



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE ADMINISTRAÇÃO, ECONOMIA, CONTABILIDADE E GESTÃO
PÚBLICA - FACE
PROGRAMA DE PÓS-GRADUAÇÃO EM ECONOMIA

IGOR MUNIZ DA SILVA

GOVERNANÇA DE DADOS NA SEGURANÇA PÚBLICA: DIAGNÓSTICO
NACIONAL À LUZ DO MODELO DE MATURIDADE DE DADOS

BRASÍLIA
2026

IGOR MUNIZ DA SILVA

**GOVERNANÇA DE DADOS NA SEGURANÇA PÚBLICA:
DIAGNÓSTICO NACIONAL À LUZ DO MODELO DE MATURIDADE
DE DADOS**

Dissertação apresentada ao Programa de Pós-Graduação em Economia, Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da Universidade de Brasília, como requisito parcial para obtenção do título de Mestre em Economia.

Orientador: Prof. Dr. Leonardo Cavalcanti Da Silva

RESUMO

Este estudo tem por objetivo avaliar o estágio de maturidade de dados da Segurança Pública Nacional à luz do Modelo de Maturidade de Dados do Governo Federal. Tal modelo, estruturado em dez dimensões analíticas, permite diagnosticar capacidades institucionais relacionadas à governança, à qualidade e ao uso estratégico dos ativos informacionais. O propósito central consiste em caracterizar os níveis nacionais de maturidade de dados da segurança pública, com vistas a subsidiar o fortalecimento da gestão e a consolidação de uma governança pública orientada por evidências. A pesquisa baseou-se em levantamento primário junto a 26 unidades federativas, registrando-se a ausência apenas do Estado do Rio de Janeiro. Os resultados evidenciam uma maturidade de dados heterogênea e que reflete assimetrias federativas, no qual dimensões como Dados como Ativo Estratégico e Análise de Dados apresentam níveis situados entre os estágios emergente e desenvolvido, ao passo que componentes estruturantes da infraestrutura informacional exibem lacunas críticas. Destacam-se, entre os temas de maior disparidade entre os entes federativos, o Glossário de Termos de Negócio, o Monitoramento da Interoperabilidade e a Estratégia de Inteligência Artificial. Conclui-se que o aprimoramento da capacidade estatal no campo da segurança pública depende da superação da fragmentação semântica e da institucionalização de uma governança formal de dados, capaz de transformar o alinhamento estratégico em arranjos operacionais efetivos. No contexto desse esforço de integração nacional, evidenciam-se o potencial de coordenação do Sistema Único de Segurança Pública e o papel estruturante do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas.

Palavras-chave: Governança de Dados, Interoperabilidade, Modelo de Maturidade de Dados, SINESP, Segurança Pública, SUSP.

ABSTRACT

This study aims to assess the data maturity stage of the National Public Security based on the Federal Government's Data Maturity Model. This model, structured into ten analytical dimensions, enables the diagnosis of institutional capacities related to data governance, quality, and the strategic use of information assets. The main objective is to characterize the national level of data maturity in public security to support managerial strengthening and the consolidation of evidence-based public governance. The research was grounded in a primary survey conducted with 26 federative units, with data missing only from the state of Rio de Janeiro. The results evidence a heterogeneous data maturity that reflects federative asymmetries, where dimensions such as Data as a Strategic Asset and Data Analytics range from emerging to developed stages, foundational components of informational infrastructure exhibit critical gaps. The Business Terms Glossary, Interoperability Monitoring, and Artificial Intelligence Strategy stand out as the most discrepant themes among the federative entities. The study concludes that enhancing state capacity in public security depends on overcoming semantic fragmentation and institutionalizing formal data governance capable of transforming strategic alignment into effective operational arrangements. Within this national integration effort, the coordinating potential of the Unified Public Security System and the structuring role of the National Public Security Information System are highlighted.

Keywords: Data Governance; Interoperability; Data Maturity Model; SINESP; Public Security; SUSP.

SUMÁRIO

1 INTRODUÇÃO	9
1.1 Objetivos	12
1.1.1 Objetivo geral	12
1.1.2 Objetivos específicos	12
1.2 Justificativa	12
2 REVISÃO DE LITERATURA	15
2.1 Dados como Ativo Estratégico e sua Governança na Segurança Pública	15
3 METODOLOGIA	25
4 RESULTADOS E DISCUSSÃO	28
4.1 Amostra, consistência e reprodutibilidade dos dados	28
4.2 Análise geral	29
4.3 Análise por dimensão	31
4.4 Análise por temas dentro das dimensões	37
4.4.1 Governança de Dados	37
4.4.2 Dados como Ativo Estratégico	39
4.4.3 Conhecimento sobre os Dados	41
4.4.4 Dados Abertos	43
4.4.5 Gerenciamento de Dados	44
4.4.6 Análise de Dados	46
4.4.7 Interoperabilidade de Dados	48
4.4.8 Ética de Dados	50
4.4.9 Qualidade de Dados	52
4.4.10 Inteligência Artificial	53
4.4.11 Ranking global dos temas	55
4.5 Identificação de gaps críticos	57
5 CONSIDERAÇÕES FINAIS	62

SUMÁRIO DE TABELAS

Tabela 1 - Níveis de Maturidade	19
Tabela 2 - Dimensões e Temas do Modelo de Maturidade de Dados	20
Tabela 3 - Dados das Dimensões	32
Tabela 4 - Níveis Médios de Maturidade por Tema	55
Tabela 5 - Índices de Criticidade	59

SUMÁRIO DE GRÁFICOS

Gráfico 1 - Avaliação da Maturidade de Dados	19
Gráfico 2 - Distribuição dos níveis de maturidade	30
Gráfico 3 - Distribuição de Maturidade por Dimensão	32
Gráfico 4 - Mapa de Calor da Correlação entre Dimensões	34
Gráfico 5 - Maturidade na Dimensão Governança de Dados	38
Gráfico 6 - Maturidade na Dimensão Dados como Ativo Estratégico	40
Gráfico 7 - Maturidade na Dimensão Conhecimento sobre os Dados	41
Gráfico 8 - Maturidade na Dimensão Dados Abertos	43
Gráfico 9 - Maturidade na Dimensão Gerenciamento de Dados	45
Gráfico 10 - Maturidade na Dimensão Análise de Dados	47
Gráfico 11 - Maturidade na Dimensão Interoperabilidade de Dados	49
Gráfico 12 - Maturidade na Dimensão Ética de Dados	51
Gráfico 13 - Maturidade na Dimensão Qualidade de Dados	52
Gráfico 14 - Maturidade na Dimensão Inteligência Artificial	54
Gráfico 15 - 10 maiores Gaps Críticos	59

LISTA DE SIGLAS

CAD – Central de Atendimento e Despacho

DAMA-DMBOK – Data Management Body of Knowledge (Guia de Conhecimento para Gestão de Dados)

IQR – Intervalo Interquartil

MMD – Modelo de Maturidade de Dados

MVI – Mortes Violentas Intencionais

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

PNSPDS – Política Nacional de Segurança Pública e Defesa Social

PNUD – Programa das Nações Unidas para o Desenvolvimento

PPE – Procedimento Policial Eletrônico

SENASP – Secretaria Nacional de Segurança Pública

SINESP – Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas

SUSP – Sistema Único de Segurança Pública

UNODC – United Nations Office on Drugs and Crime (Escritório das Nações Unidas sobre Drogas e Crime)

1 INTRODUÇÃO

A construção de políticas públicas eficazes é um dos pilares fundamentais do contrato social que estrutura o Estado moderno. Segundo a perspectiva contratualista, a entrega da liberdade individual em favor de uma autoridade central encontra sua legitimidade na promessa de proteção coletiva, segurança e bem-estar (Brito, 2022). No campo da segurança pública, essa obrigação estatal assume contornos ainda mais sensíveis, uma vez que busca proteger o direito à vida, à integridade física e patrimonial.

Contudo, a operacionalização dessa proteção enfrenta um desafio estrutural, visto que, enquanto a gestão da segurança pública é descentralizada entre as unidades federativas por força do pacto federativo brasileiro, a dinâmica criminal contemporânea ignora fronteiras, assumindo uma natureza essencialmente transterritorial. Essa desconexão entre a circunscrição administrativa e a fluidez do crime organizado torna imperativa a integração sistemática das operações e dados de segurança pública.

Mais do que o simples compartilhamento de informações, faz-se mister que esses dados sejam estruturados de forma organizada e inteligível, permitindo que a inteligência governamental converta registros isolados em informações que orientem ações coordenadas. A efetividade das ações estatais no enfrentamento da violência, no controle da criminalidade e na promoção da segurança pública está intrinsecamente vinculada à capacidade do Estado de produzir, gerir e utilizar dados de forma qualificada. Conforme Silveira (2024), a segurança pública alcança resultados eficazes quando seus gestores baseiam suas decisões em dados e na análise de informações sobre a criminalidade.

Nesse cenário, os dados transcendem a condição de meros registros para assumirem o papel de insumo estratégico na formulação, execução e monitoramento de políticas públicas. Na segurança pública, em especial, onde a eficácia operacional depende de respostas céleres, a transição para uma gestão ancorada em evidências permite que as decisões deixem de ser reativas e passem a ser orientadas por uma inteligência preditiva e precisa.

A segurança pública contemporânea opera em um ambiente marcado por crescente complexidade, no qual os fenômenos criminais tornam-se mais dinâmicos, multifacetados e interdependentes. Figueiredo (2021) coloca que, no centro das discussões sobre criminalidade, emergem aspectos intrincados e obstáculos significativos que precisam

ser abordados tanto pelas políticas em nível nacional (englobando todas as esferas político-administrativas) quanto pelos órgãos estatais incumbidos da segurança.

Ao mesmo tempo, a sociedade está profundamente conectada e imersa em fluxos constantes de dados. Dados oriundos de boletins de ocorrência, câmeras de videomonitoramento, sensores, redes sociais, prontuários, bases de mobilidade urbana, sistemas penitenciários, além de dados administrativos e judiciais, formam um ecossistema informacional de valor inestimável para orientar intervenções estratégicas.

Entretanto, possuir dados não significa, necessariamente, saber utilizá-los. O desafio reside em transformar esse oceano de dados brutos em informação qualificada, conhecimento estratégico e inteligência capaz de orientar políticas públicas baseadas em evidências. A UNODC (2024) enfatiza a necessidade de adotar uma abordagem holística para a governança de dados. Isso inclui a formulação de uma visão de longo prazo, o desenvolvimento dos instrumentos regulatórios necessários, a coordenação das diferentes instituições e o desenho de uma arquitetura de dados alinhada às necessidades e aos recursos do país.

Diante disso, o fortalecimento da maturidade de dados nas instituições públicas, em especial nas Secretarias de Segurança Pública, emerge como requisito indispensável para que o Estado se aproprie soberanamente de sua capacidade analítica. Trata-se de assegurar que os dados estejam organizados, protegidos, padronizados, compartilhados e efetivamente utilizados como ativos estratégicos, conforme propõe o Modelo de Maturidade de Dados (MMD) do Governo Federal Brasileiro (Brasil, 2024).

Tal diretriz encontra respaldo nas recomendações internacionais da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que define a construção de um setor público orientado por dados como pilar essencial para governos modernos, eficientes, transparentes e centrados no cidadão (OCDE, 2019). No Brasil, marcos normativos como a Lei nº 14.129/2021 (Lei do Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) também estabelecem obrigações formais e éticas quanto à gestão, proteção e uso dos dados na administração pública.

Em um cenário onde os dados são cruciais, é vital que o Estado não apenas os colete, mas garanta sua governança, proteção e conversão em valor público. A omissão nesse ponto compromete a eficácia das políticas e gera opacidade, iniquidade e o risco de captura de

dados públicos por interesses privados. Neste contexto, o Programa das Nações Unidas para o Desenvolvimento (PNUD, 2025) aponta a fragmentação dos sistemas digitais e a insuficiente qualidade dos dados como falhas centrais no uso de dados públicos. Sistemas isolados e falhas na governança limitam o acesso e a oferta de serviços integrados, afetando comunidades marginalizadas. Por sua vez, dados precários levam a serviços ineficazes, decisões erradas e sistemas de Inteligência Artificial que não promovem equidade, minando a confiança e reforçando desigualdades.

Com base na hipótese de que a maturidade de dados na Segurança Pública é marcada por assimetria e heterogeneidade entre os entes federados, o presente trabalho se propõe a responder em que estágio de maturidade de dados a segurança pública nacional se encontra.

Dessa forma, o objetivo geral desta pesquisa é mensurar a maturidade de dados da Segurança Pública Nacional por meio da aplicação do modelo de maturidade de dados. Ao fazê-lo, busca oferecer subsídios práticos para o fortalecimento institucional da segurança pública no Brasil, alinhado às melhores práticas internacionais e às exigências de uma governança pública ética, eficiente e orientada a dados.

Os objetivos específicos deste trabalho são analisar o Modelo de Maturidade de Dados do Poder Executivo Federal, suas dimensões e temas no contexto das Secretarias de Segurança Pública; mapear o nível de maturidade de dados em uma amostra de Secretarias Estaduais de Segurança Pública, com base nos critérios do MMD; identificar índices que apresentaram maior desvio em relação aos parâmetros de referência estabelecidos; e, por fim, apontar recomendações para o fortalecimento da governança de dados nessas Secretarias.

Destaca-se que, conforme compromisso de confidencialidade firmado com a Secretaria Nacional de Segurança Pública (SENASP) no OFÍCIO Nº 376/2026/CGA-DGI/DGI/SENASP/MJ, a análise dos dados foi realizada de forma agregada, a fim de não se individualizar ou ranquear as Unidades Federativas, além de se evitar negligenciar particularidades estruturais de cada ente federado.

1.1 Objetivos

1.1.1 Objetivo geral

Avaliar o estágio de maturidade de dados da Segurança Pública Nacional através da aplicação do Modelo de Maturidade de Dados do Governo Federal às Secretarias de Segurança Pública do Brasil.

1.1.2 Objetivos específicos

- Analisar o Modelo de Maturidade de Dados do Poder Executivo Federal, suas dimensões e temas no contexto das Secretarias de Segurança Pública;
- Mapear o nível de maturidade de dados em uma amostra de Secretarias Estaduais de Segurança Pública, com base nos critérios do MMD;
- Identificar índices que apresentaram maior desvio em relação aos parâmetros de referência estabelecidos;
- Apontar recomendações para o fortalecimento da governança de dados nas Secretarias de Segurança Pública.

1.2 Justificativa

Vive-se em uma sociedade em que os dados se tornaram o elemento central da dinâmica econômica, política e social. No contexto da segurança pública, essa realidade é ainda mais evidente. A capacidade de formular políticas públicas baseadas em evidências, de operar sistemas inteligentes e de promover intervenções eficientes depende, de forma crescente, da governança, da qualidade e da integração dos dados disponíveis.

Historicamente, o foco principal de estudos e iniciativas sobre a reutilização de dados tem se voltado para o setor privado, aproveitando os dados governamentais abertos, conforme aponta o *European Data Portal* (2020). Isso se deve ao potencial evidente de criação de valor econômico por meio de políticas de dados abertos, assumindo-se que o setor privado é o principal beneficiário, alavancando dados do governo para gerar serviços com maior retorno em valor público e receita.

Embora os dados do Anuário Brasileiro de Segurança Pública¹ apontem uma retração de 5,4% na taxa de mortes violentas intencionais (MVI), o cenário nacional revela uma transição crítica nas dinâmicas de violência. Observa-se um crescimento considerável em categorias específicas, notadamente no número de desaparecimentos e em crimes de gênero, como o feminicídio e o estupro. Paralelamente, a segurança pública enfrenta o desafio da digitalização da criminalidade, com a ascensão de delitos como o *stalking* e diversas modalidades de crimes em ambiente virtual.

Nesse cenário desafiador, o Estado, e, notadamente os órgãos de segurança pública, deparam-se com a premente necessidade de otimizar sua capacidade institucional na gestão de dados como um ativo estratégico. A inação neste campo representa o risco de perpetuar assimetrias informacionais que, por sua vez, exacerbam desigualdades sociais e fragilizam a eficácia da atuação estatal no cumprimento de suas funções essenciais.

Para mitigar tais riscos e catalisar a transformação digital, torna-se imperativo adotar boas práticas de governança de dados no setor público. Conforme Belli et al. (2024), recomenda-se, entre outras ações, a estruturação de um processo de governança de dados que atenda às demandas da transformação digital. Isso inclui o desenvolvimento de fluxos de dados robustos, a definição de rigorosos requisitos de qualidade de dados e a implementação de modelos decisórios informados por dados confiáveis.

O Modelo de Maturidade de Dados adotado pelo Governo Federal reflete essa preocupação ao estabelecer parâmetros para que os órgãos públicos avaliem o nível em que são capazes de transformar dados em ativos geradores de valor. Este modelo revela que a maturidade de dados não se resume à infraestrutura tecnológica, mas envolve governança, qualidade, interoperabilidade, segurança da informação, ética e uso inteligente dos dados para apoiar decisões estratégicas.

Ao mesmo tempo, a OCDE (2019) alerta que, sem uma cultura orientada a dados, os governos não conseguirão entregar serviços públicos de qualidade, tampouco formular políticas eficazes, transparentes e baseadas em evidências. Na segurança pública, essa lacuna impacta diretamente a capacidade de reduzir a violência, otimizar recursos, garantir direitos e proteger vidas.

¹ Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf>. Acesso em: 20 jan. 2026

Neste cenário, fortalecer a maturidade de dados nas Secretarias de Segurança Pública deixa de ser uma escolha e passa a ser uma necessidade institucional, legal e ética. A Lei do Governo Digital já estabelece como princípios a interoperabilidade, a segurança, a transparência e o uso inteligente dos dados na administração pública, alinhando o país às melhores práticas internacionais.

Assim, os resultados deste estudo pretendem oferecer subsídios para o fortalecimento da governança de dados nas instituições de segurança pública, contribuindo para um modelo de gestão mais eficiente, transparente, responsável e, sobretudo, capaz de gerar valor público e impacto social positivo.

2 REVISÃO DE LITERATURA

2.1 Dados como Ativo Estratégico e sua Governança na Segurança Pública

O mundo contemporâneo é marcado por uma crescente centralidade dos dados como ativos estratégicos. No contexto da segurança pública, isso significa que a capacidade de inovar na gestão da informação e dos dados está diretamente associada ao desenvolvimento de respostas mais eficientes e inteligentes para os desafios da criminalidade e da violência.

Nesse sentido, as organizações públicas que tratam os dados como ativos estratégicos são capazes de aprimorar seus processos decisórios, desenvolver políticas públicas baseadas em evidências e gerar valor público, conforme as diretrizes internacionais da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2019).

Ao mesmo tempo, é preciso reconhecer que vivemos sob a lógica do que Zuboff (2020) denominou de capitalismo de vigilância, um modelo econômico que se apropria de dados comportamentais, muitas vezes sem consentimento, para produzir mercados preditivos e maximizar ganhos privados. Esse fenômeno lança luz sobre os riscos de uma exploração de dados que não esteja orientada pelo interesse público, pela transparência, pela ética e pela proteção dos direitos fundamentais. Além disso, o avanço das tecnologias de informação e comunicação, embora promissor, desloca o eixo de poder para quem controla os fluxos de dados e as infraestruturas digitais (Zuboff, 2020).

O fortalecimento da governança de dados representa uma evolução conceitual que reflete a crescente centralidade dos ativos informacionais na sociedade e, por conseguinte, na administração pública contemporânea. Conforme a OCDE (2019), a governança de dados emerge como um conjunto estruturado de práticas, processos e políticas que garantem a qualidade, a segurança, a interoperabilidade, a ética e o uso estratégico dos dados no setor público.

Sem uma governança robusta, dados permanecem dispersos, subutilizados ou sujeitos a erros, comprometendo a capacidade institucional de transformar dados em informação e informação em inteligência para a tomada de decisão. Thompson et al. (2015) oferecem contribuição relevante ao demonstrar, por meio de auditoria em aplicações do setor público, que a mera existência de dados governamentais não implica governança adequada. Os autores identificaram falhas organizacionais e procedimentais significativas em contextos

policiais, evidenciando que dados governamentais sem mecanismos institucionais adequados não garantem práticas de governança eficazes.

Já O'Hara (2012), ao discutir como o ecossistema de dados abertos afeta a qualidade e a confiança nas informações públicas, ilustra tensões entre objetivos de transparência e distorções de mercado informacional. O autor argumenta que a entrada de dados públicos em mercados de informação pode distorcer incentivos de qualidade, afetando análises sobre crime e justiça. Esta perspectiva é particularmente relevante para a segurança pública, onde dados de baixa qualidade podem comprometer investigações, gerar vieses em análises preditivas e minar a confiança pública em instituições policiais.

Afzal e Panagiotopoulos (2020), ao fazerem uma revisão de literatura sobre policiamento inteligente, sintetizam efeitos organizacionais dos dados na polícia, ligando governança à transformação institucional e à alteração de papéis profissionais. Os autores corroboram a importância dos dados como força central no policiamento inteligente e entendem a importância de delimitar a terminologia complexa do policiamento inteligente a processos mais específicos (análise de dados, funções inteligentes e intervenções multifacetadas) que levam a resultados (aplicação da lei e manutenção da ordem) e impactos (confiança pública e eficácia coletiva).

Esta perspectiva é complementada por Afzal et al. (2024), que, ao oferecerem uma revisão integrativa sobre dados na polícia, destacam a importância da governança de dados para a segurança pública ao enxergar tempos de resposta mais rápidos, melhores decisões e maior transparência no policiamento orientado por dados. Corroborando o ponto, Costa (2022) indica que a inserção da governança no ciclo da política pública é imprescindível devido à natureza multinível da segurança pública no Brasil.

Nota-se ainda que transparência e a responsabilização (*accountability*) constituem objetivos centrais da governança de dados no setor público, mas são tensionados por questões de retenção, uso e finalidade dos dados. Arango et al. (2021) analisam melhores práticas para transparência de dados policiais, propondo visualizações e análises que promovam *accountability*. Sampson (2020) discute a necessidade de balanço entre possibilidades técnicas, permissibilidade legal e aceitabilidade social para responsabilização institucional de agências de polícia, argumentando que a responsabilização digital exige

mecanismos que vão além da mera disponibilização de dados, incluindo auditabilidade, explicabilidade e supervisão independente.

Dentro da Segurança Pública há ainda de se considerar suas particularidades quanto ao manejo de dados. Gültekin-Várkonyi (2024), por exemplo, identificou quatro riscos de governança de dados associados ao uso de tecnologias de reconhecimento facial (*Facial Recognition Technology* - FRT) por agências de aplicação da lei sob a legislação da União Europeia. Os riscos incluem a não conformidade com o princípio de minimização de dados, uma vez que sistemas de FRT frequentemente coletam e processam mais dados do que o estritamente necessário para finalidades específicas; a violação do princípio de limitação de finalidade, quando dados coletados para uma finalidade são reutilizados para outras sem base legal adequada; problemas de precisão de dados e sistemas, especialmente vieses que afetam desproporcionalmente grupos demográficos específicos; e desafios administrativos na criação de algoritmos que atendam simultaneamente requisitos técnicos e legais.

