a fragmentação institucional e promover a comunicação entre sistemas e diferentes níveis administrativos.

De forma complementar, o princípio do *once-only* (apenas uma vez) estabelece um parâmetro operacional para a oferta de serviços públicos digitais. De acordo com esse conceito, cidadãos e empresas não devem ser solicitados a fornecer repetidamente as mesmas informações a diferentes entidades governamentais. Uma vez que um dado padrão — como identidade, endereço ou situação cadastral — seja informado a uma autoridade pública, a administração deve ser capaz de reutilizá-lo internamente, sempre que necessário e autorizado, sem solicitar novamente ao usuário.

A aplicação desse princípio pressupõe a existência de sistemas interoperáveis, marcos adequados de proteção de dados e mecanismos claros de consentimento, contribuindo para a redução da burocracia, a simplificação dos processos administrativos e o fortalecimento de serviços centrados no usuário.

Plataformas nacionais de dados abertos e barramentos de interoperabilidade exemplificam esse modelo, ao permitir que diferentes sistemas acessem informações por meio de padrões unificados, com controle de acesso centralizado e monitoramento das transações. Além de favorecer a integração institucional, o modelo de plataforma amplia o potencial de reutilização dos dados públicos para fins econômicos e sociais. Dados governamentais abertos e bem estruturados têm sido utilizados para o desenvolvimento de aplicações nas áreas de mobilidade, saúde, educação e finanças, contribuindo para a criação de novos serviços e modelos de negócio.

No entanto, a efetividade do governo como plataforma depende de arranjos de governança que assegurem qualidade dos dados, definição clara de responsabilidades, proteção de informações sensíveis e sustentabilidade operacional das infraestruturas compartilhadas.

À medida que essas infraestruturas habilitadoras e princípios de integração se consolidam, o foco do governo digital se desloca progressivamente para o uso estratégico dos dados na formulação e implementação de políticas públicas, caracterizando o setor público orientado por dados (*data-driven public sector*). Nesse modelo, os dados gerados e compartilhados pelo Estado são utilizados de forma sistemática ao longo de todo o ciclo de políticas públicas, desde a identificação de desafios sociais até o monitoramento e a avaliação de resultados (OCDE, 2019).

Nesse arranjo, os dados contribuem para:

- diagnóstico mais preciso de problemas públicos;
- formulação de políticas baseadas em evidências;
- monitoramento contínuo de programas e serviços;
- avaliação de impactos e retroalimentação do processo decisório.

A institucionalização desse uso exige não apenas disponibilidade de dados, mas também mecanismos de governança que garantam sua qualidade, interoperabilidade e uso ético. Sem essas condições, o potencial analítico dos dados permanece limitado, e decisões continuam a ser tomadas com base em informações fragmentadas ou incompletas.

Evidências internacionais indicam que países que investem em sistemas integrados de dados e em capacidades analíticas avançadas conseguem responder com maior agilidade a crises, alocar recursos públicos de forma mais eficiente e aprimorar políticas sociais, especialmente em contextos de elevada complexidade institucional (BANCO MUNDIAL, 2021).

Assim, a infraestrutura de dados não apenas apoia a gestão administrativa, mas passa a influenciar diretamente a capacidade do Estado de aprender com suas próprias políticas e de ajustar intervenções ao longo do tempo.

À medida que o uso de dados se expande no setor público, emergem riscos e desafios que demandam respostas institucionais e mecanismos de governança.

A ampliação da coleta, do compartilhamento e da reutilização de dados aumenta a exposição a incidentes de segurança e a violações de privacidade, exigindo investimentos contínuos em proteção técnica, gestão de riscos e capacidades de prevenção e resposta a incidentes.

Paralelamente, o uso crescente de algoritmos e sistemas automatizados no desenho e na implementação de políticas públicas reforça a necessidade de salvaguardas éticas, transparência e mecanismos de supervisão adequados. Sem esses instrumentos, há o risco de reprodução de vieses, discriminação e decisões opacas, com impactos negativos sobre a confiança pública e a equidade das políticas.

Outro desafio recorrente é a fragmentação institucional e a resistência organizacional à padronização e ao compartilhamento de informações. A superação desses obstáculos depende de coordenação central, liderança política e incentivos institucionais claros para a adoção de práticas de governança de dados.

Adicionalmente, a expansão de serviços públicos baseados em dados pode aprofundar desigualdades existentes caso não seja acompanhada por políticas de inclusão digital, conectividade e letramento digital. A governança responsável dos dados deve, portanto, incorporar uma perspectiva de inclusão, garantindo que os benefícios da transformação digital sejam amplamente distribuídos.

Quando sustentada por arranjos adequados de governança, a consolidação dos dados como infraestrutura pública gera benefícios sistêmicos que se manifestam em múltiplas dimensões da gestão pública e do desenvolvimento socioeconômico. Do ponto de vista administrativo, a integração de bases de dados reduz redundâncias, minimiza retrabalho e viabiliza a automação de processos, resultando em ganhos de eficiência, melhoria na coordenação interinstitucional e redução de custos operacionais (OCDE, 2019). A interoperabilidade entre sistemas também facilita a oferta de serviços públicos integrados, reduzindo a necessidade de que cidadãos e empresas forneçam repetidamente as mesmas informações a diferentes órgãos.

No plano social, infraestruturas de dados bem estruturadas permitem o desenho de políticas mais focalizadas, proativas e centradas no usuário. Exemplos incluem a identificação automática de elegibilidade para benefícios sociais, o envio de comunicações personalizadas e a antecipação de demandas por serviços públicos, contribuindo para maior efetividade e equidade das intervenções estatais (ONU, 2022).

Do ponto de vista econômico, a disponibilização de dados públicos abertos e padronizados favorece o desenvolvimento de ecossistemas de inovação, ao estimular a criação de aplicações, serviços e modelos de negócio por atores externos ao governo. Esses ecossistemas geram efeitos positivos sobre a competitividade, a produtividade e a criação de valor, reforçando o papel dos dados como ativo estratégico para o desenvolvimento.

Adicionalmente, a transparência associada à abertura, à integração e ao uso responsável dos dados contribui para o fortalecimento da confiança pública, ao ampliar as possibilidades de controle social, participação cívica e acompanhamento das políticas públicas. Dessa forma, a infraestrutura de dados consolida-se como um elemento central para uma governança pública mais eficiente, inclusiva e orientada a resultados.

2. TENDÊNCIAS GLOBAIS: POLÍTICAS PÚBLICAS ORIENTADAS POR DADOS

As tendências tecnológicas não se restringem ao plano técnico ou conceitual, mas vêm se traduzindo em transformações concretas na organização e no funcionamento dos Estados. De acordo com a *UNE-Government Survey 2022*, publicada pela Nações Unidas, praticamente todos os 193 Estados-membros possuem alguma iniciativa de digitalização governamental em curso, ainda que apresentem níveis distintos de maturidade institucional, tecnológica e normativa. Observa-se, nesse contexto, uma transição progressiva de abordagens fragmentadas — nas quais o uso intensivo de dados se restringia a poucas agências pioneiras — modelos integrados de governo (*whole-of-government*) e, em alguns casos, de toda a sociedade (*whole-of-society*).

Essa evolução reflete o reconhecimento crescente de que a governança de dados deixou de ser um tema predominantemente técnico, circunscrito às áreas de tecnologia da informação, para ocupar posição central na agenda estratégica dos governos. O uso estruturado e responsável de dados passou a ser compreendido como um fator habilitador para a melhoria dos serviços públicos, o fortalecimento da capacidade estatal e a aceleração do progresso em direção aos Objetivos de Desenvolvimento Sustentável (ODS).

A OCDE reforça esse diagnóstico por meio de instrumentos como o *Digital Government Index* e de estudos analíticos, a exemplo de *The Path to Becoming a Data-Driven Public Sector* (2019), que evidenciam a disseminação de estratégias nacionais de dados e de transformação digital com forte ênfase na integração, no compartilhamento e no uso estratégico de informações no setor público.

Outra tendência recorrente diz respeito à criação ou ao fortalecimento de arranjos centrais de coordenação da governança de dados. Diversos países têm instituído agências, unidades ou funções de liderança com mandatos formais para definir padrões, arquiteturas de referência e diretrizes nacionais, com o objetivo de reduzir a fragmentação histórica dos ecossistemas digitais governamentais. Exemplos incluem iniciativas observadas na Austrália, Estônia, Dinamarca, Itália e Colômbia, bem como modelos complementares adotados pelo Canadá, pelo Reino Unido e pela França.

Paralelamente, observa-se uma tendência crescente de investimento em infraestruturas públicas digitais de larga escala, especialmente em países que buscam acelerar a inclusão social e econômica. Experiências como as da Índia e da Coreia do Sul ilustram como plataformas nacionais de identificação digital, pagamentos e compartilhamento de dados podem gerar efeitos sistêmicos positivos, ampliando o acesso a serviços, estimulando a inovação e fortalecendo a capacidade do Estado de implementar políticas em escala.

Em conjunto, essas tendências globais demonstram que tratar dados como infraestrutura pública não é apenas um conceito teórico, mas sim uma prática viável que traz ganhos concretos de eficiência e qualidade governamental.

Em consonância com esse padrão, o Brasil tem orientado sua estratégia institucional para a consolidação de mecanismos voltados à integração, padronização e coordenação das iniciativas de dados em escala governamental. Esse processo de transformação tem sido progressivamente organizado em torno da IND, concebida como um conjunto articulado de instrumentos, padrões e mecanismos de coordenação destinados a promover a interoperabilidade, a governança e o uso responsável de dados no setor público.

A IND constitui, assim, o eixo estruturante da abordagem brasileira para a consolidação de um Estado orientado por dados. Sua configuração institucional e operacional, bem como seus desafios e oportunidades, serão analisados de forma detalhada nos capítulos subsequentes deste relatório.

PARTE II – INFRAESTRUTURA NACIONAL DE DADOS (IND)

3. CONSTRUÇÃO DE UMA INFRAESTRUTURA PÚBLICA DE DADOS BRASILEIRA

As transformações descritas evidenciam que o avanço do governo digital depende menos da adoção isolada de tecnologias e mais da capacidade dos Estados de organizar, coordenar e governar o uso de dados em escala sistêmica. Nesse contexto, a superação de arranjos fragmentados, a definição de responsabilidades institucionais e a construção de arquiteturas comuns de interoperabilidade e proteção de direitos tornam-se condições centrais para que os dados operem, de fato, como infraestrutura pública. É a partir dessa compreensão que se consolida, no Brasil, a IND.

Ao reunir e qualificar iniciativas existentes, ao mesmo tempo em que institui novos mecanismos de coordenação, governança e suporte tecnológico, a IND estabelece uma arquitetura institucional comum para o uso estratégico, seguro e responsável das informações na formulação de políticas públicas e na prestação de serviços à população.

Em seguida, analisa-se a institucionalização da IND como política pública estruturante, descrevendo seus principais componentes, a lógica de organização por eixos e sua aplicação em ecossistemas temáticos. Esse enquadramento estabelece a base para a análise detalhada de cada eixo da IND, apresentada nos capítulos subsequentes.

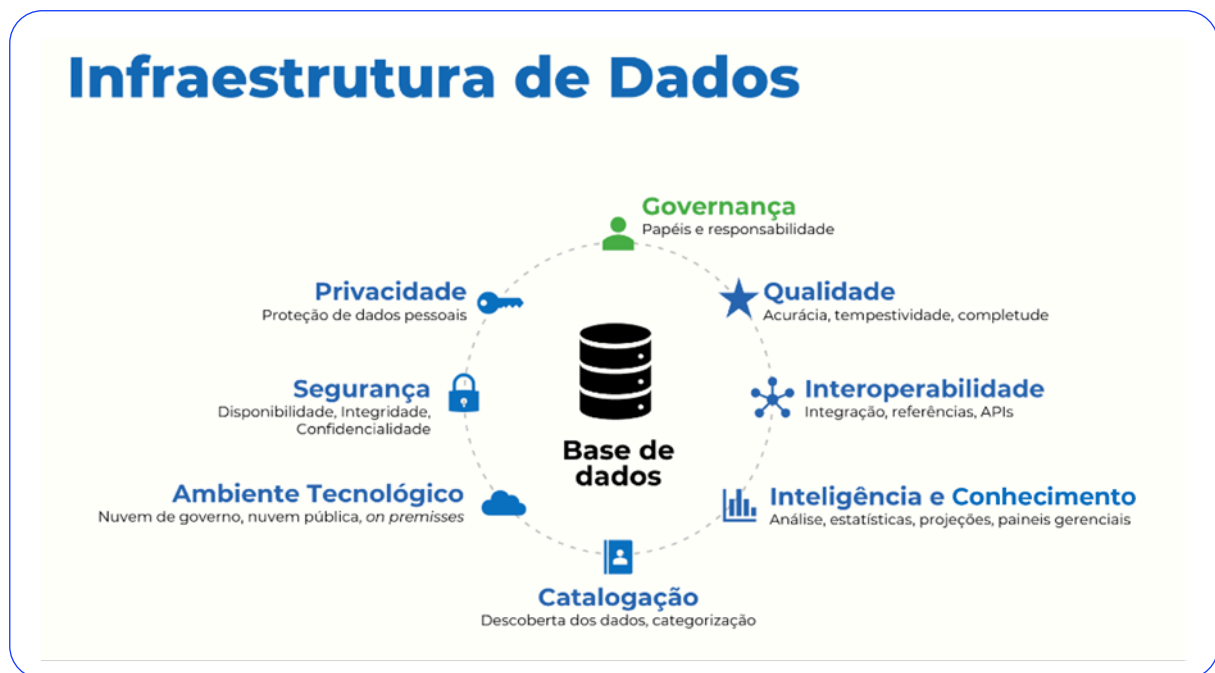
3.1. Limites do Modelo Descentralizado de Gestão de Dados

A gestão de dados no setor público tem sido tradicionalmente organizada de forma descentralizada, com bases produzidas e mantidas por órgãos e entidades segundo lógicas setoriais, padrões técnicos heterogêneos e arranjos institucionais pouco articulados. Esse modelo resultou em fragmentação informacional, duplicação de cadastros, inconsistências entre registros e limitações à integração entre sistemas. Como consequência, cidadãos e empresas passaram a fornecer repetidamente as mesmas informações ao Estado, enquanto gestores públicos enfrentaram dificuldades para acessar conjuntos de dados integrados capazes de subsidiar o ciclo de formulação, implementação e avaliação de políticas públicas.

À medida que os serviços digitais se expandiram e que o uso intensivo de dados passou a apoiar processos decisórios e operacionais do Estado, tornou-se evidente que a transformação digital não poderia avançar de forma sustentável sem uma infraestrutura pública capaz

de organizar, integrar e governar o ciclo de vida dos dados governamentais. A ausência de mecanismos estruturados de interoperabilidade, catalogação, padronização e responsabilização institucional limitava tanto a eficiência administrativa quanto a capacidade de o Estado operar de forma coordenada e orientada por evidências.

Nesse sentido, a literatura internacional e as experiências de governo digital convergem para a compreensão de que uma infraestrutura pública de dados envolve um conjunto articulado de funções ao longo de todo o ciclo de vida da informação, incluindo governança institucional, garantia de qualidade, mecanismos de interoperabilidade, proteção da privacidade, segurança da informação, ambientes tecnológicos adequados e capacidades analíticas para geração de conhecimento. Essas dimensões são interdependentes e condicionam, em conjunto, a capacidade do Estado de transformar dados em valor público.



Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (MGI). Material institucional.

Essas funções não se organizam de forma linear, mas como um sistema integrado, no qual fragilidades em qualquer uma das dimensões comprometem o desempenho global da infraestrutura de dados. A governança define responsabilidades e regras de uso; a qualidade assegura confiabilidade; a interoperabilidade permite a integração entre sistemas; a catalogação viabiliza a descoberta e o reuso; a segurança e a privacidade protegem direitos e ativos institucionais; os ambientes tecnológicos sustentam o processamento e o armazenamento; e as capacidades analíticas convertem dados em informação e conhecimento para a tomada de decisão.

3.2. Institucionalização da Infraestrutura Nacional de Dados no Brasil

Desde o início dos anos 2000, o Brasil vem desenvolvendo uma trajetória contínua de modernização administrativa baseada no uso estratégico das tecnologias digitais. A fase inicial, associada ao paradigma do Governo Eletrônico, concentrou-se na informatização de processos e na disponibilização de serviços por meio da internet, com foco em portais institucionais, compras públicas eletrônicas, certificação digital e padronização técnica. Esse período foi fundamental para a construção de capacidades básicas de tecnologia da informação no setor público federal e para a ampliação do acesso da população a serviços públicos digitais.

Ao longo da década de 2010, essa agenda incorporou de forma mais sistemática os princípios de transparência, participação social e abertura de dados, impulsionada, entre outros marcos, pela promulgação da Lei de Acesso à Informação, em 2011, e pela criação da Infraestrutura Nacional de Dados Abertos (INDA) e do Portal Brasileiro de Dados Abertos, em 2012. Nesse estágio, os dados passaram a ser reconhecidos como insumos relevantes para o controle social, a pesquisa e a inovação, embora o foco principal permanecesse voltado à publicação das informações, e não à integração operacional entre sistemas governamentais.

A partir de 2016, com a instituição da Política de Governança Digital e da Estratégia de Governança Digital, consolida-se no país a transição para o paradigma de Governo Digital, que reposiciona os serviços públicos a partir da perspectiva do usuário, priorizando simplificação, integração de canais e entrega de valor público. A digitalização acelerada de serviços, intensificada nos anos seguintes com a consolidação do portal gov.br e de mecanismos de autenticação única do cidadão, evidenciou, contudo, limites estruturais relacionados à fragmentação de bases de dados, à duplicação de cadastros e às restrições à coordenação intersetorial.

Paralelamente, o Estado brasileiro consolidou, ao longo de décadas, extensas infraestruturas setoriais de dados, como os sistemas estatísticos oficiais, os sistemas nacionais de informações em saúde, educação e assistência social, além de grandes cadastros administrativos nas áreas tributária, previdenciária e trabalhista. Embora esses sistemas tenham ampliado significativamente a capacidade estatal de produção e armazenamento de informações, sua organização predominantemente vertical e setorial limitou o uso transversal dos dados para fins de formulação, monitoramento e avaliação de políticas públicas integradas.

Nesse contexto, em 2019, o Decreto nº 10.046 instituiu formalmente a governança no compartilhamento de dados no âmbito da administração pública federal, estabelecendo princípios, responsabilidades institucionais e instâncias de coordenação para o intercâmbio de informações entre órgãos, além de criar o Cadastro Base do Cidadão como referência para

identificação unívoca nos serviços públicos. Esse marco normativo representou uma mudança qualitativa ao deslocar o compartilhamento de dados do campo de iniciativas pontuais para uma política pública estruturada, orientada por critérios de interesse público, segurança da informação e proteção de dados pessoais, em consonância com os princípios posteriormente consolidados pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Essa evolução institucional convergiu, também, com o enquadramento internacional das Infraestruturas Públicas Digitais (*Digital Public Infrastructure – DPI*), que compreendem dados, interoperabilidade e identidade digital como camadas estruturantes e reutilizáveis da capacidade estatal. Iniciativas globais como a campanha “50-in-5: DPI for People and Planet”, lançada em 2023, reforçaram esse entendimento ao promover a articulação entre políticas de governo digital, governança de dados e inclusão socioeconômica por meio de infraestruturas digitais públicas escaláveis.

Em 2024, o Brasil formalizou sua adesão a essa agenda internacional, reconhecendo ativos já consolidados — como a identidade digital integrada ao gov.br, sistemas nacionais de registros administrativos e plataformas de integração — como fundamentos para a ampliação do acesso a serviços públicos, o fortalecimento da coordenação estatal e a promoção do desenvolvimento digital inclusivo.

É nesse contexto de amadurecimento da política de governo digital e de alinhamento a referenciais internacionais de DPI que a IND é institucionalizada como política pública integrada no âmbito da Estratégia de Governo Digital 2024–2027.

A IND passa, assim, a ser concebida como uma infraestrutura que combina componentes técnicos — como plataformas de interoperabilidade, catálogos de metadados, serviços de integração e ambientes computacionais — com mecanismos de governança, definição de responsabilidades institucionais e desenvolvimento de capacidades organizacionais, preservando a custódia descentralizada dos dados e fortalecendo a coordenação transversal entre órgãos e níveis de governo.

Ao estruturar esses elementos de forma integrada, a IND busca transformar dados dispersos em ativos públicos capazes de sustentar políticas públicas mais eficazes, serviços mais simples e personalizados, e processos decisórios mais informados. Seu funcionamento está orientado pelo princípio de que os dados devem ser coletados apenas uma vez (*once-only*), mantidos sob responsabilidade clara (fonte única de verdade) e reutilizados de forma segura e legítima sempre que necessário para a execução de políticas públicas (*data-driven public sector*).

Para organizar essa complexidade, a IND foi estruturada, em sua fase atual de consolidação, em oito eixos temáticos que agrupam funções complementares e interdependentes. Esses eixos constituem a espinha dorsal da infraestrutura no estágio vigente de maturidade institucional, preservando, contudo, caráter adaptativo e passível de expansão conforme a evolução das demandas governamentais e das capacidades estatais em dados.

Esses eixos não operam de forma isolada. Ao contrário, constituem camadas interdependentes de uma mesma infraestrutura pública, que precisam atuar de maneira coordenada para que os dados possam ser efetivamente transformados em valor público.

A governança de dados define responsabilidades e regras para a gestão de dados no âmbito federal; a interoperabilidade permite a circulação dos dados; os catálogos asseguram sua descoberta; a privacidade e a segurança garantem o uso legítimo; os ambientes tecnológicos viabilizam o processamento e armazenamento; e os mecanismos de decisão baseada em dados e inteligência artificial ampliam o uso analítico e preditivo das informações.

A lógica da IND parte do reconhecimento de que nenhum eixo é suficiente por si só para produzir os resultados esperados da política de dados. A interoperabilidade, por exemplo, depende da existência de padrões semânticos e de responsabilidades definidas pela governança; a abertura e catalogação de dados exigem ambientes tecnológicos adequados; a aplicação de inteligência artificial depende da qualidade, da integração e da segurança das bases utilizadas; e a decisão baseada em dados requer tanto acesso às informações quanto capacidades analíticas institucionais.

Dessa forma, os eixos devem ser compreendidos como partes de uma arquitetura integrada, na qual avanços em uma dimensão tendem a reforçar as demais, enquanto fragilidades em qualquer delas comprometem o desempenho do conjunto. Essa abordagem sistêmica é particularmente relevante em contextos federativos e multissetoriais, nos quais múltiplos órgãos, níveis de governo e parceiros externos interagem em torno do uso de dados.

A organização por eixos também permite que diferentes áreas da administração pública avancem de forma progressiva, respeitando distintos níveis de maturidade institucional, ao mesmo tempo em que permanecem alinhadas a uma arquitetura comum de dados.

Além de organizarem a infraestrutura em nível transversal, os eixos da IND também funcionam como referência para sua aplicação em contextos temáticos específicos, denominados ecossistemas de dados. Nesses ecossistemas — como saúde, educação, meio ambiente ou primeira infância — os mesmos princípios, instrumentos e mecanismos da IND são mobilizados de forma adaptada às características setoriais e aos fluxos de dados próprios de cada política pública.

Os capítulos subsequentes deste relatório apresentam, de forma detalhada, cada um dos eixos da IND, descrevendo seus objetivos, arranjos institucionais, instrumentos operacionais e principais iniciativas em curso. A análise de cada eixo busca evidenciar como esses componentes contribuem, de maneira complementar, para a consolidação de uma infraestrutura pública de dados capaz de sustentar a transformação digital do Estado brasileiro e fortalecer sua capacidade de formulação e execução de políticas públicas baseadas em evidências.

4. GOVERNANÇA

Este capítulo descreve a governança de dados no setor público brasileiro como um arranjo institucional estruturante para o uso coordenado, seguro e estratégico da informação no Estado. Apresenta os fundamentos do modelo adotado, sua evolução normativa, o desenho institucional e os principais mecanismos operacionais que sustentam sua implementação no âmbito da IND.

A crescente digitalização dos serviços públicos e a ampliação do uso de dados nos processos decisórios tornaram mais visíveis os limites de modelos de gestão da informação baseados em estruturas setoriais pouco articuladas. No Brasil, dados públicos foram historicamente produzidos e geridos de forma descentralizada, com padrões técnicos e semânticos heterogêneos e reduzida interoperabilidade entre sistemas. Esse arranjo resultou em fragmentação informacional, duplicação de cadastros e dificuldades para a consolidação de diagnósticos integrados necessários à formulação, implementação e avaliação de políticas públicas.

Os dados eram gerados predominantemente como subprodutos de rotinas administrativas específicas de cada órgão, resultando em regras, padrões e ciclos de vida isolados. Esse cenário consolidou o que a literatura técnica denomina “silos de dados” — ambientes onde bases e cadastros coexistem sem o compartilhamento necessário para sustentar políticas públicas transversais.

A ausência de uma coordenação centralizada manifesta-se em falhas estruturais, tais como:

- **Redundância e Custos Elevados:** Duplicidade na coleta de informações e na manutenção de bases semelhantes.
- **Inconsistência de Dados:** Divergências entre registros de diferentes órgãos sobre o mesmo fato ou cidadão.
- **Assimetria de Informação:** Dificuldade em consolidar diagnósticos precisos para a tomada de decisão governamental.

A superação desse cenário exige um modelo de governança capaz de organizar normas, responsabilidades e processos ao longo de todo o ciclo de vida do dado. Nesse contexto, a IND foi concebida como um arcabouço integrador que articula instrumentos normativos, organizacionais e tecnológicos, tendo a governança de dados como seu eixo estruturante.

4.1. Evolução do Marco Normativo: da Transparência à Governança Sistêmica

As políticas de governança digital e de governança de dados no Brasil resultam de um processo contínuo de amadurecimento normativo iniciado em 2016, com a instituição da primeira Política de Governança Digital, e progressivamente aperfeiçoado ao longo da última década por meio de sucessivas estratégias, marcos legais e instrumentos de coordenação interinstitucional. Atualmente, esse arcabouço pode ser compreendido a partir de três dimensões complementares de governança:

- **Acesso e Transparência:** Consolidada pela Lei de Acesso à Informação (Lei nº 12.527/2011), que estabeleceu a publicidade como regra e o sigilo como exceção.
- **Proteção e Salvaguardas:** A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) introduziu parâmetros éticos e legais para o tratamento de informações de indivíduos, definindo responsabilidades claras para o Poder Público.
- **Eficiência e Integração:** A Lei de Governo Digital (Lei nº 14.129/2021) e o Decreto nº 10.046/2019 estruturaram o compartilhamento de dados e a criação de registros de referência — bases de dados consideradas fontes fidedignas e de uso obrigatório para a simplificação de serviços.

Dessa forma, a nova Política de Governança de Dados do governo federal, atualmente em consulta pública, representa uma mudança de paradigma: a governança deixa de ser vista apenas como um conjunto de regras de compartilhamento para se tornar uma política pública permanente, com foco na gestão integral do ciclo de vida do dado (coleta, tratamento, armazenamento, uso e descarte).

4.2. A Política de Governança de Dados: Objetivos e Inovações do Novo Marco

A Política de Governança de Dados tem como objetivo assegurar que os dados públicos sejam confiáveis, íntegros e acessíveis, apoiando a melhoria da prestação de serviços e a formulação de políticas baseadas em evidências. Seus objetivos centrais incluem:

1. instituir padrão para implementação e manutenção de mecanismos e instâncias de governança;
2. estabelecer diretrizes para que os órgãos e entidades implementem a governança de dados de forma integrada, com observância das boas práticas das diferentes dimensões de gestão de dados;
3. orientar a elaboração de políticas internas e estratégias de dados nos órgãos;
4. fomentar o uso estratégico de dados para qualificação de políticas públicas;
5. estabelecer diretrizes para interoperabilidade e compartilhamento com garantia de qualidade, segurança e proteção de dados.

Diferente dos arranjos normativos anteriores — notadamente representados pelo Decreto nº 10.046/2019, que possuía um enfoque predominantemente voltado à operacionalização do compartilhamento e à abertura de bases específicas — a nova Política de Governança de Dados introduz avanços estruturantes que alteram a dinâmica operacional dos órgãos. Este novo marco transcende a visão do dado como um insumo administrativo estático, estabelecendo-o como um ativo estratégico que exige governança ativa e contínua. Com isso, a responsabilidade institucional desloca-se da simples custódia para a gestão integral do ciclo de vida do dado, institucionalizando mecanismos de curadoria, qualidade e interoperabilidade como pilares obrigatórios da gestão pública moderna. Dentre os avanços que a nova política traz estão:

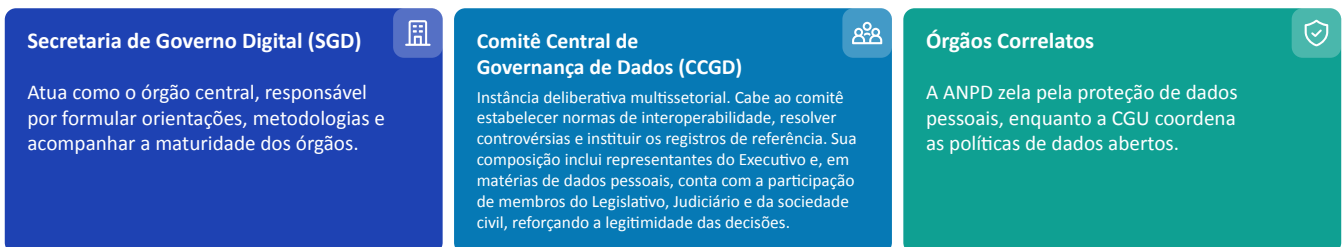
- **Expansão dos Registros de Referência:** O novo marco amplia a governança sobre os Registros de Referência, definindo-os como: informações íntegras e precisas oriundas de uma ou mais fontes de dados, centralizadas ou descentralizadas, sobre elementos fundamentais para a prestação de serviços e para a gestão de políticas públicas.
- **Interoperabilidade:** O “ponto de inflexão” administrativo é a dispensa de convênios ou acordos de cooperação técnica para o compartilhamento entre órgãos federais.

Esta medida elimina o “gatekeeping burocrático”, onde agências retinham dados como forma de poder institucional. O compartilhamento torna-se a regra, pautado pelo interesse público e pela eficiência fiscal.

- **Obrigatoriedade do PGDADOS:** A Política torna compulsória a implementação do Programa de Governança de Dados (PGDADOS) em todos os órgãos da administração direta, autárquica e fundacional, vinculando a estratégia institucional a indicadores de maturidade monitorados centralmente.
- **Modelo de Governança Multinível:** A nova estrutura de governança é descentralizada na execução, mas centralizada na coordenação, sob a liderança da Secretaria de Governo Digital (SGD) e do Comitê Central de Governança de Dados.

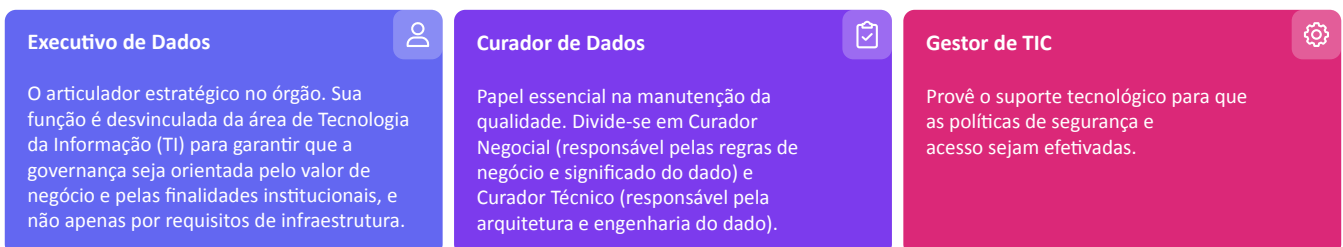
Nesse sentido, o modelo de governança de dados adotado possui uma lógica federada, que concilia coordenação central de diretrizes com autonomia executiva dos órgãos. A coordenação central é responsável pela definição de normas, padrões e instrumentos comuns, bem como pelo monitoramento da implementação da política. Os órgãos, por sua vez, mantêm autonomia para operacionalizar a governança de dados em consonância com suas atribuições e níveis de maturidade institucional.

Nível Central:



Fonte: Elaboração própria.

Nível Setorial:



Fonte: Elaboração própria.

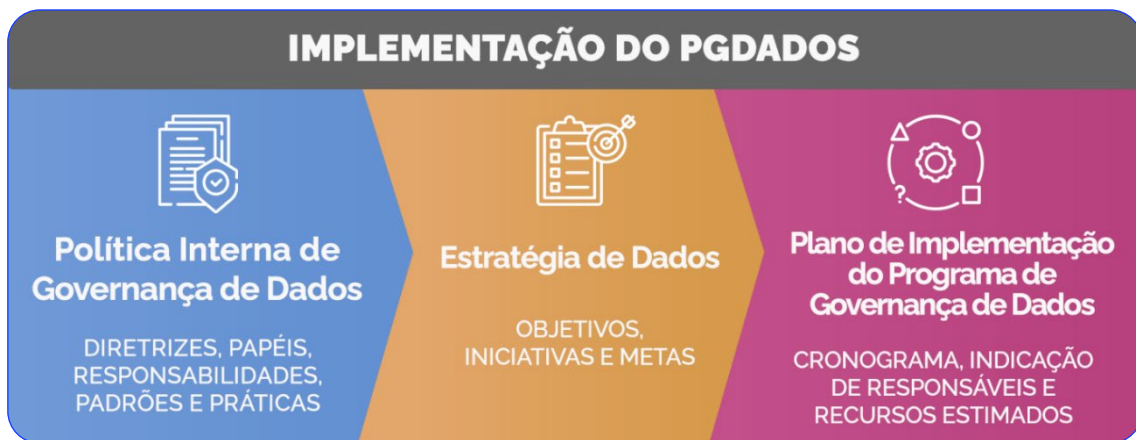
Esse arranjo busca assegurar coerência sistêmica sem comprometer a flexibilidade necessária à gestão setorial, criando um equilíbrio entre padronização e adaptação institucional.

4.3. Operacionalização: O Programa de Governança de Dados (PGDADOS)

A operacionalização da Política de Governança de Dados no âmbito dos órgãos e entidades da administração pública federal ocorre por meio do Programa de Governança de Dados (PGDADOS). O programa constitui o principal instrumento de tradução das diretrizes normativas em práticas institucionais concretas, permitindo que os princípios e objetivos da política sejam incorporados à rotina administrativa das organizações.

O programa é estruturado a partir de três instrumentos complementares:

1. **Política Interna de Governança de Dados:** Formaliza os princípios e responsabilidades no âmbito do órgão.
2. **Estratégia de Dados:** Planejamento que alinha o uso dos dados aos objetivos finalísticos da instituição.
3. **Plano de Implementação:** Roteiro operacional com metas, cronogramas e atribuições específicas.



Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (MGI).
Guia de Implementação do Programa de Governança de Dados (PGDADOS), 2025.

Esses três instrumentos operam de maneira articulada. A Política Interna estabelece o “como” e o “quem”; a Estratégia de Dados define o “para quê” e o “o quê”; e o Plano de Implementação organiza o “quando” e o “como fazer”. Essa integração permite alinhar governança, planejamento e execução, evitando que a política de dados se restrinja a enunciados formais sem repercussão prática.