A construção de um setor público orientado por dados (*data-driven public sector*) é um dos pilares do Governo Digital, conforme reconhecido na Recomendação do Conselho da OCDE sobre Estratégias de Governo Digital (OCDE, 2014; 2019). O documento estabelece que governos devem tratar dados como um ativo estratégico, promovendo sua governança, proteção, interoperabilidade e utilização para geração de valor público.

O relatório *The Path to Becoming a Data-Driven Public Sector* (OCDE, 2019) destaca que, para que o setor público efetivamente se torne orientado por dados, são necessárias ações em governança de dados, ao implementar de estruturas institucionais, marcos legais, padrões e arquiteturas para gestão de dados; em aplicação de dados para geração de valor público, com seu uso para planejamento, formulação, implementação, monitoramento e avaliação de políticas públicas; e confiança pública, a partir da construção de mecanismos que assegurem o uso ético dos dados, a proteção da privacidade e a transparência, prevenindo abusos, opacidade e riscos de discriminação.

No campo da segurança pública, isso significa que decisões operacionais, investimentos, definições de políticas preventivas ou repressivas e o monitoramento de resultados devem estar lastreados por dados de qualidade, atualizados, interoperáveis e acessíveis.

2.2 Práticas em Governança de Dados e o Modelo de Maturidade de Dados

Colocada a relevância da governança de dados, aborda-se sua efetiva implementação, o que exige a adoção de guias e estruturas metodológicas que permitam transitar de uma gestão puramente reativa para uma postura estratégica e proativa. Esses *frameworks* operam como modelos de referência que fornecem instruções, critérios de operação e processos padronizados para implantar, manter e controlar os ativos informacionais de uma organização.

Dentre os referenciais mais respeitados mundialmente, destaca-se o *Data Management Body of Knowledge* (DAMA-DMBOK), desenvolvido pela *DAMA International*. Este guia fornece uma base estruturada de conhecimentos consensuais que formam o alicerce da disciplina de gestão de dados, sendo flexível o suficiente para evoluir conforme os avanços tecnológicos e as necessidades de cada organização (Dama International, 2017). O modelo organiza a gestão em diversos domínios interdependentes como qualidade, segurança, metadados e arquitetura de dados; posicionando a governança de dados no centro dessa estrutura de coordenação.

A aplicação prática desses frameworks repercute no setor público. Costa et al. (2023) propõem um *framework* específico para avaliação e evolução contínua de portais de dados abertos governamentais.

No Brasil, o Modelo de Maturidade de Dados, desenvolvido pelo Governo Federal (2024), fornece um referencial para que os órgãos da administração pública avaliem sua capacidade de governança e gestão de dados. O MMD, que referencia em seu corpo o DAMA-DMBOK, está estruturado em 30 temas distribuídos em 10 dimensões. Na sua base, cada pergunta operacionaliza um desses temas, sendo o nível a síntese numérica da maturidade declarada (Brasil, 2024).

Gráfico 1 - Avaliação da Maturidade de Dados



Fonte: Brasil, 2026

A progressão entre os níveis reflete o grau de sofisticação institucional na governança de dados:

Tabela 1 - Níveis de Maturidade

Nível de Maturidade	Descrição das Características
Nível 1 (Não Iniciado)	Ausência total de processos formais. A organização não reconhece o valor estratégico dos dados e falta atribuição de responsabilidades ou supervisão sobre os dados.
Nível 2 (Iniciado)	Surgimento de iniciativas isoladas, geralmente restritas às áreas de TI, sem integração com os objetivos de negócio ou diretrizes estratégicas.
Nível 3 (Emergente)	A alta gestão passa a reconhecer a importância dos dados. Há o início da quebra de silos organizacionais e a formalização de normas legais.
Nível 4 (Desenvolvido)	Políticas de governança são formalizadas e aplicadas de forma descentralizada. Os dados são tratados como prioridade organizacional e passam por revisões periódicas.
Nível 5 (Otimizado)	A governança de dados é uma referência absoluta. A gestão está totalmente integrada à estratégia, com alta automação, cultura de melhoria contínua e capacidade preditiva.

Fonte: (Brasil, 2024)

As dimensões representam as disciplinas que dividem as diversas práticas e processos de governança e gestão, enquanto os temas constituem as unidades de avaliação granular que permitem identificar pontos fortes e fragilidades específicas. A seguir, apresentam-se as 10 dimensões e seus respectivos temas que compõem o modelo.

Tabela 2 - Dimensões e Temas do Modelo de Maturidade de Dados

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
Governança de Dados	Abrange aspectos essenciais para a estruturação e consolidação da governança de dados na organização. Ela busca fortalecer a interação entre os atores, definir papéis e responsabilidades, e estabelecer diretrizes e políticas para o uso seguro e estratégico dos dados, alinhando a gestão aos objetivos institucionais e promovendo uma cultura orientada a dados.	Estrutura Organizacional para Governança de Dados	Refere-se à existência de uma estrutura formalmente estabelecida, com papéis, responsabilidades e mecanismos de comunicação claros, garantindo colaboração entre áreas e supervisão contínua do progresso e efetividade do Programa de Governança de Dados.
		Promoção da Cultura de Dados pela Alta Gestão	Aborda o compromisso ativo da alta gestão em promover uma cultura orientada a dados, atuando como exemplo e engajando equipes na valorização dos dados como ativos estratégicos.
		Princípios e Políticas de Dados	Analisa a definição e implementação de princípios e políticas para garantir que los dados sejam geridos de forma ética, segura e estratégica, alinhados aos objetivos institucionais e regulamentações.
		Letramento em Dados	Trata da promoção contínua de capacitação entre os envolvidos para o uso efetivo de dados no apoio à tomada de decisões, assegurando o desenvolvimento de habilidades necessárias em todas as áreas, alinhadas aos objetivos estratégicos e demandas institucionais.
Dados como Ativo Estratégico	Avalia como a governança e gestão de dados estão alinhadas aos objetivos estratégicos institucionais e às entregas para a sociedade.	Alinhamento com Objetivos Estratégicos	Assegura que as atividades de coleta, análise e tomada de decisão com base em dados estejam estritamente alinhadas

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
	Analisa também o impacto do uso estratégico dos dados na redução de riscos, no suporte ao planejamento estratégico e na maximização da efetividade das políticas públicas.		à visão, missão e metas institucionais.
		Gestão Orientada a Dados	Atua no reconhecimento dos dados como um recurso estratégico primordial, utilizados de forma sistemática para embasar decisões em todos os níveis hierárquicos da instituição.
		Dados como Pilar para Entregas à Sociedade	Analisa como estão estruturadas a governança e a gestão para que estas funcionem como mecanismos de melhoria da qualidade e da consistência das políticas públicas.
Conhecimento sobre os Dados	Aborda aspectos fundamentais para garantir que os dados sejam compreendidos, documentados e estruturados de forma padronizada. Seu objetivo é assegurar que os dados sejam descritos, organizados e gerenciados de maneira clara e acessível.	Documentação dos Ativos de Dados	Estabelece práticas para o registro padronizado de informações essenciais, abrangendo aspectos como propriedade, formato, origem e descrição dos ativos institucionais.
		Glossário de Termos de Negócio	Foca na manutenção e no uso de um vocabulário comum para padronizar definições, reduzir ambiguidades e promover uma comunicação clara e assertiva entre as diferentes áreas da organização.
		Modelagem de Dados	Envolve a adoção de práticas para organizar e documentar as bases de dados, o que garante a padronização necessária para facilitar a gestão e o uso estratégico das informações.
		Gestão de Metadados	Atua no gerenciamento de informações sobre los dados para aprimorar a capacidade da instituição em processar, manter, integrar, proteger, auditar e governar seu patrimônio informativo de maneira eficiente.

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
Dados Abertos	Trata de dados disponíveis para acesso, uso e redistribuição sem restrições técnicas ou legais significativas. São dados de interesse público produzidos ou custodiados por órgãos governamentais, disponibilizados livre e gratuitamente para promover transparência, participação social e inovação.	Implementação da Política de Dados Abertos	Estabelece que a estratégia da instituição deve ser operacionalizada por meio de processos bem definidos para a seleção, publicação e manutenção contínua dos conjuntos de dados.
		Ecosistema de Dados Abertos	Foca em contribuições que promovam um ambiente integrado, constituído por um conjunto de atores, tecnologias, processos e políticas voltados à disponibilização, ao acesso e à reutilização de dados governamentais de forma livre e aberta para todos os interessados.
Gerenciamento de	Aborda o manejo de dados mestres,	Geral	
		Gerenciamento de Dados Mestres e de Referência	Estabelece processos definidos para gerenciar essas informações críticas e assegurar a padronização e a integridade das bases utilizadas pela organização.
		Ciclo de Vida dos Dados	Orienta que as informações institucionais sigam um fluxo estruturado, com práticas de coleta, armazenamento, uso e descarte devidamente normatizadas.
		Dados não Estruturados	Preconiza a adoção de ferramentas e boas práticas voltadas à coleta e análise de conteúdos complexos visando garantir o seu aproveitamento estratégico para a geração de novos insights.
		Gerenciamento de Dados	Organiza a captura e a

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
Dados	de referência, não estruturados e geoespaciais. Os dados são tratados como ativos estratégicos e utilizados para apoiar a tomada de decisões, fomentar políticas públicas e garantir a interoperabilidade.	Geoespaciais	utilização de dados de localização de forma estruturada a fim de que a integração de atributos espaciais e não espaciais possam fundamentar tomadas de decisão que dependam de análises territoriais precisas.
Análise de Dados	Aborda-se o tratamento de dados e disponibilização de informações, demandando infraestrutura robusta, ferramentas adequadas e dados relevantes. Inclui práticas e tecnologias que garantem o armazenamento, processamento e manipulação eficaz dos dados, assegurando a confiabilidade dos resultados. Desenvolve capacidade analítica, abrangendo conhecimentos matemáticos, estatísticos, computacionais e negociais, e promove uma cultura orientada a dados.	Infraestrutura e Ferramentas para Análise de Dados	Estabelece a necessidade de recursos tecnológicos adequados para o processamento e a análise eficiente de grandes volumes de informações.
		Relevância e Suficiência dos Dados	Foca em garantir que o material coletado seja pertinente e quantitativamente capaz de fundamentar as análises e decisões exigidas pela gestão institucional.
		Desenvolvimento da Capacidade Analítica	Orienta que a instituição promova ações de capacitação contínua para fortalecer as habilidades técnicas dos servidores no manuseio e interpretação de dados.
		Tomada de Decisão Baseada em Dados	Busca verificar se as escolhas estratégicas e operacionais estão fundamentadas em evidências confiáveis e alinhadas aos objetivos organizacionais, a fim de que se tenha maior assertividade e transparência na administração pública.
Interoperabilidade de Dados	Aborda a definição e aplicação de padrões e diretrizes para o compartilhamento de dados de forma estruturada e consistente. Inclui aspectos técnicos como formatos padronizados, protocolos de comunicação e interfaces de programação, além da harmonização de vocabulários e ontologias para garantir a compreensão mútua dos dados compartilhados. Avalia também integração entre sistemas, monitoramento e avaliação da	Padrões e Normas para Interoperabilidade	Avalia a adoção de normas, diretrizes e padrões que assegurem a consistência e a compatibilidade dos dados que transitam entre diferentes sistemas, aplicativos e plataformas.
		Integração de Sistemas	Verifica em que nível os ambientes heterogêneos da instituição estão conectados e se permitem a troca eficiente de informações com

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
	interoperabilidade, e políticas de compartilhamento de dados com atores externos.		mecanismos de interoperabilidade e canais de comunicação devidamente padronizados.
		Monitoramento e Avaliação da Interoperabilidade	Propõe o acompanhamento contínuo dos sistemas para a identificação precoce de gargalos com ações corretivas que conduzem à confiabilidade dos dados processados.
		Compartilhamento de Dados com Atores Externos	Avalia se o fluxo de informações para fora da instituição está ocorrendo de maneira eficiente, segura e em conformidade com as regulamentações vigentes.
Ética de Dados	Trata de políticas e práticas que promovem a transparência e a responsabilidade no uso de dados. Inclui ações voltadas a consentimento informado, anonimização, minimização de dados e respeito à privacidade.	Ética no Tratamento de Dados	Analisado se princípios éticos sólidos no tratamento de dados estão sendo adotados de forma a garantir imparcialidade, equidade e transparência. Verifica também o nível de implementação de políticas para identificação e mitigação de vieses, auditorias regulares e treinamentos contínuos a fim de que as decisões baseadas em dados sejam justas e responsáveis.
Qualidade de Dados	Aborda a capacidade da organização de assegurar que os dados sejam precisos, completos, consistentes, atualizados, íntegros e adequados ao uso. Visa fornecer uma base confiável para a tomada de decisões estratégicas e operacionais, minimizando riscos e promovendo maior eficiência organizacional.	Gestão de Qualidade de Dados	Preconiza a implementação de uma abordagem governada para o planejamento e controle de atividades que assegure uma coleta e uso das informações adequados aos seus propósitos.
		Cultura de Qualidade de Dados	Atua na base humana da organização, fomentando uma mentalidade em que cada colaborador compreenda sua responsabilidade direta na manutenção e no aprimoramento da confiabilidade das informações.

Dimensão	Descrição da Dimensão	Tema	Descrição do Tema
		Medição e Controle da Qualidade de Dados	Avalia se há monitoramento contínuo e uso de métricas avançadas, como o registro e a análise de tendências.
Inteligência Artificial	Aborda a garantia da qualidade, integridade, segurança e ética dos dados utilizados em processos que envolvem Inteligência Artificial. As práticas visam assegurar o alinhamento desses processos com os objetivos estratégicos da instituição.	Estratégia para Inteligência Artificial	Analisa a adoção de uma estratégia estruturada para o uso da Inteligência Artificial alinhada aos objetivos institucionais, com governança clara, infraestrutura adequada e monitoramento contínuo.

Fonte: (Brasil, 2024)

3 METODOLOGIA

Trata-se de uma pesquisa de natureza hipotético-dedutiva, na qual, a partir da identificação de uma lacuna no conhecimento acerca da maturidade de dados nas Secretarias de Segurança Pública, formula-se um problema de pesquisa e perguntas que buscam respostas empíricas, as quais serão testadas à luz dos referenciais teóricos e dos dados coletados (LAKATOS e MARCONI, 2010).

Quanto aos objetivos, a pesquisa classifica-se como exploratória e descritiva. De acordo com Gil (2002), pesquisas descritivas têm como finalidade “a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis”. Já a pesquisa exploratória tem como propósito central o “aprofundamento de ideias e a descoberta de percepções que contribuam para a compreensão do problema”. Neste contexto, a pesquisa se propõe a aprofundar a compreensão sobre o nível de maturidade de dados nas Secretarias de Segurança Pública e descrever de que forma esse nível impacta a formulação de políticas públicas baseadas em evidências.

Quanto à sua finalidade, trata-se de uma pesquisa aplicada, uma vez que busca gerar conhecimento útil para solucionar problemas concretos, oferecendo recomendações e diretrizes para fortalecer a governança de dados e a capacidade analítica das Secretarias de

Segurança Pública. Como destaca Gil (2002), a pesquisa aplicada visa a “produção de conhecimentos para aplicação prática, dirigidos à solução de problemas específicos”.

O procedimento metodológico estruturou-se em quatro etapas sequenciais: a pesquisa bibliográfica para fundamentação teórica em eixos como governança de dados e federalismo; a análise documental de marcos normativos, como a LGPD e o guia do MMD; a aplicação do instrumento de coleta junto aos gestores das SSPs; e a análise estatística dos dados obtidos. A pesquisa foi direcionada às 27 Secretarias de Segurança Pública do Brasil, tendo alcançado 26 unidades federativas (96,3% do universo), com a ausência apenas do estado do Rio de Janeiro, que não respondeu ao MMD. A coleta foi realizada via questionário estruturado que avaliou 30 temas distribuídos em 10 dimensões, utilizando uma escala ordinal de cinco pontos (Nível 1: Não Iniciado a Nível 5: Otimizado).

A análise de dados empregou técnicas de estatística descritiva e inferencial, utilizando a linguagem de programação *Python* para o processamento. A fidedignidade do instrumento foi testada pelo Alfa de Cronbach. Este índice quantifica a consistência interna da escala, variando de 0 a 1, onde valores mais elevados indicam que os itens medem o mesmo constructo subjacente de forma coerente². Além de medidas de tendência central (média e mediana) e dispersão (desvio padrão e amplitude interquartil), foi aplicado um Índice de Prioridade de Gaps (IPG). Este índice permitiu identificar os gargalos estruturais prioritários ao combinar a magnitude da deficiência de maturidade com a heterogeneidade federativa.

Por fim, a metodologia reconhece limitações, como a natureza de percepção dos dados, uma vez que a autoavaliação não exigiu evidências documentais, estando sujeita a vieses de subjetividade ou desejabilidade social. Aponta-se também a ausência de variáveis explicativas externas (como dados orçamentários e de recursos humanos), o que restringe a análise à descrição do estado atual da maturidade, sem estabelecer relações causais definitivas.

Adicionalmente, ressalta-se que a presente análise não realizou a individualização nominal das Unidades Federativas, fundamentando-se no compromisso ético firmado junto à SENASP para o tratamento agregado dos dados. Para além da restrição institucional, a renúncia ao ranqueamento explícito justifica-se pelo risco em se negligenciar as heterogeneidades estruturais e socioeconômicas subjacentes a cada ente federado, podendo

² Disponível em: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC4205511/>>. Acesso em: 12 jan. 2026.

induzir a comparações valorativas superficiais que estigmatizam gestões ou ignoram disparidades orçamentárias históricas. Assim, busca-se focar na identificação de padrões de governança e lacunas técnicas em detrimento de uma hierarquização competitiva, a fim de mitigar o risco de uma leitura puramente punitiva dos dados e assegurar que o foco permaneça na compreensão das fragilidades do sistema de segurança pública como um todo.

4 RESULTADOS E DISCUSSÃO

4.1 Amostra, consistência e reprodutibilidade dos dados

A base analisada contém respostas de 25 unidades federativas (UFs) mais o Distrito Federal, com ausência do Rio de Janeiro (RJ). Cada uma respondeu a todos os 30 temas do Modelo de Maturidade de Dados, totalizando 780 registros (26×30), o que representa uma taxa de adesão de 96,3% em relação ao planejamento amostral inicial (n=810).

Para aferir a confiabilidade do instrumento de coleta e o grau de inter-relacionabilidade entre os temas avaliados, aplicou-se o coeficiente Alfa de Cronbach (α). No presente estudo, a análise das respostas brutas revelou um α de 0,66, valor que se situa no limite da aceitabilidade para pesquisas de caráter exploratório (onde o consenso acadêmico geralmente estabelece $\alpha > 0,70$)³.

A magnitude do coeficiente inicial (0,66) pode ser atribuída à natureza multidimensional do Modelo de Maturidade de Dados, que abrange 30 temas distintos distribuídos em 10 dimensões independentes. Essa diversidade temática pode gerar uma menor correlação média entre os itens individuais, refletindo as assimetrias operacionais e as percepções variadas dos respondentes sobre pontos técnicos específicos da gestão de dados. Um valor de alfa mais baixo pode indicar que os itens não estão fortemente correlacionados ou que o constructo é composto por dimensões que não necessariamente caminham juntas em nível micro⁴.

Contudo, observou-se um salto expressivo na consistência interna para 0,96 quando os dados foram agregados por Unidade Federativa e Dimensão. Esse fenômeno de elevação do alfa após a agregação sugere que, ao nível macro (organizacional), os componentes da maturidade de dados das Secretarias de Segurança Pública apresentam uma forte convergência sistêmica. Em termos estatísticos, a agregação atua como um filtro que reduz o ruído das variações individuais, evidenciando a robustez das dimensões enquanto pilares estruturantes da capacidade estatal.

³ Disponível em: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC4205511/>>. Acesso em: 12 jan. 2026.

⁴ Disponível em: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC4205511/>>. Acesso em: 12 jan. 2026.

Entretanto, esse valor elevado (acima de 0,90 ou 0,95) sugere uma possível redundância entre os itens avaliados⁵. Duas hipóteses podem explicar essa alta intercorrelação: a interdependência sistêmica natural das dimensões ou um "efeito institucional", onde a governança transversalmente eleva a maturidade reportada em todas as áreas.

Dessa forma, é crucial que a interpretação macro seja complementada por uma análise detalhada e granular. Isso previne que o sucesso geral ofusque e mascare gargalos e deficiências operacionais em áreas específicas.

Este achado é, em essência, compatível com a estrutura do MMD. Como as dimensões avaliam capacidades distintas, a tentativa de forçar um único fator tenderia a diminuir o coeficiente α . Conseqüentemente, o tratamento metodológico mais robusto é considerar o MMD como um perfil multidimensional, e não como um índice global unificado ou como a análise isolada de temas.

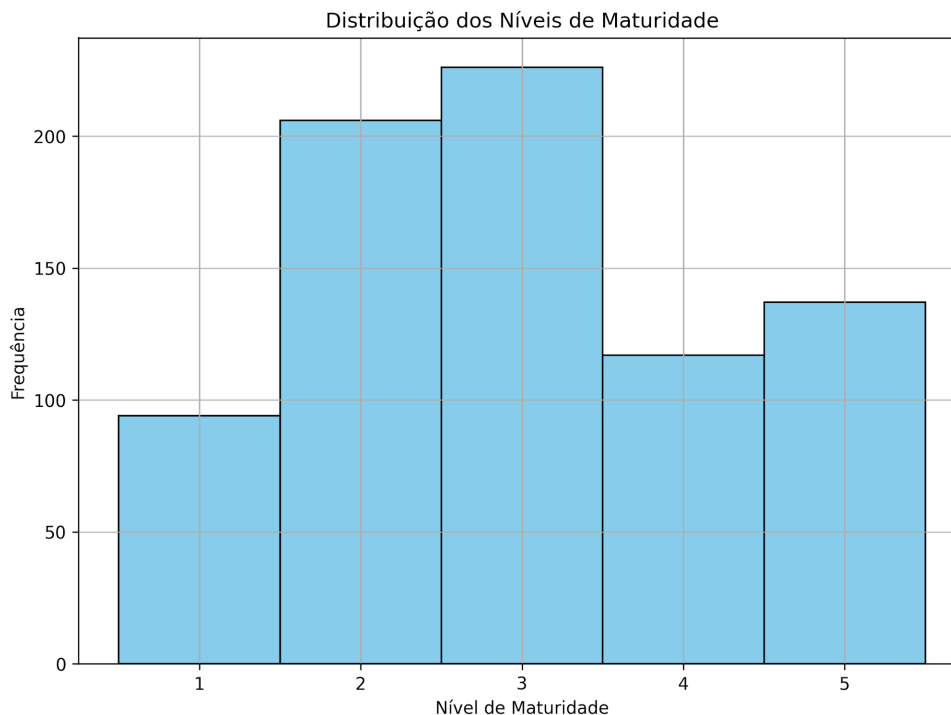
4.2 Análise geral

Os resultados apresentados neste capítulo baseiam-se na aplicação do MMD às Secretarias de Segurança Pública das unidades federativas brasileiras. Os níveis de maturidade variam de 1 (estágio inicial ou inexistente) a 5 (estágio otimizado e institucionalizado), conforme definido pelo Modelo de Maturidade de Dados.

Conforme discutido anteriormente, a natureza do MMD é inerentemente multidimensional, o que torna a média geral uma medida de percepção global, não devendo ser utilizada para capturar assimetrias e particularidades estruturais.

A distribuição global dos níveis mostra aproximadamente 12% das respostas no nível 1 (94 registros), 26% no nível 2 (206), 29% no nível 3 (226), 15% no nível 4 (117) e 18% no nível 5 (137), resultando em média geral próxima de 3,0 na escala de maturidade.

⁵ Disponível em: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC4205511/>>. Acesso em: 12 jan. 2026.

Gráfico 2 - Distribuição dos níveis de maturidade

Fonte: Elaboração própria

A predominância de níveis 2 e 3 no conjunto das respostas indica que, em grande parte dos temas, as SSPs se encontram entre a fase de iniciativas pontuais ainda não institucionalizadas (nível 2) e a de arranjos mais estruturados porém em consolidação (nível 3). Ao mesmo tempo, a presença consistente de respostas em níveis 4 e 5 em algumas UFs sugere que alguns temas já alcançam patamares de formalização e integração mais elevados.

A distribuição agregada dos níveis (com concentração em 2 e 3, média próxima a 3,0 e presença relevante, mas não majoritária, de respostas em 4 e 5) indica um cenário que não é mais puramente ausente ou fragmentado, tampouco já estruturado ou plenamente orientado a dados. À luz dos níveis propostos, o padrão observado é mais compatível com um estágio emergente, no qual existem arranjos formais em expansão, práticas de referência em alguns estados e temas, mas também heterogeneidades marcantes e bolsões ainda incipientes.

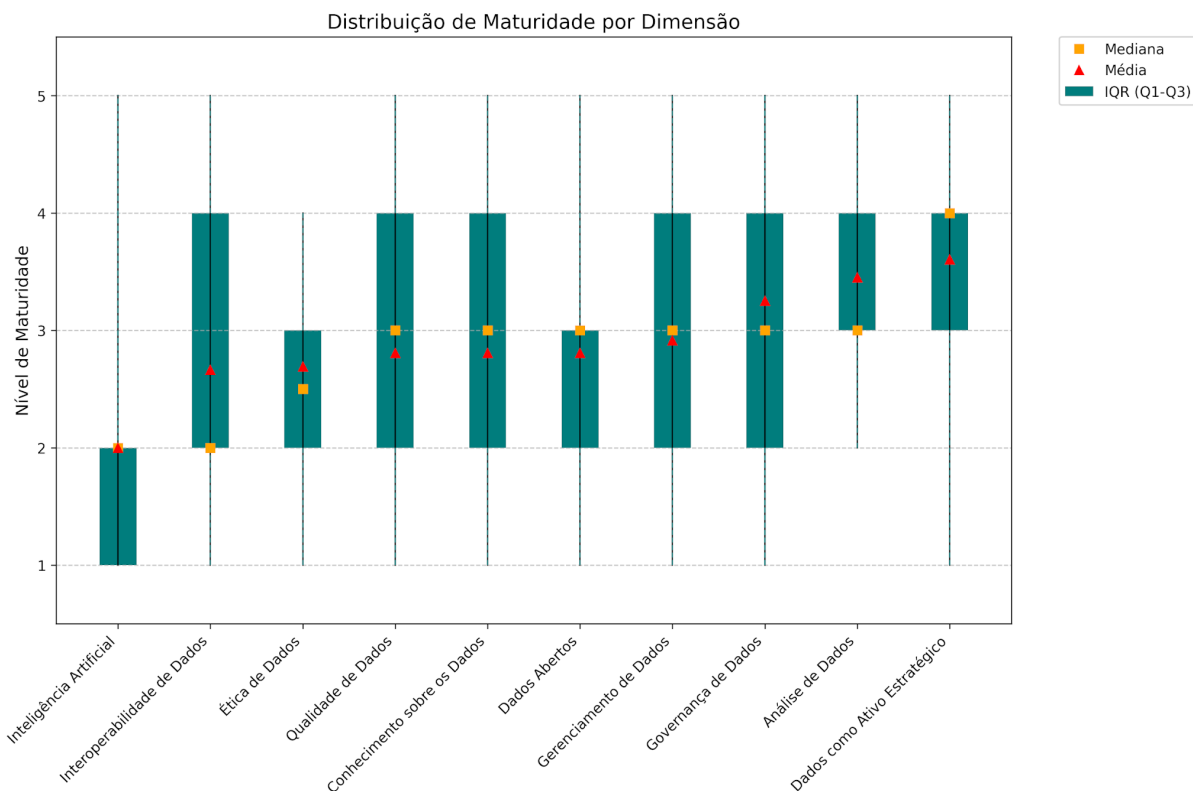
A análise de dispersão revela assimetrias federativas consideráveis, com desvio padrão médio de 1,20. Além disso, 93,3% dos temas atingiram o nível máximo de maturidade

em pelo menos uma unidade federativa, demonstrando que a excelência é tecnicamente viável, mas permanece geograficamente concentrada.

4.3 Análise por dimensão

A análise agregada por dimensão possibilita a identificação de áreas institucionais com diferentes níveis de desenvolvimento, apontando aquelas que exigem maior esforço de evolução ou aprimoramento. Para cada dimensão avaliada, foram calculados média, mediana, desvio-padrão, primeiro quartil (também chamado de “Q1”, valor abaixo do qual se encontram 25% das observações) e terceiro quartil (também chamado de “Q3”, valor abaixo do qual se encontram 75% das observações). A partir desses quartis, calcula-se o Intervalo Interquartil (IQR), medida de dispersão menos sensível a outliers que avalia a variabilidade dos 50% centrais dos dados, sendo obtido pela diferença entre Q3 e Q1.

No contexto do Modelo de Maturidade de Dados, o IQR pode ser utilizado para analisar a heterogeneidade e dispersão da maturidade de dados entre as Secretarias de Segurança Pública. Um IQR pequeno indica que os níveis de maturidade estão concentrados e uniformes, sugerindo pouca variação entre as instituições. Por outro lado, um IQR grande sinaliza alta dispersão e assimetria, indicando possível desigualdade institucional nos níveis de maturidade.

Gráfico 3 - Distribuição de Maturidade por Dimensão

Fonte: Elaboração própria

Tabela 3 - Dados das Dimensões

DIMENSÃO	Quantidade de Itens	Média	Mediana	Desvio Padrão	Valor Mínimo	Valor Máximo	Q1	Q3
Dados como Ativo Estratégico	78	3,60	4,00	1,02	1	5	3	4
Análise de Dados	104	3,45	3,00	1,06	2	5	3	4
Governança de Dados	104	3,25	3,00	1,15	1	5	2	4
Gerenciamento de Dados	104	2,91	3,00	1,28	1	5	2	4
Conhecimento sobre os Dados	104	2,81	3,00	1,43	1	5	2	4
Dados Abertos	52	2,81	3,00	1,31	1	5	2	3
Qualidade de Dados	78	2,81	3,00	1,32	1	5	2	4
Ética de Dados	26	2,69	2,50	0,88	1	4	2	3
Interoperabilidade de Dados	104	2,66	2,00	1,25	1	5	2	4
Inteligência Artificial	26	2,00	2,00	1,06	1	5	1	2

Fonte: Elaboração própria

Os resultados indicam dimensões que apresentam níveis médios mais elevados, refletindo maior institucionalização de práticas relacionadas à gestão e análise de dados. O perfil agregado mostra maturidade média acima de 3 nas dimensões Dados como Ativo

Estratégico (3,60), Análise de Dados (3,45), Governança de Dados (3,25); além de apresentar Gerenciamento de Dados próximo do nível emergente (2,91).

Em contrapartida, outras dimensões demonstram médias inferiores, sinalizando desafios estruturais na governança de dados. A dimensão Inteligência Artificial registrou o nível mais baixo (2,00), seguida pela Interoperabilidade de Dados (2,66) e Ética de Dados (2,69). Qualidade de Dados, Dados Abertos e Conhecimento sobre os Dados ficaram empatados, todos com média de 2,81.

Os resultados dessa análise de correlação bivariada foram organizados e estão visualmente apresentados no gráfico de matriz de correlação subsequente. Para complementar a análise e investigar a natureza e a intensidade das inter-relações entre os construtos avaliados, realizou-se um estudo de correlação. Para tanto, empregou-se o coeficiente de Pearson, que mede a direção e a intensidade das relações lineares entre variáveis quantitativas. Este coeficiente assume valores adimensionais que variam entre -1 e +1⁶. A análise foi conduzida com as médias obtidas em cada dimensão do modelo teórico proposto, e os resultados dessa correlação bivariada estão organizados e visualmente apresentados no gráfico de matriz de correlação a seguir.

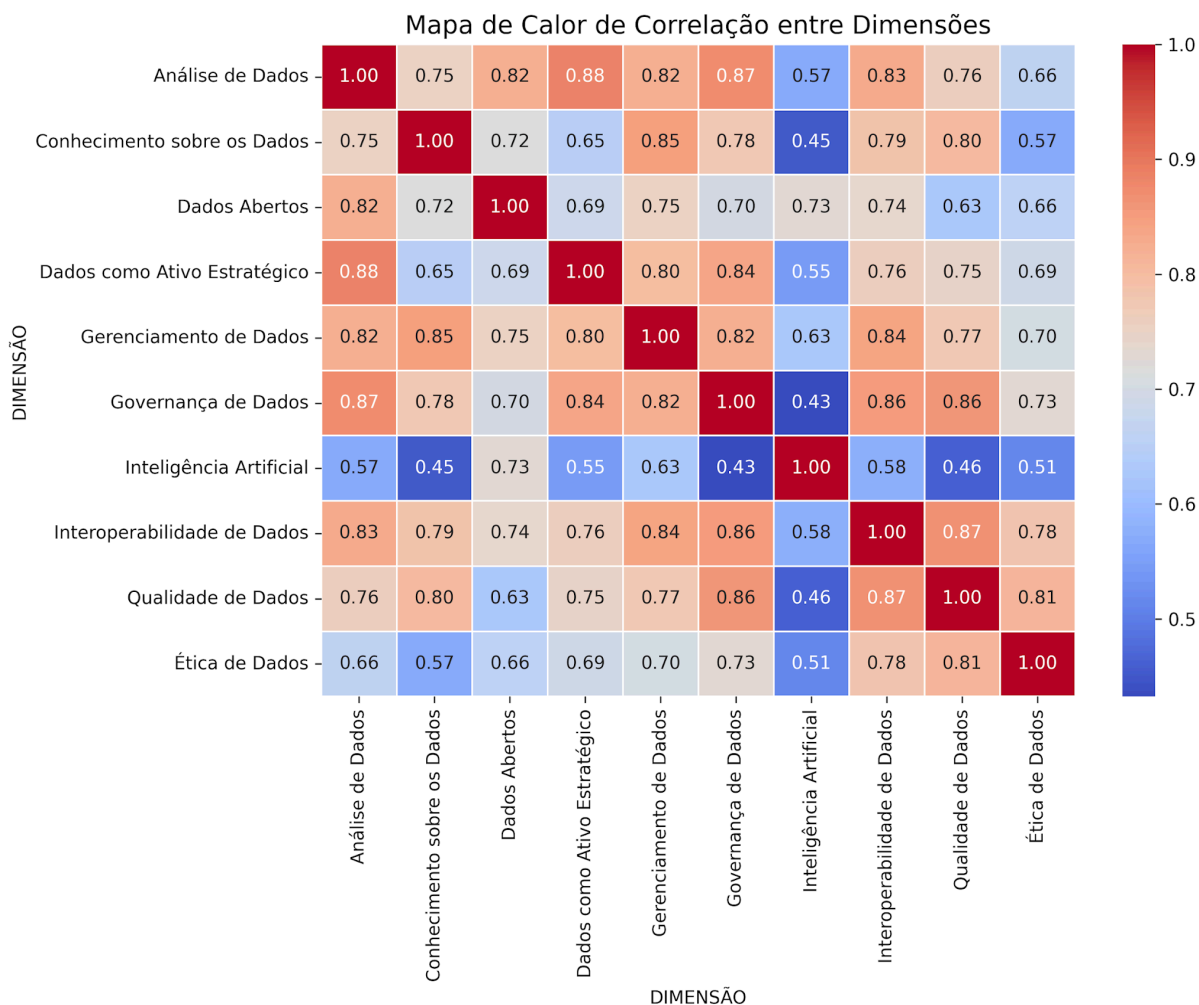
6

Disponível

em:

<<http://www5.eesc.usp.br/saate/index.php/saate/Indicar-a-T%C3%A9cnica/Associar/2.-%C3%81rvore-de-decis%C3%A3o/Gloss%C3%A1rio/Coeficiente-de-correla%C3%A7%C3%A3o-de-Pearson>>. Acesso em: Acesso em: 12 jan. 2026.

Gráfico 4 - Mapa de Calor da Correlação entre Dimensões



Fonte: Elaboração própria

Os resultados obtidos demonstram a existência de correlações positivas significativas, o que sugere que o progresso institucional na governança de dados é um fenômeno que, embora multidimensional, tende a se manifestar de maneira sistêmica. Essa estrutura de alta correlação positiva entre a maioria das dimensões também indica que os aspectos da maturidade de dados não são independentes. Significa que um investimento direcionado a uma área específica é propenso a gerar benefícios secundários em outras áreas correlacionadas. Além disso, a ausência de correlações negativas sugere que o avanço em uma dimensão não prejudica o desenvolvimento de outra.

As maiores correlações se encontram em Análise de Dados e Dados como Ativo Estratégico (0,88); Análise de Dados e Governança de Dados (0,87); Interoperabilidade de Dados e Qualidade de Dados (0,87); e Governança de Dados e Qualidade de Dados (0,86).

A forte correlação entre Análise de Dados e Dados como Ativo Estratégico sugere que o desenvolvimento de uma capacidade analítica robusta permite transformar a coleta de informações em valor real. Assim, os dados só se tornam efetivamente um ativo estratégico quando são utilizados de forma sistemática para embasar decisões e maximizar a efetividade das políticas públicas entregues à sociedade (OCDE, 2019). Não obstante, sugere que onde a organização percebe decisões orientadas a dados, também percebe maior institucionalização estratégica e de governança.

A sofisticação técnica em Análise e Governança de Dados é indiciada como dependente de uma base organizacional robusta. A área analítica geralmente exige a definição de padrões, papéis e decisões de priorização. Nesse contexto, a governança emerge como uma resposta necessária a situações de conflito ou escassez. Não obstante, a dimensão de Governança de Dados promove o letramento em dados e a cultura organizacional, pilares que sustentam o desenvolvimento da capacidade analítica dos servidores. Isso pode ainda ser interpretado como um mecanismo de legitimação: organizações que já colhem valor visível de análises tendem a formalizar governança para proteger e ampliar esses ganhos num efeito de retroalimentação.

No que tange à Interoperabilidade de Dados e Qualidade de Dados, sugere-se que a eficiência na troca de informações entre sistemas heterogêneos está intrinsecamente ligada à confiabilidade do que é compartilhado. O MMD estabelece que um nível alto de interoperabilidade envolve “definição de formatos padronizados, protocolos de comunicação e interfaces de programação, além da harmonização de vocabulários e ontologias para garantir a compreensão mútua dos dados compartilhados” (Brasil, 2024). Esses mesmos padrões são fundamentais para a dimensão de Qualidade de Dados, pois asseguram que os dados sejam precisos, íntegros e adequados ao uso ao transitar entre diferentes plataformas e instituições. Assim, a integração de sistemas expõe as inconsistências latentes: no esforço de interoperar, os problemas de qualidade de dados se tornam evidentes e, conseqüentemente, passíveis de gerenciamento.

Abre-se destaque particular para a forte correlação entre Análise de Dados e Dados Abertos (0,82). Este valor sugere uma associação positiva entre a capacidade de Análise de Dados e a maturidade em Dados Abertos, podendo indicar que organizações que utilizam dados abertos aprimoram suas habilidades analíticas ao permitir a interação ou atuação da sociedade, ou, inversamente, que uma capacidade analítica robusta é um fator impulsionador para a abertura de dados.

As correlações mais baixas observadas estão majoritariamente ligadas à Inteligência Artificial: Governança de Dados (0,43), Conhecimento sobre os Dados (0,45), Qualidade de Dados (0,46) e Ética de Dados (0,46). Isso é reforçado pelo piso significativo na dimensão Inteligência Artificial, onde aproximadamente 34,6% das respostas se encontram no nível 1 e apenas 3,85% atingem o nível 5.

Esse dado sugere que a Estratégia de Inteligência Artificial é percebida em termos de projetos piloto isolados, e não como uma estratégia formal estabelecida. Isso significa que a implementação dessas ferramentas prescinde dos fundamentos básicos para sua sustentação, sendo um processo que se desvincula de uma governança de dados clara, integrada, com infraestrutura adequada e monitoramento contínuo, elementos que, inclusive, são vinculados a níveis altos na dimensão Inteligência artificial pelo MMD. Essa desconexão corrobora a análise da MIT Technology Review⁷, que aponta que cerca de 95% dos projetos de IA não geram o retorno esperado. O principal motivo reside no fato de as empresas focarem em experimentos isolados sem considerar a escalabilidade, a integração com os processos existentes e o real valor de negócio.

Outra dinâmica se reflete na capacidade de desenvolver Análise de Dados e Inteligência Artificial, já que o MMD define que que níveis mais altos nessas dimensões pressupõem não apenas tecnologia, mas dados relevantes, suficientes e de qualidade, além de capacidades analíticas avançadas e processos decisórios orientados por evidências. Em outras palavras, baixa governança e baixa qualidade alimentam um círculo vicioso que impede o amadurecimento de analytics e IA, especialmente em contextos de segurança pública que dependem fortemente de dados geoespaciais, integrados e tempestivos para planejar policiamento, prevenção e resposta rápida a incidentes.

7

Disponível

em:

<<https://mittechreview.com.br/por-que-95-dos-projetos-de-ia-nao-dao-retorno/>>. Acesso em: 12 fev. 2026

Não obstante, verifica-se na dimensão Ética de Dados que a maior parte dos valores (6 de 9, correspondendo a 67% das correlações) exhibe uma correlação inferior a 0,7. Além disso, apresenta ausência total de respostas no nível 5. O desenvolvimento e fortalecimento das demais dimensões sem a devida observância a princípios, políticas e diretrizes que assegurem imparcialidade, equidade e transparência para mitigar vieses pode aumentar a probabilidade de reprodução de preconceitos algorítmicos contra populações vulneráveis. Tal cenário não apenas fragiliza a legitimidade democrática do Estado, como também pode tornar as instituições reféns de assimetrias informacionais, aproximando a gestão pública da lógica extrativa do capitalismo de vigilância tratado por Zuboff (2020), em detrimento da soberania analítica necessária para a proteção do interesse público.

Destaca-se também a moderada associação com a Qualidade de Dados (0,46) e o Conhecimento sobre os Dados (0,45), que enfatiza o risco inerente do efeito *Garbage In, Garbage Out* (em tradução livre, "entra lixo, sai lixo"). Nesse cenário, modelos preditivos e algoritmos de reconhecimento operam sobre bases inconsistentes, fragmentadas ou insuficientemente documentadas, o que pode gerar resultados que induzem ao erro em decisões operacionais críticas e na alocação de recursos públicos.

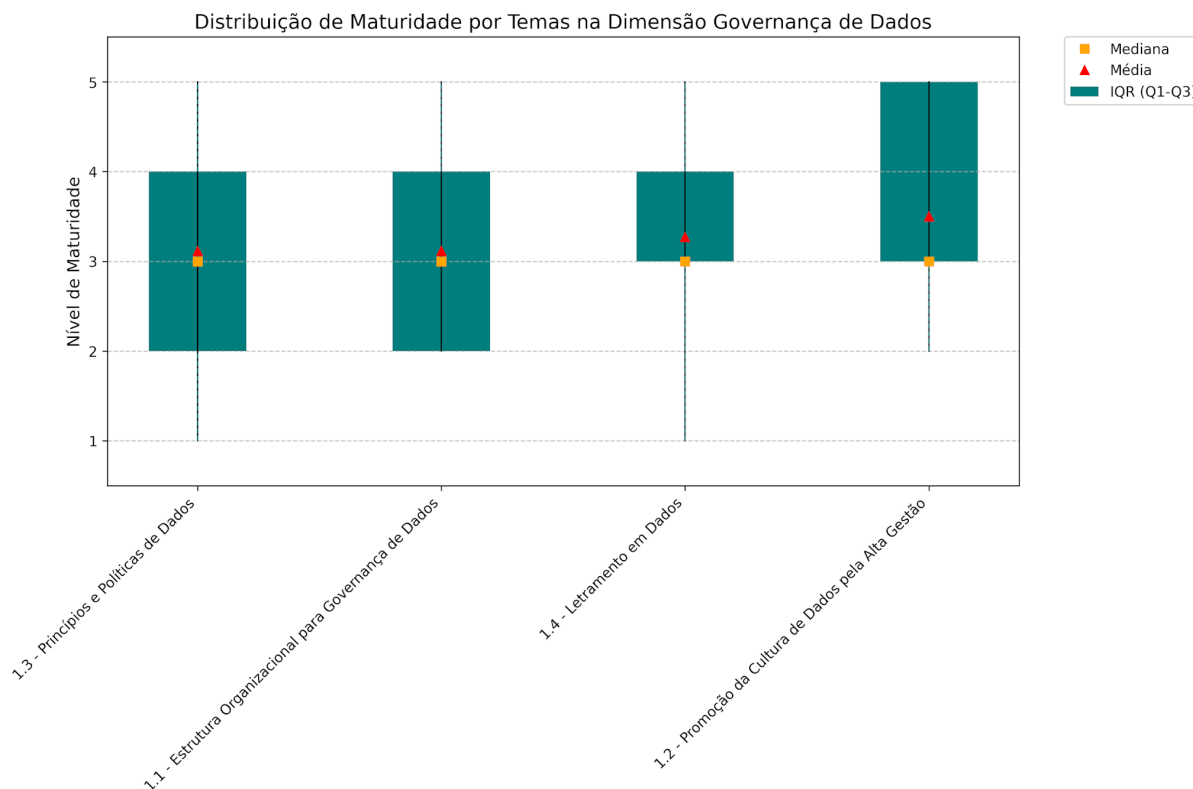
De modo geral, as dimensões que apresentaram os menores níveis de maturidade estão relacionadas à integração e interoperabilidade de dados; metadados e padronização das informações; aplicação de analytics avançado e inteligência artificial; e processos de verificação de qualidade. Tais achados indicam que os desafios institucionais primários não residem meramente na geração de dados em si, mas na sua estruturação, integração e utilização estratégica.

4.4 Análise por temas dentro das dimensões

4.4.1 Governança de Dados

A dimensão Governança de Dados apresenta desempenho intermediário, com média geral de 3,25 e mediana de 3,0, posicionando-se solidamente no Nível 3 (Emergente) do MMD. Esta dimensão compreende quatro temas fundamentais: Promoção da Cultura de Dados pela Alta Gestão (média = 3,50; mediana = 3,0), Letramento em Dados (média = 3,27; mediana = 3,0), Estrutura Organizacional para Governança de Dados (média = 3,12; mediana = 3,0) e Princípios e Políticas de Dados (média = 3,12; mediana = 3,0).