Além disso, o PGDADOS desempenha papel relevante na articulação da governança de dados com outras políticas e instrumentos institucionais, como o planejamento estratégico, as políticas de segurança da informação, as iniciativas de dados abertos e as estratégias de

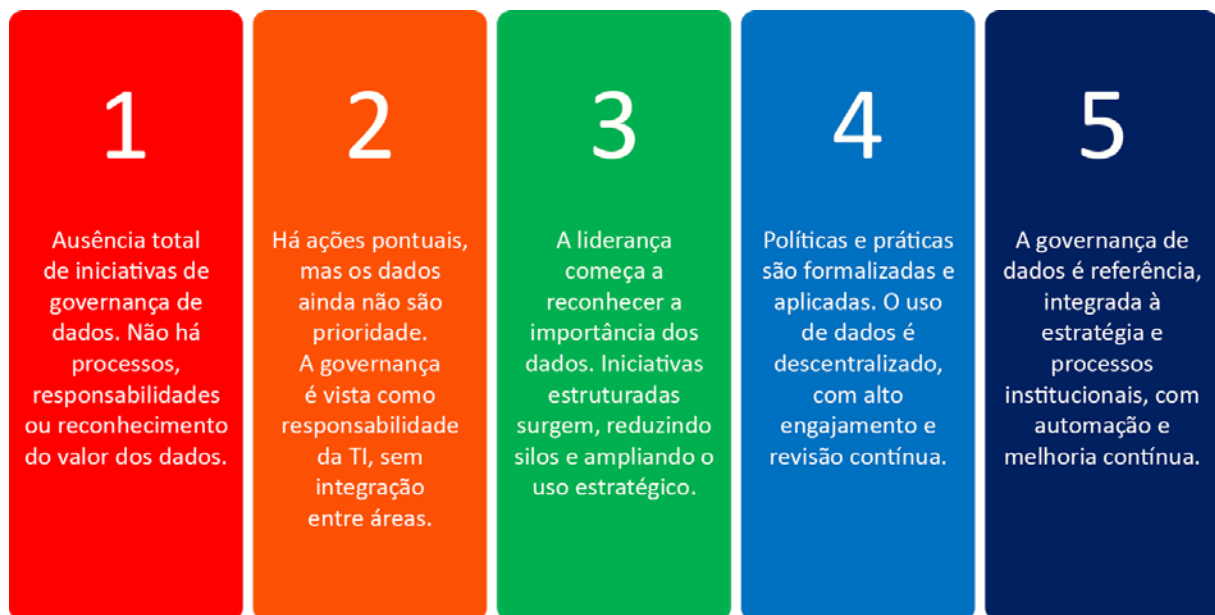
transformação digital. Ao integrar esses diferentes domínios, o programa contribui para reduzir sobreposições, promover coerência institucional e fortalecer a cultura de dados no setor público.

A natureza contínua do PGDADOS reforça o entendimento de que a governança de dados não constitui um projeto com início e fim definidos, mas um processo permanente de aprimoramento organizacional. Esse caráter evolutivo cria as condições para que as capacidades institucionais em governança e gestão de dados sejam progressivamente ampliadas, em consonância com a maturidade do órgão e com as diretrizes estabelecidas no âmbito da IND.

4.4. Monitoramento e Evolução: Modelo de Maturidade de Dados (MMD)

A evolução das capacidades institucionais em governança e gestão de dados é acompanhada por meio do Modelo de Maturidade de Dados (MMD). O MMD é um instrumento de diagnóstico para a melhoria contínua.

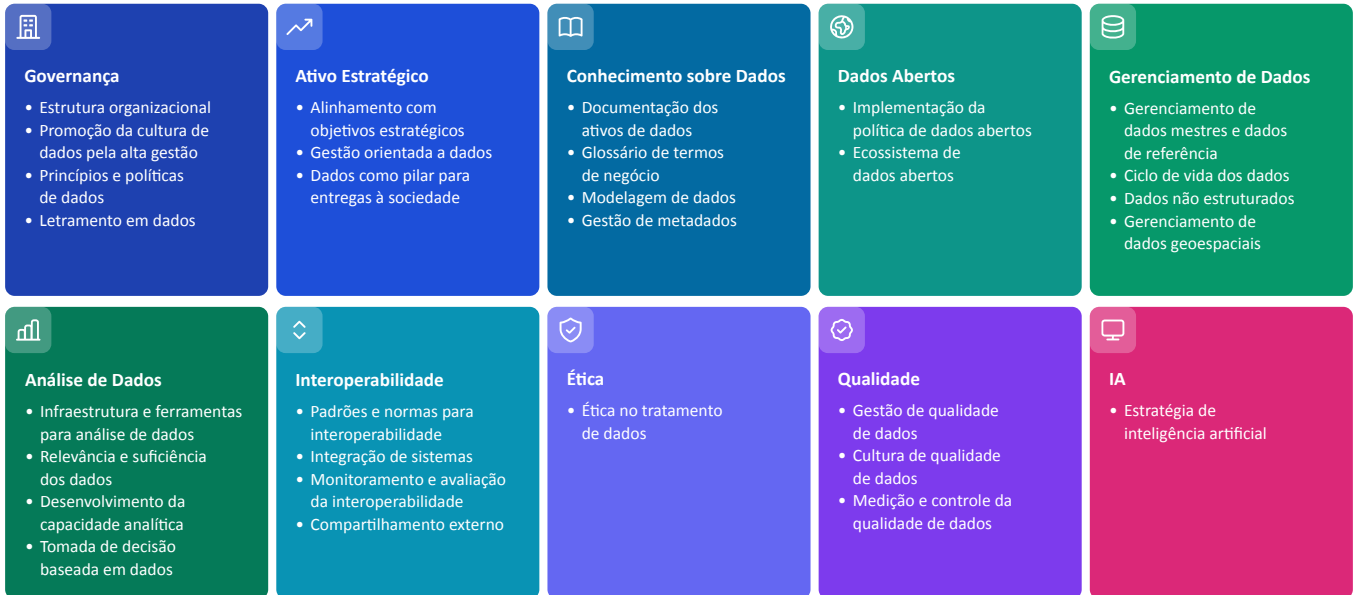
A avaliação ocorre em cinco níveis:



Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (MGI), Modelo de Maturidade de Dados, 2025.

Além disso, o MMD está estruturado em Dimensões e Temas. As Dimensões representam as disciplinas, servindo como divisores das diversas práticas e processos que compõem a governança e a gestão de dados dentro de uma organização. Os Temas são as especialidades, as unidades de avaliação granular, os elementos específicos que compõem cada Dimensão. Cada Tema representa uma prática ou processo que deve ser avaliado individualmente.

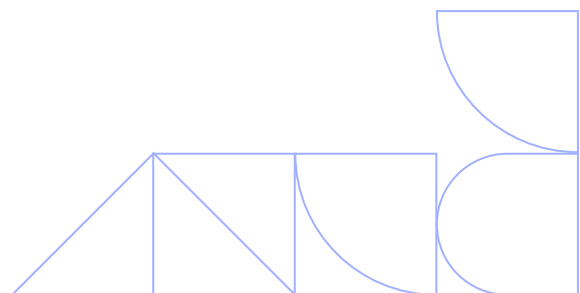
A Avaliação do MMD possui 10 Dimensões e 30 Temas, o que proporciona uma visão abrangente e detalhada da maturidade em governança e gestão de dados da organização.



Fonte: Elaboração própria, com base no Ministério da Gestão e da Inovação em Serviços Públicos (MGI), Modelo de Maturidade de Dados, 2025.

Ao avaliar cada Tema e atribuir um nível de maturidade, as instituições podem identificar sua maturidade naquela Dimensão, e conseqüentemente, seus pontos fortes e fracos, definir estratégias de melhoria e avançar para níveis mais elevados em governança e gestão de dados.

Assim, a governança de dados, no âmbito da IND, organiza-se como uma função transversal que estabelece princípios, responsabilidades e mecanismos de coordenação aplicáveis a todo o ecossistema de dados do setor público. Esse arranjo cria a base institucional sobre a qual se estruturam os demais eixos da IND, garantindo coerência, segurança jurídica e alinhamento estratégico na produção e no uso das informações públicas. À luz desse enquadramento, o capítulo seguinte examina o eixo da interoperabilidade, responsável por viabilizar a integração técnica e semântica entre sistemas e a circulação controlada de dados entre órgãos e níveis de governo.



5. INTEROPERABILIDADE

A interoperabilidade constitui um princípio estruturante para a conexão e integração de dados no setor público e para a operacionalização de políticas de governo digital. Do ponto de vista técnico, refere-se à capacidade de sistemas de informação distintos, baseados em arquiteturas e linguagens diversas, de comunicar-se entre si de forma automatizada, segura e semanticamente compreensível, permitindo o intercâmbio consistente de dados entre órgãos e níveis de governo.

No contexto da administração pública brasileira, a interoperabilidade responde à necessidade de superar arranjos institucionais nos quais os sistemas de informação operam de maneira isolada, com limitada capacidade de compartilhamento e reutilização de dados. Ao estabelecer padrões comuns de comunicação e integração entre sistemas, a interoperabilidade viabiliza o intercâmbio estruturado de informações governamentais, reduzindo redundâncias, aumentando a consistência dos registros e ampliando a capacidade de coordenação entre políticas públicas.

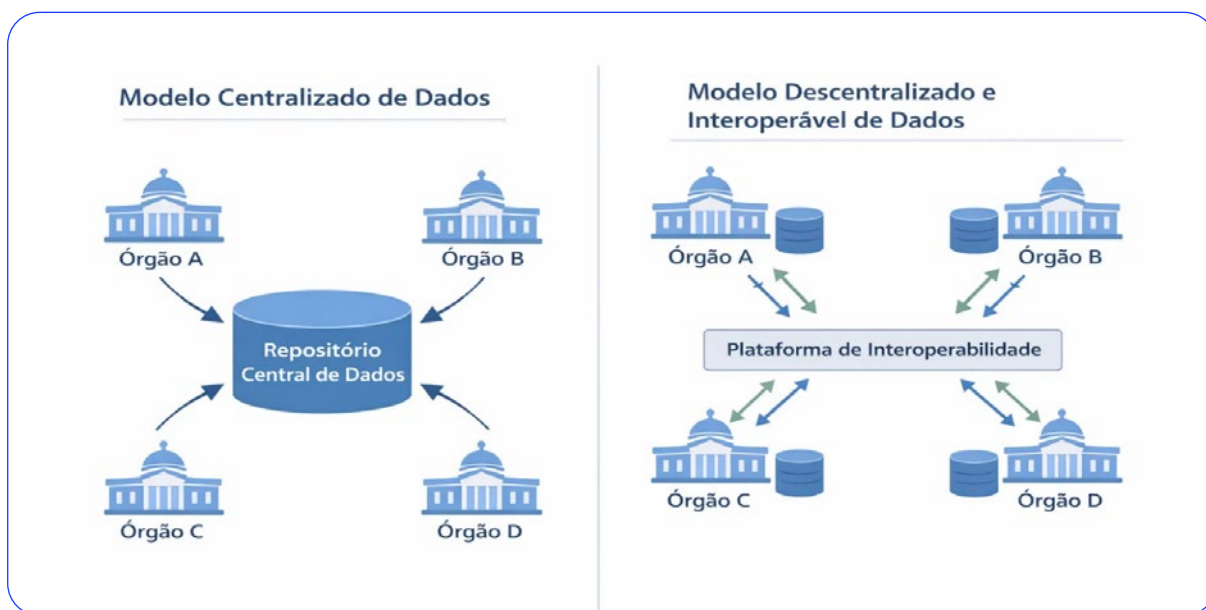
Esse modelo de integração sustenta a aplicação do princípio *once-only* (apenas uma vez), segundo o qual informações já fornecidas por cidadãos e empresas ao Estado devem ser reutilizadas sempre que necessário, evitando solicitações repetidas e os silos de informações.

Na prática, essa integração produz ganhos mensuráveis para diferentes atores. Para cidadãos e empresas, reduz custos de tempo e esforço, ao eliminar a necessidade de apresentar repetidamente as mesmas informações, enfrentar deslocamentos ou reunir documentos já disponíveis ao Estado. Para a administração pública, diminui retrabalho, inconsistências cadastrais e divergências entre bases que deveriam ser convergentes, contribuindo para maior eficiência operacional e melhor qualidade das informações utilizadas na formulação e execução de políticas.

Para transformar essa visão em realidade, é necessária uma arquitetura de dados para que esses efeitos se materializem de forma consistente e em escala.

5.1. O Modelo Brasileiro: Descentralizado e Interoperável

As decisões sobre a arquitetura de dados são escolhas estratégicas de Estado, que definem como os ativos de informação da população são gerenciados e protegidos. Tais escolhas possuem implicações diretas para a segurança, a privacidade e a eficiência governamental, exigindo uma abordagem que equilibre integração e responsabilidade.



Fonte: Elaboração própria.

No desenho da arquitetura nacional de dados, o Brasil optou por um modelo descentralizado e federado. Diferentemente de abordagens baseadas na centralização de grandes volumes de informações em repositórios únicos, esse modelo evita a concentração excessiva de dados sensíveis, reduzindo a criação de pontos únicos de falha e a exposição a riscos sistêmicos de segurança ou a usos indevidos das informações. A descentralização preserva a responsabilidade dos órgãos sobre os dados sob sua custódia, ao mesmo tempo em que permite sua utilização integrada para finalidades públicas legítimas.

Nesse arranjo, os papéis institucionais no ecossistema de dados são claramente delimitados. Os órgãos gestores permanecem responsáveis pela produção, manutenção, atualização e qualidade das informações, bem como pela observância dos padrões técnicos, semânticos e normativos aplicáveis. Os órgãos consumidores utilizam os dados exclusivamente para finalidades compatíveis com suas atribuições legais e em conformidade com a legislação vigente, especialmente no que se refere à proteção de dados pessoais e à segurança da informação.

A interoperabilidade é viabilizada por meio de uma plataforma de integração que atua como camada intermediária entre os sistemas governamentais. Essa camada organiza os fluxos de informação, padroniza as trocas de dados e assegura a rastreabilidade e a segurança das transações, sem assumir a custódia permanente das informações compartilhadas. Ao centralizar a complexidade técnica da integração, a plataforma reduz o ônus operacional para os órgãos detentores dos dados e cria condições para a ampliação progressiva do intercâmbio de informações em escala governamental.

Essa arquitetura resulta em um modelo descentralizado, rastreável e em conformidade com as normas de segurança e privacidade. Sua materialização ocorre por meio do Conecta gov.br, a plataforma que viabiliza a interoperabilidade.

5.2. Conecta gov.br: A Plataforma Nacional de Integração de Dados

O programa Conecta gov.br é o principal instrumento operacional para a interoperabilidade na IND do Poder Executivo federal. Projetado para ser o componente da troca de informações no governo, o Conecta gov.br opera como uma infraestrutura intergovernamental centralizada que torna a visão de um Estado integrado uma realidade funcional.

Sob a coordenação da Secretaria de Governo Digital (SGD), a plataforma funciona como um “barramento de serviços” (*service bus*) ou *gateway* nacional. Sua função é intermediar a troca segura e automatizada de dados entre os diversos sistemas governamentais, eliminando a necessidade de integrações bilaterais (ponto a ponto), que são mais complexas e custosas.

A base tecnológica para essa funcionalidade são as APIs (*Application Programming Interfaces*) — mecanismos padronizados que permitem a comunicação automatizada entre diferentes sistemas de informação. Em termos simples, as APIs permitem que um sistema público solicite informações a outro sistema, receba a resposta adequada e utilize esses dados para prestar um serviço ao cidadão, sem a necessidade de intervenções manuais.

O Conecta gov.br oferece uma estrutura comum que coordena o compartilhamento de dados por meio de quatro funções principais:

- **Catálogo de APIs:** Funciona como um inventário de ativos de dados disponíveis para compartilhamento, promovendo a transparência sobre quais informações existem e onde podem ser acessadas. Essa ferramenta é crucial para superar os silos de informação e sistemas isolados que historicamente não compartilham dados.
- **Controle de Acesso:** A plataforma verifica as autorizações necessárias antes de cada transação, garantindo que apenas órgãos habilitados possam acessar os dados e exclusivamente para finalidades legítimas, em conformidade com a legislação.
- **Padronização:** Ao definir regras técnicas comuns para a comunicação entre sistemas, a plataforma reduz custos e a complexidade associados ao desenvolvimento e à manutenção das integrações.
- **Monitoramento:** A plataforma acompanha o funcionamento das integrações em tempo real, permitindo a gestão da disponibilidade dos serviços e a mensuração do impacto das trocas de dados na prestação de serviços públicos.

A plataforma atua exclusivamente como camada de orquestração do intercâmbio de informações, não realizando o armazenamento permanente dos dados transacionados. A custódia, a atualização e a qualidade das informações permanecem sob responsabilidade dos órgãos gestores das bases de dados, em conformidade com o modelo descentralizado adotado.

Nesse contexto, a qualidade e a confiabilidade dos dados compartilhados assumem papel central para a efetividade da interoperabilidade. Para esse fim, o modelo brasileiro incorpora os Registros de Referência como instrumentos complementares à plataforma de integração, estabelecendo fontes oficiais e autoritativas para informações essenciais ao funcionamento do Estado.

5.3. Registros de Referência: *Fonte Única da Verdade*

Os Registros de Referência consistem em conjuntos de dados oficiais, íntegros e padronizados, definidos como fontes autoritativas para informações essenciais à gestão pública. Eles estabelecem, para cada tipo de informação fundamental, uma “Fonte Única da Verdade” reconhecida como válida, garantindo que todos os órgãos utilizem os mesmos dados de forma consistente. Assim, um Registro de Referência é o local oficial onde determinado tipo de informação deve ser buscado. Isso significa que, para cada dado fundamental, existe uma única base reconhecida como válida por todo o Estado.

A importância desse modelo está no fato de que ele elimina divergências e duplicações. Um dado passa a ser corrigido em um único lugar e, automaticamente, torna-se válido para todo o governo. Isso reduz erros, evita conflitos de informação, aumenta a segurança jurídica e melhora a qualidade dos serviços públicos prestados à população.

A utilização de Registros de Referência integra o esforço de padronização e racionalização do uso de informações essenciais no setor público. No contexto do Governo Digital, esse instrumento se associa à diretriz de atuação integrada entre órgãos e à eliminação de exigências desnecessárias ao usuário, inclusive por meio de interoperabilidade de dados, de modo a reduzir redundâncias e inconsistências na prestação de serviços públicos.

Para viabilizar a aplicação consistente desses instrumentos, informações consideradas referenciais podem ser disponibilizadas aos sistemas governamentais por mecanismos de interoperabilidade, incluindo APIs no âmbito do Conecta gov.br, permitindo acesso automatizado e padronizado a dados sob custódia do órgão responsável, com redução de cadastros paralelos e validações repetitivas.