Gráfico 5 - Maturidade na Dimensão Governança de Dados



Fonte: Elaboração própria

A análise dos resultados revela relativa homogeneidade entre os temas, com variação de apenas 0,38 pontos entre os temas de maior e menor desempenho. Esta homogeneidade sugere que os desafios de governança de dados são sistêmicos, afetando simultaneamente múltiplos aspectos da estruturação, cultura e políticas. Contudo, a liderança da Promoção da Cultura de Dados pela Alta Gestão indica que o compromisso da liderança vem se consolidando sensivelmente em níveis superiores aos demais aspectos.

O tema Promoção da Cultura de Dados pela Alta Gestão, com média de 3,50 e mediana de 3,0, indica que a maioria das unidades federativas já conta com lideranças comprometidas com a valorização dos dados como ativos estratégicos. O desvio padrão de 1,10 e a amplitude interquartil de 2,0 ($Q1 = 3,0$; $Q3 = 5,0$) revelam heterogeneidade significativa, com 25% das unidades federativas já em níveis avançados ($Q3 = 5,0$), caracterizados por lideranças que atuam como exemplos e engajam ativamente equipes na valorização dos dados. Esta liderança constitui um ativo crítico para a consolidação da

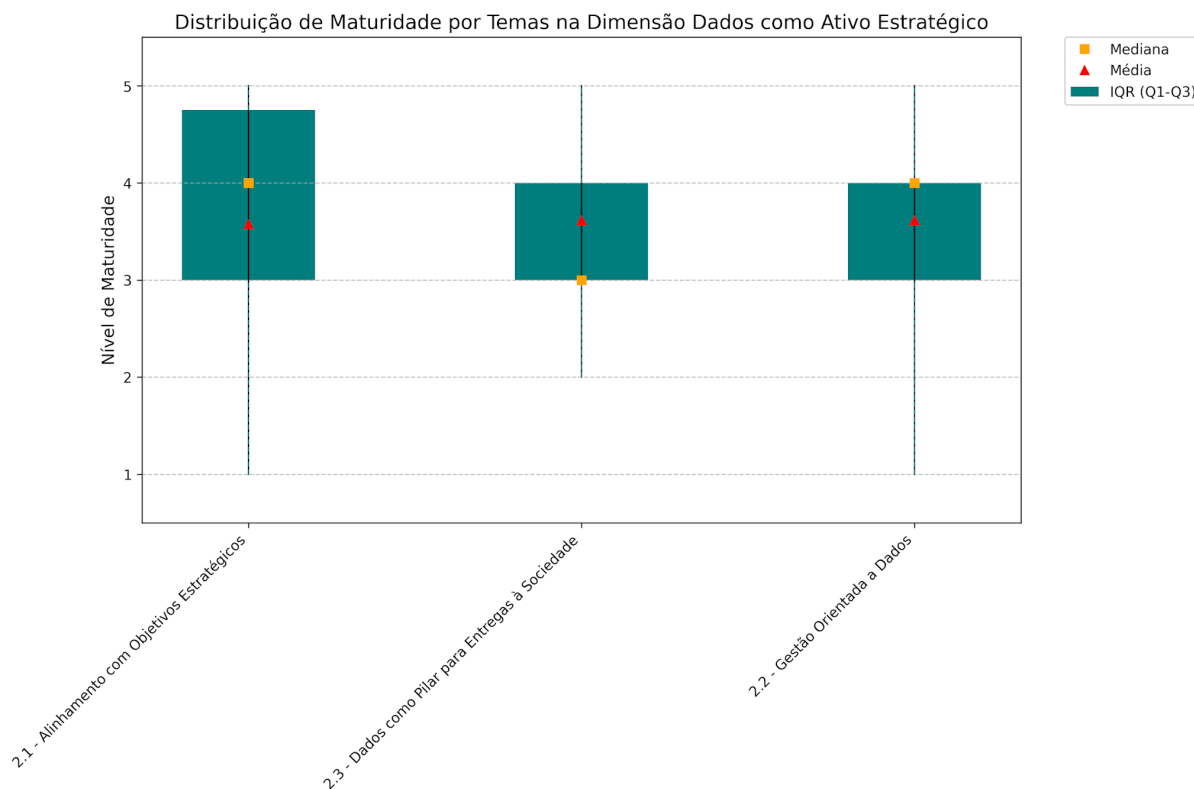
governança de dados, uma vez que mudanças culturais dependem fundamentalmente do compromisso e exemplo da alta gestão.

O Letramento em Dados, com média de 3,27 e mediana de 3,0, apresenta a maior dispersão da dimensão (desvio padrão = 1,12; IQR = 1,0), indicando heterogeneidade na capacidade de promover capacitação contínua para o uso efetivo de dados. A presença de unidades federativas no Nível 1 (mínimo = 1) evidencia que algumas organizações ainda não implementaram programas estruturados de letramento em dados, limitando a capacidade de suas equipes de utilizar dados de forma efetiva para tomada de decisões.

A Estrutura Organizacional para Governança de Dados e os Princípios e Políticas de Dados apresentam desempenho idêntico (média = 3,12; mediana = 3,0), mas com dispersões distintas. A Estrutura Organizacional apresenta desvio padrão de 1,14 e IQR de 2,0 (Q1 = 2,0; Q3 = 4,0), enquanto Princípios e Políticas apresentam desvio padrão de 1,24 e IQR de 2,0 (Q1 = 2,0; Q3 = 4,0). Estas dispersões indicam que, embora a maioria das unidades federativas tenha iniciado a estruturação de governança e a definição de políticas, estas iniciativas ainda não estão consolidadas e apresentam variações significativas em termos de abrangência e efetividade.

4.4.2 Dados como Ativo Estratégico

A dimensão Dados como Ativo Estratégico apresenta o segundo melhor desempenho entre todas as dimensões avaliadas, com média geral de 3,60 e mediana de 3,67, posicionando-se solidamente no Nível 3 (Emergente) com tendência ao Nível 4 (Desenvolvido). Esta dimensão compreende três temas: Dados como Pilar para Entregas à Sociedade (média = 3,62; mediana = 3,0), Gestão Orientada a Dados (média = 3,62; mediana = 4,0) e Alinhamento com Objetivos Estratégicos (média = 3,58; mediana = 4,0).

Gráfico 6 - Maturidade na Dimensão Dados como Ativo Estratégico

Fonte: Elaboração própria

A homogeneidade das médias dos três temas (variação de apenas 0,04 pontos) e a elevação consistente das medianas (todas iguais ou superiores a 3,0) indicam que o reconhecimento dos dados como recurso estratégico vem se consolidando na maioria das organizações de segurança pública brasileiras.

O tema Dados como Pilar para Entregas à Sociedade indica que a maioria das unidades federativas já estrutura sua governança e gestão de dados com foco na melhoria da qualidade e consistência das políticas públicas. O desvio padrão moderado de 0,94 e a amplitude interquartil de 1,0 (Q1 = 3,0; Q3 = 4,0) sugerem relativa convergência nacional neste aspecto, embora persistam unidades federativas em níveis iniciais (mínimo = 2).

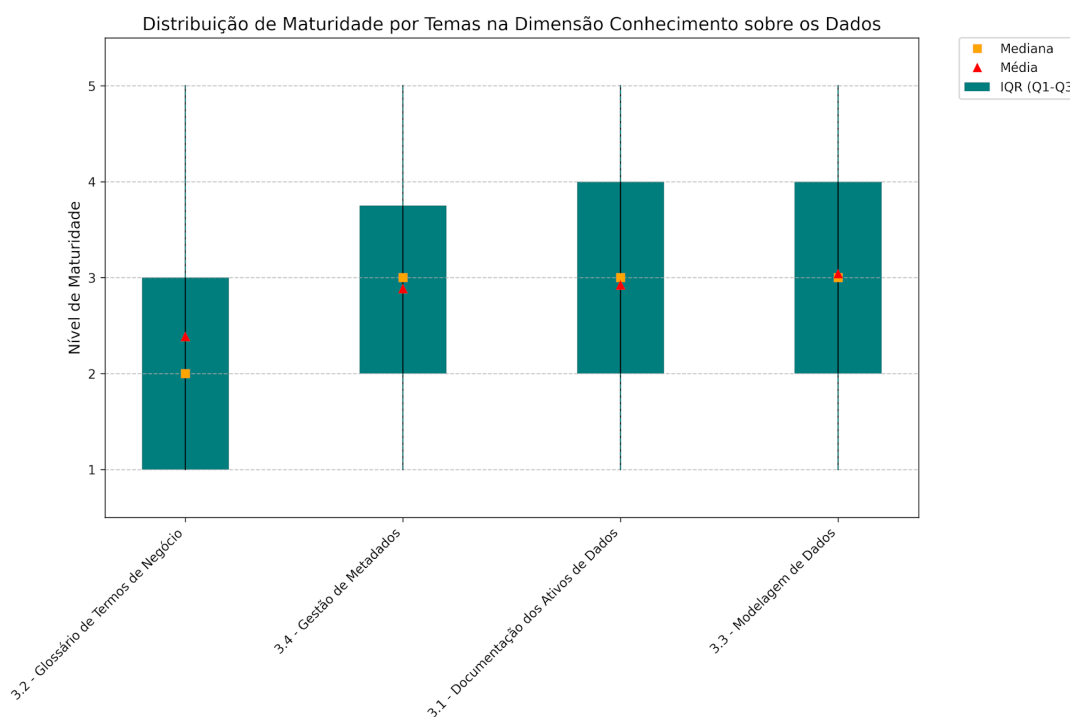
O tema Gestão Orientada a Dados apresenta desempenho idêntico em termos de média (3,62), mas mediana superior (4,0), indicando que mais de 50% das unidades federativas já reconhecem os dados como recurso estratégico utilizado sistematicamente para embasar decisões em todos os níveis hierárquicos. O desvio padrão de 0,98 e a amplitude

interquartil de 1,0 (Q1 = 3,0; Q3 = 4,0) confirmam a relativa homogeneidade, embora a presença de unidades federativas no Nível 1 (mínimo = 1) evidencie que a universalização desta prática ainda não foi alcançada.

4.4.3 Conhecimento sobre os Dados

A dimensão Conhecimento sobre os Dados apresenta desempenho intermediário, com média geral de 2,81 e mediana de 3,0, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende quatro temas fundamentais: Modelagem de Dados (média = 3,04; mediana = 3,0), Documentação dos Ativos de Dados (média = 2,92; mediana = 3,0), Gestão de Metadados (média = 2,88; mediana = 3,0) e Glossário de Termos de Negócio (média = 2,38; mediana = 2,0).

Gráfico 7 - Maturidade na Dimensão Conhecimento sobre os Dados



Fonte: Elaboração própria

A relativa homogeneidade das médias dos três primeiros temas (variação de apenas 0,16 pontos) contrasta com o desempenho significativamente inferior do Glossário de

Termos de Negócio, que se posicionou como o segundo tema de menor maturidade em todo o diagnóstico nacional. Esta discrepância sugere que, embora as organizações de segurança pública tenham avançado na estruturação técnica de suas bases de dados (modelagem) e no registro de informações básicas sobre seus ativos (documentação), a padronização semântica e a construção de linguagem comum entre áreas permanecem como desafios críticos.

O tema Modelagem de Dados, com média de 3,04 e mediana de 3,0, indica que a maioria das unidades federativas já adotou práticas estruturadas de organização de bases de dados, superando o estágio de sistemas ad hoc e não documentados. Contudo, o desvio padrão de 1,37 e a amplitude interquartil de 2,0 (Q1 = 2,0; Q3 = 4,0) revelam heterogeneidade significativa. Enquanto 25% das unidades federativas (Q3 = 4,0) já implementaram modelos de dados padronizados e documentados que facilitam a gestão e o uso estratégico, 25% (Q1 = 2,0) ainda operam com modelagens incipientes ou inexistentes. Esta dispersão sugere um comprometimento da interoperabilidade entre sistemas e a capacidade de integração de dados entre unidades federativas, o que influencia na limitação do potencial de análises nacionais integradas.

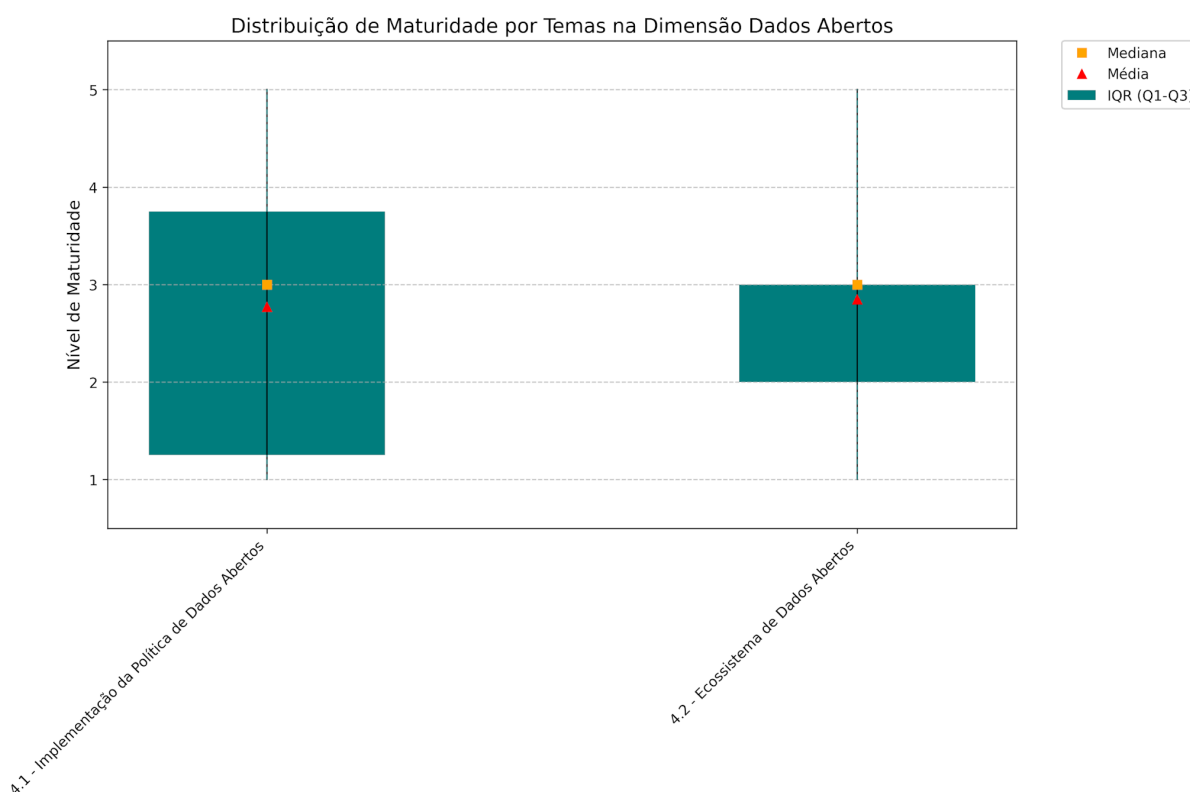
A Documentação dos Ativos de Dados e a Gestão de Metadados apresentam desempenho similar (médias de 2,92 e 2,88, respectivamente), ambos com mediana de 3,0 e dispersões elevadas (desvios padrão de 1,44 e 1,40, respectivamente). Estes resultados indicam que, embora a maioria das unidades federativas tenha iniciado práticas de registro de informações sobre seus dados (propriedade, formato, origem), estas práticas ainda não estão sistematizadas e institucionalizadas. A amplitude interquartil de 2,0 em ambos os temas (Q1 = 2,0; Q3 = 4,0) indica uma polarização entre unidades federativas com catálogos de dados estruturados e atualizados (Nível 4) e aquelas com esforços iniciados e pontuais (Nível 2).

O Glossário de Termos de Negócio, com média de 2,38 e mediana de 2,0, configura-se como o principal gargalo da dimensão. O desvio padrão de 1,50 e a amplitude interquartil de 2,0 (Q1 = 1,0; Q3 = 3,0) indicam que a maioria das unidades federativas ainda não implementou glossários formais que padronizem definições e reduzam ambiguidades na comunicação entre áreas. Esta lacuna tem implicações críticas para a qualidade dos dados, uma vez que a ausência de definições compartilhadas gera inconsistências na coleta, interpretação e análise de informações e, conseqüentemente, compromete a confiabilidade dos diagnósticos e a efetividade das políticas baseadas em evidências.

4.4.4 Dados Abertos

A dimensão Dados Abertos apresenta desempenho intermediário-baixo, com média geral de 2,81 e mediana de 3,0, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende dois temas: Implementação da Política de Dados Abertos (média = 2,77; mediana = 3,0) e Ecossistema de Dados Abertos (média = 2,85; mediana = 3,0). A proximidade das médias dos dois temas (diferença de apenas 0,08 pontos) sugere que os desafios enfrentados pelas organizações de segurança pública são similares em ambos os aspectos.

Gráfico 8 - Maturidade na Dimensão Dados Abertos



Fonte: Elaboração própria

O tema Implementação da Política de Dados Abertos, com média de 2,77 e mediana de 3,0, indica que a maioria das unidades federativas iniciou processos de abertura de dados, mas ainda não consolidou práticas sistemáticas e abrangentes. O desvio padrão de

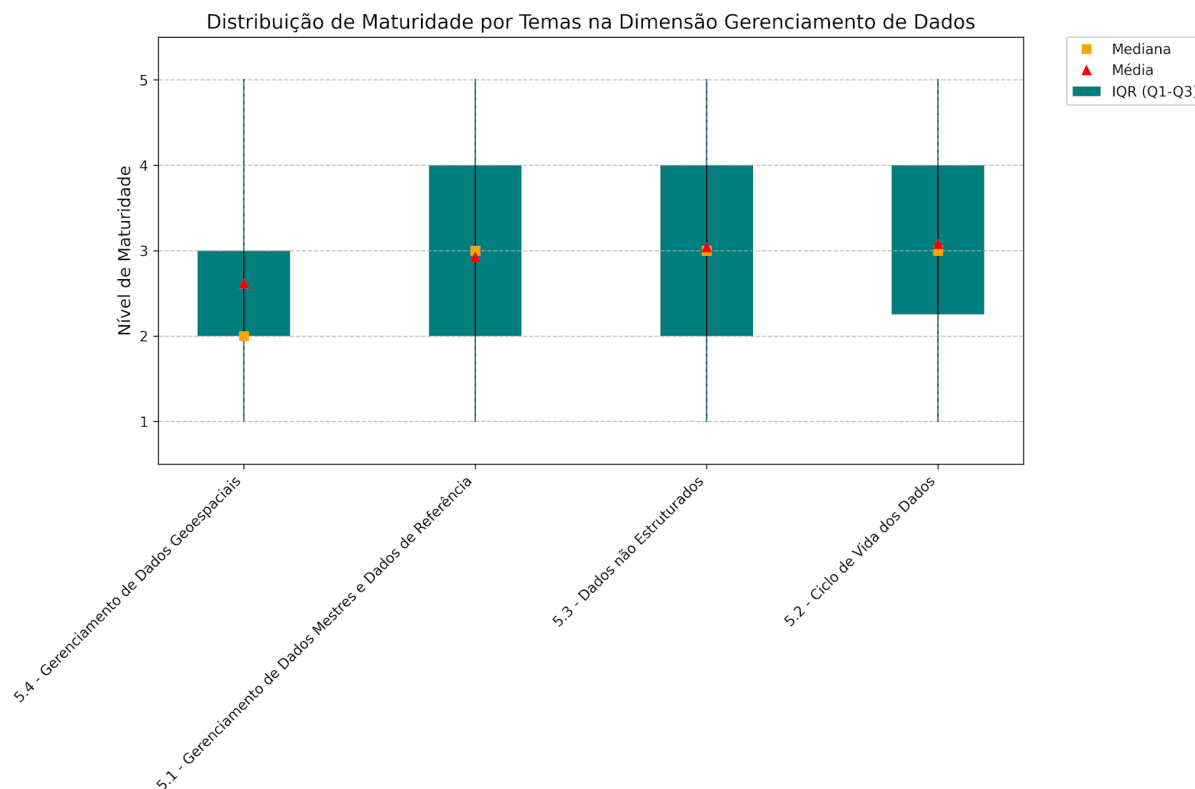
1,45 e a amplitude interquartil de 2,5 ($Q1 = 1,25$; $Q3 = 3,75$) revelam heterogeneidade significativa, com 25% das unidades federativas ainda em estágios iniciais ($Q1 = 1,25$, entre Nível 1 e 2) e 25% já em estágios avançados ($Q3 = 3,75$, entre Nível 3 e 4). Esta dispersão reflete diferenças na priorização política da transparência, na capacidade técnica para preparação e publicação de dados, e na compreensão dos benefícios da abertura de dados para a participação social e a inovação.

O Ecossistema de Dados Abertos, com média de 2,85 e mediana de 3,0, apresenta desempenho ligeiramente superior, mas ainda insuficiente para caracterizar um ecossistema maduro. O desvio padrão de 1,19 e a amplitude interquartil de 1,0 ($Q1 = 2,0$; $Q3 = 3,0$) indicam menor dispersão do que na Implementação da Política, sugerindo que as contribuições para o ecossistema de dados abertos são relativamente homogêneas entre as unidades federativas. Contudo, a mediana de 3,0 e $Q3$ de 3,0 indicam que a maioria das unidades federativas ainda não alcançou níveis avançados de engajamento com o ecossistema, limitando-se a publicações básicas sem estratégias de promoção de reutilização, engajamento com usuários ou fomento à inovação baseada em dados abertos.

A análise conjunta dos dois temas revela que, embora a maioria das unidades federativas tenha iniciado processos de abertura de dados (mediana = 3,0 em ambos os temas), estas iniciativas permanecem incipientes e não consolidadas. A transição para níveis superiores de maturidade demanda não apenas a publicação de mais conjuntos de dados, mas também a melhoria da qualidade dos dados publicados (completude, atualização, granularidade), a adoção de formatos e padrões que facilitem a reutilização, e o estabelecimento de canais de comunicação com usuários que permitam identificar demandas e avaliar impactos.

4.4.5 Gerenciamento de Dados

A dimensão Gerenciamento de Dados apresenta desempenho intermediário, com média geral de 2,91 e mediana de 3,0, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende quatro temas: Ciclo de Vida dos Dados (média = 3,08; mediana = 3,0), Dados não Estruturados (média = 3,04; mediana = 3,0), Gerenciamento de Dados Mestres e Dados de Referência (média = 2,92; mediana = 3,0) e Gerenciamento de Dados Geoespaciais (média = 2,62; mediana = 2,0).

Gráfico 9 - Maturidade na Dimensão Gerenciamento de Dados

Fonte: Elaboração própria

A análise dos resultados revela certa heterogeneidade entre os temas, com variação de 0,46 pontos entre o tema de maior e menor desempenho. Esta heterogeneidade sugere que os desafios de gerenciamento de dados variam entre diferentes tipos de dados e processos, com avanços mais consolidados em aspectos gerais (ciclo de vida) e lacunas críticas em aspectos especializados (dados geoespaciais).