A adoção dessa arquitetura, que combina uma plataforma de orquestração com fontes de dados consistentes e reconhecidas, constitui um instrumento concreto de melhoria da

eficiência estatal, da segurança jurídica e da qualidade dos serviços públicos oferecidos à população, gerando impactos socioeconômicos mensuráveis e duradouros.

5.4. Impacto Socioeconômico e Valor Público

O modelo de interoperabilidade adotado pelo Estado brasileiro, estruturado sobre a plataforma Conecta gov.br e os Registros de Referência, gera valor público concreto e mensurável. Ao integrar sistemas e padronizar o uso de informações essenciais, esse modelo transforma a forma como o governo presta serviços e toma decisões, produzindo ganhos reais para a sociedade e para a administração pública.

Para a população, os efeitos são diretos e perceptíveis: serviços mais simples, mais rápidos e menos burocráticos, com redução da exigência de documentos, eliminação da repetição de informações e maior previsibilidade no atendimento.

Para o poder público, a interoperabilidade representa aumento de eficiência, redução de custos operacionais e melhoria da qualidade da informação utilizada na gestão pública. A convergência para fontes únicas e confiáveis de dados diminui retrabalhos, corrige inconsistências e fortalece a segurança jurídica, criando bases mais sólidas para a formulação e a execução de políticas públicas.

Com o objetivo de mensurar esses efeitos, o governo desenvolveu um instrumento específico para estimar as economias geradas pela interoperabilidade desde o início da implementação do modelo, em 2020. A ferramenta consolida os ganhos decorrentes da eliminação de exigências redundantes, da automatização de fluxos de informação e do uso de dados padronizados, permitindo a quantificação objetiva dos benefícios financeiros associados ao intercâmbio de dados entre sistemas governamentais.



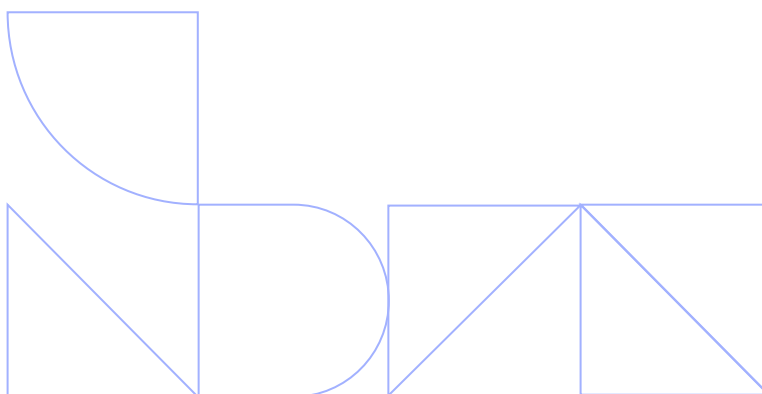
Fonte: BRASIL. Governo Digital. Conecta GOV.BR — Infraestrutura Nacional de Dados: Interoperabilidade. Brasília, 2025.

A metodologia adotada baseia-se na identificação de tarefas eliminadas ou simplificadas em serviços específicos, na estimativa do tempo economizado por cidadãos e agentes públicos e na monetização desse tempo a partir de parâmetros como remuneração média dos servidores e renda média dos usuários. Sempre que possível, o cálculo incorpora também estimativas relacionadas à redução de erros, inconsistências e ocorrências indevidas associadas ao uso de informações fragmentadas.

Os resultados já observados evidenciam que o investimento em interoperabilidade e governança de dados gera retorno significativo. A combinação entre uma plataforma de orquestração robusta e registros oficiais consistentes permite ampliar a escala dos serviços digitais, otimizar recursos públicos e elevar a capacidade do Estado de responder às necessidades da sociedade.

Mais do que uma iniciativa tecnológica, esse modelo consolida uma visão de Estado moderno, eficiente e orientado ao interesse público, no qual a transformação digital se traduz em benefícios tangíveis, mensuráveis e sustentáveis para o desenvolvimento do país.

Para que esse intercâmbio ocorra de forma eficiente, é necessário que os ativos de dados existentes sejam identificados e descritos de maneira estruturada. O capítulo seguinte trata do Catálogo Nacional de Dados, eixo responsável por organizar e dar visibilidade aos dados disponíveis no setor público.



6. CATÁLOGO NACIONAL DE DADOS

A consolidação da IND pressupõe que os ativos de dados existentes no setor público sejam identificáveis, descritos de forma padronizada e passíveis de descoberta por órgãos e usuários autorizados. Nesse arranjo, o Catálogo Nacional de Dados desempenha a função de tornar visível o universo de dados sob custódia da administração pública, reduzindo assimetrias informacionais e criando condições para o reuso de informações na prestação de serviços e na formulação de políticas públicas.

Para endereçar esse desafio, é crucial compreender a distinção entre dados e metadados. Os dados são a informação bruta em si. Os metadados, por sua vez, são “dados sobre os dados”, funcionando como um descritor que informa o conteúdo, o contexto, a qualidade, a estrutura e a acessibilidade da informação.

O Catálogo opera sobre metadados, isto é, informações estruturadas que descrevem conjuntos de dados e serviços de dados, indicando seu conteúdo, finalidade, responsável institucional, condições de acesso, periodicidade de atualização e outros atributos relevantes para uso e governança. Assim, sua contribuição principal não está no armazenamento de dados brutos, mas na organização de descrições confiáveis e comparáveis que permitem localizar e compreender ativos de dados distribuídos em múltiplos órgãos e sistemas.

No contexto da IND, o Catálogo constitui o componente de “descoberta” da infraestrutura de dados. Ao oferecer um ponto de referência comum para a descrição dos ativos de informação, ele viabiliza que iniciativas de interoperabilidade e compartilhamento sejam conduzidas de forma mais eficiente, uma vez que órgãos demandantes podem identificar previamente quais dados existem, sob qual governança e por quais meios podem ser acessados. Dessa forma, o Catálogo contribui para transformar um ecossistema de dados disperso em um ambiente mais coordenado, com maior previsibilidade institucional e melhores condições para integração entre sistemas e políticas públicas.

A implementação do Catálogo Nacional de Dados está ancorada em um arcabouço normativo que estabelece a catalogação como requisito obrigatório da governança de dados no setor público federal. O principal instrumento é o Decreto nº 10.046, de 2019, que dispõe sobre a governança no compartilhamento de dados e determina que os órgãos e entidades da administração pública publiquem e mantenham catálogo dos dados sob sua gestão, conferindo caráter vinculante à prática de catalogação. Ademais, nos termos do art. 30 do referido Decreto, a Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos poderá expedir normas complementares para sua execução, observadas as competências do Comitê Central de Governança de Dados e a legislação de acesso à informação. Ao estabelecer a obrigatoriedade do inventário de dados, o decreto transforma a catalo-

gação de uma boa prática administrativa em um dever institucional, integrando-a às rotinas formais de gestão da informação. Nesse contexto, o Catálogo Nacional de Dados consolida-se não apenas como plataforma centralizadora que viabiliza o cumprimento dessa exigência de forma padronizada, consistente e auditável, mas também como instrumento estruturado a partir de padrão governamental de metadados — o DCAT-BR. A adoção desse padrão assegura interoperabilidade semântica e técnica entre catálogos distintos, reduz a heterogeneidade de soluções isoladas e fortalece a coordenação interinstitucional no ecossistema de dados públicos. A base normativa também articula o Catálogo à política de dados abertos. O decreto prevê que conjuntos de dados classificados para compartilhamento amplo sejam devidamente catalogados e publicizados, assegurando que a transparência e a reutilização da informação ocorram de maneira estruturada e detectável. Dessa forma, o Catálogo atua como elemento de ligação entre as agendas de governança de dados, compartilhamento interinstitucional e abertura de dados ao público.

O instrumento se materializa no Portal de Dados Abertos e Catálogo Nacional de Dados, que constituem os principais pontos de acesso aos conjuntos de dados produzidos e disponibilizados pelo governo federal e por governos estaduais. No âmbito federal, a estratégia previa a abertura de aproximadamente 9 mil bases de dados, tendo sido concluída, até 2025, a disponibilização de 74% desse total.

Essas plataformas viabilizam o acesso estruturado, a reutilização e a interoperabilidade de dados públicos, apoiando a produção de evidências, o desenvolvimento de soluções digitais e a oferta de serviços orientados às necessidades da sociedade.

Observa-se elevado nível de utilização e aderência ao serviço, refletindo sua consolidação como componente da IND, conforme demonstrado na figura a seguir:



Fonte: Ministério da Gestão e da Inovação em Serviços Públicos (MGI).
Portal Brasileiro de Dados Abertos (dados.gov.br), 2025.

Além de definir o “o que” deve ser catalogado, o marco legal estabelece responsabilidades institucionais claras, ao vincular cada conjunto de dados a um órgão gestor e a um nível de compartilhamento específico. Esse enquadramento normativo confere previsibilidade jurídica ao uso dos dados e cria as condições para que a catalogação funcione como instrumento operacional da política de governança de dados, sustentando práticas de integração, reutilização e controle ao longo da IND.

6.1. Arranjos Institucionais e Papéis na Governança de Dados

Para que um catálogo de dados seja útil e confiável, a qualidade e a atualização de seus metadados são essenciais. Isso depende de um arranjo institucional com papéis e responsabilidades claramente definidos, onde diferentes atores colaboram ao longo do ciclo de vida da informação. A produção e manutenção de metadados de qualidade não é uma tarefa puramente técnica, mas um processo de governança que requer atribuições específicas.

O Decreto Nº 10.046, de 2019, estabelece os papéis fundamentais que sustentam o processo de catalogação de dados. As responsabilidades são distribuídas da seguinte forma:

- **Gestor de dados:** Definido como “o órgão ou entidade responsável pela governança de determinado conjunto de dados”. O gestor é a autoridade máxima sobre aquele ativo de informação, sendo sua responsabilidade primária garantir a qualidade, a categorização do nível de compartilhamento e a correta publicação dos metadados no Catálogo. Esta definição não é meramente burocrática; ela atribui ao Gestor de Dados a responsabilidade pela execução do ciclo de vida da catalogação, desde a identificação do ativo até sua manutenção contínua, como detalhado adiante.
- **Custodiante de dados:** Descrito como “o órgão ou entidade que, total ou parcialmente, zela pelo armazenamento, pela operação, pela administração e pela preservação de dados”. O custodiante é o responsável pela infraestrutura tecnológica que armazena os dados, mas não necessariamente pela sua governança. A distinção é crucial para cenários onde um órgão provê a infraestrutura para outro.

A clareza dessas funções é vital para que os instrumentos técnicos de catalogação sejam aplicados de forma consistente e eficaz em toda a administração pública.

6.2. Padrões de Metadados e Interoperabilidade Semântica

A capacidade de integrar, comparar e reutilizar dados em escala governamental depende da adoção de padrões comuns para a descrição dos ativos de informação. No âmbito do Catálogo Nacional de Dados, esses padrões asseguram que os metadados produzidos por diferentes órgãos sejam compreensíveis entre si, permitindo a interoperabilidade semântica e a descoberta consistente de dados em todo o setor público.

O padrão adotado é o DCAT-BR, versão nacional do *Data Catalog Vocabulary* recomendado internacionalmente para a publicação de catálogos de dados. Esse vocabulário estabelece um modelo estruturado para a descrição de conjuntos de dados e serviços de dados, definindo atributos essenciais como título, descrição, responsável institucional, condições de

acesso e formas de disponibilização. A utilização de um padrão comum reduz ambiguidades, aumenta a comparabilidade das descrições e viabiliza o processamento automatizado das informações catalogadas.

De forma complementar, o uso de vocabulários controlados, como o Vocabulário Controlado de Governo Eletrônico (VCGE), contribui para a padronização temática dos metadados. Esses instrumentos permitem classificar os conjuntos de dados segundo áreas de política pública e domínios de atuação governamental, facilitando tanto a navegação por usuários humanos quanto a agregação de informações por sistemas automatizados. Ao alinhar terminologias e categorias, os vocabulários controlados fortalecem a coerência semântica do Catálogo e ampliam sua utilidade analítica.

A adoção sistemática desses padrões transforma o Catálogo Nacional de Dados em um componente interoperável da IND, capaz de dialogar com outras plataformas e instrumentos de governança. Mais do que uma exigência técnica, a padronização dos metadados constitui um requisito institucional para o reuso qualificado da informação, ao criar uma base comum de entendimento sobre os dados disponíveis e suas condições de uso no setor público.

6.3. Monitoramento e Qualidade dos Metadados

O valor estratégico do Catálogo Nacional de Dados está diretamente associado à qualidade, à completude e à atualização dos metadados nele registrados. Sem esses atributos, o Catálogo perde sua função central de apoiar a descoberta, o reuso e a integração de dados, tornando-se um inventário parcial ou pouco confiável. Por essa razão, o monitoramento contínuo da qualidade dos metadados constitui um elemento essencial da governança do Catálogo no âmbito da IND.

A avaliação da qualidade dos metadados envolve múltiplas dimensões complementares. A cobertura refere-se à extensão com que os ativos de dados relevantes de cada órgão estão efetivamente catalogados, sendo fundamental para evitar a persistência de silos informacionais. A completude diz respeito ao grau de preenchimento dos campos obrigatórios e recomendados, condição necessária para que usuários e sistemas compreendam adequadamente o conteúdo, o contexto e as limitações dos dados descritos.

A atualização dos metadados é igualmente crítica, pois descrições desatualizadas podem induzir a interpretações equivocadas, gerar retrabalho e comprometer a confiança dos usuários no Catálogo. Já a consistência está relacionada à aderência aos padrões adotados, como o DCAT-BR e os vocabulários controlados, assegurando que os metadados sejam comparáveis e interoperáveis em escala governamental.

O acompanhamento sistemático dessas dimensões permite identificar lacunas, orientar ações corretivas e promover a melhoria contínua do processo de catalogação. Ao incorporar práticas regulares de monitoramento, o Catálogo Nacional de Dados deixa de ser um repositório estático de descrições e se consolida como um instrumento ativo de governança da informação, capaz de sustentar análises integradas, decisões baseadas em evidências e a efetividade dos demais eixos da IND.

6.4. Integração Sistêmica do Catálogo na Infraestrutura Nacional de Dados

O Catálogo Nacional de Dados integra-se de forma transversal aos demais eixos da IND, atuando como o componente que confere visibilidade, contexto e inteligibilidade ao conjunto de ativos de informação do setor público. Ao organizar e padronizar a descrição dos dados disponíveis, o Catálogo estabelece o ponto de partida para iniciativas de interoperabilidade, compartilhamento e uso estratégico da informação no âmbito governamental.

Essa integração sistêmica manifesta-se, em primeiro lugar, na articulação com os mecanismos de interoperabilidade, ao permitir que órgãos identifiquem previamente quais conjuntos de dados existem, sob qual governança e por quais meios podem ser acessados. De modo complementar, o Catálogo sustenta a política de dados abertos ao estruturar a publicidade dos dados de compartilhamento amplo, ampliando a transparência e facilitando o reuso por atores externos ao governo.

O Catálogo também reforça a governança de dados ao associar cada ativo de informação a responsabilidades institucionais claramente definidas, transformando diretrizes normativas em um inventário concreto e passível de acompanhamento. Ao exigir a adoção de padrões comuns de metadados e vocabulários controlados, ele contribui ainda para a padronização semântica e para a coerência do ecossistema de dados em escala nacional.

Em conjunto, essas funções posicionam o Catálogo Nacional de Dados como um elemento estruturante da IND, que conecta normas, processos e tecnologias e cria condições para que os dados governamentais sejam efetivamente descobertos, compreendidos e reutilizados. Com essa base estabelecida, o eixo seguinte aprofunda os instrumentos voltados à qualificação e ao uso avançado da informação, dando continuidade à construção de um Estado orientado por dados.

7. PRIVACIDADE E SEGURANÇA

A privacidade e a segurança da informação constituem um eixo transversal da IND, presente em todas as etapas do ciclo de vida dos dados utilizados pelo Estado. Essas dimensões definem as condições de legitimidade, confiabilidade e sustentabilidade do uso intensivo de dados na ação governamental.

A ampliação do uso de dados pelo setor público expande a capacidade estatal de coordenação, eficiência e entrega de políticas e serviços. Esse movimento, no entanto, altera de maneira estrutural o perfil de riscos enfrentado pelo Estado.

A concentração e a interconexão de informações sensíveis sobre cidadãos, políticas públicas e funções estratégicas aumentam a exposição a incidentes de segurança, acessos não autorizados e usos incompatíveis com a finalidade pública. As consequências desse cenário alcançam direitos fundamentais, a confiança nas instituições e a soberania nacional.

Diante disso, a proteção da informação deixa de ser um tema operacional isolado e passa a exigir respostas ancoradas em políticas públicas, governança clara e capacidades institucionais permanentes.

7.1. Programa de Privacidade e Segurança da Informação (PPSI)

Em resposta aos riscos inerentes à gestão de dados no setor público, o governo federal instituiu uma política pública específica voltada ao fortalecimento das práticas de privacidade e segurança da informação. Trata-se do Programa de Privacidade e Segurança da Informação (PPSI), formalmente estabelecido pela Portaria SGD/MGI nº 852/2023.

Desde sua criação, o PPSI passou por um processo de evolução institucional que culminou na versão 2.0, instituída pela Portaria SGD/MGI nº 9.511/2025. Essa atualização consolidou uma inflexão relevante na arquitetura do programa ao combinar maior simplicidade operacional com o fortalecimento da governança. A incorporação explícita da Alta Administração como instância de responsabilidade estratégica reforça a conexão entre decisão política, gestão de riscos e implementação.

O objetivo principal do PPSI é elevar o nível de maturidade e resiliência em privacidade e segurança da informação no âmbito da Administração Pública Federal. Seu escopo de aplicação abrange todos os órgãos e entidades da administração direta, autárquica e fundacional que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

Para transformar esse objetivo em prática administrativa, o PPSI estrutura-se em cinco áreas temáticas interdependentes:

- **Governança:** definição de estruturas, papéis e responsabilidades;
- **Maturidade:** estabelecimento de mecanismos para mensuração e evolução das capacidades institucionais;
- **Metodologia:** definição do framework de controles e medidas a serem adotados;
- **Pessoas:** capacitação e conscientização dos agentes públicos;
- **Tecnologia:** orientação para a adoção de soluções e ferramentas tecnológicas seguras.