O tema Ciclo de Vida dos Dados, com média de 3,08 e mediana de 3,0, indica que a maioria das unidades federativas já estruturou práticas de coleta, armazenamento, uso e descarte de dados. Contudo, o desvio padrão de 1,32 e a amplitude interquartil de 1,75 (Q1 = 2,25; Q3 = 4,0) revelam heterogeneidade significativa, com 25% das unidades federativas ainda em estágios iniciais (Q1 = 2,25, entre Nível 2 e 3) e 25% já em estágios avançados (Q3 = 4,0). Esta dispersão reflete diferenças na maturidade dos processos de gestão de dados e na capacidade de implementar controles ao longo de todo o ciclo de vida.

O tema Dados não Estruturados apresenta desempenho similar (média = 3,04; mediana = 3,0), mas com dispersão ligeiramente inferior (desvio padrão = 1,25; IQR = 2,0). Este resultado indica que a maioria das unidades federativas já iniciou a adoção de práticas e ferramentas para coleta, armazenamento e análise de dados não estruturados (como textos, imagens, vídeos e áudios), reconhecendo sua importância crescente para a segurança pública contemporânea. Contudo, a mediana de 3,0 e Q3 de 4,0 indicam que a maioria ainda não alcançou níveis avançados de aproveitamento estratégico destes dados.

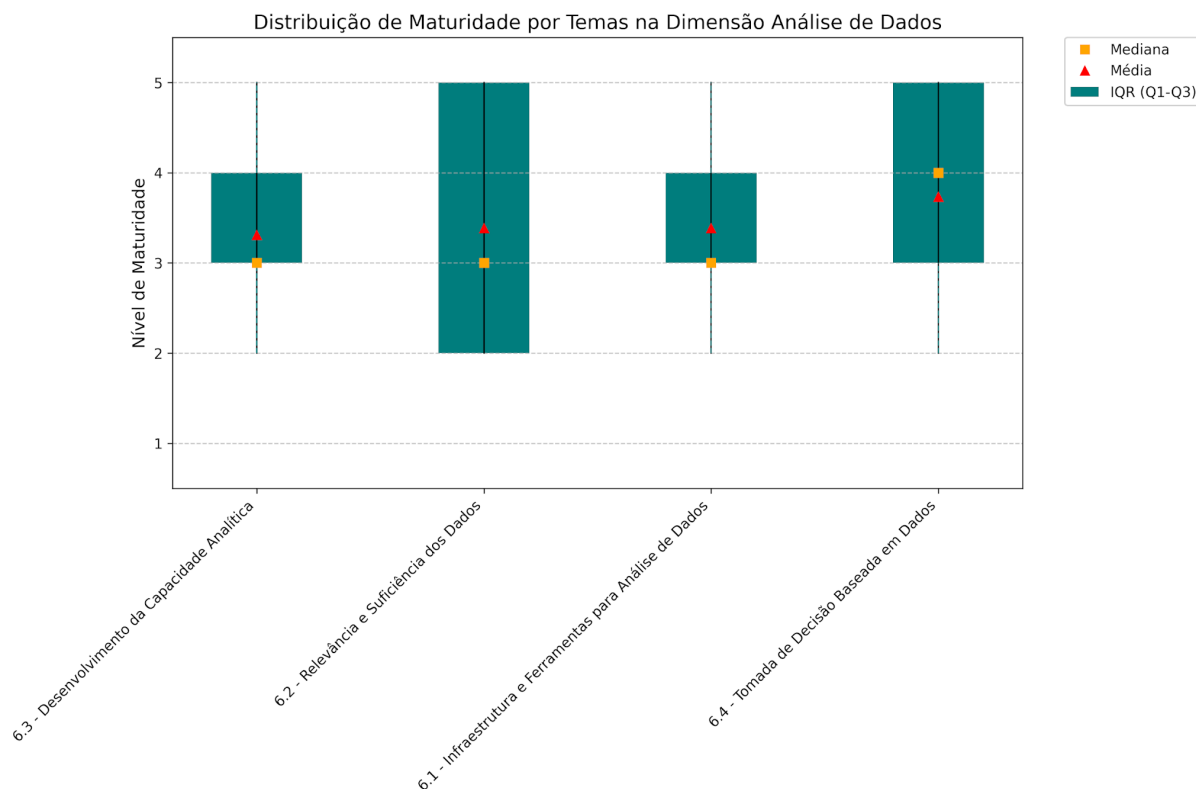
O Gerenciamento de Dados Mestres e Dados de Referência, com média de 2,92 e mediana de 3,0, apresenta a maior dispersão da dimensão (desvio padrão = 1,44; IQR = 2,0), indicando heterogeneidade significativa na capacidade de gerenciar dados críticos que servem como referência para múltiplos sistemas e processos. A presença de unidades federativas no Nível 1 (mínimo = 1) evidencia que algumas organizações ainda não implementaram processos estruturados de gerenciamento de dados mestres, comprometendo a consistência e integridade de suas bases de dados.

O Gerenciamento de Dados Geoespaciais, com média de 2,62 e mediana de 2,0, configura-se como o principal gargalo da dimensão e um dos temas de menor maturidade em todo o diagnóstico nacional. O desvio padrão de 1,10 e a amplitude interquartil de 1,0 (Q1 = 2,0; Q3 = 3,0) indicam que a maioria das unidades federativas ainda não estruturou adequadamente a captura, armazenamento e utilização de dados geoespaciais, apesar de sua importância crítica para análises de padrões espaciais de criminalidade e planejamento de operações policiais.

4.4.6 Análise de Dados

A dimensão Análise de Dados apresenta o desempenho mais robusto entre todas as dimensões avaliadas, com média geral de 3,45 e mediana de 3,50, posicionando-se solidamente no Nível 3 (Emergente) com tendência ao Nível 4 (Desenvolvido). Esta dimensão compreende quatro temas fundamentais: Tomada de Decisão Baseada em Dados (média = 3,73; mediana = 4,0), Relevância e Suficiência dos Dados (média = 3,38; mediana = 3,0), Infraestrutura e Ferramentas para Análise de Dados (média = 3,38; mediana = 3,0) e Desenvolvimento da Capacidade Analítica (média = 3,31; mediana = 3,0).

Gráfico 10 - Maturidade na Dimensão Análise de Dados



Fonte: Elaboração própria

O tema Tomada de Decisão Baseada em Dados destaca-se como o de maior maturidade em todo o diagnóstico nacional, com 75% das unidades federativas ($Q3 = 5,0$) atingindo níveis entre 3 e 5, e 50% alcançando o nível máximo de maturidade. Este resultado indica que a cultura de decisões fundamentadas em evidências já se encontra relativamente consolidada nas organizações de segurança pública brasileiras, refletindo os investimentos realizados nas últimas duas décadas em sistemas de informação criminal e plataformas de inteligência policial. O desvio padrão moderado (1,04) sugere convergência nacional neste aspecto, embora persistam unidades federativas no Nível 2 (Iniciado), evidenciando que a universalização desta prática ainda não foi alcançada.

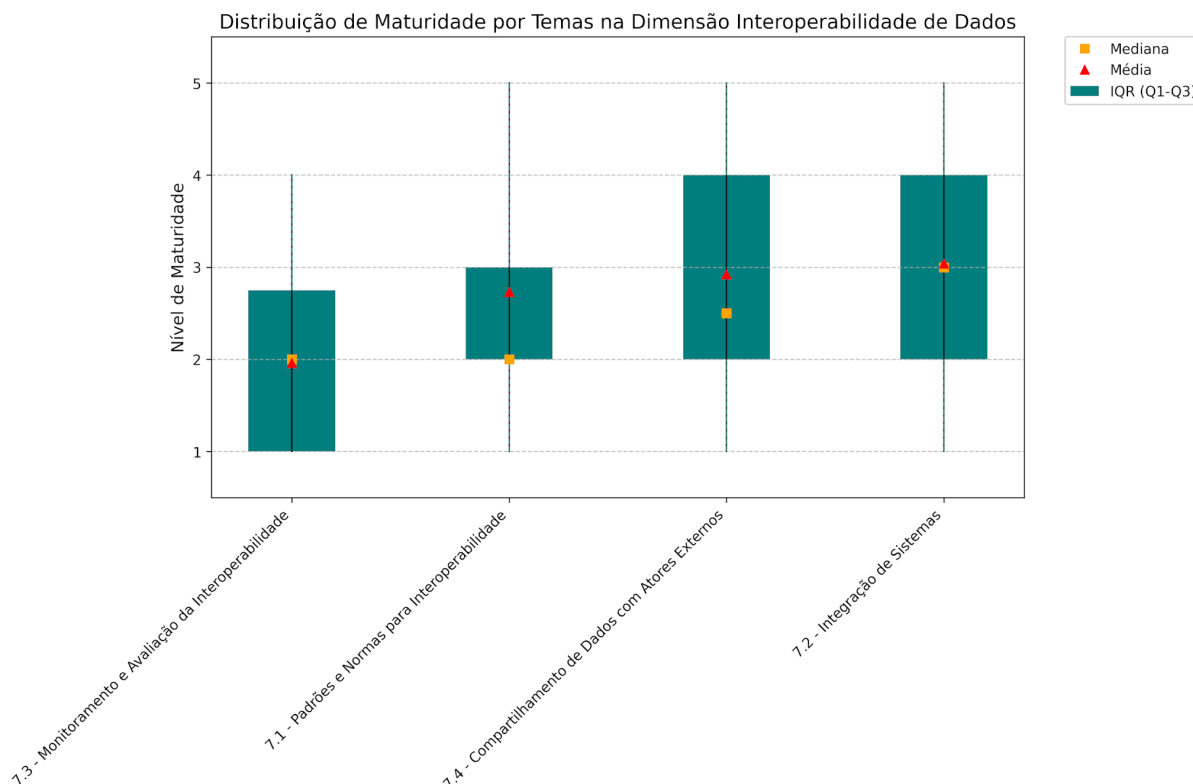
Os temas Relevância e Suficiência dos Dados e Infraestrutura e Ferramentas para Análise de Dados apresentam desempenho idêntico em termos de média (3,38) e mediana (3,0), mas diferem significativamente na dispersão. O primeiro exibe desvio padrão de 1,36 e IQR de 3,0 ($Q1 = 2,0$; $Q3 = 5,0$), indicando polarização entre unidades federativas

que consideram seus dados plenamente adequados (Nível 5) e aquelas que ainda enfrentam lacunas críticas de cobertura e relevância (Nível 2). Esta heterogeneidade sugere que a suficiência dos dados está fortemente associada à capacidade de investimento em sistemas de coleta e à maturidade dos processos de identificação de necessidades informacionais. O segundo tema, com desvio padrão de 0,98 e IQR de 1,0 (Q1 = 3,0; Q3 = 4,0), demonstra maior homogeneidade, indicando que a infraestrutura tecnológica básica para análise de dados caminha para uma disseminação, embora nem sempre otimizada.

O Desenvolvimento da Capacidade Analítica, caracterizado pela existência de equipes especializadas em ciência de dados e análise preditiva integradas aos processos decisórios estratégicos, apresenta média de 3,31 e desvio padrão de 0,79, a menor dispersão da dimensão; sugerindo que os investimentos em capacitação analítica têm sido relativamente uniformes no território nacional. Contudo, a mediana de 3,0 e Q3 de 4,0 indicam que a maioria das unidades federativas ainda não alcançou o Nível 5 (Otimizado), onde há planejamento estruturado e orçamento destacado para tal.

4.4.7 Interoperabilidade de Dados

A dimensão Interoperabilidade de Dados apresenta o segundo desempenho mais crítico entre todas as dimensões avaliadas, com média geral de 2,66 e mediana de 2,63, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende quatro temas: Integração de Sistemas (média = 3,04; mediana = 3,0), Compartilhamento de Dados com Atores Externos (média = 2,92; mediana = 2,5), Padrões e Normas para Interoperabilidade (média = 2,73; mediana = 2,0) e Monitoramento e Avaliação da Interoperabilidade (média = 1,96; mediana = 2,0).

Gráfico 11 - Maturidade na Dimensão Interoperabilidade de Dados

Fonte: Elaboração própria

A análise dos resultados revela heterogeneidade significativa entre os temas, com variação de 1,08 pontos entre o tema de maior e menor desempenho. Esta heterogeneidade indica que os desafios de interoperabilidade variam significativamente entre diferentes aspectos, com avanços relativos na integração interna de sistemas e lacunas críticas no monitoramento e avaliação da interoperabilidade.

O tema Integração de Sistemas, com média de 3,04 e mediana de 3,0, apresenta o melhor desempenho da dimensão, indicando que a maioria das unidades federativas já iniciou processos de integração de sistemas heterogêneos. Contudo, o desvio padrão de 1,25 e a amplitude interquartil de 2,0 ($Q1 = 2,0$; $Q3 = 4,0$) revelam heterogeneidade significativa, com 25% das unidades federativas ainda em estágios iniciais ($Q1 = 2,0$) e 25% já em estágios avançados ($Q3 = 4,0$). Esta dispersão reflete diferenças na complexidade dos ambientes de TI e na capacidade de implementar mecanismos de interoperabilidade.

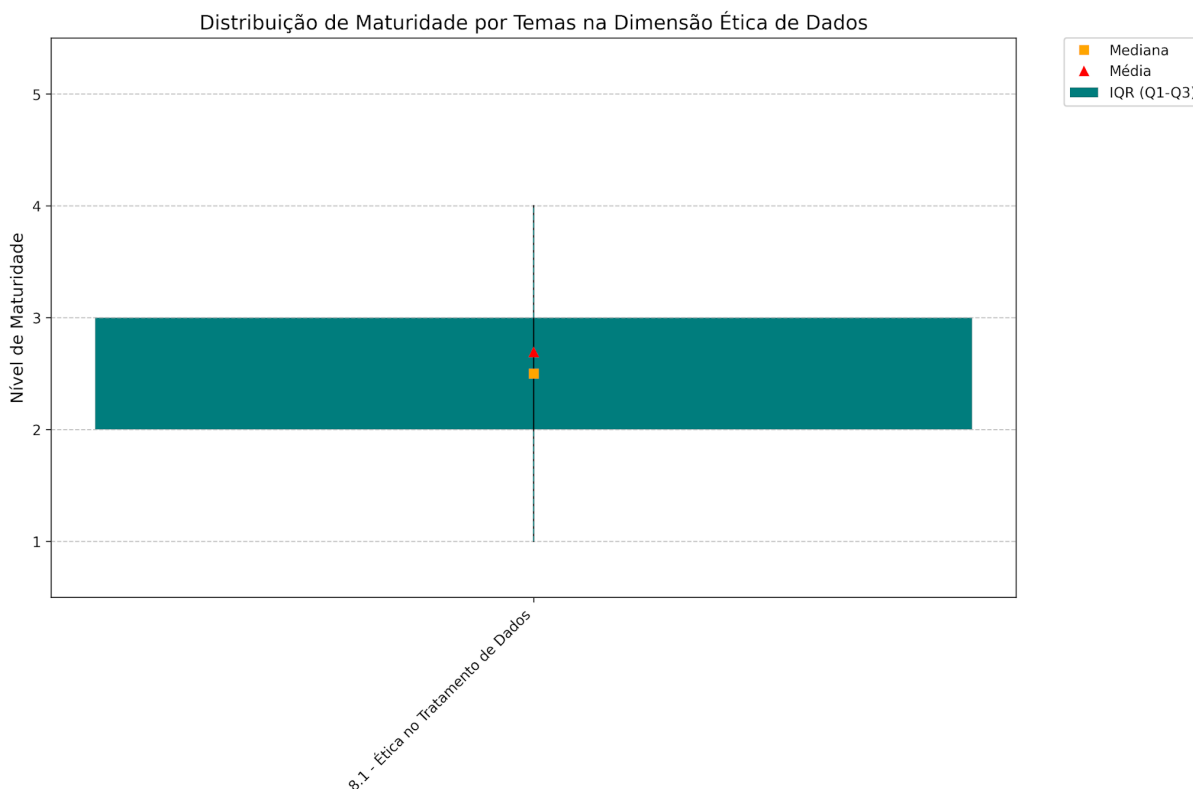
O Compartilhamento de Dados com Atores Externos, com média de 2,92 e mediana de 2,5, apresenta desempenho intermediário, indicando que a maioria das unidades federativas ainda enfrenta desafios significativos para compartilhar dados de forma eficiente, segura e em conformidade com as regulamentações. O desvio padrão de 1,16 e a amplitude interquartil de 2,0 (Q1 = 2,0; Q3 = 4,0) evidenciam heterogeneidade similar à observada em Integração de Sistemas.

Os temas Padrões e Normas para Interoperabilidade (média = 2,73; mediana = 2,0) e Monitoramento e Avaliação da Interoperabilidade (média = 1,96; mediana = 2,0) apresentam os desempenhos mais críticos da dimensão. O primeiro indica que a maioria das unidades federativas ainda não adotou plenamente padrões e normas que garantam consistência e compatibilidade dos dados compartilhados. O segundo, com a segunda menor média de todo o diagnóstico nacional, evidencia que o monitoramento contínuo da interoperabilidade permanece como uma prática extremamente incipiente, comprometendo a capacidade de identificar problemas e implementar melhorias.

4.4.8 Ética de Dados

A dimensão Ética de Dados apresenta desempenho crítico, com média de 2,69 e mediana de 2,5, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende um único tema: Ética no Tratamento de Dados, que apresenta os mesmos indicadores da dimensão. O desvio padrão de 0,88 e a amplitude interquartil de 1,0 (Q1 = 2,0; Q3 = 3,0) revelam que a maioria das unidades federativas ainda se encontra em estágios iniciais de implementação de princípios éticos no tratamento de dados.

Gráfico 12 - Maturidade na Dimensão Ética de Dados



Fonte: Elaboração própria

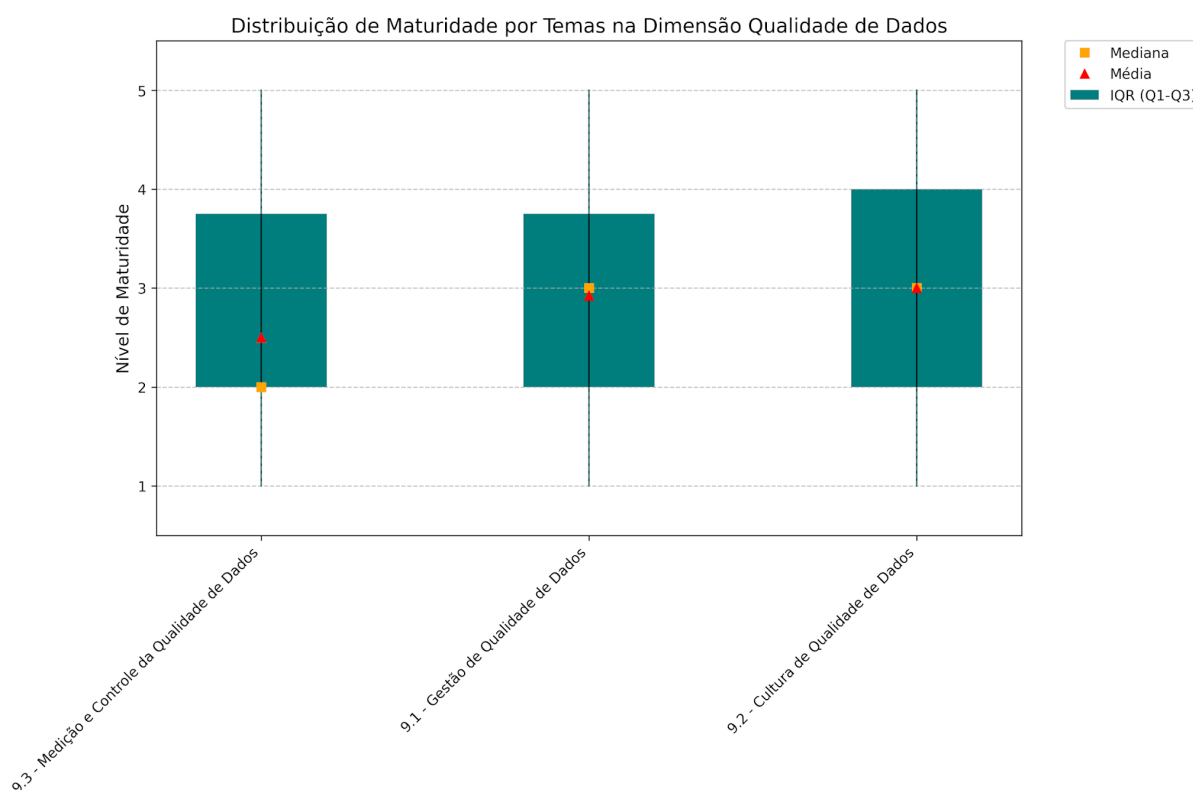
Este resultado indica que a ética de dados permanece como um desafio significativo na segurança pública brasileira, apesar da crescente atenção a questões de privacidade, discriminação e transparência no uso de dados. A mediana de 2,5 e Q3 de 3,0 evidenciam que a maioria das unidades federativas ainda não consolidou políticas robustas de ética de dados, limitando-se a iniciativas pontuais ou ao cumprimento mínimo de requisitos legais.

A presença de unidades federativas no Nível 4 (máximo = 4) demonstra que a implementação de práticas avançadas de ética de dados é viável no contexto brasileiro. Contudo, a concentração de 75% das unidades federativas (Q3 = 3,0) em níveis iniciais e intermediários indica que a difusão de práticas éticas robustas permanece limitada, refletindo desafios de compreensão dos princípios éticos, capacidade de implementação de controles, e priorização política da ética de dados.

4.4.9 Qualidade de Dados

A dimensão Qualidade de Dados apresenta desempenho crítico, com média geral de 2,81 e mediana de 2,83, posicionando-se no limiar entre o Nível 2 (Iniciado) e o Nível 3 (Emergente) do MMD. Esta dimensão compreende três temas: Cultura de Qualidade de Dados (média = 3,0; mediana = 3,0), Gestão de Qualidade de Dados (média = 2,92; mediana = 3,0) e Medição e Controle da Qualidade de Dados (média = 2,5; mediana = 2,0).

Gráfico 13 - Maturidade na Dimensão Qualidade de Dados



Fonte: Elaboração própria

A análise dos resultados revela heterogeneidade significativa entre os temas, com variação de 0,5 pontos entre o tema de maior e menor desempenho. Esta heterogeneidade indica que os desafios de qualidade de dados variam entre diferentes aspectos, com avanços relativos na promoção de cultura de qualidade e lacunas críticas na medição e controle sistemáticos.

O tema Cultura de Qualidade de Dados, com média de 3,0 e mediana de 3,0, apresenta o melhor desempenho da dimensão, indicando que a maioria das unidades federativas já iniciou processos de promoção de mentalidade orientada à qualidade dos dados. Contudo, o desvio padrão de 1,36 e a amplitude interquartil de 2,0 (Q1 = 2,0; Q3 = 4,0) revelam heterogeneidade significativa, com 25% das unidades federativas ainda em estágios iniciais (Q1 = 2,0) e 25% já em estágios avançados (Q3 = 4,0). Esta dispersão reflete diferenças na capacidade de promover mudanças culturais e no compromisso da liderança com a qualidade dos dados.

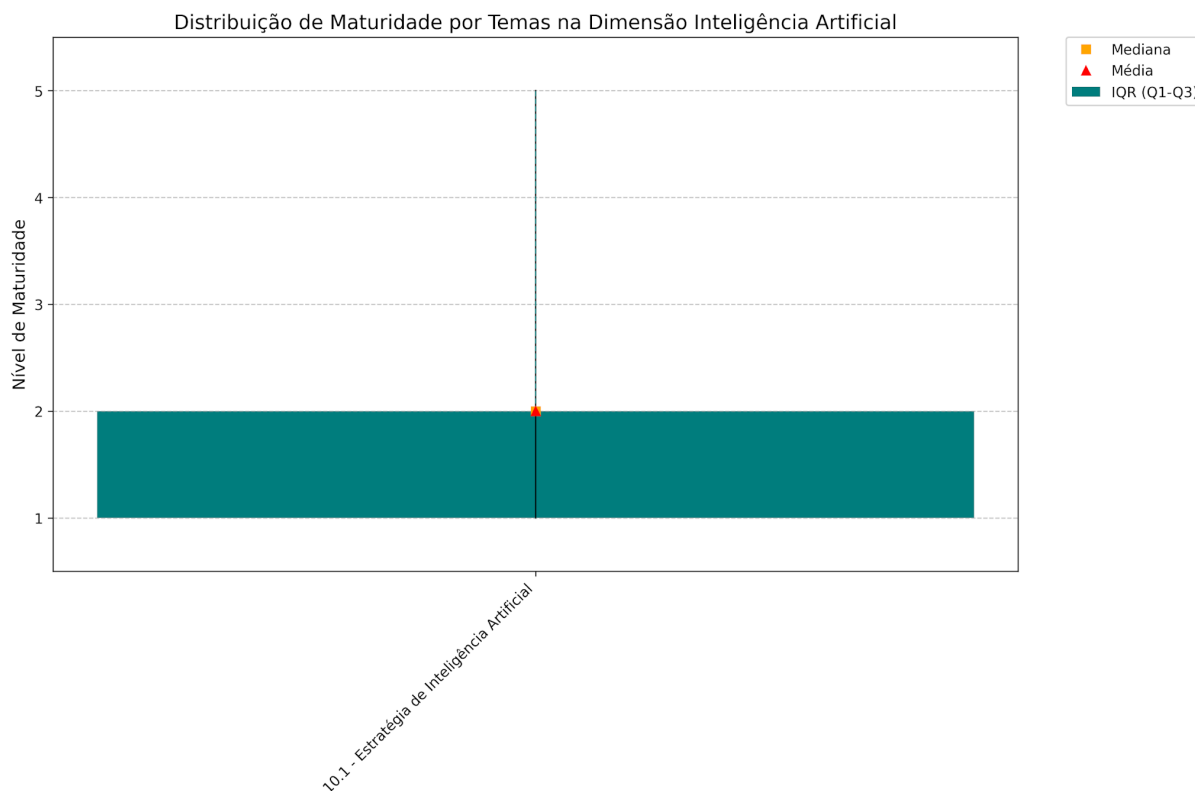
A Gestão de Qualidade de Dados, com média de 2,92 e mediana de 3,0, apresenta desempenho ligeiramente inferior, indicando que a maioria das unidades federativas ainda não consolidou abordagens governadas para planejar, implementar e controlar atividades de qualidade de dados. O desvio padrão de 1,38 e a amplitude interquartil de 1,75 (Q1 = 2,0; Q3 = 3,75) evidenciam heterogeneidade similar à observada em Cultura de Qualidade de Dados.

A Medição e Controle da Qualidade de Dados, com média de 2,5 e mediana de 2,0, configura-se como o principal gargalo da dimensão e um dos temas de menor maturidade em todo o diagnóstico nacional. O desvio padrão de 1,21 e a amplitude interquartil de 1,75 (Q1 = 2,0; Q3 = 3,75) indicam que a maioria das unidades federativas ainda não implementou processos sistemáticos de aferição e monitoramento da qualidade dos dados. Esta lacuna compromete a capacidade de identificar problemas de qualidade, priorizar investimentos em melhorias e avaliar a efetividade de intervenções.

4.4.10 Inteligência Artificial

A dimensão Inteligência Artificial apresenta o desempenho mais crítico entre todas as dimensões avaliadas, com média de 2,0 e mediana de 2,0, posicionando-se no Nível 2 (Iniciado) do MMD. Esta dimensão compreende um único tema: Estratégia de Inteligência Artificial, que apresenta os mesmos indicadores da dimensão. O desvio padrão de 1,06 e a amplitude interquartil de 1,0 (Q1 = 1,0; Q3 = 2,0) revelam que a maioria das unidades federativas ainda se encontra em estágios iniciais de adoção de IA, com 75% das unidades federativas (Q3 = 2,0) não ultrapassando o Nível 2.

Gráfico 14 - Maturidade na Dimensão Inteligência Artificial



Fonte: Elaboração própria

Este resultado indica que a integração de Inteligência Artificial aos processos de segurança pública permanece como um desafio crítico e generalizado, não se tratando de assimetria federativa, mas de limitação nacional. A mediana de 2,0 e Q3 de 2,0 evidenciam que a maioria das unidades federativas ainda não desenvolveu estratégias estruturadas para uso de IA, limitando-se a iniciativas pontuais e experimentais, sem integração aos processos centrais da organização.

A presença de unidades federativas no Nível 5 (máximo = 5) demonstra que a excelência em IA para segurança pública é tecnicamente viável no contexto brasileiro. Contudo, a concentração de 75% das unidades federativas nos Níveis 1 e 2 indica que a difusão de práticas avançadas de IA permanece extremamente limitada, refletindo barreiras significativas de capacidade técnica, recursos, e compreensão dos potenciais e riscos da IA.

4.4.11 Ranking global dos temas

A maturidade por temas está concentrada nos níveis intermédios (2 e 3), com uma dispersão significativa que revela pontos fortes e lacunas nas diferentes áreas e estados.

Tabela 4 - Níveis Médios de Maturidade por tema

Tema	Dimensão	Nível Médio
Tomada de Decisão Baseada em Dados	Análise de Dados	3,73
Gestão Orientada a Dados	Dados como Ativo Estratégico	3,62
Dados como Pilar para Entregas à Sociedade	Dados como Ativo Estratégico	3,62
Alinhamento com Objetivos Estratégicos	Dados como Ativo Estratégico	3,58
Promoção da Cultura de Dados pela Alta Gestão	Governança de Dados	3,50
Infraestrutura e Ferramentas para Análise de Dados	Análise de Dados	3,38
Relevância e Suficiência dos Dados	Análise de Dados	3,38
Desenvolvimento da Capacidade Analítica	Análise de Dados	3,31
Letramento em Dados	Governança de Dados	3,27
Estrutura Organizacional para Governança de Dados	Governança de Dados	3,12
Princípios e Políticas de Dados	Governança de Dados	3,12
Ciclo de Vida dos Dados	Gerenciamento de Dados	3,08
Modelagem de Dados	Conhecimento sobre os Dados	3,04
Dados não Estruturados	Gerenciamento de Dados	3,04
Integração de Sistemas	Interoperabilidade de Dados	3,04
Cultura de Qualidade de Dados	Qualidade de Dados	3,00
Documentação dos Ativos de Dados	Conhecimento sobre os Dados	2,92
Gerenciamento de Dados Mestres e Dados de Referência	Gerenciamento de Dados	2,92
Compartilhamento de Dados com Atores Externos	Interoperabilidade de Dados	2,92
Gestão de Qualidade de Dados	Qualidade de Dados	2,92
Gestão de Metadados	Conhecimento sobre os Dados	2,88
Ecosistema de Dados Abertos	Dados Abertos	2,85
Implementação da Política de Dados Abertos	Dados Abertos	2,77
Padrões e Normas para Interoperabilidade	Interoperabilidade de Dados	2,73
Ética no Tratamento de Dados	Ética de Dados	2,69

Gerenciamento de Dados Geoespaciais	Gerenciamento de Dados	2,62
Medição e Controle da Qualidade de Dados	Qualidade de Dados	2,50
Glossário de Termos de Negócio	Conhecimento sobre os Dados	2,38
Estratégia de Inteligência Artificial	Inteligência Artificial	2,00
Monitoramento e Avaliação da Interoperabilidade	Interoperabilidade de Dados	1,96

Fonte: Elaboração própria

É possível notar que as maiores médias de maturidade estão concentradas em temas que envolvem o uso estratégico da informação para a gestão. O destaque principal é o tema "Tomada de Decisão Baseada em Dados", que lidera com uma média de 3,73. Logo em seguida, temas como "Dados como Pilar para Entregas à Sociedade" e "Gestão Orientada a Dados" aparecem com médias de 3,62, o que indica que as organizações analisadas caminham para o nível Desenvolvido no que diz respeito à percepção do valor dos dados para o negócio e para a sociedade.

Em contrapartida, as menores médias revelam áreas que ainda estão em estágios iniciais de desenvolvimento ou enfrentam barreiras técnicas e normativas. O índice mais baixo é observado em "Monitoramento e Avaliação da Interoperabilidade", com apenas 1,96, seguido por "Estratégia de Inteligência Artificial", com média de 2,00. Esses números sugerem que, embora se saiba da importância de usar dados, a capacidade de monitorar como essas informações transitam entre sistemas e a criação de uma estratégia formal para tecnologias emergentes, como a IA, ainda são desafios críticos.

De forma geral, a disparidade entre a maior média (3,73) e a menor (1,96) evidencia um desequilíbrio entre a cultura de dados e a infraestrutura técnica. Enquanto temas ligados à Governança e Ativos Estratégicos tendem a apresentar melhores resultados, tópicos de execução mais detalhada, como o "Glossário de Termos de Negócio" (2,38) e o "Gerenciamento de Dados Geoespaciais" (2,61), figuram na parte inferior da lista. Esse cenário ressalta que o fortalecimento técnico e a padronização de conceitos são passos necessários para que a maturidade em dados alcance níveis mais homogêneos em todas as dimensões avaliadas.

4.5 Identificação de gaps críticos

Para identificar as áreas que demandam intervenção mais urgente na gestão de dados das Secretarias de Segurança Pública, foi elaborado um Índice de Criticidade. Este indicador composto permite uma análise multidimensional, integrando a distância em relação ao estado de excelência e o grau de heterogeneidade na implementação dos processos. O índice é calculado pela seguinte equação:

$$(5 - \bar{x}) \cdot (\sigma + 1)$$

Onde:

- 5 representa o valor máximo da escala de maturidade (Nível 5 - Otimizado);
- \bar{x} corresponde à média aritmética dos níveis de maturidade observados no tema;
- σ representa o desvio padrão dos níveis reportados pelas unidades federativas.

O déficit de maturidade $(5 - \bar{x})$ mensura a distância linear entre a realidade observada e a maturidade máxima definida pelo referencial teórico do Modelo de Maturidade de Dados. Em termos analíticos, quanto menor a média aritmética de um determinado tema, maior será a magnitude desse hiato, evidenciando carências sistêmicas que limitam a capacidade estatal de gestão orientada a dados.

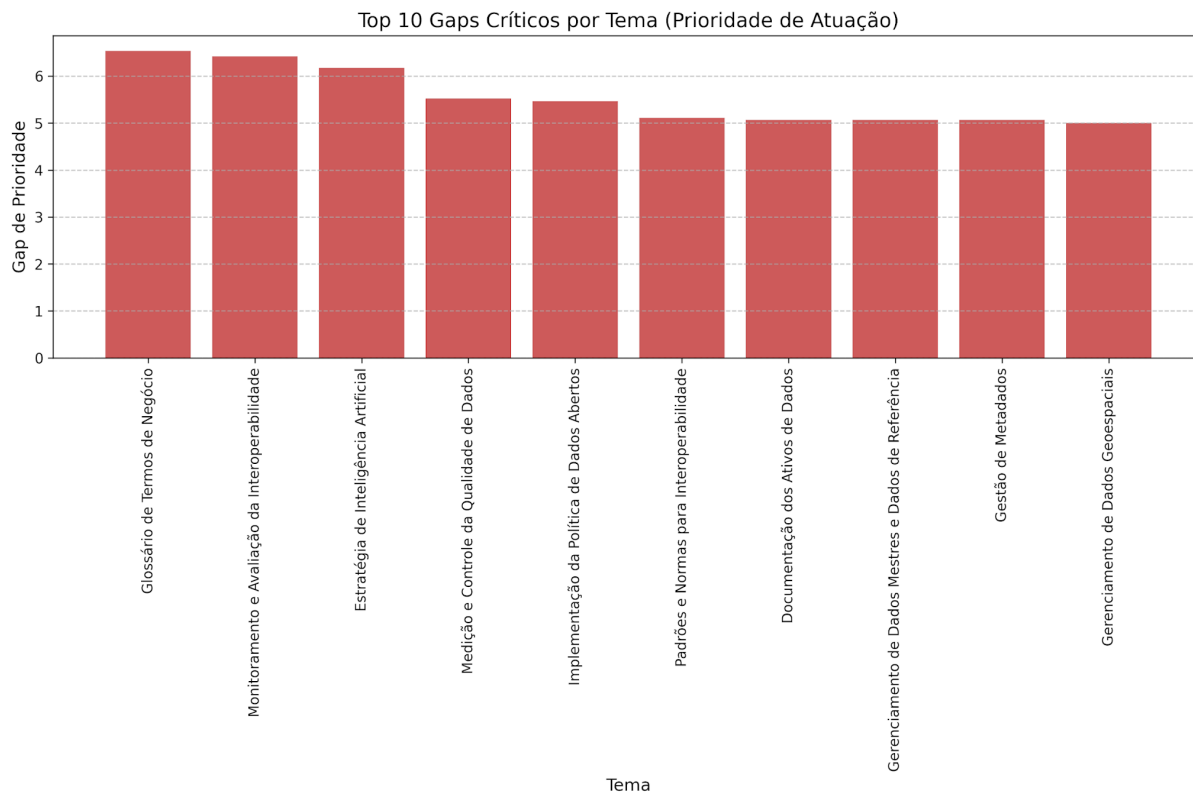
Já o fator de ponderação por heterogeneidade $(\sigma + 1)$ atua como um mecanismo de penalização para domínios que apresentam elevada dispersão estatística. Um alto desvio padrão (σ) sinaliza que a implementação dos processos é fragmentada ou carece de padronização nacional, o que denota incerteza institucional e assimetrias técnicas profundas entre as unidades federativas. O incremento de uma unidade na equação desempenha função de estabilização ao assegurar que temas com dispersão nula (que indicam uma uniformidade entre os entes) mantenham seu peso relativo, enquanto atua como um multiplicador de prioridade em áreas onde o dissenso técnico e a desarticulação federativa são mais agudos.

A adoção deste índice justifica-se pela premissa de que a média aritmética, isoladamente, possui limitações para diagnosticar gargalos estruturais, uma vez que pode

mascarar desigualdades regionais por meio de um efeito de compensação. Ao priorizar domínios com elevado Índice de Criticidade, a análise direciona o foco para os pontos de inércia institucional, onde os níveis de maturidade são simultaneamente exíguos e inconsistentes. Dessa forma, permite-se que as recomendações estratégicas deste trabalho incidam sobre os temas com maior potencial de promover uma evolução convergente das Secretarias de Segurança Pública a fim de mitigar o risco de consolidação de "ilhas de eficiência" isoladas em um cenário nacional marcado pela fragmentação informacional.

Ademais, a sensibilidade do índice à dispersão estatística oferece uma vantagem pragmática na gestão do conhecimento federativo, pois temas com alto índice frequentemente revelam a coexistência de estados em situação precária com unidades que já atingiram patamares de excelência. Essa dualidade facilita a identificação de *benchmarks* internos, permitindo que o Ministério da Justiça e as próprias SSPs utilizem paradigmas institucionais preexistentes para acelerar a curva de implementação em estados retardatários, o que não apenas valida o esforço das unidades de referência, mas também reduz os custos de transação e o tempo de maturação das políticas, visto que as soluções já foram testadas e adaptadas às especificidades do arcabouço jurídico e operacional brasileiro.

Os resultados indicam que os principais gaps estruturais concentram-se em temas relacionados a Glossário de Termos de Negócio, Monitoramento e Avaliação de Interoperabilidade, Estratégia de Inteligência Artificial e Medição e Controle de Qualidade de Dados.

Gráfico 15 - 10 maiores Gaps Críticos

Fonte: Elaboração própria

Tabela 5 - Índices de Criticidade

DIMENSÃO	TEMA	Índice de Criticidade
Conhecimento sobre os Dados	Glossário de Termos de Negócio	6,54
Interoperabilidade de Dados	Monitoramento e Avaliação da Interoperabilidade	6,42
Inteligência Artificial	Estratégia de Inteligência Artificial	6,17
Qualidade de Dados	Medição e Controle da Qualidade de Dados	5,52
Dados Abertos	Implementação da Política de Dados Abertos	5,47
Interoperabilidade de Dados	Padrões e Normas para Interoperabilidade	5,11
Conhecimento sobre os Dados	Documentação dos Ativos de Dados	5,07
Gerenciamento de Dados	Gerenciamento de Dados Mestres e Dados de Referência	5,07
Conhecimento sobre os Dados	Gestão de Metadados	5,07
Gerenciamento de Dados	Gerenciamento de Dados Geoespaciais	5,00
Qualidade de Dados	Gestão de Qualidade de Dados	4,95
Dados Abertos	Ecosistema de Dados Abertos	4,72

Qualidade de Dados	Cultura de Qualidade de Dados	4,71
Conhecimento sobre os Dados	Modelagem de Dados	4,65
Interoperabilidade de Dados	Compartilhamento de Dados com Atores Externos	4,49
Gerenciamento de Dados	Ciclo de Vida dos Dados	4,47
Interoperabilidade de Dados	Integração de Sistemas	4,41
Gerenciamento de Dados	Dados não Estruturados	4,41
Ética de Dados	Ética no Tratamento de Dados	4,35
Governança de Dados	Princípios e Políticas de Dados	4,23
Governança de Dados	Estrutura Organizacional para Governança de Dados	4,04
Análise de Dados	Relevância e Suficiência dos Dados	3,81
Governança de Dados	Letramento em Dados	3,66
Análise de Dados	Infraestrutura e Ferramentas para Análise de Dados	3,20
Governança de Dados	Promoção da Cultura de Dados pela Alta Gestão	3,16
Dados como Ativo Estratégico	Alinhamento com Objetivos Estratégicos	3,09
Análise de Dados	Desenvolvimento da Capacidade Analítica	3,03
Dados como Ativo Estratégico	Gestão Orientada a Dados	2,75
Dados como Ativo Estratégico	Dados como Pilar para Entregas à Sociedade	2,69
Análise de Dados	Tomada de Decisão Baseada em Dados	2,59

Fonte: Elaboração própria

A fragmentação semântica, evidenciada pela ausência de um Glossário de Termos de Negócio, constitui o principal ponto crítico na infraestrutura informacional das Secretarias de Segurança Pública. Essa lacuna impede uma governança de dados eficaz e a comunicação ubíqua, pois conceitos cruciais são interpretados de maneiras diversas entre estados e departamentos, resultando em dados que não se interconectam. Para superar esse desafio, é fundamental, conforme o Banco Mundial (2022), transitar de uma abordagem baseada em silos para uma de governo integral. Em vez de cada entidade governamental atuar isoladamente em prol de objetivos específicos, os departamentos, em diferentes níveis de governo, setores e fronteiras, devem colaborar para atingir metas conjuntas.

Essa inconsistência compromete a integridade da análise nacional, uma vez que a integração de sistemas (Tema 7.2) torna-se meramente mecânica, sem garantir a equivalência conceitual necessária para a produção de inteligência estatística fidedigna. Tal fato se comunica como segundo maior gap identificado, qual seja no tema Monitoramento e a Avaliação Contínua da Interoperabilidade (Tema 7.3), o que acaba colaborando para que o

Estado brasileiro seja incipiente na identificação de gargalos de fluxo, perpetuando silos informacionais que dificultam a identificação de padrões criminais transfronteiriços.

Essa precariedade na maturidade de dados colide diretamente com o arcabouço normativo do Sistema Único de Segurança Pública (SUSP), instituído pela Lei nº 13.675/2018, e que coloca o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP), com a finalidade de armazenar, tratar e integrar dados e informações para auxiliar na formulação, implementação, execução, acompanhamento e avaliação das políticas relacionadas à segurança pública (Brasil, 2018).

O SINESP apresenta-se como o pilar institucional e tecnológico fundamental para a superação das assimetrias federativas e a consolidação de uma governança de dados robusta. Instituído como ferramenta central da Política Nacional de Segurança Pública e Defesa Social (PNSPDS), o SINESP atua como o eixo integrador que permite a convergência de registros dispersos em uma plataforma unificada, viabilizando consultas operacionais, investigativas e estratégicas em colaboração direta com os entes federados.

A eficácia do sistema reside na oferta de soluções estruturantes que padronizam o fluxo informacional em todo o território nacional. Destaca-se o SINESP PPE (Procedimentos Policiais Eletrônicos), que atua na gênese do dado ao uniformizar o registro de ocorrências e a gestão de procedimentos, combatendo as ambiguidades semânticas e a falta de critérios comuns entre os estados. Complementarmente, o SINESP CAD (Central de Atendimento e Despacho) integra o ciclo de atendimento de emergência e o despacho de viaturas, otimizando o tempo de resposta e garantindo que a gestão operacional seja orientada por evidências em tempo real.

Além do suporte à atividade policial ostensiva e judiciária, o ecossistema do SINESP promove a interoperabilidade por meio do SINESP Infoseg, que interliga bases de dados de justiça, fiscalização e segurança, e estende o controle social através do SINESP Cidadão. Esta última ferramenta permite que a sociedade participe ativamente da segurança pública ao acessar informações sobre veículos roubados e mandados de prisão.

A legislação federal não apenas faculta, mas obriga a padronização e categorização de dados e informações (Art. 37, §1º da Lei 13.675), estabelecendo que o intercâmbio de informações entre os integrantes do SUSP deve ocorrer de forma integrada e

segura. Portanto, a evolução da maturidade nos temas de glossário e interoperabilidade não deve ser encarada como uma meta tecnológica acessória, mas como o requisito básico para o cumprimento do pacto federativo previsto em lei.

5 CONSIDERAÇÕES FINAIS

O diagnóstico nacional da governança de dados na segurança pública brasileira, conduzido à luz do Modelo de Maturidade de Dados, valida a hipótese central desta pesquisa de que a maturidade de dados no setor de segurança pública é marcadamente heterogênea e reflete assimetrias federativas. A análise de 30 temas distribuídos em 10 dimensões, abrangendo 26 unidades federativas, revelou uma maturidade média nacional 3,00 e mediana 2,87, posicionando o setor no limiar entre os níveis "Emergente" (Nível 3) e "Desenvolvido" (Nível 4) do MMD. Este resultado, embora sugira avanços em relação à ausência total de iniciativas estruturadas, expõe fragilidades críticas na consolidação de práticas sistemáticas e sustentáveis de governança de dados.