Essa organização expressa a lógica do programa: alinhar direção estratégica, capacidades institucionais e instrumentos operacionais. Nessa configuração, o PPSI 2.0 consolida-se como o principal mecanismo operacional do eixo de privacidade e segurança no âmbito da IND, funcionando como elo entre política pública, governança e implementação. Ao estabelecer um patamar mínimo comum e um percurso estruturado de melhoria contínua, o programa incorpora a proteção de dados e a segurança da informação como componentes permanentes da gestão pública digital.

A implementação desse arranjo é apoiada por frameworks, guias, modelos e cartilhas que orientam os órgãos públicos na estruturação, no acompanhamento e na consolidação de suas práticas. Esses instrumentos permitem acomodar diferentes níveis de maturidade institucional, preservando o alinhamento com uma arquitetura comum.

Entre eles, destaca-se o Guia do Framework de Privacidade e Segurança da Informação (MGI, 2025), que oferece diretrizes para a identificação, o monitoramento e o tratamento de lacunas institucionais em privacidade e segurança da informação. O guia fundamenta-se em controles desenvolvidos por referências normativas e técnicas internacionalmente reconhecidas, como o *Center for Internet Security* (CIS), o *National Institute of Standards and Technology* (NIST), as normas ISO/IEC e a ABNT NBR, assegurando convergência com padrões globais e aderência ao contexto regulatório brasileiro.

O framework está dividido em 3 segmentos Base, Segurança da Informação e Privacidade. Estruturados de forma progressiva, de modo a conectar fundamentos institucionais, controles técnicos e proteção de direitos.

O segmento base do framework concentra as ações essenciais que sustentam os demais componentes da política de privacidade e segurança da informação. Ele abrange dois controles centrais: a estruturação básica da governança, que define os papéis institucionais fundamentais — como Alta Administração, gestores de segurança da informação e de TIC, encarregado pelo tratamento de dados pessoais e responsável pela gestão da integridade — assegurando alinhamento estratégico, operacional e responsabilização; e os instrumentos fundamentais, que reúnem os principais programas, políticas e processos necessários à implementação da governança, incluindo os Programas de Governança em Privacidade e em Segurança da Informação, as políticas institucionais e os processos de gestão da segurança da informação alinhados à normativa vigente.

Nesse sentido, o PPSI distribui responsabilidades entre instâncias estratégicas, táticas e operacionais, assegurando que a privacidade e a segurança da informação sejam tratadas como temas institucionais, sob liderança direta da Alta Administração. As principais responsabilidades incluem:

- **Alta Administração:** responsável pela gestão dos riscos organizacionais relacionados à privacidade e à segurança da informação, incluindo o estabelecimento e o monitoramento do sistema de controles internos, a definição de prioridades e a alocação de recursos;
- **Gestores de TIC e de Segurança da Informação:** responsáveis pelo planejamento, execução e monitoramento das ações de tecnologia da informação e das medidas de privacidade e segurança nas soluções tecnológicas, considerando, quando aplicável, a cadeia de suprimentos;
- **Encarregado pelo Tratamento de Dados Pessoais:** responsável pela condução do diagnóstico de privacidade e pela orientação dos agentes de tratamento quanto ao planejamento, à implementação e ao acompanhamento das medidas de proteção de dados pessoais;
- **Responsável pela Gestão da Integridade:** atua no diagnóstico dos instrumentos fundamentais de governança do PPSI e na coordenação dos riscos à integridade associados à privacidade e à segurança da informação;
- **Comitê de Segurança da Informação:** delibera sobre matérias relacionadas à Política Nacional de Segurança da Informação e normas correlatas e, no âmbito do PPSI, apoia a definição de estratégias e a elaboração dos instrumentos fundamentais de governança em segurança da informação;

- **Comitê de Proteção de Dados Pessoais:** delibera sobre temas relacionados à Lei Geral de Proteção de Dados Pessoais, às resoluções da Autoridade Nacional de Proteção de Dados (ANPD) e a demais normas aplicáveis;
- **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):** responsável pela prevenção, tratamento e resposta a incidentes cibernéticos nos órgãos e entidades que administram sua própria infraestrutura de rede.

Já o segmento de segurança da informação essencialmente fundamentado no CIS Controls, cujo escopo foi correlacionado a decretos, normas da SGD/MGI e do GSI/PR, garantindo aderência ao ambiente regulatório brasileiro está dividido em 18 controles. Esses controles abrangem aspectos como o mapeamento de tratamentos, a gestão de riscos à privacidade, a adoção de salvaguardas técnicas e organizacionais e a incorporação de princípios de proteção de dados nos processos e sistemas governamentais.

De forma complementar, os segmentos de segurança da informação concentram controles destinados à proteção dos ativos informacionais do Estado contra acessos não autorizados, incidentes cibernéticos e indisponibilidade de sistemas. Esses controles abrangem medidas preventivas, detectivas e corretivas, incluindo gestão de vulnerabilidades, resposta a incidentes, continuidade de serviços e proteção das infraestruturas tecnológicas que sustentam o governo digital.

Ao estruturar a política em segmentos articulados e progressivos, o Framework do PPSI 2.0 oferece um referencial comum para toda a Administração Pública Federal, compatível com diferentes níveis de maturidade institucional. Esse desenho permite que os órgãos avancem de forma gradual, mantendo alinhamento com uma arquitetura comum de privacidade e segurança da informação, integrada à IND e às demais agendas de transformação digital do Estado.

7.2. Prevenção e Resposta a Incidentes

Ao traduzir esses controles em práticas efetivas, torna-se evidente que o funcionamento do framework não depende somente da existência de normas e orientações, como também da capacidade de prevenir e responder a incidentes de segurança da informação.

Nesse contexto, o Centro Integrado de Segurança Cibernética (CISC Gov.br), criado a partir do PPSI 1.0, desempenha função estratégica como instância central de coordenação da segurança cibernética no SISP. Sua atuação visa fortalecer a capacidade de defesa coletiva da Administração Pública Federal, promovendo respostas rápidas, integradas e consistentes a ameaças e incidentes.

Entre as principais funções coordenadas pelo CISC Gov.br destacam-se:

- a coordenação das equipes de resposta a incidentes (ETIR) dos órgãos, garantindo sincronização de esforços e compartilhamento tempestivo de informações;
- a implementação de monitoramento contínuo e de ações de inteligência de ameaças, permitindo a identificação proativa de vulnerabilidades e atividades maliciosas;
- a emissão de alertas e orientações para o ecossistema de governo digital, disseminando informações sobre novas ameaças e recomendando medidas preventivas e corretivas.

A eficácia do CISC Gov.br é ampliada por sua articulação com outras instituições estratégicas, atuando como um hub no ecossistema nacional de segurança cibernética. A cooperação com o Gabinete de Segurança Institucional (GSI), a Autoridade Nacional de Proteção de Dados (ANPD), a Polícia Federal (PF) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) assegura uma resposta abrangente, que integra capacidades técnicas de detecção, investigação, regulação e defesa nacional.

Essa abordagem evidencia que a resiliência institucional resulta tanto da coordenação interna quanto da cooperação interinstitucional, configurando uma postura de defesa em múltiplas camadas, sustentada por processos contínuos de capacitação e aprimoramento das práticas de segurança.

7.3. Capacitação e Cultura Organizacional

O Centro de Excelência em Privacidade e Segurança (CEPS Gov.br) atua na promoção da cultura organizacional em privacidade e segurança da informação. Ao reconhecer que os fatores humanos são componentes críticos da infraestrutura, o CEPS desenvolve ações de capacitação por meio de cursos de especialização, jogos educativos e disseminação de boas práticas.

Essas iniciativas visam fortalecer as competências dos agentes públicos, assegurando que as diretrizes normativas sejam incorporadas às rotinas operacionais e reduzindo riscos associados a falhas humanas, desconhecimento normativo ou aplicação inadequada de controles.

7.4. Monitoramento e Melhoria Contínua

O monitoramento desempenha função estratégica na gestão do PPSI ao permitir a avaliação sistemática da evolução da política, a identificação de gargalos e a orientação da alocação de recursos. No PPSI 2.0, esse acompanhamento integra um processo contínuo de aprendizagem institucional e aprimoramento progressivo.

A implementação do programa é acompanhada por meio de ciclos anuais de avaliação. Essa periodicidade, adotada a partir do PPSI 2.0 em substituição aos ciclos semestrais da versão anterior, oferece aos órgãos maior previsibilidade e tempo adequado para planejar e executar melhorias estruturais de maior complexidade.

A mensuração do nível de implementação e da maturidade institucional baseia-se em três indicadores principais:

- **iBase:** avalia o grau de implementação das medidas do segmento de Governança;
- **iPriv:** mede o nível de implementação das medidas de Privacidade;
- **iSeg:** mensura o grau de implementação das medidas de Segurança da Informação.

Ferramentas como o Painel do PPSI 2.0 conferem transparência ao processo de monitoramento, permitindo a visualização do progresso por categorias e do total de medidas implementadas em relação ao conjunto de exigências. Ressalta-se que o objetivo desse acompanhamento é subsidiar o diagnóstico e a gestão para a melhoria contínua, e não a aplicação de mecanismos meramente fiscalizatórios ou punitivos.

A análise longitudinal desses dados possibilita a identificação de desafios recorrentes e orienta o aperfeiçoamento contínuo da agenda de privacidade e segurança da informação no âmbito da IND.



8. INFORMAÇÕES GEOESPACIAIS

A dimensão territorial constitui o fundamento sobre o qual se estruturam as políticas públicas. A eficácia na oferta de serviços, na distribuição de infraestrutura e na proteção ambiental depende da compreensão de que as dinâmicas socioeconômicas se manifestam de forma heterogênea no espaço geográfico. Portanto, a informação geoespacial é parte da infraestrutura crítica que permite ao Estado localizar demandas e alocar recursos com precisão.

Nesse contexto, a IND incorpora o eixo de Informações Geoespaciais como parte de uma estratégia mais ampla de organização do uso de dados públicos, reconhecendo que a integração da dimensão espacial é fundamental para o planejamento, a execução e a avaliação de políticas públicas. A incorporação sistemática de dados georreferenciados amplia a capacidade de coordenação entre áreas de governo e fortalece a utilização de evidências no processo decisório.

8.1. Articulação entre IND e Infraestrutura Nacional de Dados Espaciais (INDE)

O eixo de Informações Geoespaciais da IND não substitui a Infraestrutura Nacional de Dados Espaciais (INDE), mas se articula a ela como parte de um ecossistema mais amplo de dados públicos. A INDE é a política setorial estruturante: seu foco é a organização, padronização e disseminação de dados espaciais. Ela estabelece os protocolos técnicos e as normas que garantem que um dado geográfico seja confiável, interoperável e acessível.

Enquanto a INDE concentra-se na organização especializada da geoinformação, a IND atua como infraestrutura integradora, conectando dados espaciais aos demais eixos de governança, interoperabilidade, catálogos, serviços digitais e uso analítico de dados. Essa articulação permite que informações georreferenciadas deixem de ser utilizadas apenas em contextos técnicos específicos e passem a integrar processos mais amplos de formulação de políticas públicas e prestação de serviços.

Nesse arranjo, a dimensão territorial é incorporada à lógica de integração de dados administrativos e operacionais do Estado, permitindo análises multissetoriais e aplicações práticas em diferentes áreas de atuação governamental.

8.2. Arranjo Institucional e Responsabilidades

A governança das informações geoespaciais no âmbito do Poder Executivo Federal é organizada por um modelo institucional distribuído, que combina coordenação técnica, definição de padrões e execução descentralizada nos órgãos produtores e usuários de dados. Nesse arranjo, destacam-se:

- **Comissão Nacional de Cartografia (CONCAR)**, vinculada ao Ministério do Planejamento e Orçamento, responsável pela coordenação da política cartográfica nacional e pela homologação de padrões técnicos aplicáveis à INDE;
- **Infraestrutura Nacional de Dados Espaciais (INDE)**, responsável por promover o ordenamento da geração, do armazenamento, do acesso e do compartilhamento de dados geoespaciais, além de incentivar a adoção de padrões e a divulgação de metadados;
- **Instituto Brasileiro de Geografia e Estatística (IBGE)**, responsável pela gestão do Diretório Brasileiro de Dados Geoespaciais, por meio do Sistema Integrado de Geoinformação (SIG Brasil), que funciona como ponto de descoberta de metadados;
- **Secretaria de Governo Digital (SGD/MGI)**, que atua na integração das informações geoespaciais às estratégias de governança de dados, interoperabilidade e serviços digitais, promovendo o alinhamento do uso de dados espaciais à lógica da IND;
- **Órgãos produtores de dados geoespaciais**, responsáveis pela geração, atualização e compartilhamento de bases e metadados, com participação obrigatória no âmbito do Executivo Federal e facultativa para outros entes federativos;
- **Órgãos usuários de dados geoespaciais**, que utilizam as informações para formulação de políticas públicas, planejamento e prestação de serviços, observando diretrizes de qualidade, segurança e uso ético dos dados.

Esse modelo busca compatibilizar a autonomia setorial na produção de dados com a necessidade de padronização e integração, criando condições para o reuso de informações e para a construção de análises territoriais mais abrangentes.

9. INTELIGÊNCIA ARTIFICIAL

As iniciativas de Inteligência Artificial (IA) conduzidas pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI) estão estruturadas de forma alinhada ao **Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028**, publicado em julho de 2024 e coordenado pelo Ministério da Ciência, Tecnologia e Inovação (MCTI). O PBIA organiza a política nacional de IA em cinco eixos:

- **Infraestrutura e Desenvolvimento de IA** – foco na criação e fortalecimento de capacidades tecnológicas, como centros de processamento e infraestrutura de dados e computação para IA.
- **Difusão, Formação e Capacitação em IA** – ações para ampliar a formação de profissionais, qualificação técnica e a difusão de conhecimentos sobre IA na sociedade e no setor produtivo.
- **IA para Melhoria dos Serviços Públicos** – aplicação de soluções de inteligência artificial para otimizar serviços públicos, aumentando eficiência e qualidade.
- **IA para Inovação Empresarial** – incentivo à adoção de IA no setor produtivo e estímulo à inovação nas empresas.
- **Apoio ao Processo Regulatório e de Governança da IA** – desenvolvimento de marcos regulatórios, governança ética e mecanismos de controle para uso responsável da IA.

Com investimento previsto de aproximadamente R\$ 23 bilhões ao longo de quatro anos, o plano busca posicionar o país como referência em inovação e uso estratégico da inteligência artificial, com ênfase no setor público. Nos dois primeiros anos de execução, cerca de R\$ 6,5 bilhões já foram aplicados, resultando na implementação de mais de 54 ações distribuídas entre os diferentes eixos.¹

No contexto da IND, a IA constitui simultaneamente um eixo temático e um vetor operacional. Embora, do ponto de vista formal da governança federal, parte das ações esteja vinculada ao PBIA, na prática a agenda de IA conduzida pelo MGI é tratada como componente integrado da IND, dada sua relação direta com interoperabilidade, uso estratégico de dados e modernização de serviços públicos.

1. Fonte: MCTI, 2025. Dados disponíveis em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial>.

9.1. Núcleo de Inteligência Artificial

Para a agenda federal de IA, o MGI e a IND operam por meio do Núcleo de Inteligência Artificial, um arranjo interinstitucional de coordenação e implementação que articula diferentes órgãos e parceiros técnicos. Ainda que o MGI (por meio da SGD e da IND) exerça função central de coordenação, a execução das frentes envolve múltiplos parceiros, como empresas públicas federais, escola de governo e instituições de fomento, refletindo a natureza sistêmica e colaborativa da política pública. O portfólio do Núcleo de IA organiza-se em 6 frentes agrupadas em 3 dimensões:

1. Soluções de IA

A frente de Soluções de IA tem como objetivo apoiar órgãos públicos no desenvolvimento e na adoção de aplicações de inteligência artificial voltadas a desafios concretos da administração pública. Essa dimensão organiza-se em duas frentes complementares: prospecção e estruturação e experimentação técnica de soluções, que, em conjunto, estruturam um fluxo contínuo de transformação de problemas institucionais em projetos tecnicamente viáveis.

A frente de prospecção e estruturação concentra-se na identificação e qualificação de demandas dos órgãos, incluindo etapas de captura de ideias, priorização, enquadramento do problema e definição do provedor da solução. Até 2026, está previsto que 25 projetos, distribuídos em 10 áreas de atuação, estejam nessa fase, com foco na tradução de necessidades operacionais em escopos técnicos compatíveis com processos de contratação ou fomento.

A frente de experimentação e validação técnica, por sua vez, destina-se à avaliação da viabilidade das soluções propostas, por meio de testes com algoritmos, protótipos e provas de conceito. Para o mesmo horizonte temporal, outros 25 projetos deverão estar nessa etapa, permitindo analisar desempenho, adequação ao contexto institucional e requisitos de integração com sistemas existentes antes de eventual escalonamento.

Um dos instrumentos centrais para viabilizar ambas as frentes é o modelo de fomento por meio de parcerias com o ecossistema nacional de inovação. Nesse arranjo, órgãos públicos apresentam problemas e demandas — como automação de processos, análise de manifestações de usuários, triagens e apoio a decisões administrativas — que orientam a formulação de chamadas públicas para que startups e empresas brasileiras proponham e desenvolvam soluções.

Instituições como Finep e BNDES atuam como financiadoras, enquanto o governo federal, na condição de demandante e comprador público, direciona o desenvolvimento tecnológico para necessidades reais da gestão pública.

O modelo combina, assim, dois objetivos complementares: viabilizar soluções de IA aplicáveis ao setor público e, simultaneamente, estimular o amadurecimento do mercado nacional de tecnologia, com efeitos sobre capacidades produtivas, geração de emprego qualificado e ampliação da oferta futura de serviços ao Estado.

Além dos projetos vinculados às rodadas de fomento, o portfólio inclui iniciativas conduzidas diretamente no âmbito do MGI, em diferentes estágios de planejamento e implementação, que complementam as frentes financiadas externamente e permitem testar soluções em contextos institucionais específicos.