A heterogeneidade observada manifesta-se de forma contundente nos indicadores de dispersão: o desvio padrão médio de 1,20 e a IQR médio de 1,67 revelam que a capacidade estatal para gestão de dados na segurança pública não se distribui uniformemente no território nacional. Notavelmente, 93,3% dos temas atingiram o nível máximo de maturidade em pelo menos uma unidade federativa, demonstrando que a excelência técnica é viável no contexto brasileiro, mas permanece geograficamente concentrada. Esta constatação reforça a tese de que as disparidades observadas decorrem menos de limitações técnicas intrínsecas e mais de assimetrias na capacidade institucional, recursos disponíveis, continuidade de processos de gestão e priorização política.

A assimetria federativa revela-se particularmente crítica nos temas identificados pelo Índice de Prioridade de Gaps como gargalos estruturais: Estratégia de Inteligência Artificial (média = 2,0; IPG = 3,17), Monitoramento e Avaliação da Interoperabilidade (média = 1,96; IPG = 3,38), Glossário de Termos de Negócio (média = 2,38; IPG = 3,92), Medição e Controle da Qualidade de Dados (média = 2,5; IPG = 3,02), Gerenciamento de Dados Geoespaciais (média = 2,62; IPG = 2,62), Ética no Tratamento de Dados (média = 2,69; IPG = 2,04), Padrões e Normas para Interoperabilidade (média = 2,73; IPG = 2,84) e Implementação da Política de Dados Abertos (média = 2,77; IPG = 3,24). Estes

temas representam os principais obstáculos à consolidação de uma governança de dados robusta e federativamente equitativa, demandando intervenções prioritárias e coordenadas.

A análise dimensional evidencia que, embora a dimensão Análise de Dados apresente desempenho relativamente robusto (média = 3,45), com destaque para o tema Tomada de Decisão Baseada em Dados (média = 3,73), as dimensões estruturantes da governança permanecem fragilizadas. A dimensão Interoperabilidade de Dados, com média de 2,66, revela a persistência de sistemas fragmentados e a ausência de arquiteturas integradas de compartilhamento de dados. A dimensão Qualidade de Dados, com média de 2,81, expõe a fragilidade dos mecanismos de medição, controle e garantia de qualidade, comprometendo a confiabilidade dos dados utilizados para formulação de políticas. A dimensão Conhecimento sobre os Dados, com média de 2,75, indica deficiências críticas na documentação, catalogação e gestão de metadados, dificultando a descoberta, compreensão e uso efetivo dos ativos de dados.

Embora a estratégia metodológica adotada seja eminentemente descritiva, os padrões identificados são coerentes com algumas hipóteses causais plausíveis sobre a capacidade estatal em segurança pública. A combinação de alta maturidade em Dados como Ativo Estratégico e Análise de Dados, associada a níveis ainda intermediários em Governança de Dados, sugere que avanços na institucionalização da governança e na cultura orientada a dados tendem a se traduzir em decisões mais informadas, planejamento mais preciso e maior capacidade de monitorar resultados. Em sentido inverso, a concentração dos menores níveis e dos maiores índices de criticidade em temas como Glossário de Termos de Negócio, Monitoramento e Avaliação da Interoperabilidade e Medição e Controle da Qualidade de Dados indica que deficiências semânticas e técnicas na infraestrutura informacional atuam como gargalos estruturais que limitam a capacidade de o Estado coordenar políticas federativas e produzir evidências comparáveis em escala nacional.

Os resultados apresentados ao longo deste trabalho sugerem que a maturidade de dados nas Secretarias Estaduais de Segurança Pública não é um fenômeno aleatório, mas possivelmente resultado de combinações específicas de capacidades fiscais, administrativas, tecnológicas e institucionais. A heterogeneidade observada entre unidades federativas, bem como a presença de “ilhas de excelência” em praticamente todos os temas do MMD, é compatível com a hipótese de que estados com maior capacidade de investimento, maior

maturidade em governo digital e estruturas organizacionais mais estáveis em segurança pública tendem a apresentar níveis mais elevados de governança de dados.

Do ponto de vista causal, a literatura e os achados empíricos convergem para um encadeamento no qual a institucionalização de estruturas formais de governança de dados, o fortalecimento da cultura orientada a dados e a existência de equipes técnicas especializadas aumentam a probabilidade de que decisões estratégicas sejam baseadas em evidências. Isso, por sua vez, tende a melhorar o planejamento, a alocação de recursos e o monitoramento de políticas, retroalimentando a percepção de valor dos dados e, potencialmente, atraindo novos investimentos em infraestrutura informacional. Em contraste, a persistência de baixos níveis em temas como glossários de negócio, interoperabilidade e qualidade de dados sugere um círculo vicioso em que a ausência de padrões semânticos e de monitoramento técnico impede a construção de indicadores comparáveis e dificulta a coordenação federativa por meio do SUSP e do SINESP.

Destaca-se contudo, que tais inferências devem ser lidas como hipóteses causais consistentes com a literatura e com o desenho do MMD, e não como relações causais identificadas no sentido estrito, dado que o presente estudo não incorporou variáveis explicativas externas nem técnicas de inferência causal dedicadas.

Investigações futuras poderiam testar essas hipóteses de maneira mais rigorosa, incorporando variáveis explicativas como gasto em segurança pública per capita, esforço fiscal próprio, quadro de pessoal técnico, indicadores de governo digital e de violência, bem como medidas de pressão por transparência e *accountability*. A combinação entre o MMD e esses indicadores permitiria estimar, por exemplo, em que medida diferenças de capacidade fiscal ou de maturidade digital explicam as variações de maturidade de dados entre estados, contribuindo para uma compreensão mais fina dos condicionantes estruturais da governança de dados na segurança pública brasileira.

A maturidade de dados constitui um determinante crítico da capacidade estatal para formulação, implementação e avaliação de políticas públicas baseadas em evidências. Os achados desta pesquisa revelam que a heterogeneidade e as assimetrias federativas na governança de dados comprometem a capacidade estatal brasileira no planejamento estratégico e alocação de recursos, monitoramento de políticas e produção de evidências, e integração federativa.

A capacidade de planejar estrategicamente e alocar recursos de forma eficiente depende fundamentalmente da disponibilidade de dados confiáveis, tempestivos e relevantes sobre a realidade da segurança pública. A baixa maturidade nos temas Relevância e Suficiência dos Dados (média = 3,38) e Medição e Controle da Qualidade de Dados (média = 2,5) indica que muitas unidades federativas carecem de informações adequadas para diagnóstico preciso de problemas, identificação de prioridades e dimensionamento de necessidades.

A deficiência de dados geoespaciais estruturados (média = 2,62) dificulta a análise espacial da criminalidade, a identificação de *hotspots* e a alocação territorial de recursos. A fragilidade na gestão de dados mestres e dados de referência (média = 2,92) compromete a integração de informações de múltiplas fontes, impedindo análises holísticas que considerem simultaneamente aspectos criminais, socioeconômicos, demográficos e de infraestrutura. A insuficiência de capacidade analítica (média = 3,31) limita a sofisticação das análises realizadas, restringindo-as a estatísticas descritivas básicas e impedindo o uso de técnicas avançadas de modelagem preditiva, análise de redes criminais e avaliação de impacto de políticas.

Nesse sentido, a baixa maturidade em Relevância e Suficiência dos Dados e em Medição e Controle da Qualidade de Dados indica não apenas um problema técnico, mas um fator que tende a produzir diagnósticos imprecisos e, portanto, planos mal calibrados em relação às necessidades reais dos territórios.

A capacidade de monitorar a implementação de políticas, avaliar seus resultados e produzir evidências sobre sua efetividade depende da existência de sistemas de informação integrados, indicadores padronizados e processos robustos de medição. A baixa maturidade nos temas Monitoramento e Avaliação da Interoperabilidade (média = 1,96) e Implementação da Política de Dados Abertos (média = 2,77) revela fragilidades críticas nesta dimensão da capacidade estatal.

A fragilidade em indicadores padronizados e comparáveis entre unidades federativas impede a avaliação rigorosa da efetividade de políticas nacionais. Além disso, a fragilidade dos mecanismos de monitoramento dificulta a identificação tempestiva de desvios de implementação, a correção de rumos e a responsabilização de gestores.

A baixa maturidade em transparência ativa e dados abertos (média = 2,77) compromete o controle social e a *accountability* democrática. A ausência de dados públicos estruturados, acessíveis e compreensíveis impede que pesquisadores, organizações da sociedade civil, jornalistas e cidadãos realizem análises independentes, identifiquem problemas e proponham soluções. Wimmer et al. (2020) enfatiza que confiança e transparência são elementos chave para uma transformação pública orientada a dados.

A produção de evidências robustas demanda, adicionalmente, capacidade analítica avançada e infraestrutura adequada. A maturidade relativamente alta em Infraestrutura e Ferramentas para Análise de Dados (média = 3,38) sugere que muitas unidades federativas já dispõem de recursos tecnológicos básicos. Contudo, a baixa maturidade em Estratégia de Inteligência Artificial (média = 2,0) indica que o potencial de técnicas avançadas de análise (aprendizado de máquina, processamento de linguagem natural, análise preditiva etc.) permanece pouco explorado. A incorporação destas técnicas, quando fundamentada em princípios éticos robustos, pode ampliar significativamente a capacidade estatal de antecipar problemas, identificar padrões ocultos e otimizar a alocação de recursos.

A integração federativa constitui o desafio mais complexo e politicamente sensível da governança de dados na segurança pública brasileira. O Sistema Único de Segurança Pública, instituído pela Lei nº 13.675/2018, estabelece como princípios a integração, a interoperabilidade das redes de dados e o compartilhamento de informações (Brasil, 2018). Além disso, a referida norma prevê a coordenação dos órgãos de segurança pública para a promoção da governança, visando a eficácia das atividades de prevenção e controle de infrações penais (Brasil, 2018).

O dilema do SUSP reside na tensão entre a necessidade de padronização nacional e a preservação da autonomia definida pelo pacto federativo. Estados com maior capacidade institucional e sistemas de informação mais desenvolvidos tendem a resistir à adoção de padrões nacionais que possam representar retrocessos em relação a suas práticas atuais. Estados com menor capacidade carecem de recursos técnicos e financeiros para implementar padrões nacionais sem apoio substancial da União. Esta dinâmica gera um impasse que reforça a fragmentação e as assimetrias.

Denford et al. (2020) identifica que modelos puramente centralizados ou puramente descentralizados variam consideravelmente a depender do tipo de organização.

Modelos centralizados geram resistência política e desconsideram especificidades locais; modelos descentralizados perpetuam fragmentação e inviabilizam integração. O modelo federal de governança de TI, que combina elementos centralizados (padrões, políticas, arquitetura) com elementos descentralizados (implementação, operação, adaptação local), emerge como alternativa mais adequada.

A implementação de um modelo federal de governança de dados no SUSP demanda a criação de estruturas de governança compartilhada, que incluam representantes da União, dos estados e de organizações técnicas especializadas, conforme preconiza o art. 24, IX da Lei nº 13.675/2018. Estas estruturas devem ser responsáveis pelo desenvolvimento e manutenção de padrões técnicos e semânticos, pela definição de políticas de qualidade de dados e segurança da informação, pelo estabelecimento de protocolos de interoperabilidade, pelo monitoramento da implementação e avaliação de resultados, pela mediação de conflitos e construção de consensos, e pela promoção de capacitação e compartilhamento de boas práticas (Veldi, 2025).

Nesse cenário, o SUSP e o SINESP constituem pilares institucionais fundamentais para a superação das assimetrias federativas e a consolidação de uma governança de dados robusta na segurança pública brasileira. Contudo, os achados desta pesquisa revelam que a ausência de padrões técnicos e semânticos comuns, a fragilidade dos mecanismos de interoperabilidade e a insuficiência de arquiteturas integradas de compartilhamento de dados comprometem severamente a capacidade destes sistemas de cumprirem seus objetivos estratégicos.

A ausência de padronização normativa inviabiliza o *benchmarking* nacional, impedindo a comparação rigorosa entre estados e a replicação de boas práticas. Esse cenário é agravado por irregularidades semânticas, refletidas na baixa maturidade do Glossário de Termos de Negócio (média = 2,38), que compromete a integridade dos dados. Como as unidades federativas adotam critérios heterogêneos para classificar crimes e mensurar indicadores, a consolidação de estatísticas nacionais torna-se precária, dificultando uma visão sistêmica e confiável da criminalidade no país.

O SINESP, concebido como repositório nacional de dados de segurança pública, enfrenta desafios estruturais que limitam sua efetividade. A baixa maturidade dos temas Padrões e Normas para Interoperabilidade (média = 2,73) e Monitoramento e Avaliação

da Interoperabilidade (média = 1,96) indica que o SINESP opera, em grande medida, como um agregador de dados heterogêneos, sem capacidade efetiva de garantir qualidade, consistência e comparabilidade. A ausência de mecanismos robustos de validação, a fragilidade dos processos de medição e controle de qualidade (média = 2,5) e a insuficiência de metadados estruturados (média = 2,88) comprometem a confiabilidade dos dados armazenados, perpetuando dados de baixa qualidade que geram análises imprecisas, que por sua vez fundamentam políticas inefetivas.

Costa (2022) destacou a relevância do SINESP como principal meio, instrumento, fonte e banco de dados a ser utilizado na elaboração de diagnóstico dentro da estratégia de formulação dos Planos Estaduais de Segurança Pública e Defesa Social

Em seu trabalho, Nunes (2025) defende uma governança multinível para o SUSP, “uma espécie de sistema complexo, menos hierarquizado, que articula e é articulado mediante redes de agentes díspares que se integram de forma colaborativa, coesa e transparente para identificar problemas, construir soluções e tomar decisões coletivas mais acertadas e em prol do bem comum”.

A consolidação do SUSP e do SINESP como instrumentos efetivos de governança de dados demanda, portanto, uma transformação estrutural que transcenda a mera agregação de dados. É necessário estabelecer uma arquitetura de interoperabilidade semântica, fundamentada em padrões comuns, processos de qualidade robustos e mecanismos de governança compartilhada, que permita a produção de evidências confiáveis para formulação, monitoramento e avaliação de políticas nacionais de segurança pública.

Nesse sentido, cabe ao SINESP assumir um protagonismo indutor por meio do desenvolvimento centralizado de ativos informacionais críticos, como glossários unificados e protocolos de interoperabilidade técnica. Ao internalizar o esforço de padronização conceitual e metodológica, a União gera um ganho de escala que beneficia todas as Unidades Federativas, mitigando as assimetrias tecnológicas regionais. Esse movimento não apenas otimiza recursos, mas atua como um catalisador de excelência, elevando o nível de maturidade institucional das UFs e abre caminho para que o fluxo de dados da segurança pública nacional seja interpretado sob uma lógica comum e tecnicamente coesa.

Diante do diagnóstico apresentado, que evidenciou assimetrias federativas profundas e lacunas técnicas em temas fundacionais, com destaque para a precariedade nos

glossários de negócio e na gestão de metadados, esta pesquisa sinaliza que a evolução da segurança pública brasileira não depende apenas de incrementos tecnológicos isolados, mas de uma reconfiguração estrutural de sua governança informacional. Os dados demonstraram que, embora existam ilhas de excelência operando no patamar otimizado de maturidade, a fragmentação sistêmica e a baixa interoperabilidade, situadas majoritariamente nos níveis iniciais, operam como barreiras intransponíveis para a plena execução das políticas baseadas em evidências previstas no SUSP.

Nesse contexto, os desdobramentos futuros desta investigação devem transcender o diagnóstico descritivo para focar na proposição e na avaliação de uma Infraestrutura Nacional de Dados para a Segurança Pública. Diferente de um repositório centralizado de informações, a Infraestrutura deve ser concebida como um ecossistema federativo e multinível de padrões, normas e tecnologias que habilite a descoberta, o acesso e o uso estratégico de dados criminais de forma soberana e integrada. Sob a ótica da economia da informação, tal infraestrutura atuaria na redução drástica dos custos de transação entre os entes federados e o Governo Federal, mitigando falhas de mercado associadas à subprodução de dados fidedignos e à assimetria informacional que, na configuração atual, beneficia a criminalidade transfronteiriça em detrimento da capacidade de resposta estatal.

Para operacionalizar essa transição, recomenda-se que a SENASP institua Grupos de Trabalho técnicos focados especificamente nos domínios que apresentaram os maiores IPGs. A composição desses grupos deve ser orientada pelo aproveitamento das competências estatais já consolidadas, integrando representantes das Secretarias Estaduais mais bem avaliadas em cada tema específico. Dessa forma, colocando os estados que atingiram os maiores níveis de maturidade como indutores e consultores dos demais entes, o MJSP possibilita a validação de boas práticas regionais, acelera a curva de implementação nacional e transforma o conhecimento de vanguarda em um bem público compartilhado por toda a federação.

Adicionalmente, urge propor mecanismos de incentivos fiscais e orçamentários, vinculados ao Fundo Nacional de Segurança Pública, que condicionem o repasse de recursos à conformidade com padrões de maturidade e abertura de dados. Por essa integração sistêmica e colaborativa, abre-se via para garantir que a informação custodiada pelo Estado cumpra sua função social de promover proteção, justiça e desenvolvimento para a sociedade brasileira.

necessários para que o uso estratégico dos dados alcance sua plena maturidade no setor de segurança pública.

A ausência do estado do Rio de Janeiro a amostra, embora represente uma lacuna no mapeamento da maturidade em nível nacional, oferece uma oportunidade singular para estudos de caso futuros. A realização do MMD na Secretaria de Segurança Pública do RJ é altamente recomendada, pois permitiria uma análise mais completa da diversidade federativa brasileira, especialmente considerando a complexidade e o volume de dados de segurança pública gerados em um dos estados mais populosos e com desafios urbanos notórios.

Para pesquisas futuras, recomenda-se a expansão desta investigação sob diferentes perspectivas. Primeiramente, a aplicação do MMD em instituições específicas do ecossistema de segurança pública — como as Polícias Militar, Civil e Científica, além do Corpo de Bombeiros — viabilizaria uma análise granular da maturidade setorial. Adicionalmente, propõe-se a realização de estudos longitudinais, com aplicações bienais, para monitorar a evolução do gerenciamento de dados e aferir a eficácia dos investimentos realizados. Por fim, abordagens qualitativas, fundamentadas em estudos de caso, permitiriam investigar as variáveis subjetivas e contextuais (como cultura organizacional, liderança e limitações orçamentárias) que influenciam os níveis de maturidade em dimensões críticas, notadamente em Interoperabilidade, Ética de Dados e Inteligência Artificial.

REFERÊNCIAS

- AFZAL, M. et al. **Data in policing: an integrative review**. International Journal of Public Administration, v. 47, 2024. DOI: <https://doi.org/10.1080/01900692.2024.2360586>.
- AFZAL, M.; PANAGIOTOPOULOS, P. **Smart policing: a critical review of the literature**. In: INTERNATIONAL CONFERENCE ON ELECTRONIC GOVERNMENT, 2020. Anais [...] Cham: Springer, 2020. DOI: https://doi.org/10.1007/978-3-030-57599-1_5.
- ARANGO, J. et al. **An analysis and visualization of best practices for police data transparency**. In: SYSTEMS AND INFORMATION ENGINEERING DESIGN SYMPOSIUM, 2021. Anais [...] [S. l.]: IEEE, 2021. DOI: <https://doi.org/10.1109/SIEDS52267.2021.9483786>.
- BELLI, Luca et al. **Governança de dados no setor público: dados abertos, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável**. Rio de Janeiro: Lumen Juris, 2024. E-book. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/493b07ff-10c4-4951-8b0b-a4cc708bd61c/content>. Acesso em: 18 nov. 2025.
- BRASIL. **Decreto nº 10.332, de 28 de abril de 2020. Estratégia de Governo Digital para o período de 2020 a 2022**. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm. Acesso em: 2 mar. 2024.
- BRASIL. **Estratégia Brasileira para a Transformação Digital (E-Digital): ciclo 2022-2026**. Brasília, DF: gov.br, 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf. Acesso em: 2 mar. 2024.
- BRASIL. **Lei nº 13.675, de 11 de junho de 2018. Institui o Sistema Único de Segurança Pública (SUSP)**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113675.htm. Acesso em: 27 mar. 2026.
- BRASIL. **Lei nº 14.129, de 29 de março de 2021. Lei do Governo Digital**. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 2 mar. 2024.
- BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Modelo de Maturidade de Dados – MMD**. Brasília, DF, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/maturidade-de-dados>. Acesso em: 20 nov. 2025.

BRASIL. **Governo Digital. O que é.** Brasília, DF, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/transformacao-digital/o-que-e>. Acesso em: 2 mar. 2024.

BRITO, F. A. D. **Liberdade, segurança e polícia: uma abordagem filosófica sob a ótica contratualista.** Filosofia e Educação, Campinas, v. 14, p. 204-215, 2022. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rfe/article/view/8665787>. Acesso em: 6 mar. 2024.

COSTA, C. L. da et al. **Towards the evaluation and continuous evolution of open government data portals: a framework proposal.** In: INTERNATIONAL CONFERENCE ON ELECTRONIC GOVERNMENT AND THE INFORMATION SYSTEMS PERSPECTIVE, 2023. Proceedings [...] Cham: Springer, 2023. p. 243-257. DOI: 10.1007/978-3-031-33261-6_21.

COSTA, G. S. **O papel dos mecanismos de governança na formulação dos planos estaduais de segurança pública.** 2022. Dissertação (Mestrado Profissional em Administração Pública) – Universidade de Brasília, Brasília, 2022.

DAMA INTERNATIONAL. **DAMA-DMBOK: Data Management Body of Knowledge.** 2. ed. Basking Ridge: Technics Publications, 2017.

DENFORD, J. S.; DAWSON, G. S.; DESOUZA, K. C.; PANG, M.-S. **Centralization and decentralization decisions: multiple contingencies for IT governance in the public sector.** AIS Transactions on Replication Research, Atlanta, v. 6, n. 1, p. 1-25, 2020. DOI: 10.17705/1attr.00064.

EUROPEAN DATA PORTAL. **Creating public sector value through the use of open data.** [S. l.]: Publications Office of the European Union, 2020. Disponível em: https://data.europa.eu/sites/default/files/report/Creating%20public%20sector%20value%20through%20the%20use%20of%20open%20data_ENG_0.pdf. Acesso em: 12 mar. 2026.

FIGUEIREDO, S. O. et al. **Fatores determinantes do controle da criminalidade em gestão de políticas de segurança pública.** Revista de Administração Pública, Rio de Janeiro, v. 55, n. 2, p. 438-458, 2021. Disponível em: <http://dx.doi.org/10.1590/0034-761220200058>. Acesso em: 20 fev. 2026.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.

GÜLTEKIN-VÁRKONYI, D. **Navigating data governance risks: facial recognition in law enforcement under EU legislation.** Internet Policy Review, v. 13, n. 3, 2024. DOI: <https://doi.org/10.14763/2024.3.1798>.

LAKATOS, E. M.; MARCONI, M. de A. **Metodologia do trabalho científico.** 7. ed. São Paulo: Atlas, 2010.