2. Plataforma de IA para o setor público

No componente tecnológico, o Núcleo de IA desenvolve uma abordagem baseada em infraestrutura compartilhada e reutilizável: em vez de cada órgão contratar e construir isoladamente suas próprias soluções, busca-se disponibilizar uma plataforma central para acelerar a adoção e reduzir custos de transação.

A primeira prioridade é uma plataforma voltada a IA generativa, dado que a maior demanda identificada entre órgãos envolve chatbots, assistentes e agentes. A plataforma foi concebida para oferecer funcionalidades que suportem a criação e operação dessas soluções, incluindo mecanismos de segurança e controle (*guardrails*) e integração com técnicas de recuperação de informações (*retrieval augmented generation – RAG*) a partir de dados do governo, em linha com princípios e instrumentos da IND.

O desenho tecnológico busca ser agnóstico em relação a modelos de linguagem (LLMs), permitindo o uso combinado de modelos abertos e proprietários conforme necessidades de desempenho, custo e sensibilidade do uso. A disponibilização dessa plataforma aos órgãos pretende reduzir duplicações, acelerar cronogramas e aumentar a consistência institucional de soluções de IA. Após a consolidação do caso de uso de IA generativa, prevê-se a ampliação do portfólio tecnológico para outras categorias de IA, como processamento de imagens e biometria, entre outras.

3. Estruturantes

Já a dimensão Estruturante se divide em 3 frentes: capacitação; ética; e observatório.

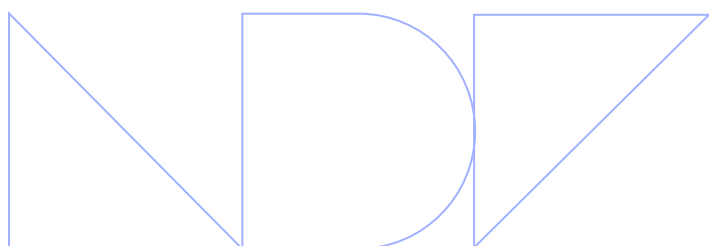
Na frente de capacitação, as ações foram desenhadas para diferentes perfis de servidores — desde alta liderança e gestão até perfis técnicos e agentes públicos — reconhecendo que a adoção efetiva exige competências distintas conforme responsabilidades e funções. Os programas são estruturados por trilhas, compostas por módulos e cursos, com metas de capacitação em larga escala. Estima-se que 115 mil servidores estarão capacitados em 2026.

Por sua vez a frente de ética e uso responsável, foi elaborada uma ferramenta orientadora em versão beta, concebida como um instrumento de avaliação e mitigação de riscos associados a sistemas de IA — incluindo riscos de discriminação, imprecisão, alucinações e outros impactos adversos. A estratégia de implementação segue abordagem incremental: aplicação em pilotos com órgãos selecionados, coleta de sugestões técnicas e institucionais, diálogo com atores relevantes e, posteriormente, publicação de versão final. Em etapa posterior, está prevista a eventual normatização do instrumento, após amadurecimento por testes e validação prática.

9.2. Observatório do Núcleo de IA

Por fim, o Núcleo mantém uma frente contínua de monitoramento e estatísticas de adoção de IA no setor público, por meio de levantamentos periódicos. A pesquisa busca mapear soluções existentes, tecnologias utilizadas, barreiras de implementação e grau de incorporação de práticas éticas. Os resultados são utilizados para orientar prioridades, identificar gargalos (como insuficiência de pessoal, recursos financeiros e infraestrutura) e apoiar o planejamento de ações futuras.

Ao articular soluções, infraestrutura e frentes estruturantes, a estratégia de IA no âmbito da IND consolida um arranjo voltado não apenas à experimentação tecnológica, mas à incorporação progressiva da inteligência artificial como instrumento regular de gestão pública. Essa incorporação, contudo, depende de condições que extrapolam o domínio específico da IA, como a existência de bases de dados confiáveis, mecanismos de interoperabilidade e estruturas de governança capazes de sustentar o uso intensivo de informação pelo Estado. Por essa razão, a agenda de IA se conecta diretamente aos demais eixos da IND, que estabelecem os fundamentos institucionais e tecnológicos para sua efetiva implementação.



10. AMBIENTE TECNOLÓGICO

Na IND, o eixo de Ambiente Tecnológico descreve o conjunto de arquiteturas, padrões, ferramentas, conexões e ativos de informação que sustentam a operação de sistemas governamentais e a prestação de serviços públicos digitais no âmbito do Poder Executivo Federal.

Nesse sentido, o ambiente tecnológico não se limita à infraestrutura física de tecnologia da informação, mas abrange também os mecanismos que permitem a integração entre sistemas, a interoperabilidade de dados e a operação contínua de serviços digitais em escala nacional.

À medida que políticas públicas e serviços passam a depender de fluxos de dados mais frequentes e integrados, a robustez desse ambiente se torna um fator crítico para garantir disponibilidade, desempenho, segurança e padronização, reduzindo riscos de interrupção e aumentando a previsibilidade operacional.

O ambiente tecnológico da IND é composto por três grandes camadas de infraestrutura: data centers, serviços de computação em nuvem e redes de conectividade. Esses componentes operam de forma complementar, permitindo diferentes arranjos técnicos conforme os requisitos de cada órgão e de cada tipo de dado ou sistema.

10.1. Data Centers

Os data centers constituem a base tradicional da infraestrutura de tecnologia da informação do governo federal, sendo responsáveis por assegurar a **disponibilidade, integridade e segurança das informações institucionais**. Os órgãos podem utilizar tanto data centers próprios quanto soluções baseadas em nuvem, de acordo com suas necessidades operacionais e estratégicas.

Os modelos de data center adotados na Administração Pública Federal são classificados em:

- **Data center tradicional**, caracterizado por instalações físicas gerenciadas diretamente pelos órgãos, que exigem investimentos contínuos em infraestrutura, energia, resfriamento, segurança e manutenção. Embora ofereçam maior controle direto sobre dados e sistemas, apresentam desafios relacionados à escalabilidade e à otimização de custos;
- **Data center híbrido**, que combina infraestrutura própria com serviços em nuvem, permitindo que determinadas cargas de trabalho permaneçam em ambientes internos enquanto outras são processadas em ambientes externos, ampliando a flexibilidade operacional e a resiliência dos sistemas.

No âmbito normativo, a Instrução Normativa SGD/ME nº 94/2022 estabelece que a computação em nuvem deve ser a estratégia prioritária para criação, ampliação ou renovação de infraestrutura de tecnologia da informação. A utilização de alternativas, como expansão de data centers próprios, exige comprovação de inviabilidade técnica da solução em nuvem por meio de estudo técnico preliminar.

A norma também determina que serviços em nuvem contratados devem atender às normas de segurança da informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e que os fornecedores privados possuam certificações reconhecidas para mitigação de riscos. Adicionalmente, os contratos devem garantir portabilidade de dados e de softwares, reduzindo riscos de aprisionamento tecnológico e permitindo a transferência de ambientes entre provedores ou infraestruturas.

10.2 Nuvem

A computação em nuvem passou a ocupar papel central no ambiente tecnológico da Administração Pública Federal, especialmente a partir de 2018, quando o governo federal iniciou processos de contratação conjunta para facilitar a aquisição e a gestão desses serviços pelos órgãos, promovendo padronização, compartilhamento de experiências e economia de recursos.

Não existe uma plataforma única e centralizada de fornecimento de nuvem para todos os órgãos. Cada órgão pode aderir às contratações centralizadas ou realizar seus próprios processos de contratação, o que resulta em múltiplos ambientes de gestão de nuvem, conforme os provedores contratados. Além disso, empresas públicas, como Serpro e Dataprev, ofertam serviços de nuvem, viabilizando ambientes híbridos que combinam infraestrutura local e serviços em nuvem pública ou privada.

Os serviços de nuvem são organizados segundo três modelos principais:

- **Infraestrutura como Serviço (IaaS)**, que fornece recursos básicos de computação, como servidores, rede e armazenamento, permitindo que os órgãos instalem sistemas operacionais e aplicações conforme suas necessidades;
- **Plataforma como Serviço (PaaS)**, que oferece ambientes completos para desenvolvimento e hospedagem de aplicações, incluindo licenças, infraestrutura e sistemas de comunicação;
- **Software como Serviço (SaaS)**, em que o fornecedor é responsável por toda a infraestrutura e pela operação do sistema, e o órgão utiliza a aplicação por meio da internet.

A definição do tipo de nuvem a ser utilizado está vinculada à classificação e criticidade dos dados, conforme estabelecido na Portaria SGD/MGI nº 5.950/2023. Essa classificação orienta a escolha entre diferentes modelos de implantação:

- **Nuvem pública**, operada por provedores públicos ou privados, destinada a dados sem restrição de acesso;
- **Nuvem privada ou interna**, dedicada ao uso exclusivo do órgão ou de entidades vinculadas, podendo ser operada por empresas públicas, com exigência de isolamento lógico e físico dos recursos;
- **Nuvem comunitária**, compartilhada por grupos específicos de órgãos com requisitos comuns, sob controle de pelo menos um dos participantes;
- **Nuvem híbrida**, que integra duas ou mais infraestruturas distintas, mantendo interoperabilidade e portabilidade de dados;
- **Nuvem de governo**, caracterizada por ambientes de nuvem privada ou comunitária geridos exclusivamente por órgãos ou empresas públicas.

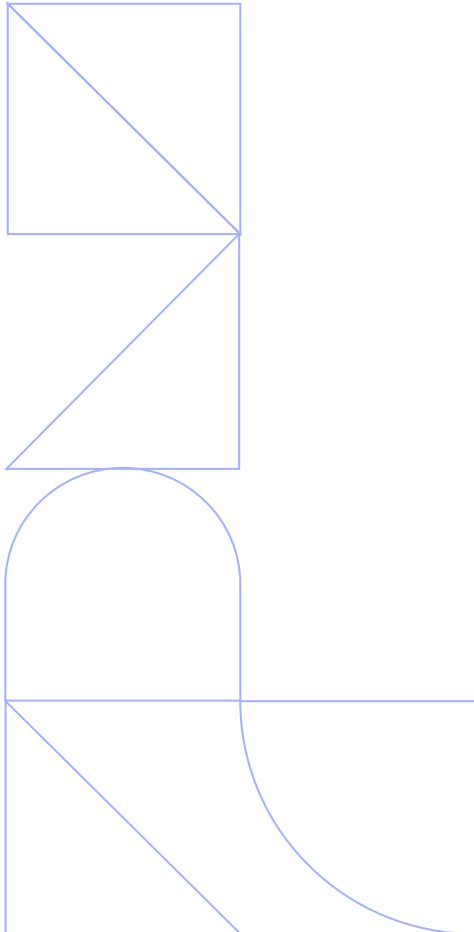
Esse arranjo permite acomodar diferentes níveis de sensibilidade das informações, conciliando requisitos de segurança, soberania digital e flexibilidade operacional.

10.3 Conectividade e Infovia Brasília

A conectividade é elemento central para a integração entre sistemas, órgãos e serviços digitais, permitindo o tráfego contínuo e seguro de dados no ambiente tecnológico da IND. No âmbito federal, destaca-se a Infovia Brasília, uma rede óptica metropolitana que atende órgãos federais e distritais no Distrito Federal, oferecendo serviços de alta disponibilidade e desempenho em ambiente seguro.

Implantada a partir de 2003, a Infovia resulta de arranjos institucionais que combinam infraestrutura própria do governo federal e o uso compartilhado de dutos e postes da Companhia Energética de Brasília. A operação da rede é realizada pelo Serpro, enquanto a expansão da malha contou com parcerias com instituições como a RNP, o Governo do Distrito Federal e a Telebras, permitindo ampliar a cobertura para além do Plano Piloto.

Atualmente, a rede conecta mais de 200 pontos em mais de 80 órgãos da Administração Pública Federal, com malha superior a 230 km de fibra óptica, sustentando aplicações corporativas e serviços digitais utilizados pelos órgãos federais em Brasília. Além da Infovia, outras tecnologias de conectividade, como SD-WAN e MPLS, integram o ambiente tecnológico, observadas as diretrizes do Decreto nº 12.124, de 30 de julho de 2024, aplicável à contratação de serviços de telecomunicações no setor público.



11. DECISÃO BASEADA EM DADOS

A consolidação de uma infraestrutura pública de dados encontra sua expressão mais direta quando as informações produzidas, integradas e governadas pelo Estado passam a orientar, de forma sistemática, as escolhas institucionais, a organização dos serviços e a formulação de políticas públicas. Nesse sentido, a decisão baseada em dados representa o ponto de convergência dos diferentes eixos da IND, traduzindo capacidades técnicas e arranjos de governança em uso efetivo de informações para a ação governamental.

Mais do que um conjunto de ferramentas analíticas, esse eixo reflete uma mudança estrutural na forma como o Estado utiliza seus próprios registros administrativos e fluxos informacionais: os dados deixam de ser subprodutos da atividade burocrática e passam a constituir insumos estratégicos para processos decisórios, operacionais e de planejamento. A decisão baseada em dados, portanto, depende não apenas da existência de bases integradas, mas da capacidade institucional de convertê-las em conhecimento aplicável, orientado por objetivos de eficiência, equidade e qualidade dos serviços públicos.

Esse processo exige a articulação de múltiplas capacidades: interoperabilidade entre sistemas, padrões de qualidade e governança dos dados, ambientes tecnológicos para processamento em escala, salvaguardas de privacidade e segurança, além de competências analíticas nos quadros técnicos da administração. Sem essa base estruturante, o uso de dados tende a permanecer restrito a iniciativas isoladas, com impacto limitado sobre políticas públicas e processos administrativos. Com ela, abre-se a possibilidade de decisões mais informadas, respostas mais rápidas a mudanças sociais e maior coordenação entre áreas governamentais.

No âmbito da execução da política federal, o eixo de decisão baseada em dados tem sido operacionalizado, de forma prioritária, por meio de aplicações voltadas à melhoria da experiência do cidadão e à eficiência dos serviços digitais, especialmente no ecossistema do portal gov.br, que concentra grande parte da interação entre Estado e sociedade. A opção por priorizar esse ambiente reflete uma estratégia institucional de concentrar esforços iniciais em casos de uso de alta escala, elevada visibilidade e impacto mensurável sobre a prestação de serviços públicos.

Entre os principais instrumentos atualmente em operação destacam-se três frentes complementares.

A recomendação de serviços utiliza análises de perfil e padrões de uso para sugerir, de forma contextualizada, serviços relevantes ao cidadão, considerando situações de vida, histórico de interações e informações cadastrais disponíveis no ecossistema governamental.

Essa funcionalidade contribui para organizar a jornada do usuário, reduzir barreiras de acesso e aumentar a probabilidade de que direitos e deveres administrativos sejam corretamente identificados e acionados no momento oportuno.

As notificações personalizadas constituem um mecanismo proativo de comunicação governamental, no qual o Estado identifica condições específicas — como prazos, elegibilidade a benefícios ou etapas de processos administrativos — e encaminha alertas direcionados aos usuários. Ao substituir comunicações genéricas por mensagens orientadas por dados, esse instrumento amplia a efetividade da comunicação pública, reduz assimetrias de informação e contribui para maior adesão a políticas e serviços.

A Caixa Postal Digital do Cidadão, integrada à conta gov.br, funciona como canal seguro e institucional para o envio de comunicações oficiais, protegendo o usuário contra fraudes e assegurando a integridade das mensagens. Esse instrumento fortalece a relação direta entre Estado e cidadão, permitindo comunicações estruturadas sobre direitos, deveres e serviços, com rastreabilidade e confiabilidade institucional.

Esses mecanismos ilustram como a decisão baseada em dados opera como camada de uso intensivo da infraestrutura informacional organizada pelos demais eixos da IND. A interoperabilidade possibilita o acesso integrado às bases; os catálogos e padrões permitem localizar e compreender os dados disponíveis; a governança define responsabilidades e condições de uso; a segurança e a privacidade asseguram proteção dos direitos; e os ambientes tecnológicos viabilizam o processamento analítico necessário para aplicações em escala.

À medida que essas capacidades se consolidam, amplia-se também o potencial de incorporação de técnicas analíticas mais avançadas, incluindo modelos preditivos e aplicações de inteligência artificial, capazes de apoiar políticas públicas em contextos de maior complexidade e incerteza. Essa evolução, contudo, requer alinhamento permanente com marcos éticos, mecanismos de transparência e supervisão institucional, de modo a garantir que o uso de dados fortaleça a legitimidade da ação estatal e preserve a confiança da sociedade.

Assim, a decisão baseada em dados não representa apenas uma etapa final da arquitetura da IND, mas um processo contínuo de aprendizagem institucional, no qual o Estado aprimora sua capacidade de observar a realidade, avaliar resultados e ajustar suas intervenções ao longo do tempo. Ao integrar dados, análise e ação pública em um mesmo ciclo, esse eixo materializa o objetivo central da IND: transformar informação em capacidade estatal e capacidade estatal em valor público.

12. ECOSISTEMA DE DADOS

Além dos 8 eixos transversais que estruturam a IND, o MGI vem desenvolvendo o conceito de ecossistemas de dados como uma forma de aplicar os instrumentos da IND em contextos temáticos e setoriais específicos. Essa abordagem parte do reconhecimento de que, em muitos domínios de política pública, os dados relevantes não se concentram em um único órgão ou sistema, mas distribuem-se entre múltiplos atores institucionais.

Os ecossistemas de dados são concebidos como arranjos organizacionais e técnicos voltados à articulação de fluxos de informação, responsabilidades institucionais e necessidades analíticas em torno de um determinado tema — como saúde, educação, meio ambiente ou transporte — ou de recortes transversais que atravessam diferentes políticas públicas, como a primeira infância. Trata-se de uma frente em construção, orientada à aplicação coordenada das disciplinas da IND em realidades setoriais com dinâmicas próprias.

Essa estratégia reforça a compreensão da IND como uma infraestrutura distribuída, capaz de sustentar tanto integrações horizontais entre órgãos quanto integrações verticais em cadeias de políticas públicas, sem pressupor a centralização física de dados em repositórios únicos.