NUNES, C. F. O. **Framework da governança multinível do Sistema Único de Segurança Pública (SUSP)** – Brasil. 2025. Tese (Doutorado) – Universidade Federal de Santa Catarina, Florianópolis, 2025.

OCDE. **Revisão do Governo Digital do Brasil**. Brasília, DF: OCDE, 2018.

O'HARA, K. **Data quality, government data and the open data infosphere**. [S. l.: s. n.], 2012.

SAMPSON, F. **Digital accountability for LEAs: balancing technical possibility, legal permissibility and societal acceptability**. [S. l.: s. n.], 2020. DOI: <https://doi.org/10.7190/SHU-THESIS-00334>.

SILVEIRA, C. T. **Segurança pública baseada no uso de dados**. Brazilian Journal of Business, Curitiba, v. 7, n. 1, p. 1-12, 2025. Disponível em: <https://doi.org/10.34140/bjbv7n1-034>. Acesso em: 20 fev. 2026.

UNITED NATIONS DEVELOPMENT PROGRAMME. **Building a fairer digital future starts with trusted data: a governance assessment framework for digital public infrastructure**. New York: UNDP, 2025. Disponível em: <https://www.undp.org/digital/blog/building-fairer-digital-future-starts-trusted-data-governance-assessment-framework-digital-public-infrastructure>. Acesso em: 18 fev. 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Guidelines for the governance of statistical data in the criminal justice system**. Vienna: UNODC, 2024. Disponível em: https://www.unodc.org/documents/data-and-analysis/statistics/Statistical_guidelines_governance.pdf. Acesso em: 20 fev. 2026.

VELDI, S. R. **The role of middleware in building scalable e-government platforms: a technical framework for digital governance**. Sarcouncil Journal of Multidisciplinary, v. 5, n. 7, p. 310-321, 2025. Disponível em: <https://sarcouncil.com/download-article/SJMD-122-2025-310-321.pdf>. Acesso em: 20 fev. 2026.

WIMMER, M. A.; NEURONI, A. C.; FRECÈ, J. T. **Approaches to good data governance in support of public sector transformation through once-only**. In: PEREIRA, G. V.; JANSSEN, M. et al. (ed.). *Electronic government*. Cham: Springer, 2020. p. 211-223. DOI: 10.1007/978-3-030-57599-1_16.

WORLD BANK. **Interoperability: towards a data-driven public sector**. Washington, DC: World Bank, 2022. Disponível em: <https://documents1.worldbank.org/curated/en/099550101092318102/pdf/P1694820242a9c041083900346bab0910eb.pdf>. Acesso em: 12 nov. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a disputa por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.

APÊNDICES

APÊNDICE A – Dados obtidos

DADOS GERAIS

n_itens	media	mediana	desvio	min_nivel	max_nivel	q1	q3	margem_e rro_planej ada	margem_e rro_atual	umento_err
780	2,9961538 46	3	1,2652096 29	1	5	2	4	3.44%	3.51%	0.0656%

ALFA CRONBACH RESPOSTAS

Metrica	Valor	CI_Inferior	CI_Superior
Alfa de Cronbach	0,9796434409	0,966	0,989

NIVEL POR DIMENSÃO

DIMENSÃO	n_itens	media	mediana	desvio	min_nivel	max_nivel	q1	q3
Dados como Ativo Estratégico	78	3,602564103	4	1,023613964	1	5	3	4
Análise de Dados	104	3,451923077	3	1,060131955	2	5	3	4
Governança de Dados	104	3,25	3	1,146967297	1	5	2	4
Gerenciamento de Dados	104	2,913461538	3	1,277973038	1	5	2	4
Conhecimento sobre os Dados	104	2,807692308	3	1,428400715	1	5	2	4
Dados Abertos	52	2,807692308	3	1,314153146	1	5	2	3
Qualidade de Dados	78	2,807692308	3	1,319756887	1	5	2	4
Ética de Dados	26	2,692307692	2,5	0,884046639 9	1	4	2	3
Interoperabilidade de Dados	104	2,663461538	2	1,251101083	1	5	2	4

Inteligência Artificial	26	2	2	1,058300524	1	5	1	2
-------------------------	----	---	---	-------------	---	---	---	---

CORRELAÇÃO POR DIMENSÃO

Análise de Dados	Conhecimento sobre os Dados	Dados Abertos	Dados como Ativo Estratégico	Gerenciamento de Dados	Governança de Dados	Inteligência Artificial	Interoperabilidade de Dados	Qualidade de Dados	Ética de Dados
1	0,75015248 22	0,82391582 4	0,88258320 67	0,82260870 74	0,87050837 25	0,56770326 42	0,83109717 93	0,76083717 95	0,66126004 39
0,75015248 22	1	0,71553492 05	0,64874936 39	0,84890299 32	0,77692830 22	0,45178236 6	0,78671372 36	0,80327624 81	0,56566022 49
0,82391582 4	0,71553492 05	1	0,68550458 13	0,75228757 63	0,69935667 01	0,72719927 5	0,7390745	0,62913233 77	0,65597770 01
0,88258320 67	0,64874936 39	0,68550458 13	1	0,79827727 43	0,84004689 85	0,54511460 07	0,76195593 77	0,74949850 14	0,69173999 58
0,82260870 74	0,84890299 32	0,75228757 63	0,79827727 43	1	0,82486924 48	0,62842270 07	0,84179320 81	0,77408421 37	0,70175763 89
0,87050837 25	0,77692830 22	0,69935667 01	0,84004689 85	0,82486924 48	1	0,43250201 33	0,85518042 72	0,86045184 32	0,73160639 32
0,56770326 42	0,45178236 6	0,72719927 5	0,54511460 07	0,62842270 07	0,43250201 33	1	0,57873782 12	0,45962196 12	0,51304687 69
0,83109717 93	0,78671372 36	0,7390745	0,76195593 77	0,84179320 81	0,85518042 72	0,57873782 12	1	0,86708719 06	0,78478633 83
0,76083717 95	0,80327624 81	0,62913233 77	0,74949850 14	0,77408421 37	0,86045184 32	0,45962196 12	0,86708719 06	1	0,81168876 5
0,66126004 39	0,56566022 49	0,65597770 01	0,69173999 58	0,70175763 89	0,73160639 32	0,51304687 69	0,78478633 83	0,81168876 5	1

NÍVEL POR TEMA

DIMENSÃO	NUM TEMA	TEMA	n_itens	media	mediana	desvio	min_nivel	max_nivel	q1	q3
Análise de Dados	6,4	Tomada de Decisão Baseada em Dados	26	3,7307692 31	4	1,0414486 95	2	5	3	5
Dados como Ativo Estratégico	2,3	Dados como Pilar para Entregas à Sociedade	26	3,6153846 15	3	0,9413574 487	2	5	3	4
Dados como Ativo Estratégico	2,2	Gestão Orientada a Dados	26	3,6153846 15	4	0,9829312 52	1	5	3	4
Dados como Ativo Estratégico	2,1	Alinhamento com Objetivos Estratégicos	26	3,5769230 77	4	1,1721118 35	1	5	3	4,75
Governança de Dados	1,2	Promoção da Cultura de Dados pela Alta	26	3,5	3	1,1045361 02	2	5	3	5

		Gestão								
Análise de Dados	6,2	Relevância e Suficiência dos Dados	26	3,384615385	3	1,358732441	2	5	2	5
Análise de Dados	6,1	Infraestrutura e Ferramentas para Análise de Dados	26	3,384615385	3	0,982931252	2	5	3	4
Análise de Dados	6,3	Desenvolvimento da Capacidade Analítica	26	3,307692308	3	0,7883771062	2	5	3	4
Governança de Dados	1,4	Letramento em Dados	26	3,269230769	3	1,115623317	1	5	3	4
Governança de Dados	1,1	Estrutura Organizacional para Governança de Dados	26	3,115384615	3	1,142870879	2	5	2	4
Governança de Dados	1,3	Princípios e Políticas de Dados	26	3,115384615	3	1,243444348	1	5	2	4
Gerenciamento de Dados	5,2	Ciclo de Vida dos Dados	26	3,076923077	3	1,324328567	1	5	2,25	4
Gerenciamento de Dados	5,3	Dados não Estruturados	26	3,038461538	3	1,24838357	1	5	2	4
Conhecimento sobre os Dados	3,3	Modelagem de Dados	26	3,038461538	3	1,370569786	1	5	2	4
Interoperabilidade de Dados	7,2	Integração de Sistemas	26	3,038461538	3	1,24838357	1	5	2	4
Qualidade de Dados	9,2	Cultura de Qualidade de Dados	26	3	3	1,356465997	1	5	2	4
Qualidade de Dados	9,1	Gestão de Qualidade de Dados	26	2,923076923	3	1,383418286	1	5	2	3,75
Interoperabilidade de Dados	7,4	Compartilhamento de Dados com Atores Externos	26	2,923076923	2,5	1,163548948	1	5	2	4
Conhecimento sobre os Dados	3,1	Documentação dos Ativos de Dados	26	2,923076923	3	1,440085468	1	5	2	4
Gerenciamento de Dados	5,1	Gerenciamento de Dados Mestres e Dados de Referência	26	2,923076923	3	1,440085468	1	5	2	4
Conhecimento sobre os Dados	3,4	Gestão de Metadados	26	2,884615385	3	1,395046181	1	5	2	3,75
Dados Abertos	4,2	Ecosistema de Dados Abertos	26	2,846153846	3	1,18969938	1	5	2	3
Dados Abertos	4,1	Implementação da Política de Dados Abertos	26	2,769230769	3	1,45072926	1	5	1,25	3,75

Interoperabilidade de Dados	7,1	Padrões e Normas para Interoperabilidade	26	2,730769231	2	1,250845868	1	5	2	3
Ética de Dados	8,1	Ética no Tratamento de Dados	26	2,692307692	2,5	0,8840466399	1	4	2	3
Gerenciamento de Dados	5,4	Gerenciamento de Dados Geoespaciais	26	2,615384615	2	1,098250357	1	5	2	3
Qualidade de Dados	9,3	Medição e Controle da Qualidade de Dados	26	2,5	2	1,208304597	1	5	2	3,75
Conhecimento sobre os Dados	3,2	Glossário de Termos de Negócio	26	2,384615385	2	1,4987174	1	5	1	3
Inteligência Artificial	10,1	Estratégia de Inteligência Artificial	26	2	2	1,058300524	1	5	1	2
Interoperabilidade de Dados	7,3	Monitoramento e Avaliação da Interoperabilidade	26	1,961538462	2	1,112861869	1	4	1	2,75

GAPS CRÍTICOS

DIMENSÃO	TEMA	n_itens	media	mediana	desvio	gap_prioridade
Conhecimento sobre os Dados	Glossário de Termos de Negócio	26	2,384615385	2	1,4987174	6,535107047
Interoperabilidade de Dados	Monitoramento e Avaliação da Interoperabilidade	26	1,961538462	2	1,112861869	6,419849524
Inteligência Artificial	Estratégia de Inteligência Artificial	26	2	2	1,058300524	6,174901573
Qualidade de Dados	Medição e Controle da Qualidade de Dados	26	2,5	2	1,208304597	5,520761493
Dados Abertos	Implementação da Política de Dados Abertos	26	2,769230769	3	1,45072926	5,467011425
Interoperabilidade de Dados	Padrões e Normas para Interoperabilidade	26	2,730769231	2	1,250845868	5,1076887
Conhecimento sobre os Dados	Documentação dos Ativos de Dados	26	2,923076923	3	1,440085468	5,067869817
Gerenciamento de Dados	Gerenciamento de Dados Mestres e Dados de Referência	26	2,923076923	3	1,440085468	5,067869817
Conhecimento sobre os Dados	Gestão de Metadados	26	2,884615385	3	1,395046181	5,066443844
Gerenciamento de Dados	Gerenciamento de Dados Geoespaciais	26	2,615384615	2	1,098250357	5,003520082
Qualidade de Dados	Gestão de Qualidade de Dados	26	2,923076923	3	1,383418286	4,95017644
Dados Abertos	Ecossistema de	26	2,846153846	3	1,18969938	4,716275588

	Dados Abertos					
Qualidade de Dados	Cultura de Qualidade de Dados	26	3	3	1,356465997	4,712931993
Conhecimento sobre os Dados	Modelagem de Dados	26	3,038461538	3	1,370569786	4,649963811
Interoperabilidade e de Dados	Compartilhamento de Dados com Atores Externos	26	2,923076923	2,5	1,163548948	4,493524738
Gerenciamento de Dados	Ciclo de Vida dos Dados	26	3,076923077	3	1,324328567	4,469862629
Interoperabilidade e de Dados	Integração de Sistemas	26	3,038461538	3	1,24838357	4,410290849
Gerenciamento de Dados	Dados não Estruturados	26	3,038461538	3	1,24838357	4,410290849
Ética de Dados	Ética no Tratamento de Dados	26	2,692307692	2,5	0,8840466399	4,347799938
Governança de Dados	Princípios e Políticas de Dados	26	3,115384615	3	1,243444348	4,228029732
Governança de Dados	Estrutura Organizacional para Governança de Dados	26	3,115384615	3	1,142870879	4,038487426
Análise de Dados	Relevância e Suficiência dos Dados	26	3,384615385	3	1,358732441	3,810260097
Governança de Dados	Letramento em Dados	26	3,269230769	3	1,115623317	3,66165574
Análise de Dados	Infraestrutura e Ferramentas para Análise de Dados	26	3,384615385	3	0,982931252	3,203196638
Governança de Dados	Promoção da Cultura de Dados pela Alta Gestão	26	3,5	3	1,104536102	3,156804153
Dados como Ativo Estratégico	Alinhamento com Objetivos Estratégicos	26	3,576923077	4	1,172111835	3,091082227
Análise de Dados	Desenvolvimento da Capacidade Analítica	26	3,307692308	3	0,7883771062	3,026484334
Dados como Ativo Estratégico	Gestão Orientada a Dados	26	3,615384615	4	0,982931252	2,745597118
Dados como Ativo Estratégico	Dados como Pilar para Entregas à Sociedade	26	3,615384615	3	0,9413574487	2,68803339
Análise de Dados	Tomada de Decisão Baseada em Dados	26	3,730769231	4	1,041448695	2,591069498

APÊNDICE B – Código *Python* utilizado para o tratamento dos dados

```

import re
import math
import unicodedata
import os
from pathlib import Path

import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import pingouin as pg
import seaborn as sns
from sklearn.preprocessing import StandardScaler

# =====
# CONFIGURAÇÕES DE AMBIENTE E MAPEAMENTO DE COLUNAS
# =====

ROOT_PATH = "/path/to/dados/"
CSV_PATH = f"{ROOT_PATH}Resultados Tratados MMD.csv"
OUT_XLSX = f"{ROOT_PATH}Analise_MMD_publicacao.xlsx"
OUT_GRAPHS = f"{ROOT_PATH}Gráficos/"

# Definição das variáveis do dataset
DIM_COL = "DIMENSÃO"
NUM_TEMA = "NUM TEMA"
TEMA_COL = "TEMA"
NIVEL_COL = "NÍVEL"
ENT_COL = "ESTADO"

os.makedirs(OUT_GRAPHS, exist_ok=True)

# =====
# FUNÇÕES AUXILIARES (HELPERS)
# =====

def _norm(text: str) -> str:
    """Normaliza strings para nomes de arquivos (remove acentos e espaços)."""
    text = text.lower().strip()
    text = unicodedata.normalize('NFKD', text).encode('ascii', 'ignore').decode('utf-8')
    text = re.sub(r'^a-z0-9\s', '', text)
    return re.sub(r'\s+', '_', text)

def coerce_level(series: pd.Series) -> pd.Series:
    """Limpa e converte a coluna de nível para numérico inteiro."""
    s = series.astype(str).str.strip().str.replace(", ", ".", regex=False)
    s = s.str.extract(r"^(d+)", expand=False)
    return pd.to_numeric(s, errors="coerce").astype("Int64")

# =====
# CARGA E PROCESSAMENTO DE DADOS
# =====

# Leitura com detecção automática de separador
df_raw = pd.read_csv(CSV_PATH, sep=None, engine="python")

# Seleção e Limpeza
df = df_raw[[DIM_COL, NUM_TEMA, TEMA_COL, NIVEL_COL, ENT_COL]].copy()
df[NIVEL_COL] = coerce_level(df[NIVEL_COL])

# Filtragem: Mantém apenas respostas válidas na escala Likert 1-5
df = df.dropna(subset=[NIVEL_COL])
df = df[(df[NIVEL_COL] >= 1) & (df[NIVEL_COL] <= 5)]
df = df.sort_values(NUM_TEMA)

print(f"Dataset processado: {len(df)} linhas válidas de {df[ENT_COL].nunique()} entidades.")

# =====
# 1) ANÁLISES ESTATÍSTICAS DESCRITIVAS
# =====

def get_stats(group):
    """Gera bloco de estatísticas descritivas para os agrupamentos."""
    return group.agg(
        n_itens="count",
        media="mean",
        mediana="median",

```

```

        desvio="std",
        min_nivel="min",
        max_nivel="max",
        q1=lambda x: x.quantile(0.25),
        q3=lambda x: x.quantile(0.75)
    )

overall = get_stats(df[NIVEL_COL]).to_frame().T.reset_index(drop=True)
by_ent = get_stats(df.groupby(ENT_COL)[NIVEL_COL]).reset_index().sort_values("media", ascending=False)
by_dim = get_stats(df.groupby(DIM_COL)[NIVEL_COL]).reset_index().sort_values("media", ascending=False)
by_theme = get_stats(df.groupby([DIM_COL, NUM_TEMA, TEMA_COL])[NIVEL_COL]).reset_index().sort_values([NUM_TEMA])

# Análise de Gaps (Priorização: Baixa média e Alto desvio aumentam a urgência)
gaps_theme = by_theme.copy()
gaps_theme["gap_prioridade"] = (5 - gaps_theme["media"]) * (gaps_theme["desvio"].fillna(0) + 1)
gaps_theme = gaps_theme.sort_values("gap_prioridade", ascending=False)

# =====
# 2) CONSISTÊNCIA INTERNA (ALFA DE CRONBACH) E CORRELAÇÃO
# =====

# Pivotagem para matriz de correlação e confiabilidade
df_pivot = df.pivot(index=ENT_COL, columns=TEMA_COL, values=NIVEL_COL)
by_ent_dim_pivot = df.groupby([ENT_COL, DIM_COL])[NIVEL_COL].mean().unstack()

def calculate_cronbach(data, label):
    val, ci = pg.cronbach_alpha(data=data)
    return pd.DataFrame({'Metrica': [f'Alfa de Cronbach ({label})'], 'Valor': [val], 'CI_Inf': [ci[0]], 'CI_Sup': [ci[1]]})

alfa_respostas = calculate_cronbach(df_pivot, "Temas")
alfa_dimensoes = calculate_cronbach(by_ent_dim_pivot, "Dimensões")

# Matrizes de Correlação (Pearson)
by_theme_corr = df_pivot.corr()
by_dim_corr = by_ent_dim_pivot.corr()

# =====
# 3) FUNÇÕES DE VISUALIZAÇÃO GRÁFICA
# =====

def radar_plot(labels: list, values: list, title: str, savepath: str = None):
    num_vars = len(labels)
    angles = np.linspace(0, 2 * np.pi, num_vars, endpoint=False).tolist()

    # Fechamento do polígono do radar
    values = values + values[:1]
    angles = angles + angles[:1]

    fig, ax = plt.subplots(figsize=(8, 8), subplot_kw=dict(polar=True))
    ax.plot(angles, values, linewidth=2, linestyle='solid', color='#1f77b4')
    ax.fill(angles, values, '#1f77b4', alpha=0.25)

    ax.set_xticks(angles[:-1])
    ax.set_xticklabels(labels, fontsize=9)
    ax.set_ylim(0, 5)
    ax.set_yticks(range(1, 6))
    plt.title(title, size=15, pad=30)

    if savepath:
        plt.savefig(savepath, bbox_inches='tight', dpi=300)
        plt.close()

def plot_candlestick_like(df_data: pd.DataFrame, x_col: str, title: str, file_name: str):
    """Gera visualização de quartis e amplitude (estilo candlestick)."""
    df_plot = df_data.sort_values('media', ascending=True)
    plt.figure(figsize=(12, 6))

    # Corpo do Box (Q1 ao Q3)
    plt.bar(df_plot[x_col], df_plot['q3'] - df_plot['q1'], bottom=df_plot['q1'],
            color='teal', alpha=0.6, width=0.5, label='IQR (Q1-Q3)')

    # Hastes (Min e Max)
    for i, row in df_plot.iterrows():
        plt.plot([row[x_col], row[x_col]], [row['min_nivel'], row['max_nivel']], color='black', lw=1, zorder=1)

    plt.scatter(df_plot[x_col], df_plot['mediana'], color='orange', marker='s', s=50, label='Mediana', zorder=3)

```

```

plt.scatter(df_plot[x_col], df_plot['media'], color='red', marker='^', s=50, label='Média', zorder=3)

plt.xticks(rotation=45, ha='right')
plt.ylabel('Nível de Maturidade')
plt.title(title)
plt.legend(loc='upper left', bbox_to_anchor=(1, 1))
plt.tight_layout()
plt.savefig(os.path.join(OUT_GRAPHS, file_name), dpi=300)
plt.close()

# =====
# 4) EXECUÇÃO DAS PLOTAGENS E EXPORTAÇÃO
# =====

# Gráficos de Radar Geral e por Dimensão
radar_plot(by_dim[DIM_COL].tolist(), by_dim['media'].tolist(), "Radar de Maturidade - Visão por Dimensão", os.path.join(OUT_GRAPHS,
"radar_geral_dimensoes.png"))

# Candlesticks
plot_candlestick_like(by_ent, ENT_COL, 'Distribuição de Maturidade por Estado', "candlestick_estados.png")
plot_candlestick_like(by_dim, DIM_COL, 'Distribuição de Maturidade por Dimensão', "candlestick_dimensoes.png")

# Heatmaps de Correlação
plt.figure(figsize=(10, 8))
sns.heatmap(by_dim_corr, annot=True, cmap='coolwarm', fmt=".2f")
plt.title("Correlação entre Dimensões")
plt.savefig(os.path.join(OUT_GRAPHS, "heatmap_correlacao_dimensoes.png"), dpi=300)
plt.close()

# Exportação Excel
with pd.ExcelWriter(OUT_XLSX, engine="openpyxl") as writer:
    df.to_excel(writer, index=False, sheet_name="Respostas_Tratadas")
    overall.to_excel(writer, index=False, sheet_name="Estatisticas_Gerais")
    by_ent.to_excel(writer, index=False, sheet_name="Nivel_por_Estado")
    by_dim.to_excel(writer, index=False, sheet_name="Nivel_por_Dimensao")
    by_theme.to_excel(writer, index=False, sheet_name="Nivel_por_Tema")
    gaps_theme.to_excel(writer, index=False, sheet_name="Gaps_Prioridade")
    alfa_respostas.to_excel(writer, index=False, sheet_name="Confiabilidade_Cronbach")
    by_dim_corr.to_excel(writer, sheet_name="Correlacao_Dimensoes")

print(f"✅ Processamento concluído. Resultados salvos em: {ROOT_PATH}")

```