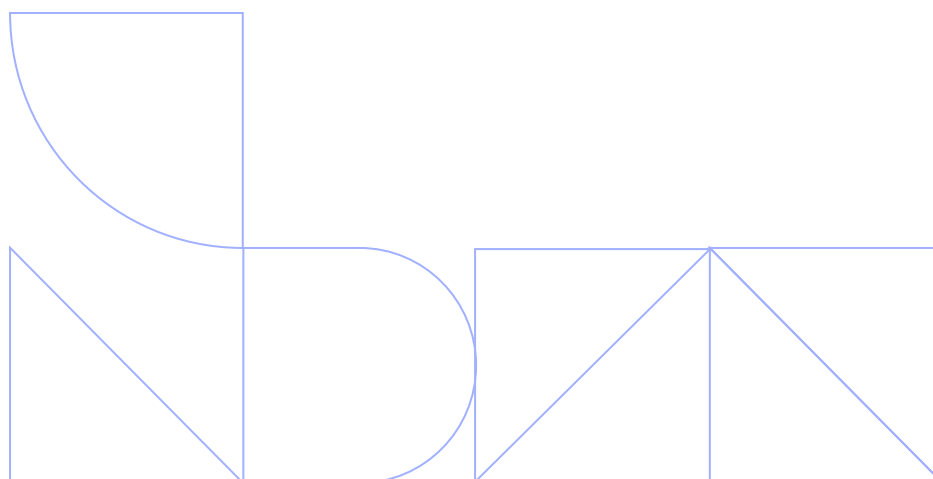
Em setores como saúde, educação ou assistência social, os dados necessários à formulação e à execução de políticas públicas são produzidos por uma diversidade de instituições, incluindo órgãos federais, estaduais e municipais, unidades prestadoras de serviços, entidades reguladas e, em alguns casos, organizações privadas. Esse cenário impõe desafios específicos de coordenação, padronização e compartilhamento de informações.

No caso da saúde, por exemplo, além do ministério setorial, participam do ecossistema hospitais, clínicas, laboratórios, farmácias, operadoras de planos de saúde, secretarias estaduais e municipais e órgãos reguladores. Cada um desses atores opera sistemas próprios, com lógicas distintas de coleta, armazenamento e uso de dados. Situação semelhante ocorre em áreas como educação, meio ambiente e infraestrutura.

Essa multiplicidade de atores implica que os desafios de governança, interoperabilidade, proteção de dados pessoais e qualidade da informação variam conforme o contexto temático. Políticas públicas com forte componente territorial, elevado grau de sensibilidade de dados ou grande heterogeneidade institucional exigem soluções de coordenação específicas, que não podem ser plenamente endereçadas apenas por instrumentos transversais.

No conjunto da IND, os ecossistemas de dados desempenham o papel de conectar capacidades técnicas e instrumentos institucionais às realidades específicas das políticas públicas. Ao aplicar os eixos da IND em recortes temáticos, essa abordagem permite enfrentar desafios de coordenação intersetorial, ampliar o uso de evidências na gestão pública e promover serviços mais integrados ao cidadão.

Essa estratégia consolida a IND como uma infraestrutura adaptável, capaz de sustentar tanto soluções transversais quanto aplicações especializadas, fortalecendo a capacidade do Estado de utilizar dados de forma coordenada, segura e orientada a resultados sociais.



13. A INFRAESTRUTURA NACIONAL DE DADOS COMO CAPACIDADE ESTATAL

A consolidação da IND expressa a transição do Estado brasileiro para um modelo de governança sistêmica da informação, no qual os dados deixam de ser tratados como subprodutos administrativos e passam a constituir um elemento estruturante da capacidade estatal. Nesse arranjo, a produção, o compartilhamento e o uso de dados são organizados de forma coordenada, com regras comuns, responsabilidades institucionais definidas e integração entre políticas públicas, sistemas e níveis de governo.

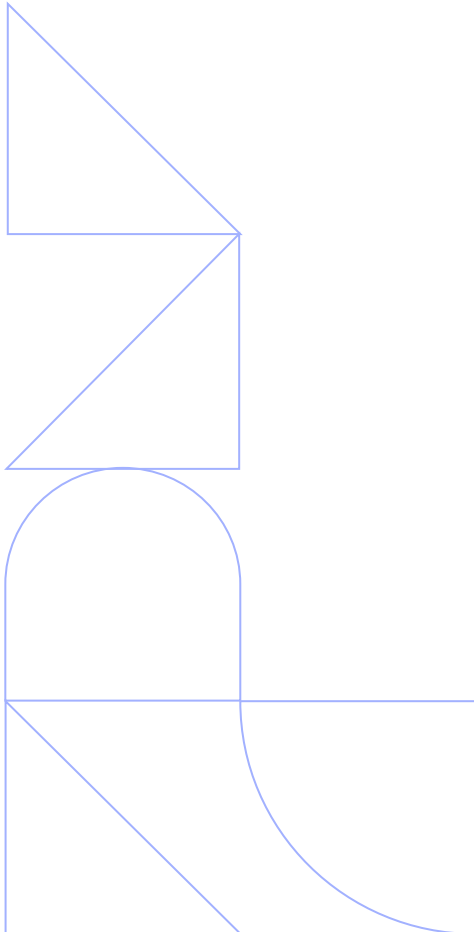
Os resultados já observáveis da IND são concretos, mensuráveis e verificáveis em escala nacional e internacional. O Estado brasileiro opera, atualmente, seus dados de maneira integrada, com efeitos diretos sobre a simplificação de serviços, a redução de custos administrativos e o fortalecimento da capacidade de coordenação governamental. A plataforma Conecta Gov.br, por exemplo, viabilizou mais de 2,25 bilhões de transações de dados entre sistemas públicos e gerou uma economia acumulada estimada em R\$ 12,98 bilhões entre 2020 e 2025, decorrente da eliminação de exigências redundantes, da automação de fluxos informacionais e da racionalização de processos internos. Esses resultados refletem ganhos efetivos já incorporados às rotinas da administração pública, com impactos diretos para cidadãos, empresas e para o próprio Estado.

Essa evolução institucional se expressa na conformação de um ambiente no qual segurança da informação, proteção de dados pessoais e uso de tecnologias emergentes, como a inteligência artificial, passam a operar de forma integrada, e não como agendas isoladas. A convergência entre o marco de governança de dados e as salvaguardas de privacidade e segurança estabeleceu um padrão institucional de integridade que orienta a gestão e o uso de informações no setor público. Ao internalizar princípios como o *once-only* e a adoção de “fontes únicas de verdade”, o ônus da comprovação e da busca por informações é minimizado, ampliando a maturidade operacional do Estado e assegurando maior tempestividade, precisão e previsibilidade no acesso a direitos e serviços públicos.

Esses avanços produzem efeitos observáveis na relação entre Estado e sociedade. A redução da rerepresentação de documentos, a ampliação de serviços digitais integrados e o uso mais preciso e proativo da comunicação governamental contribuem para a diminuição de barreiras administrativas, o aumento da previsibilidade regulatória e a redução de custos de conformidade. De forma concomitante, a consolidação de salvaguardas institucionais de privacidade e segurança garante que a ampliação do uso de dados ocorra com proteção de direitos, rastreabilidade e responsabilização, reforçando a confiança pública como componente central do funcionamento dessa infraestrutura.

No âmbito interno da administração pública, a gestão do ciclo de vida dos dados passa a constituir uma responsabilidade institucional permanente, incorporada às rotinas de planejamento, execução e avaliação de políticas públicas. A obrigatoriedade de programas formais de governança de dados, a consolidação de registros de referência e a padronização de linguagens e classificações reduzem assimetrias informacionais entre órgãos, fortalecem a qualidade dos registros administrativos e ampliam a capacidade de uso transversal das informações públicas, em bases estáveis e reutilizáveis.

Esse processo apoia-se em um acúmulo histórico de sistemas setoriais, cadastros administrativos e competências técnicas já consolidadas. O valor agregado da IND reside precisamente na elevação desse conjunto de ativos a um novo nível de coordenação, integração e maturidade institucional. Ao articular governança, interoperabilidade, catalogação, proteção de dados, ambiente tecnológico e uso analítico em um mesmo arranjo, a IND eleva ativos já existentes a um novo patamar de coordenação e maturidade, convertendo capacidades dispersas em capacidade estatal sistêmica, apta a sustentar políticas públicas complexas em um Estado orientado por dados.



14. EXPERIÊNCIAS INTERNACIONAIS COMPARADAS

Conforme delineado nas seções anteriores, a Infraestrutura Nacional de Dados (IND) insere-se em um movimento estrutural mais amplo de consolidação de Infraestruturas Públicas Digitais no plano internacional. A análise precedente permitiu examinar seus fundamentos normativos, arquiteturais e institucionais no contexto brasileiro. Nesta seção, retoma-se o referencial internacional com o objetivo de posicionar a IND em perspectiva comparada, situando suas capacidades técnicas e seu desenho de governança no interior de padrões observados em outras jurisdições. Diante da amplitude e diversidade de experiências internacionais análogas, a análise concentrou-se em cinco casos selecionados como amostra analítica: a Australian Government Architecture (AGA), na Austrália; a Infraestructura Nacional de Datos, na Colômbia; a Agency for Digital Government, na Dinamarca; a Estonian Information System Authority (RIA), na Estônia; e a Agenzia per l'Italia Digitale (AgID), na Itália.

A seleção desses casos segue dois critérios metodológicos centrais: equivalência funcional e arranjo institucional. Equivalência funcional refere-se ao grau em que a experiência analisada desempenha funções que dialogam diretamente com aquelas atribuídas ou pretendidas para a IND brasileira, por exemplo, coordenação de padrões de interoperabilidade; catálogo nacional de dados; definição de fontes autoritativas para dados básicos; provisão de infraestrutura tecnológica comum; e estabelecimento de regras de segurança cibernética e privacidade em escala nacional. Arranjo institucional refere-se ao desenho de governança, entendido como a existência de uma autoridade central com mandato explícito de coordenação, estratégia nacional formalizada e instrumentos de imposição capazes de produzir coesão em um ecossistema historicamente fragmentado.

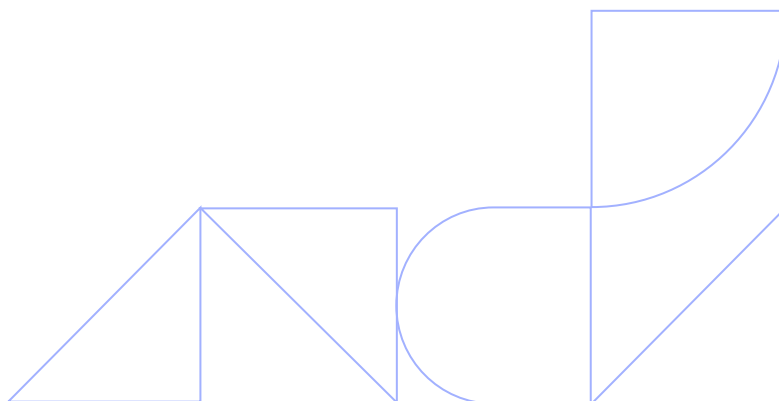


Figura 1. Mapeamento de Aderência Institucional por Eixo Estruturante da Infraestrutura Nacional de Dados (IND)

EIXO/PAÍS	AUSTRÁLIA AUSTRALIAN GOVERNMENT ARCHITECTURE (AGA)	COLÔMBIA INFRAESTRUTURA NACIONAL DE DATOS (IND)	DINAMARCA AGENCY FOR DIGITAL GOVERNMENT	ESTÔNIA INFORMATION SYSTEM AUTHORITY (RIA)	ITÁLIA AGENZIA PER L'ITALIA DIGITALE (AGID)
GOVERNANÇA DE DADOS	✓	✓	✓	✓	✓
INTEROPERABILIDADE	✓	✓	✓	✓	✓
CATÁLOGO DE DADOS	✓	✓	✓	✓	✓
PRIVACIDADE E SEGURANÇA	✓	✓	✓	✓	✓
INFORMAÇÕES GEOESPACIAIS	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL
INTELIGÊNCIA ARTIFICIAL	✓	✓	✓	✓	✓
AMBIENTE TECNOLÓGICO	✓	✓	✓	✓	✓
DECISÃO BASEADA EM DADOS	✓	✓	✓	✓	✓

Fonte: elaboração própria a partir de análise documental oficial dos países selecionados.

A análise comparada de infraestruturas nacionais de dados evidencia que a viabilidade de tais arquiteturas depende, em primeira instância, da constituição de um mandato central capaz de articular padronização técnica, indução de adesão e monitoramento de implementação sem deslocar a custódia descentralizada das bases.

A IND insere-se nesse padrão de forma estruturalmente coerente. O arranjo revela, contudo, que a forma pela qual o mandato central se materializa varia significativamente entre jurisdições.

Na Austrália, a Digital Transformation Agency (DTA) o exerce por meio da Australian Government Architecture (AGA), que integra disciplina de arquitetura, planejamento de capacidades transversais e alinhamento de investimentos digitais a objetivos sistêmicos comuns (AUSTRALIAN GOVERNMENT, 2024).

Já na Itália, o Codice dell'Amministrazione Digitale (CAD) e o Piano Triennale per l'Informatica nella Pubblica Amministrazione conferem obrigatoriedade às diretrizes da Agenzia per l'Italia Digitale (AgID), reforçadas pela exigência de um responsável interno pela transição digital em cada órgão (AGID, 2023a; AGID, 2024).

Por outro lado, na Dinamarca, a Agency for Digital Government estrutura estratégias plurianuais pactuadas em múltiplos níveis de governo (DINAMARCA, 2016; DINAMARCA, 2023);

Em comparação na Estônia, a Public Information Act ancora juridicamente o modelo e a Information System Authority (RIA) concentra competências regulatórias, técnicas e de cibersegurança (RIA, 2020; VASSIL, 2015)

Por fim, na Colômbia, o Decreto 1389/2022 e o Plan Nacional de Infraestructura de Datos (PNID) distribuem responsabilidades entre o MinTIC, o DNP, o DANE e a Agencia Nacional Digital (AND) (COLOMBIA, 2022a; COLOMBIA, 2022b).

A evidência comparada sugere que o núcleo funcional permanece convergente — mandato formal, instrumentos normativos com efetividade operacional e mecanismos de responsabilização — enquanto a forma institucional específica responde às trajetórias constitucionais e administrativas de cada Estado.

No caso brasileiro, esse núcleo é condicionado por uma especificidade estrutural ausente nas demais experiências examinadas: a combinação de escala continental, com mais de 200 milhões de habitantes, e de uma federação tripartite com autonomia constitucional de estados e municípios. Essa configuração institucional específica não encontra equivalente direto entre os casos de referência — a Austrália, embora federal, opera em escala demograficamente distinta; a Estônia e a Dinamarca não apresentam grau comparável de complexidade federativa. A consequência arquitetural mais direta é a ênfase na descentralização da custódia e na interoperabilidade como mecanismo primário de coordenação, em detrimento de soluções baseadas na centralização de bases. A concepção de ecossistemas de dados setoriais — saúde, educação, primeira infância — como modalidades temáticas de aplicação da IND reflete, igualmente, a necessidade de articular atores institucionais distribuídos nos três níveis da federação dentro de uma lógica informacional coerente.

É precisamente nessa camada de interoperabilidade que se observa uma das diferenciações arquiteturais mais relevantes. A IND opera o Conecta Gov.br como barramento nacional de APIs com controle de acesso e rastreabilidade, funcionando como camada de orquestração centralizada sem armazenamento permanente dos dados transacionados.

A Estônia e a Colômbia adotam o X-Road — solução de código aberto com arquitetura descentralizada em que cada entidade mantém servidor de segurança próprio e os dados permanecem nos sistemas de origem (RIA, 2020; AND, 2020). A Itália estrutura a Piattaforma Digitale Nazionale Dati (PDND) para integrar publicação, descoberta e governança de APIs entre administrações (DTD, 2021; AGID, 2023a). Ambas as topologias — orquestração centralizada e verificação distribuída pelas entidades participantes — preservam a custódia descentralizada e garantem rastreabilidade, mas implicam configurações distintas de escalabilidade, governança de incidentes e potencial de extensão transfronteiriça. Esta última dimensão encontra expressão mais desenvolvida na cooperação Estônia-Finlândia no âmbito do Nordic Institute for Interoperability Solutions (NIIS), consórcio internacional que transformou o X-Road em bem público multilateral com adoção por múltiplos países, incluindo a Colômbia (EUROPEAN COMMISSION, 2023). A IND, dada sua escala operacional interna, situa-se em uma trajetória de interoperabilidade exclusivamente doméstica, o que constitui uma dimensão ainda em desenvolvimento no plano institucional comparado.

A consistência informacional do Estado — condição necessária para que a interoperabilidade produza efeitos substantivos — é viabilizada, em todas as experiências examinadas, pela definição formal de fontes autoritativas para dados essenciais. Os Registros de Referência da IND cumprem essa função no arranjo brasileiro. A Dinamarca estrutura registros básicos de pessoas, empresas, imóveis, endereços e geodados distribuídos em escala nacional via Datafordeler no âmbito do Basic Data Programme (DINAMARCA, 2016; DINAMARCA, 2018); a Estônia veda normativamente a duplicação de bases e exige consulta direta às fontes autoritativas em tempo real (VASSIL, 2015; EUROPEAN COMMISSION, 2023); e a Colômbia atribui responsabilidade explícita às entidades gestoras pelos registros padronizados e interoperáveis (COLOMBIA, 2022b).

A análise indica que as trajetórias se distinguem pelo grau de consolidação operacional, não pelo princípio de desenho institucional, que permanece convergente. A experiência estoniana aponta, nesse domínio, para um padrão funcional em que serviços baseados em eventos de vida consultam dados em tempo real via X-Road com pré-preenchimento automático de formulários — modelo construído sobre uma infraestrutura de registros de longa data de consolidação (WORLD BANK, 2020; INFORMATION SYSTEM AUTHORITY, 2020). A Dinamarca registra exemplos análogos de automação de relatórios de negócios e otimização diagnóstica na saúde (DINAMARCA, 2022a).

A governança semântica, que torna os ativos informacionais identificáveis, interpretáveis e reutilizáveis, constitui camada complementar à interoperabilidade técnica em todas as experiências analisadas. A IND estrutura essa função por meio do Portal Brasileiro de Dados Abertos e do Catálogo Nacional de Dados, organizados sob DCAT-BR e o Vocabulário

Controlado de Governo Eletrônico (VCGE). Arranjos homólogos operam no data.gov.au australiano (AUSTRALIAN GOVERNMENT, 2024), no dati.gov.it italiano — com adoção obrigatória do perfil nacional DCAT-AP_IT (AGID, 2023a) —, no datos.gov.co colombiano (COLOMBIA, 2022b) e no Datavejviser.dk dinamarquês (DINAMARCA, 2023).

A experiência estoniana aprofunda o escopo dessa camada: o RIHA (Riigi Infosüsteemi Haldussüsteem), mantido pela RIA, funciona como registro obrigatório de sistemas e ativos informacionais — inclusive de caráter restrito — assegurando visibilidade estrutural abrangente do ecossistema digital do Estado (INFORMATION SYSTEM AUTHORITY, 2020). Essa extensão do inventário semântico a ativos não públicos representa uma dimensão de institucionalização cujo equivalente ainda se encontra em configuração no contexto brasileiro.

No que se refere às informações geoespaciais, observa-se um padrão institucional relativamente convergente entre as experiências analisadas. Assim como no Brasil, onde a Infraestrutura Nacional de Dados Espaciais (INDE) opera com mandato próprio e arranjo institucional específico, os demais países dispõem de órgãos ou infraestruturas dedicadas à coordenação, padronização e disponibilização de dados geoespaciais. Embora essas estruturas não estejam formalmente subordinadas às arquiteturas centrais de governança de dados ou de governo digital, elas desempenham função transversal, dada a relevância da dimensão territorial para múltiplas políticas públicas. Em diversos casos, verifica-se a existência de mecanismos de articulação técnica e normativa entre a infraestrutura geoespacial e a arquitetura nacional de dados, incluindo definição de padrões mínimos de interoperabilidade, metadados e compartilhamento, de modo a assegurar consistência semântica e compatibilidade entre os ecossistemas. Essa configuração evidencia uma diferenciação institucional — com mandatos próprios para o domínio geoespacial — combinada a uma crescente integração funcional entre as infraestruturas de dados administrativas e territoriais.

Privacidade e cibersegurança são tratadas, em todas as jurisdições examinadas, como elementos constitutivos da infraestrutura, e não como políticas externas a ela. No Brasil, esse arranjo articula a Lei Geral de Proteção de Dados Pessoais (LGPD — Lei nº 13.709/2018), a atuação regulatória da Autoridade Nacional de Proteção de Dados (ANPD), o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br), o Centro de Excelência em Privacidade e Segurança (CEPS Gov.br) e o Programa de Privacidade e Segurança da Informação (PPSI).

A Austrália opera sob o Privacy Act 1988 e o Protective Security Policy Framework (AUSTRALIAN GOVERNMENT, 2023; OAIC, 2025); a Estônia e a Itália combinam o GDPR com instrumentos nacionais como o Estonian Information Security Standard (E-ITS) e a Agenzia per la Cybersicurezza Nazionale (ACN) (EUROPEAN COMMISSION, 2023; AGID, 2023b); e a Colômbia estrutura resposta a incidentes a partir do CSIRT Governamental (DNP, 2018).

O arranjo convergente consiste na combinação de salvaguardas legais com capacidades operacionais que tornam os padrões aplicáveis em escala. A experiência estoniana introduz, nesse domínio, uma dimensão de transparência ativa para o titular dos dados: o Personal Data Usage Monitor permite que cidadãos verifiquem diretamente quais órgãos acessaram seus dados, em que momento e com qual finalidade (EUROPEAN COMMISSION, 2023). Esse instrumento transforma a rastreabilidade das transações em um direito exercitável individualmente, configurando uma etapa de institucionalização da relação entre infraestrutura e titular que se encontra em desenvolvimento no arranjo brasileiro, a despeito do marco legal que a LGPD já provê para tal.

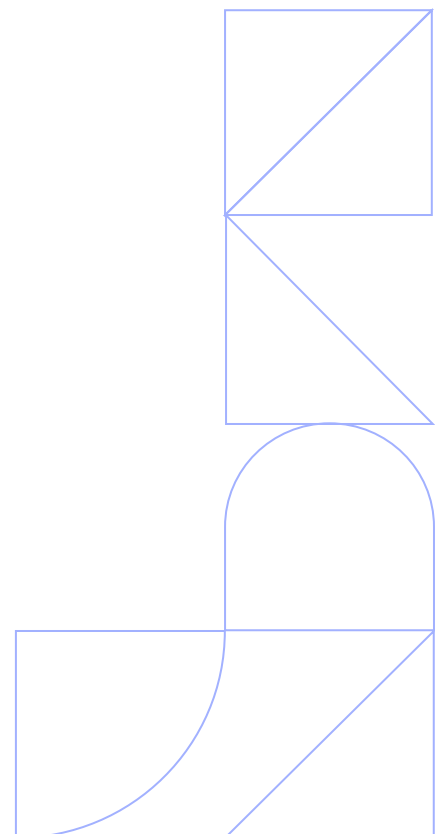
A governança de inteligência artificial apresenta padrão similar de convergência institucional: em todas as experiências examinadas, a IA é tratada como extensão da governança de dados, não como política dissociada da infraestrutura. O Brasil coordena essa agenda por meio do Plano Brasileiro de Inteligência Artificial (PBI), conduzido pelo Ministério da Ciência, Tecnologia e Inovações (MCTI), e do Núcleo de Inteligência Artificial do MGI, responsável pela coordenação federal do uso de IA. A Austrália adota política de uso responsável com exigências de responsabilização e transparência (AUSTRALIAN GOVERNMENT, 2024); a Estônia integra a governança de IA aos frameworks de risco e segurança sob coordenação da RIA (RIA, 2024); a Itália estrutura estratégia 2024–2026 articulada à AgID (AGID, 2023b); e a Colômbia formaliza diretrizes no CONPES 3975 em alinhamento aos princípios da OCDE (DNP, 2019; OCDE, 2020). A análise indica que a inserção da IA como camada complementar à infraestrutura de dados é o vetor institucional predominante nas jurisdições de referência.

A base tecnológica segue trajetória igualmente convergente: nuvem e plataformas compartilhadas são concebidas como camada habilitadora transversal, com segmentação proporcional à sensibilidade dos dados. A IND formaliza essa orientação por meio da Instrução Normativa SGD/ME nº 94/2022 e da Portaria SGD/MGI nº 5.950/2023, que definem modalidades e requisitos diferenciados por nível de risco. A Austrália adota política cloud-first via Cloud Computing Policy (POL10) (AUSTRALIAN GOVERNMENT, 2024); a Itália articula essa diretriz à construção do Polo Strategico Nazionale (PSN), infraestrutura de nuvem soberana para ativos críticos com certificação de provedores pela AgID (AGID, 2023b); a Dinamarca opera o GovCloud como ambiente seguro dedicado às agências públicas (DINAMARCA, 2023); e a Estônia estabelece padrões técnicos homogêneos para uso de provedores externos sem configurar nuvem governamental centralizada (EUROPEAN COMMISSION, 2023).

A IND contempla múltiplas modalidades de nuvem e orienta a contratação centralizada por instrumentos transversais, situando-se em um ritmo de implementação distinto dos casos em que a nuvem governamental já opera como ambiente integrado e certificado — dimensão com potencial de aprofundamento por meio das capacidades instaladas em empresas públicas como Serpro e Dataprev.

Um vetor de evolução institucional observado nas experiências comparadas e sem correspondente explícito na IND concerne ao conceito de digital-ready legislation, formalizado pela Dinamarca como política pública da Agency for Digital Government (DINAMARCA, 2018). Nesse modelo, novas leis são concebidas para serem administradas digitalmente desde sua formulação, incorporando pressupostos de interoperabilidade, reuso de registros existentes e compatibilidade com a infraestrutura disponível como condicionantes do próprio processo legislativo. O ambiente normativo brasileiro — constituído pela Lei de Acesso à Informação (Lei nº 12.527/2011), pela LGPD, pela Lei de Governo Digital (Lei nº 14.129/2021) e pelo Decreto nº 10.046/2019 — estabelece os marcos estruturantes do funcionamento da IND, mas não incorpora, ainda, uma política sistemática que condicione a produção normativa à infraestrutura de dados disponível. A institucionalização progressiva desse princípio representaria uma etapa de integração entre governança de dados e processo normativo observada em outras trajetórias de referência.

A evidência comparada, tomada em sua integralidade, posiciona a IND como capacidade estatal em constante processo de expansão no padrão internacional de Infraestruturas Públicas Digitais. O conjunto do arranjo revela uma infraestrutura cujas escolhas estruturais respondem coerentemente ao contexto nacional e cujas trajetórias de evolução encontram referências comparadas em experiências internacionais consolidadas.



REFERÊNCIAS

AGID. *Linee guida Open Data*. Roma: Agenzia per l'Italia Digitale, 2023.

AGID. *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026*. Roma: Agenzia per l'Italia Digitale, 2023b.

AGID. *Linee guida sul documento informatico*. Roma: Agenzia per l'Italia Digitale, 2024.

AND (AGENCIA NACIONAL DIGITAL). *Plataforma de Interoperabilidad (PDI)*. Bogotá: AND, 2020.

AUSTRALIAN GOVERNMENT. *2023–2030 Australian Cyber Security Strategy*. Canberra: Australian Government, 2023.

AUSTRALIAN GOVERNMENT. *Australian Government Architecture*. Canberra: Digital Transformation Agency, 2024.

AUSTRALIAN GOVERNMENT. *Protective Security Policy Framework (PSPF)*. Canberra: Australian Government, 2025.

BANCO MUNDIAL. *GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide*. Washington, DC: World Bank, 2025. Disponível em: <https://www.worldbank.org/en/programs/govtech/gtmi-2025-update>.

BANCO MUNDIAL. *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank, 2021. Disponível em: <https://www.worldbank.org/en/publication/wdr2021>.

BRASIL. *Conecta GOV.BR — Infraestrutura Nacional de Dados: Interoperabilidade*. Brasília, 2025a. Disponível em: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/interoperabilidade/conecta-gov.br>.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Diário Oficial da União: seção 1, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Diário Oficial da União: seção 1, Brasília, DF, 10 out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Diário Oficial da União: seção 1, Brasília, DF, 30 mar. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm.

BRASIL. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022. Diário Oficial da União: seção 1, Brasília, DF, 23 dez. 2022. Disponível em: <https://www.in.gov.br/web/dou/-/instrucao-normativa-sgd/me-n-94-de-23-de-dezembro-de-2022-452604048>.

BRASIL. Decreto nº 12.124, de 30 de julho de 2024. Diário Oficial da União: seção 1, Brasília, DF, 31 jul. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12124.htm.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

Estratégia de Governo Digital 2024–2027. Brasília: MGI, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/EGD2024>.

BRASIL. Ministério da Ciência, Tecnologia e Inovações (MCTI). *Plano Brasileiro de Inteligência Artificial.* Brasília: MCTI, 2025d. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial>.

COLOMBIA. Decreto 1389 de 2022. Bogotá: Gobierno de Colombia, 2022a.

COLOMBIA. *Plan Nacional de Infraestructura de Datos (PNID).* Bogotá: Gobierno de Colombia, 2022b.

DEPARTAMENTO NACIONAL DE PLANEACIÓN (DNP). Documento CONPES 3975. Bogotá: DNP, 2019.

DINAMARCA. *The Joint Government Digital Strategy 2016–2020.* Copenhagen: Digitaliseringsstyrelsen, 2016.

DINAMARCA. *Digital-ready legislation.* Copenhagen: Digitaliseringsstyrelsen, 2018.

DINAMARCA. *National Strategy for Cyber and Information Security.* Copenhagen: Government of Denmark, 2023.

EUROPEAN COMMISSION. *Digital Public Administration Factsheet: Estonia.* Brussels: European Commission, 2023.

INFORMATION SYSTEM AUTHORITY. *2020 Yearbook of RIA.* Tallinn: Information System Authority, 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *United Nations E-Government Survey 2022: The Future of Digital Government.* Nova York: United Nations, 2022.

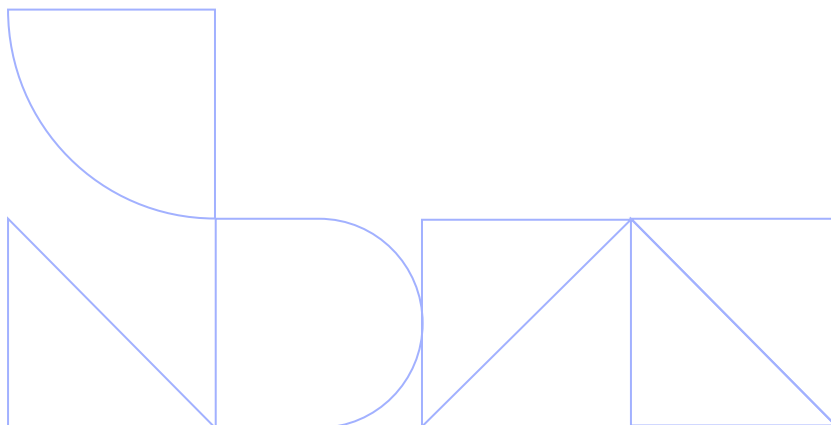
ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government.* Paris: OECD Publishing, 2020.

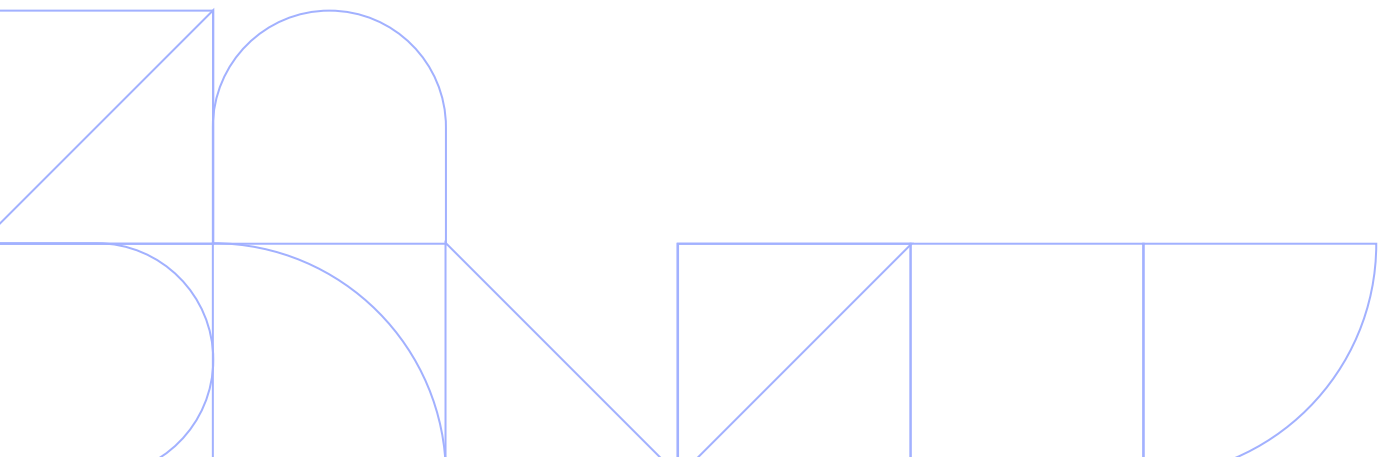
PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (PNUD); BANCO MUNDIAL; FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). *50-in-5: Digital Public Infrastructure for People and Planet.* Nova York: UNDP, 2023.

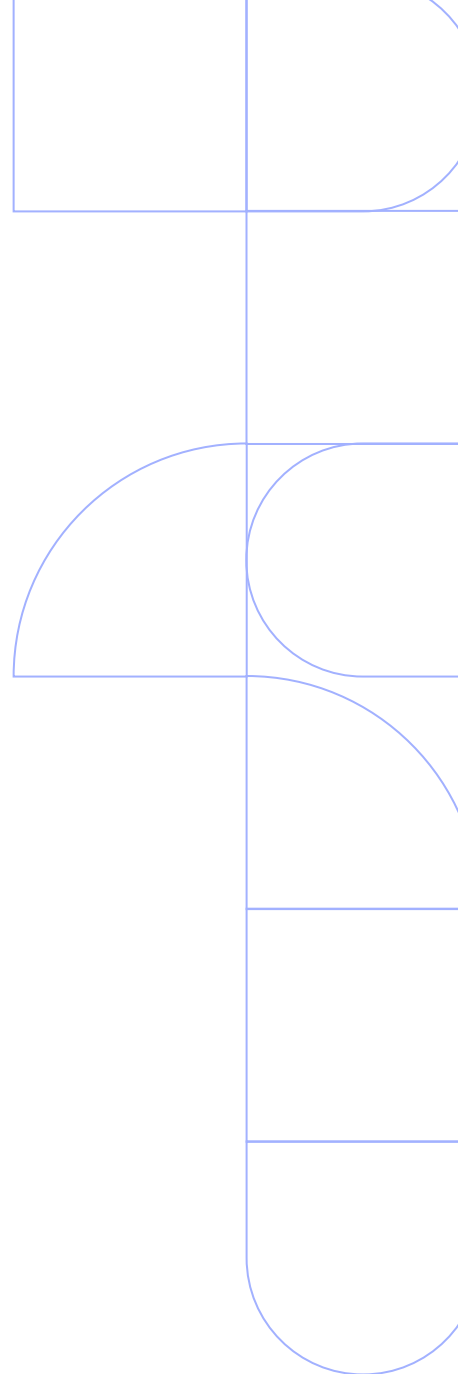
RIA. *RIA's Risks and Controls for Artificial Intelligence and Machine Learning Systems.* Tallinn: RIA, 2024.

VASSIL, K. *Estonian e-Government Ecosystem: A Case Study.* Washington, DC: World Bank Group, 2015.

WORLD BANK. *Estonia's e-Government Ecosystem.* Washington, DC: World Bank, 2020.







Este exemplar é parte do nosso compromisso com a responsabilidade ambiental.
Cada página foi impressa em papel proveniente de fontes responsáveis,
refletindo nosso cuidado em preservar os recursos naturais e minimizar
o impacto sobre o planeta. Edição limitada.



MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO

