Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

# Governança de dados no setor público

## GTT 4

## 2025

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

# RELATÓRIO FINAL

## GT nº 4 | Governança de Dados (Setor Público)


***Membros***

*Ana Paula Bialer (Coordenadora)*
*Adriana Macedo Marques (Vice Coordenadora)*
*Ana Estela Haddad*
*Bruno Ricardo Bioni*
*Renata Vicentini Mielli*
*Rony Vainzof*
*Samara Mariana de Castro*



***Agradecimentos pela contribuição***

*Isabella Miranda Silvério*
*Leonardo Rodrigo Ferreira*
*Marta Medeiros*



Brasília, DF
2024

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

# Índice

# RELATÓRIO FINAL

## GT 4 - Governança de Dados (Setor Público)

Instituído pela Portaria CNPD n° 04, de 04 de outubro de 2024[1], o Grupo de Trabalho nº 04 (GT-4) do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) dedicou-se a fornecer subsídios, no âmbito da governança de dados no setor público, para a elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade.

Com objetivo de atender suas competências de realizar análises, estudos e proposições na temática, o GT teve duração de 120 (cento e vinte) dias, a contar da entrada em vigor da portaria que instituiu o GT, com previsão de encerramento no dia 04 de fevereiro de 2025.

### 1. A DINÂMICA DAS REUNIÕES

O GT-4 iniciou suas atividades com a realização de uma reunião de alinhamento, na qual se optou pela instituição de uma dinâmica de reuniões ordinárias semanais às sexta-feiras, às 9h, com limite de duração de uma hora. Essas reuniões ocorreram por videoconferência no Google Meets. O objetivo dessa periodicidade foi manter constância na discussão dos temas prioritários e alinhamento das entregas. Ao longo do seu prazo de existência fixado em portaria, o GT-4 reuniu-se 14 (quatorze) vezes, todas de maneira online.

### 2. O PLANO DE TRABALHO APRESENTADO E O MAPEAMENTO PRELIMINAR

Cumprindo o estabelecido pela Portaria de criação, o GT-4 elaborou um plano de trabalho com foco na governança de dados no setor público.

A primeira etapa consistiu na elaboração de um mapeamento preliminar de subsídios (Anexo 01), com objetivo de embasar os estudos para elaboração de proposta à Política Nacional de Proteção de Dados Pessoais e Privacidade, relacionada ao tema da governança de dados no setor público.

O mapeamento foi estruturado em três seções principais:

1. Práticas Nacionais: Avaliação de iniciativas realizadas no país, no âmbito do Poder Executivo, nas esferas federal, estadual e municipal, e em outros poderes.

[1] https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/sei_0148148_portaria_cnpd_04_2024.pdf

2. Práticas de Entidades Normativas: Levantamento de diretrizes publicadas por organizações como a ISO e o NIST.
3. Práticas de Organizações Internacionais: Análise de exemplos internacionais relevantes para governança de dados, proteção de dados pessoais e transparência.

A partir do levantamento de materiais relevantes relacionados ao tema de cada seção, feito no intuito de orientar o desenvolvimento de estudos aprofundados, foi adicionada ao plano de trabalho a elaboração de estudo para cada seção, a fim de estruturar e desenvolver o relatório final.

Ao longo do mapeamento, observou-se que, embora existam diversas iniciativas recentes envolvendo a temática de governança de dados, muitas delas não abordam diretamente a proteção de dados pessoais. Além disso, identificou-se um maior volume de materiais de governança no Poder Executivo Federal, em comparação com outros poderes e esferas do governo.

Diante deste cenário, o GT-4 se propôs à realização de entrevistas com representantes das esferas federal, estadual e municipal do Poder Executivo, para capturar diferentes perspectivas, identificar desafios e coletar boas práticas, considerando as variáveis existentes entre as diferentes esferas de governo.

## 3. EXECUÇÃO DO PLANO DE TRABALHO

O GT-4 iniciou a execução do plano de trabalho com discussões sobre o conceito e escopo da governança de dados. Entre os desafios destacados, apontou-se a dificuldade de definição clara do que constitui a governança de dados e a necessidade de ajustar o escopo de atuação do grupo.

As reuniões do GT-4 também incluíram discussões sobre práticas existentes em Estados e Municípios, destacando a Estratégia Nacional de Governo Digital, prevista na Lei nº 14.129, de 29 de março de 2021[2] (Lei do Governo Digital), como um instrumento importante para direcionar as iniciativas locais. Adicionalmente, as entrevistas realizadas com representantes das diferentes esferas de governo contribuíram para mapear as barreiras práticas e propor soluções adaptadas às realidades locais.

[2] https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

### 3.1. Entrevistas com representantes

Com intenção de realizar um diagnóstico amplo sobre governança de dados, o GT-4 realizou 06 (seis) entrevistas para capturar diferentes perspectivas, identificar desafios e coletar boas práticas. Inicialmente, as entrevistas incluíram discussões com representantes dos três níveis do Poder Executivo (federal, estadual e municipal). Diante da riqueza de informações obtidas, foi decidido pela realização de entrevistas também com representantes do Poder Judiciário, além de uma entrevista ao final com o Coordenador-Geral de Fiscalização na ANPD.

As entrevistas foram realizadas a partir de um roteiro previamente estabelecido e estruturado a partir de uma abordagem inspirada no Design Thinking, para explorar os problemas e identificar oportunidades de maneira colaborativa e eficaz, sendo divididas em cinco etapas:

- **Introdução e Contextualização:** Apresentação do objetivo da entrevista e breve explicação sobre o Conselho Nacional de Proteção de Dados (CNPD) e o papel do Grupo de Trabalho (GT) na elaboração de diagnóstico em governança de dados no setor público.
- **Descoberta (Empatia):** Exploração dos desafios enfrentados pelos entrevistados, com foco nas práticas atuais de governança de dados, problemas recorrentes e impacto dessas dificuldades no cumprimento da LGPD.
- **Definição (Exploração dos Problemas):** Análise detalhada dos principais problemas identificados, suas causas raízes e o impacto na eficiência dos serviços públicos.
- **Ideação (Geração de Soluções):** Discussão sobre possíveis soluções, boas práticas e inovações que poderiam ser adotadas para superar os desafios da governança de dados.
- **Prototipação (Exemplos Práticos):** Coletar exemplos práticos e boas práticas que já estejam sendo aplicadas.

Ao final de cada entrevista, foi elaborado um relato (Anexo 2) com a síntese dos principais pontos discutidos e alinhamento sobre os próximos passos para a elaboração do diagnóstico e desenvolvimento de recomendações. O relato foi incluído na Ata de Reunião e compartilhado com todos os membros do GT com os respectivos links das apresentações institucionais realizadas.

A partir dos relatos compartilhados com o grupo, o GT-4 consolidou as informações em uma tabela (Anexo 3), de modo a permitir a identificação de padrões e temas centrais que se

destacam na governança de dados no setor público brasileiro, através dos desafios, ações, avanços e tendências identificados nas entrevistas.

A seguir, segue uma análise geral, quanto aos **desafios relevantes**, que correspondem aos principais problemas apontados pelos entrevistados e abrangem diversos aspectos críticos da governança de dados no setor público:

| Desafios relevantes | Descrição |
|---|---|
| **Capacitação e Conscientização** | Há uma lacuna generalizada na formação de servidores públicos, com insuficiência de treinamentos direcionados às necessidades específicas da administração pública. A dificuldade de traduzir conceitos técnicos e jurídicos em diretrizes práticas é uma barreira recorrente. |
| **Governança Fragmentada** | A diversidade de estruturas e níveis de maturidade dos órgãos públicos impede a uniformidade e a eficiência das políticas. Muitos órgãos ainda operam com estruturas limitadas, sem autonomia técnica ou integração robusta. Existe relevante inconsistência na estrutura de governança dentro de departamentos que integram um mesmo ente, para além da discrepância entre entes distintos. |
| **Interoperabilidade e Padronização** | A interoperabilidade entre sistemas e dados é um problema significativo; a ausência de padrões claros dificulta a interoperabilidade entre municípios, estados e órgãos federais, e mesmo dentro do próprio ente ou órgão. |
| **Segurança da Informação** | A segurança ainda é vista de forma restrita em alguns contextos, sendo frequentemente associada apenas à TI, enquanto deveria ser tratada de maneira mais ampla, como um componente estratégico da governança de dados. |
| **Recursos Financeiros e Sustentabilidade** | A limitação orçamentária, especialmente em municípios menores, é um desafio constante. Custos associados à adoção de tecnologias emergentes, como IA e soluções em nuvem, aumentam a pressão por modelos mais acessíveis e sustentáveis. |
| **Disparidade de Maturidade entre as Esferas federal, estadual e municipal** | Há diferenças significativas na maturidade em governança de dados entre os diferentes níveis federal, estadual e municipal. O governo federal apresenta maior avanço, com estruturas mais consolidadas, equipes técnicas capacitadas e iniciativas voltadas à centralização e interoperabilidade de dados. Os Estados demonstram progressos com algumas iniciativas voltadas para governança, mas enfrentam desafios relacionados à integração de sistemas e padronização de práticas. Os |

| Desafios relevantes | Descrição |
|---|---|
| | municípios apresentam cenário mais crítico; embora exista esforço em implementar políticas eficazes de governança de dados, muitos Municípios operam de forma fragmentada, com baixa utilização de ferramentas tecnológicas avançadas e com pouca integração entre secretarias. As capitais tendem a ser melhor estruturadas, contudo. |

Quanto às ações e boas práticas, os entrevistados destacaram uma série de iniciativas que estão sendo implementadas, consideradas bem sucedidas e replicáveis. Como exemplo, tem-se a criação de estruturas de governança, como o Comitê de Governança de Dados de São Paulo e o Comitê de Governança de Recife, os quais indicam que estruturas formais são fundamentais para organizar esforços e promover eficiência. Além disso, há iniciativas de investimento em formação para adequação à LGPD, por meio da criação de cartilhas, capacitações itinerantes e equipes de apoio ao encarregado (por exemplo, no caso do TRE-Paraná).

Além disso, Prefeituras como as do Rio de Janeiro e Recife implementaram redes de encarregados e modelos descentralizados adaptados às suas complexidades organizacionais, promovendo maior flexibilidade. Constatou-se também a criação de serviços inovadores, como o "Governo Zero Cliques" apresentado por Recife, sendo um exemplo de inovação para automatizar serviços e garantir direitos proativamente, melhorando a experiência dos cidadãos e aumentando a confiança na administração pública. Abaixo desenvolvemos esses exemplos e referências em maiores detalhes.

Embora os resultados aqui obtidos não representam a realidade total brasileira, também não se trata de resultados isolados. Neste sentido, destaca-se a Pesquisa sobre Privacidade e Proteção de Dados Pessoais 2023, realizada pelo Cetic.br|NIC.br[3], publicada em setembro de 2024, oferece uma visão detalhada das práticas e desafios enfrentados por órgãos públicos federais, estaduais e municipais no Brasil. A pesquisa mostra que 78% dos órgãos federais possuem políticas claras de privacidade e proteção de dados, comparado com 64% nos estados e apenas 52% nos municípios. Essa disparidade reflete a maturidade variada entre as esferas governamentais já destacada nas entrevistas realizadas por este GT. Além disso, as iniciativas de governança de dados nos níveis estadual e municipal muitas vezes carecem de padronização e integração, dificultando uma abordagem harmonizada.

[3] Disponível em: https://nic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf

Outrossim, a pesquisa do Cetic.br|NIC.br mostra disparidade significativa na oferta de capacitação sobre a LGPD para os funcionários de tecnologia da informação (TI) dos órgãos públicos. Em 2023, 84% dos órgãos federais reportaram oferecer cursos desse tipo, comparado a 53% dos órgãos estaduais. O Legislativo também mostrou um aumento expressivo, passando de 49% em 2021 para 75% em 2023. O Judiciário e o Ministério Público mantiveram estabilidade, com 90% e 80% respectivamente.

A nomeação de encarregados de dados pessoais foi uma das ações mais comuns, especialmente entre órgãos federais (83%) e estaduais (46%). Houve um aumento significativo entre os órgãos do Executivo (de 34% em 2021 para 46% em 2023), do Legislativo (de 40% para 66%) e do nível estadual (de 33% para 46%). Além disso, a implementação de ações como a disponibilização de canais de atendimento ao cidadão pela Internet e a publicação de políticas de privacidade também apresentou crescimento.

Apesar dos avanços, a pesquisa do Nic.br evidencia desigualdades na implementação da LGPD entre diferentes níveis de governo e poderes. No Executivo estadual, as iniciativas variam significativamente entre os estados, enquanto muitos órgãos ainda estão em fase inicial de conformidade com a legislação. A oferta de capacitação sobre a LGPD também apresenta disparidades, sendo maior nos órgãos federais do que nos estaduais. Dessa forma, a Pesquisa sobre Privacidade e Proteção de Dados Pessoais 2023 destaca tanto os progressos quanto os desafios na governança de dados no setor público brasileiro, indicando a necessidade de ações coordenadas e contínuas para promover uma cultura robusta de proteção de dados no Brasil.

## 4. CONCEITO DE GOVERNANÇA DE DADOS

### 4.1. Estudo: Práticas Nacionais

O estudo das práticas nacionais (Anexo 04) revelou um panorama diversificado e em construção em governança de dados, com iniciativas que buscam alinhar a administração pública às melhores práticas globais para o uso estratégico de dados. O levantamento identificou políticas, *frameworks* e regulamentações que têm norteado a estruturação da governança de dados no Brasil, destacando avanços, desafios e oportunidades.

A governança de dados no Brasil é sustentada por um arcabouço legal robusto, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), que regula o tratamento de dados pessoais e promove a transparência e a privacidade. Além disso, regulamentações como o Decreto nº 10.046/2019, que institui o Cadastro Base do Cidadão e estabelece diretrizes para o

compartilhamento de dados no âmbito federal, têm fortalecido a governança de dados na administração pública.

Outros instrumentos normativos, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei nº 14.129/2021, que dispõe sobre o Governo Digital, complementam esse arcabouço, criando as bases para uma governança que priorize a eficiência e a transparência, sempre com a observância dos preceitos de proteção fixados na LGPD.

A análise das práticas nacionais também evidenciou o papel crucial de órgãos e programas dedicados ao tema. O Comitê Central de Governança de Dados (CCGD), instituído pelo Decreto 10.046, de 9 de outubro de 2019[4], e a Secretaria de Governo Digital (SGD)[5] têm desempenhado papéis relevantes na promoção de boas práticas de governança de dados. Apesar dos avanços, o estudo revelou desafios importantes, como a maturidade institucional em governança de dados, que ainda varia significativamente entre as entidades, refletindo a necessidade de maior capacitação e uniformização de práticas.

O estudo também demonstrou iniciativas relevantes no fortalecimento da governança de dados e na capacitação técnica em privacidade e segurança da informação no setor público. Entre os destaques encontra-se o **Programa de Privacidade e Segurança da Informação (PPSI),** instituído pela Portaria SGD/MGI nº 852, de 28 de março de 2023[6], que conta com iniciativa liderada pelo Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital (CEPS GOV.BR)[7], em parceria com a SGD, a Enap e a Rede Nacional de Ensino e Pesquisa (RNP).

**Iniciativas Ministério da Gestão e da Inovação em Serviços Públicos (MGI)**

**a) Programa de Privacidade e Segurança da Informação (PPSI)[8]**

O Programa de Privacidade e Segurança da Informação (PPSI) é uma iniciativa do Governo Federal, instituído pela Portaria SGD/MGI Nº 852, de 28 de março de 2023, que regulamenta o Programa de Privacidade (PPSI) para implementação no âmbito dos órgãos e entidades do governo federal que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Além disso, a Portaria cria o Centro Integrado de Segurança

[4] https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm
[5] https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/secretaria-de-governo-digital
[6] https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908
[7] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca
[8] https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908

Cibernética do Governo Digital (CISC GOV.BR), o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital (CEPS GOV.BR) e institui o Framework de Privacidade e Segurança da Informação para apoio aos órgãos públicos.

O objetivo central do programa é aumentar a maturidade e a resiliência institucional, promovendo a cultura de privacidade e segurança da informação dos órgãos e entidades no âmbito do SISP. Para alcançar esses objetivos, o PPSI organiza suas ações em cinco eixos temáticos:

1. **Governança**: Com foco no alinhamento estratégico e no monitoramento das atividades do programa, garantindo que os objetivos sejam atingidos de forma eficiente e que os recursos sejam utilizados de maneira adequada.
2. **Maturidade**: Análise do estágio de implementação dos controles de privacidade e segurança pelos órgãos envolvidos, promovendo sensibilização e acompanhando os planos de ação para que lacunas identificadas sejam solucionadas.
3. **Metodologia**: Processo de criação e atualização de ferramentas, como guias e modelos práticos, que ajudem as instituições públicas a adotar padrões elevados de segurança e privacidade em suas operações.
4. **Pessoas**: Promovendo mudanças culturais dentro das organizações, por meio de ações de conscientização e capacitação. A ideia é engajar os servidores públicos na importância de práticas seguras no uso de tecnologia e na gestão de informações.
5. **Tecnologia**: Gerido pelo Centro Integrado de Segurança Cibernética do Governo Digital (CISC GOV.BR), atua no monitoramento e resposta a vulnerabilidades cibernéticas, além de apoiar ações de prevenção e resposta a incidentes.

O programa oferece uma série de controles, ferramentas de apoio e metodologias, que conforme o artigo 7º, §4º da referida Portaria SGD/MGI Nº 852, deverão observar: I - a Lei Geral de Proteção de Dados Pessoais; II - a Política Nacional de Segurança da Informação; III - os normativos emitidos pela Autoridade Nacional de Proteção de Dados Pessoais e pelo Gabinete de Segurança Institucional; e IV - as recomendações efetuadas pelos órgãos federais de controle interno e externo.

O Framework de Privacidade e Segurança da Informação instituído no programa é composto por um conjunto de controles, ferramentas práticas e metodologias que auxiliam os servidores públicos na construção e manutenção de um ambiente seguro, principalmente, na internalização dos conceitos. Oferece uma série de recursos, como guias, modelos e vídeos educativos, disponibilizados publicamente na plataforma Gov.br[9]. Combinados aos manuais de

[9] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos

boas práticas, checklists de conformidade que são disponibilizados. O framework adotado se mostra flexível, com capacidade de adaptação às realidades e necessidades de cada órgão ou entidade do governo federal que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação, também chamado de SISP.

Vale mencionar que o SISP foi instituído pelo Decreto nº 7.579, de 11 de outubro de 2011[10], com o objetivo de organizar a operação, controle, supervisão e coordenação dos recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal e possui a seguinte estrutura:

- Órgão Central - Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.
- Órgãos Setoriais - unidades de administração dos recursos de TI dos Ministérios e dos órgãos da Presidência da República.
- Comissão de Coordenação - representantes dos Órgãos Setoriais, presidida por representante do Órgão Central.
- Órgãos Seccionais - unidades de administração dos recursos de TI das autarquias e fundações.
- Órgãos Correlatos - unidades desconcentradas e formalmente constituídas de administração dos recursos de TI nos Órgãos Setoriais e Seccionais.

O PPSI contempla uma coletânea de publicações[11], como guias, cartilhas e modelos de políticas. A tabela a seguir contempla todas as publicações disponíveis no site, organizada com as categorias de Guias, Modelos e Cartilhas, e os respectivos links para acesso em a cada documento:

| Categoria | Documento | Disponível em |
|---|---|---|
| **Guias** | Guia de Gerenciamento de Vulnerabilidades | Link |
| | Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) | Link |
| | Guia de Elaboração do Processo de Gestão de Dados | Link |
| | Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs | Link |

[10] https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm
[11] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos

| Categoria | Documento | Disponível em |
|---|---|---|
| | Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web | Link |
| | Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicativos Móveis | Link |
| | Guia de Resposta a Incidentes de Segurança | Link |
| | Guia do Framework | Link |
| | Guia sobre Privacidade desde a Concepção e Por Padrão | Link |
| | Inventário de Dados Pessoais | Link |
| | Programa de Governança em Privacidade | Link |
| | Relatório de Impacto à Proteção de Dados Pessoais (RIPD | Link |
| | Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação | Link |
| | Termo de Uso e Política de Privacidade | Link |
| **Modelos** | Política de Backup | Link (versão PDF) |
| | Política de Controle de Acesso | Link (versão PDF) |
| | Política de Defesas contra Malware | Link (versão PDF) |
| | Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação | Link (versão PDF) |
| | Política de Gerenciamento de Vulnerabilidades | Link (versão PDF) |
| | Política de Gestão de Ativos | Link (versão PDF) |
| | Política de Gestão de Provedor de Serviços | Link (versão PDF) |
| | Política de Gestão de Registros (Logs) de Auditoria | Link (versão PDF) |
| | Política de Proteção de Dados Pessoais | Link (versão PDF) |
| | Política de Segurança da Informação | Link (versão PDF) |
| **Cartilhas** | Cartilha de Estruturação Básica de Gestão em Privacidade e Segurança da Informação (PPSI) | Link |

| Categoria | Documento | Disponível em |
|---|---|---|
| | Cartilha do Programa de Privacidade e Segurança da Informação (PPSI) | Link |
| | Cartilha sobre Finalidades e Hipóteses Legais | Link |

O Programa se encontra em sua segunda fase, com diversas iniciativas relevantes no fortalecimento da governança de dados e promoção da capacitação técnica em privacidade e segurança da informação, entre as quais são:

**Trilha de Aprendizagem em Privacidade e Segurança da informação**[12] (212 hs).

A **Trilha de Aprendizagem em Privacidade e Segurança da Informação**[13] é uma iniciativa disponível na Escola Virtual.Gov, fruto de parceria com o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital (CEPS GOV.BR) e a Escola Nacional da Administração Pública (ENAP). Essa trilha oferece um percurso educacional estruturado, voltado para a compreensão das responsabilidades legais, regulamentares e operacionais associadas à privacidade e à segurança da informação no âmbito governamental. A trilha é composta por uma série de cursos e conteúdos organizados para abordar os aspectos essenciais da privacidade e da segurança da informação.

**Curso Segurança para Todos**[14] **(24 hs).**

Projeto idealizado pela SGD (Digital gov.br), Escola Nacional de Administração Pública - Enap e Rede Nacional De Ensino E Pesquisa - Rnp objetivando a construção e desenvolvimento de competências necessárias para fortalecimento das competências digitais dos cidadãos brasileiros (Proteção de Dados Pessoais e Segurança Digital).

**CIS Controls 8**[15] **(100hs).**

**Enap - Escola Nacional de Administração Pública**

1. Atuação do Encarregado na LGPD: A função de orientar[16]
2. Segurança da Informação para Todos
3. Governo Data-Driven: transformação orientada por dados em governos

[12] https://www.escolavirtual.gov.br/trilha/246
[13] https://www.escolavirtual.gov.br/trilha/246
[14] https://www.escolavirtual.gov.br/curso/1256
[15] https://www.escolavirtual.gov.br/catalogo?query=cis+8&carga_horaria=
[16] https://www.escolavirtual.gov.br/curso/1041

4. Desvendando a Inteligência Artificial na Administração Pública
5. Como Trabalhar com Computadores e Dispositivos Móveis
6. Internet do Comportamento (IoB) em Serviços Públicos Digitais
7. Acervos Digitais nos Museus: realização de projetos
8. Governo Integrado: Como Construí-lo?
9. Governança de Dados na Transformação Digital
10. Governo Data-Driven: transformação orientada por dados em governos
11. LGPD: Como coordenar a atuação do município para a governança de dados aplicada
12. Governança de Dados

### 4.2. Estudo: Práticas de Entidades Normativas

A governança de dados na administração pública pode se beneficiar significativamente de práticas consolidadas e orientações técnicas desenvolvidas por entidades normativas, como a International Organization for Standardization (ISO) e o National Institute of Standards and Technology (NIST). Este capítulo apresenta uma visão geral das normas mais relevantes no campo da governança e segurança da informação, com foco em como elas podem ser aplicadas no contexto de entidades públicas.

**Normas ISO**

**ISO/IEC 27001:2022** - Information Security Management System (antes ISO 27001:2013)
Fornece um modelo para implementação , operação, monitoramento e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI).

**ISO/IEC 27701:2019 -** Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
Fornece requisitos e diretrizes para gestão da privacidade da informação

**ISO/IEC 38505-1:2017** - Information technology - Governance of IT - Governance of Data- Part 1: Application of ISO/IEC 38500 to the governance of data
Aplica os princípios da governança de TI (ISO/IEC 38500) ao contexto da governança de dados, fornecendo diretrizes para o gerenciamento estratégico de ativos de dados.

***ISO/IEC TR 38505-2:2018*** *- Information technology - Governance of IT - Governance of Data - Part. 2*
Explora os papéis e responsabilidades no ecossistema de governança de dados, detalhando

como os princípios da ISO/IEC 38505-1 podem ser implementados. Fornece um guia prático para a definição de políticas, designação de responsabilidades e estabelecimento de processos.

***ISO/IEC TS 38505-3:2021*** *- Information Technology — Governance of Data — Part 3: Guidelines for Data Classification. Edição 1, 2021*
Apresenta orientações detalhadas para a classificação de dados, considerando aspectos como sensibilidade, valor e impacto organizacional. A norma ajuda a estabelecer critérios claros para proteger informações sensíveis, promovendo a consistência e a conformidade regulatória.

**NIST - National Institute of Standards and Technology**

O NIST, uma entidade americana reconhecida por estabelecer padrões técnicos e operacionais, também oferece contribuições valiosas para a governança de dados no setor público.

***NIST SP 800-188*** *- De-Identifying Government Datasets: Techniques and Governance*
Fornece orientações sobre técnicas de desidentificação de dados governamentais para proteger a privacidade e garantir o uso seguro de conjuntos de dados, destaca métodos como generalização, supressão e randomização para minimizar os riscos de reidentificação. Enfatiza a importância de um *framework* robusto para a supervisão de práticas de desidentificação, alinhando-se aos princípios de privacidade por design.

As normas ISO e NIST oferecem diretrizes complementares que podem ser adaptadas às necessidades do setor público. Enquanto as normas ISO se concentram em um escopo mais amplo de governança de TI e segurança da informação, o NIST traz especificidades técnicas úteis para o manejo de dados em ambientes governamentais. Elas fornecem frameworks sólidos para enfrentar os desafios da era digital, garantindo que os dados sejam tratados como ativos estratégicos e protegidos contra ameaças. A integração dessas diretrizes no ecossistema público brasileiro fortalecerá a capacidade institucional de gerenciar informações de forma ética, segura e eficiente.

Destaca-se que a coletânea de práticas internacionais não possui intenção de enumerar todas a práticas tampouco de recomendar organizações ou normas específicas em detrimento de outras, mas sim possui como objetivo identificar boas práticas internacionais que possam embasar as recomendações a serem elaboradas para consideração da ANPD na elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade.

## 5. PARECER CONCLUSIVO (Considerações finais/recomendações)

O trabalho desenvolvido pelo GT-4 ao longo de todo período analisado revelou um cenário diversificado quanto à governança de dados no setor público. Embora existam avanços significativos em algumas áreas, as diferenças de maturidade entre os níveis federal, estadual e municipal demonstram a necessidade de estratégias mais inclusivas e adaptadas às realidades locais bastante distintas.

Com efeito, ainda que se perceba um movimento em direção à orientação centralizada sobre o assunto na esfera federal, verifica-se uma atuação fragmentada e sem articulação institucional dos entes federativos. Não obstante existam bons exemplos de ações isoladas, não há um regramento unificado que trata das competências, atribuições e regras mínimas de atuação, muito embora o Ministério da Gestão e Inovação tem uma produção volumosa de materiais relevantes..

As entrevistas realizadas foram fundamentais para compreender as particularidades de cada nível e identificar desafios estruturais, boas práticas e soluções inovadoras que vêm sendo implementadas. Embora houvesse intenção de entrevistar representantes de todos níveis do Poder Executivo, as limitações de tempo e a busca por maior profundidade nas análises levaram à realização de entrevistas a partir da seleção de representantes estratégicos. Ainda assim, o GT-4 conseguiu capturar informações relevantes e detalhadas, podendo ser completadas futuramente com a inclusão de novos cenários e perspectivas.

A partir das análises e discussões, apresentam-se as recomendações para elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade, bem como recomendações para a atuação da ANPD no fortalecimento da governança de dados no setor público.

### Recomendações para a Política Nacional de Proteção de Dados Pessoais e Privacidade

A partir da análise realizada e as necessidades específicas do setor público brasileiro, para fins da Política Nacional de Proteção de Dados Pessoais e da Privacidade, em matéria de governança de dados pessoais, listamos abaixo uma coletânea de objetivos, princípios e diretrizes que sugerimos sejam incorporadas na política, ainda que em parte aplicáveis tanto para setor público como setor privado.

**Objetivos da Política**

Para fins da Política Nacional de Proteção de Dados Pessoais e da Privacidade, em matéria de governança de dados, entende-se que devem ser considerados os seguintes objetivos:

1. **Objetivo geral:** assegurar o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais.
2. **Objetivos específicos (relacionados à governança de dados):**
    a. contribuir para um governo orientado por dados que assegure a privacidade, proteção de dados pessoais e o compartilhamento adequado de dados pessoais;
    b. incentivar a educação em proteção de dados pessoais, fomentando o letramento digital e a inclusão digital, de modo a contribuir para a promoção da equidade e autodeterminação informativa;
    c. fomentar a cultura em proteção de dados pessoais, promovendo a sensibilização e conscientização para tratamento adequado destes dados pelo setor público;
    d. fortalecer a participação e o controle social no tratamento de dados;
    e. promover a transparência e a prestação de contas no tratamento de dados pessoais por organizações públicas e privadas.

**Princípios e Diretrizes norteadores da Política no que tange o Poder Público**

1. **Diretrizes para Governança de Dados Pessoais:** Estabelecimento de diretrizes para que organizações tenham políticas internas de governança de dados pessoais, incluindo definição de atribuições de competências individuais dentro da organização, considerando referências como a Portaria SGD/MGI nº 852/2023;

2. **Uso apropriado, ético e responsável dos dados**, considerando preceitos como a não discriminação; a inclusão social e digital; a promoção da confiança pública e a integridade da informação.

3. **Infraestrutura e arquitetura de dados:** Garantia de infraestrutura e arquitetura de dados adequados ao volume e à natureza dos dados tratados;

4. **Qualidade e Integridade dos Dados Pessoais**: Recomenda-se a adoção de medidas contínuas para assegurar a qualidade e integridade dos dados pessoais tratados pelo Poder Público, prevenindo e evitando erros e redundâncias que possam comprometer a confiabilidade das informações.

5. **Interoperabilidade dos dados pessoais:** é recomendável a promoção da interoperabilidade dos dados pessoais tratados pelo Poder Público, criando condições para a padronização e o compartilhamento seguro e eficiente entre diferentes órgãos e entidades, em conformidade com normas de proteção de dados e segurança da informação.

6. **Canais de Interface para Titulares:** Sugere-se que os órgãos públicos estabeleçam canais acessíveis, claros e eficientes para que os titulares de dados possam exercer seus direitos, como acesso, retificação, exclusão e portabilidade de informações.

7. **Capacitação e Sensibilização contínua:** recomenda-se a adoção de programas contínuos de capacitação para servidores e gestores públicos, com foco em segurança da informação, proteção de dados pessoais e governança de dados.

8. **Fomento a cooperação entre Entes Públicos:** O fomento de iniciativas a atuação integrada entre órgãos e entidades do poder público, de diferentes níveis, federal, estadual e municipal, para troca de experiências em implementação de política e práticas de governança, conforme Lei nº 14.129, de 29 de março de 2021[17];

9. **Medidas Técnicas e Administrativas:** Para garantir uma proteção robusta dos dados pessoais tratados pelo setor público, recomenda-se a implementação de medidas técnicas e administrativas eficazes que considerem o volume e a natureza dos dados tratados.

10. **Política de Governança de Dados:** orientação quanto a adoção de política de governança de dados contendo, desde regras para a coleta ao descarte de dados,, regras para manutenção e atualização constantes dos catálogos de dados e metadados, assim como critérios definidos para reuso de dados, buscando eficiência nos recursos públicos.

**Recomendações de Mandamentos e Obrigações**

1. **Criação de um Fórum Intergovernamental:** recomenda-se a criação de um fórum intergovernamental possivelmente coordenado pela ANPD, que possa funcionar como espaço para troca de experiências e materiais entre as instituições e fixação de boas práticas envolvendo os entes federais, estaduais e municipais. Uma possibilidade seria o

[17] http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm

secretariado pela Secretaria de Governo Digital (SGD), que já possui um vasto repertório de material relevante e poderia se aproveitar do Fórum como um locus de escoamento de inúmeros materiais de referência e de treinamento. O Fórum teria, em princípio, o objetivo de facilitar a troca de experiências e materiais entre as instituições, proporcionar capacitação contínua aos participantes.

2. **Desenvolvimento de ferramentas de Autoavaliação e Monitoramento:** Para que os órgãos públicos possam avaliar sua conformidade com as normas de proteção de dados e aprimorar suas políticas, recomenda-se a criação de ferramentas acessíveis de autoavaliação e monitoramento. Essas ferramentas devem permitir:
    a. A verificação do cumprimento das diretrizes da LGPD e outras normativas aplicáveis;
    b. A identificação de riscos e áreas que necessitam de melhorias;
    c. O acompanhamento contínuo da implementação das políticas de proteção de dados, buscando-se algum grau de harmonização nesta implantação;

    Sugere-se que essas ferramentas sejam desenvolvidas em formato digital, com interface intuitiva e de fácil usabilidade, garantindo que todos os órgãos e entidades possam utilizá-las de forma eficiente.

3. **Cooperação Estratégica:** Para aprimorar a implementação de políticas de proteção de dados nos diferentes níveis da Administração Pública, recomenda-se o incentivo ao estabelecimento de coordenações estratégicas, como por exemplo entre as Controladorias Gerais dos Estados e Municípios. Essas colaborações podem contribuir para o desenvolvimento de guias e orientações conjuntas sobre a aplicação da LGPD, além de possibilitar um monitoramento mais eficiente do cumprimento das normas pelos órgãos estaduais e municipais.

## Recomendações para a Autoridade Nacional de Proteção de Dados

Muito embora o objetivo inicial do Grupo de Trabalho tenha sido a elaboração de subsídios para a elaboração da Política Nacional de Privacidade e Proteção de Dados Pessoais, ao longo do processo de nossos estudos e especialmente das entrevistas realizadas para prover um diagnóstico, identificamos algumas recomendações que nos pareceram não seriam cabíveis em termos da Política propriamente dita mas que poderiam ser levadas a conhecimento da ANPD, para que a Autoridade as considere no âmbito de suas atividades.

Nesse sentido, abaixo elencamos algumas destas considerações e recomendações:

1. **Capacitação contínua e cooperação interinstitucional:** Sugere-se que a ANPD colabore com a Escola Nacional de Administração Pública (ENAP) e outras instituições como SGD/MGI e RNP/MCTI para oferecer cursos sobre proteção de dados pessoais. Além disso, seria importante organizar reuniões periódicas para discutir atualizações nas regulamentações e promover a troca de experiências e boas práticas.

2. **Desenvolvimento de cartilhas orientativas:** Recomenda-se que a ANPD crie um *toolkit* e cartilhas orientativas para apoiar a administração pública, fornecendo orientação sobre fluxos de segurança da informação e proteção de dados pessoais.

3. **Fortalecimento e clareza da função do Encarregado de Dados Pessoais no setor público:** Recomenda-se que a ANPD crie diretrizes claras para as funções e responsabilidades dos Encarregados de Dados Pessoais no setor público, endereçando sugestões de estruturas internas a serem adotadas. Além disso, sugere-se a criação de um canal institucional de suporte aos Encarregados, facilitando a troca de experiências e a resolução de dúvidas.

4. **Ações Colaborativas:** Sugere-se a promoção de colaborações com a sociedade civil, setor privado, terceiro setor e academia, criando um ambiente inclusivo e participativo para fortalecer a proteção de dados pessoais.

Dada a transversalidade do objeto regulado da LGPD, que é espelhado pela amplitude do escopo deste GT - governança de dados, a governança de dados no setor público é um elemento central para a proteção de dados pessoais e a conformidade com a LGPD. O trabalho desenvolvido pelo GT-4 permitiu mapear os principais desafios e oportunidades na estruturação de uma Política Nacional de Governança de Dados no Setor Público, enfatizando a importância de uma abordagem coordenada entre os entes federativos.

A implementação das recomendações apresentadas contribuirá para o fortalecimento da governança de dados, garantindo maior segurança jurídica, eficiência na gestão de informações e proteção dos direitos dos titulares. A articulação entre órgãos públicos, a capacitação contínua de servidores e o desenvolvimento de diretrizes claras são passos essenciais para consolidar um ecossistema de governança de dados eficaz e alinhado aos princípios da LGPD.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

## ANEXO 01: MAPEAMENTO PRELIMINAR DE SUBSÍDIOS

**Objetivo do Documento:** Identificar materiais que possam embasar estudos para subsidiar a elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade, com foco na governança de dados pessoais no setor público. Os objetivos específicos são:

(i) identificar materiais relevantes em cada uma das seções abaixo (práticas nacionais, práticas de outras jurisdições, práticas de entidades normativas, práticas de organizações internacionais e material acadêmico);
(ii) avaliar se há material significativo para a elaboração de estudos em cada uma das seções; e
(iii) com base na decisão de elaborar um estudo para uma determinada seção, realizar a leitura do material encontrado a fim de determinar a estrutura do estudo e desenvolvê-lo.

### 1. Práticas Nacionais

| nº | Referência | Autor | Relevância | Link |
|---|---|---|---|---|
| 1 | Levantamento - Políticas públicas Nacionais Referência | CNPD | Será necessário avaliar de que forma a seção de governança de dados pessoais interage com: (i) o DECRETO Nº 8.777, DE 11 DE MAIO DE 2016, que institui a Política de Dados Abertos do Poder Executivo federal; e (ii) o DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da | https://docs.google.com/spreadsheets/d/1kKfRoYteb4Kjpdg5MZaMCrUVscH6JmPrJpr6voD_xvk/edit?usp=sharing |

| | | | | |
|---|---|---|---|---|
| | | | informação. | |
| 2 | Resolução CD/ANPD nº 20 de 3 de outubro de 2024 - Institui a Política Interna de Proteção de Dados Pessoais da Autoridade Nacional de Proteção de Dados - ANPD. | ANPD | É possível aproveitar os seguintes pontos da Resolução (com ajustes ao âmbito de aplicação): (i) objetivos; (ii) princípios e diretrizes; (iii) regras para o tratamento de dados pessoais; (iv) direitos dos titulares (v) conscientização e capacitação; e (v) penalidades. | https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-20-de-3-de-outubro-de-2024-588653756 |
| 3 | Cartilha de Governança de Dados - Poder Executivo Federal - Volume 1 - Conceitos Iniciais | Ministério da Economia | Traz: (i) definição de governança de dados; (ii) instrumentos legislativos relativos sobre gestão de dados; e (iii) traz potenciais referências para consideração. | https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/forum-governanca-de-dados/cartilha-de-governanca-de-dados-volume1-8-12.pdf |
| 4 | Cartilha de Governança de Dados - Poder Executivo Federal - Volume II Ecossistema de Dados do Poder Executivo Federal | Ministério da Gestão e da Inovação em Serviços Públicos | | https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcoss |

| | | | | |
|---|---|---|---|---|
| | | | | istemadeDados.pdf |
| 5 | Cartilha de Governança de Dados - Poder Executivo Federal - Volume III Papéis e responsabilidades de Governança de Dados no Poder Executivo Federal | Ministério da Gestão e da Inovação em Serviços Públicos | Pode: (i) elucidar a interação de atores da LGPD com outros atores de um ecossistema maior de governança de dados; e (ii) trazer potenciais referências para consideração . | https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhaGovDadosvol3.pdf |
| 6 | Decreto nº 10.046, de outubro de 2019 | | Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. | https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm |
| 7 | Acórdão 390 | TCU | | https://drive.google.com/file/d/1KKUjOtaCX2shzQIsK-DQ4VHWeDRH08Iz/view?usp=drive_link |
| 8 | Guia de Elaboração de Programa de Governança em Privacidade | Ministério da Gestão e da Inovação em Serviços Públicos | | https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf |

## 2. Práticas de Entidades Normativas

| nº | Norma | Título | Descrição | Link |
|---|---|---|---|---|
| 1 | ISO 8000-51:2023 | Data Quality - Part 51: Data governance: Exchange of data policy statements. Edição 1, 2023 | Estabelece requisitos para a governança de qualidade de dados e a troca de declarações de políticas de dados. Aplicável à estruturação de governança e qualidade no plano. | https://www.iso.org/standard/78708.html |
| 2 | ISO/IEC 38505-1:2017 | Information technology - Governance of IT - Governance of Data- Part 1: Application of ISO/IEC 38500 to the governance of data | Fornece princípios e diretrizes para a governança de dados, integrando-os à governança de TI, alinhado a gestão de dados aos objetivos estratégicos da organização | https://www.iso.org/standard/56639.html |
| 3 | ISO/IEC TR 38505-2:2018 | Information technology - Governance of IT - | Complementa a parte 1, oferecendo abordagens práticas para a implementação das diretrizes de governança de dados. | https://www.iso.org/standard/70911.html |

| nº | Norma | Título | Descrição | Link |
|---|---|---|---|---|
| | | Governance of Data - Part. 2 | | |
| 4 | ISO/IEC TS 38505-3:2021 | Information Technology - Governance of Data - Part 3: Guidelines for Data Classification. Edição 1, 2021 | Fornece diretrizes para a classificação de dados, ajudando as organizações a categorizar e proteger informações de maneira adequada | https://www.iso.org/standard/70911.html |
| 5 | ISO/IEC 27001:2022 - (antes ISO 27001:2013) | Information Security Management System | Define requisitos para um sistema de gestão de segurança da informação sob o programa de governança de TI. Apresentando áreas críticas com nível de maturidade da governança de dados. | https://www.iso.org/standard/27001#amendment |
| 6 | ISO/IEC 15944-17:2024 | Part 17 Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space | Aborda a aplicação de Privacy by Design (PbD) em transações comerciais e a proteção de dados pessoais dentro do contexto de trocas eletrônicas de informações. Ela fornece diretrizes e boas práticas para implementar princípios de privacidade em transações comerciais, com foco na conformidade de proteção de dados pessoais e governança, tanto para organizações | https://www.iso.org/obp/ui/en/#iso:std:iso-iec:15944:-17:ed-1:v1:en |

| nº | Norma | Título | Descrição | Link |
|---|---|---|---|---|
| | | context | privadas quanto para o setor público. | |
| 7 | NIST SP 800-188 | De-Identifying Government Datasets: Techniques and Governance | Publicado em setembro de 2023, fornece diretrizes para desidentificação de conjuntos de dados governamentais, reduzindo riscos de privacidade enquanto mantém a utilidade para análise. Aborda técnicas, como remoção de identificadores e geração de dados sintéticos, e recomenda práticas de governança. | https://csrc.nist.gov/pubs/sp/800/188/final |
| 8 | ISO/IEC 27002/2022 (antes ISO/IEC 27002:2013) | Information security, cybersecurity and privacy protection — Information security controls | | https://www.iso.org/standard/75652.html |

3. **Práticas de Organizações Internacionais**

| nº | Referência | Autor | Link |
|---|---|---|---|
| 1 | Good Practice Principles for Data Ethics in the Public Sector | OCDE | caa35b76-en.pdf (oecd-ilibrary.org) |

| | | | |
|---|---|---|---|
| 2 | The Path to Becoming a Data-Driven Public Sector | OCDE | The Path to Becoming a Data-Driven Public Sector \| OECD Digital Government Studies \| OECD iLibrary (oecd-ilibrary.org) |
| 3 | Recommendation of the Council on Digital Government Strategies | OCDE | OECD Legal Instruments |
| 4 | Relatório de desenvolvimento mundial 2021 | Worldbank | World Development Report 2021: Data for Better Lives \| Governing data (worldbank.org) https://www.worldbank.org/en/publication/wdr2021 |

# ANEXO 02: RELATO DAS ENTREVISTAS

## 1. Visão Geral

O Conselho Nacional de Proteção de Dados (CNPD), como órgão consultivo de apoio à Autoridade Nacional de Proteção de Dados (ANPD), garante a participação do setor empresarial, da academia e de representantes governamentais nas discussões, nos avanços normativos e na política pública de proteção de dados e privacidade no Brasil. O Grupo de Trabalho nº 4 tem como objetivo fornecer subsídios relacionados à Governança de Dados no setor público para elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade.

Neste contexto, o GT 4 realizou entrevistas nas esferas federal, estadual e municipal do poder executivo, com intenção de fazer um diagnóstico sobre o tema, captando diferentes perspectivas, identificar desafios e coletar boas práticas, considerando as diferentes esferas de governo. Além disso, realizou também entrevista com representantes do Poder Judiciário, buscando uma compreensão mais ampla. Este documento apresenta um breve relato de cada entrevista, com a identificação de temas relevantes para as próximas etapas.

## 2. Relato das Entrevistas

### Ministério da Gestão e da Inovação em Serviços Públicos (MGI)

No dia 11 de novembro de 2024, o GT 4 reuniu-se com representante do MGI, ocasião em que foi realizada uma apresentação sobre a “Base de Dados do Brasil” e a Infraestrutura Nacional de Dados.

Durante a apresentação, destacou-se que o conceito de infraestrutura nacional de dados vai além da noção de estrutura física, fazendo referência a um conjunto de elementos: (i) Qualidade: acurácia, tempestividade, completude; (ii) Interoperabilidade: integração, referências, API; (iii) Inteligência e conhecimento: Análise, estatísticas, projeções, painel gerencial; (iv) Catalogação: descoberta dos dados, categorização; (v) Ambiente tecnológico: nuvem do governo, nuvem pública, *on premisses*; (vi) Segurança: disponibilidade, integridade, confidencialidade; e (vii) Privacidade e todos os princípios de proteção de dados pessoais. **O elemento que conecta todas essas dimensões do ecossistema é a Governança, definida**

**como o estabelecimento de papéis e responsabilidades.** O modelo foi inspirado no modelo Dama-DMBoK[18].

O entrevistado apresentou exemplos práticos na área social, afirmou que o sistema de consulta do passe livre ilustra a interoperabilidade entre as diferentes bases de dados para concessão de benefícios. No caso do passe livre, é feita uma consulta no BPC e se já houver a confirmação, não precisa buscar o dado nas outras bases. Então é feita consulta de identidade, no eSocial, no CadÚnico para entender se o indivíduo tem direito por ser baixa renda ou não. Esse modelo também é aplicável a outros programas, como Bolsa Família, ID Jovem e Pé de Meia.

Outro ponto abordado foi o papel central da Governança de Dados no novo Decreto de Política de Governança de Dados, que ainda passará por consulta pública, prevê a seguinte estrutura:

- **Governança Central:** O Ministério da Gestão e Inovação (MGI) será o Gestor da Política e responsável por prover plataformas (como gov.br), apoiar órgãos na implementação, promover o aculturamento e realizar monitoramento.
    - Decreto da Política
    - Conselho Normatizador

- **Governança Interna do Órgão Implementador:** Programa de governança interna e designação dos papéis

- **Controle:** CGU  e TCU em um papel de auditoria
    - Fiscalizações, recomendações e determinações

Além disso, a apresentação mencionou que a Estratégia Nacional de Governo Digital, derivação da Lei do Governo Digital, é uma política de locus federal que oferece diretrizes para que os entes federativos desenvolvam estratégias próprias, definindo de maneira autônoma o conjunto de ações. O MGI entende que o arcabouço normativo federal servirá de inspiração para os demais poderes.

Por fim, destacou-se a criação de novas figuras estratégicas no decreto, como o "Executivo de Dados", que atuará em uma estrutura composta por curadores de negócios e áreas de TI. Observou-se que a maturidade dos órgãos públicos brasileiros ainda está em desenvolvimento, baseando-se no modelo do Reino Unido que vai de 1 a 5 (Auto diagnóstico do SISP)[19], no qual o Brasil ainda não alcançou o nível máximo (5).

[18] https://www.dama.org/cpages/body-of-knowledge
[19] https://www.gov.br/governodigital/pt-br/noticias/brasil-fortalece-parceria-com-reino-unido-na-transformacao-digital-do-setor-publico

## Prefeitura do Rio de Janeiro

No dia 18 de novembro de 2024, membros do GT 4 se reuniram com representante com atuação relevante em dados pessoais da Prefeitura do Rio de Janeiro, onde foram apresentados os principais avanços e desafios enfrentados no âmbito da proteção de dados no município, com destaque para o Decreto Rio 52.984/2024[20] que institui o Programa Municipal de Proteção de Dados Pessoais.que organiza a política municipal em cinco eixos:

> (i) Índice de Avaliação de Maturidade: consiste em uma ferramenta para medir o nível de adequação dos órgãos municipais, inspirada na avaliação aplicada pela CGU;
> (ii) Gerenciamento de riscos: Identificação e mitigação de riscos no tratamento de dados;
> (iii) Normalização e Conformidade contratual: a partir da elaboração e revisão de normativos, contratos e convênios com foco na conformidade, em colaboração com a Procuradoria dos Municípios;
> (iv) Instrumentos de Governança: criação de diretrizes e modelos[21];
> (v) Capacitação e sensibilização: Formação de agentes municipais, identificado como um desafio pela entrevistada

Quanto à governança de dados, a Prefeitura do Rio de Janeiro adota uma abordagem descentralizada, onde cada secretaria é considerada um controlador público individual. O modelo foi escolhido devido à complexidade organizacional do município e inspirado na experiência do Distrito Federal. Além disso, desde agosto de 2024 foi instituída a figura do encarregado central que coordena a rede de encarregados setoriais, ao todo, a Prefeitura do Rio possui 90 ao total, 55 órgãos e entidades municipais, sendo que 96% já possuem encarregados.

A entrevistada destacou a atuação do Fórum de Proteção de Dados dos Municípios[22], apoiado pela Frente dos Prefeitos, no qual a Prefeitura do Rio exerce o mandato representado por ela. No fórum, alguns municípios discutem a formação de consórcios intermunicipais para compartilhar a função do encarregado. A iniciativa considera a restrição de recursos.

Além disso, a entrevistada trouxe pontos de desafios e ambiguidades:

- **Controlador na Administração Pública:** a entrevistada pontuou a ambiguidade do texto da LGPD que gera confusão sobre a figura do controlador público. Citou o Guia da ANPD, que reconhece a descentralização administrativa, mas mantém a responsabilidade final na pessoa jurídica.

[20] https://lgpd.prefeitura.rio/wp-content/uploads/sites/102/2024/09/Decreto-Rio-54984_2024-2.pdf
[21] https://lgpd.prefeitura.rio/wp-content/uploads/sites/102/2023/03/Resolucao-91-SEGOVI.PGPPDP.pdf
[22] https://municipioslgpd.com.br/

- **Modelos simplificados:** Defendeu a necessidade de modelos simplificados para o setor público, argumentando que os modelos atuais, como os baseados na ISO, são excessivamente complexos e inviáveis para muitos municípios. Sugerindo, no mínimo, uma lista de elementos básicos para orientar a conformidade.

    - A prefeitura do Rio possui modelos e instrumentos que estão disponíveis no site da Prefeitura do Rio, incluindo a lista de encarregados e orientações para os cidadãos, como os fornecidos pela Subsecretaria de Proteção de Dados (exemplo: site de LGPD da Prefeitura do Rio)

- **Necessidade de capacitação:** Identificou uma lacuna na capacitação de agentes públicos, destacando a ausência de cursos voltados especificamente para o setor público. Ressaltou que a ANPD deveria assumir um papel mais ativo nesse aspecto.

Por fim, enfatizou que não há um único modelo ideal de governança de dados, mas sim a necessidade de flexibilidade para atender às diferentes culturas organizacionais e estruturas administrativas, respeitando o pacto federativo. Sugeriu que uma política nacional de proteção de dados para o setor público poderia contribuir para uniformizar critérios mínimos e apoiar estados e municípios.

## Empresa de Informática do Governo do Estado de São Paulo (Prodesp)

No dia 19 de novembro, membros do GT 4 se reuniram com representante da Prodesp (Companhia de Processamento de Dados do Estado de São Paulo). Na ocasião foram abordados desafios e avanços na gestão e governança de dados do Estado de São Paulo, com destaque para a segurança da informação e integração de dados.

O entrevistado iniciou explicando que a nível federal, a gestão de dados é marcada pela pulverização de infraestruturas. Apenas na Esplanada dos Ministérios existem cerca de 130 data centers, e empresas públicas como Dataprev e Serpro que são responsáveis pela gestão de dados de órgãos como INSS e Receita Federal. Para enfrentar os problemas de eficiência, surgiu o projeto da Nuvem Soberana que busca centralizar e integrar os dados no âmbito Federal.

No Estado de São Paulo, o cenário é diferente, com a criação da Central de Dados do Estado de São Paulo (CDE/SP), instituída pelo Decreto 64.790/2020, que atua como repositório centralizado para bases de dados estaduais. Esse repositório centralizado reúne atualmente 130 bases de dados, promovendo maior eficiência e áreas específicas como Fazenda e Polícia Militar permanecem com estruturas independentes, mas considera que a centralização tem facilitado a

gestão de dados e a extração de informações para políticas públicas e serviços. A Prodesp tem focado na catalogação, classificação e análise dessas bases, criando uma infraestrutura que permita informações de qualidade. Apesar disso, observou-se que essa integração ainda não ocorre de maneira uniforme no âmbito federal e praticamente inexistente nos municípios.

O cenário municipal é mais desafiador devido à falta de infraestrutura básica, segurança e maturidade em governança de dados. André, como representante da ABEP-TIC (Associação Brasileira de Empresas Públicas de Tecnologia), destacou que poucos municípios possuem condições de enfrentar essas demandas. Para mitigar essa realidade, a Prodesp tem implementado o programa Cidades SP, que oferece suporte básico, como digitalização de documentos, gestão de processos e soluções na nuvem. Contudo, ele ressaltou que a adoção de soluções em nuvem, embora necessária, pode gerar preocupações com custos crescentes devido ao aumento exponencial de dados e tecnologias emergentes, como inteligência artificial. André defendeu a necessidade de uma análise cuidadosa para garantir a sustentabilidade desse modelo.

Quanto aos desafios com Infraestrutura de Dados, embora a centralização seja um avanço, a integração de sistemas e a governança ainda são pontos críticos. Muitos benefícios sociais eram geridos por planilhas, sem governança adequada. Para solucionar isso, foi criada uma Gerência de Arquitetura de Dados, permitindo organizar e integrar bases como o CADÚnico e o IRGD. Hoje, a Prodesp opera o CDE/SP, promovendo políticas de catalogação e segurança. Após incidentes cibernéticos, como os ataques à Sabesp e à CPTM, a Prodesp intensificou investimentos em camadas de proteção e planos de recuperação de desastres. A partir disso, foram criadas políticas de acesso restrito a dados e sistemas de controle para ambientes de teste e homologação.

No Estado de São Paulo, o Comitê Gestor de Governança de Dados, do qual a Prodesp faz parte, é responsável por deliberar sobre o compartilhamento de dados e estabelecer os termos em que isso deve ocorrer. Ele atua como a entidade central de governança de dados no estado. A Governança em termos de proteção de dados ainda está em fase inicial, tendo em vista a nomeação de encarregados para cada entidade, essa prática ainda está em fase inicial no estado. A Prodesp avalia a possibilidade de oferecer serviços de *DPO as a service* para entidades que não possuem recursos ou maturidade suficientes.

Internamente, a Prodesp criou uma gerência dedicada à privacidade e proteção de dados, responsável pela implementação de políticas internas e pela promoção de iniciativas de aculturamento. Esse modelo está sendo replicado em outras entidades, embora ainda de forma incipiente. Quanto às normas e frameworks utilizados, a Prodesp utiliza normas de entidades normativas para a governança e proteção de dados, mas André não soube especificar quais normas são aplicadas no momento.

## Secretaria de Tecnologia da Prefeitura de Recife

No dia 19 de novembro de 2024, membros do GT4 se reuniram com representantes da Secretaria de Tecnologia da Prefeitura de Recife. A entrevista abordou as estratégias e iniciativas de governança de dados do município, com ênfase na adequação à Lei Geral de Proteção de Dados (LGPD) e nos desafios e avanços no uso de dados para políticas públicas.

Foi apresentada a estratégia robusta em desenvolvimento para aprimorar a governança de dados no município. Um dos marcos da iniciativa é a conclusão iminente da Política Nacional de Governança de Dados, que integrará aspectos da LGPD, consolidando esforços de proteção e utilização eficiente das informações municipais. Um dos desafios enfrentados está relacionado à organização e padronização dos dados, identificados como pilares fundamentais para a digitalização de serviços, automação de processos e análises de políticas públicas baseadas em evidências. Por isso, a administração municipal optou por um reposicionamento estratégico, priorizando a construção de uma base de dados mais robusta e integrada. Entre as ações-chave, destacam-se:

- **Diagnóstico de Maturidade de dados:** levantamento abrangente aplicado às secretarias municipais, avaliando os pilares de governança, qualidade, capacidade técnica, uso, transparência e segurança.
- **Estruturação de governança:** a criação de um comitê de governança de dados, que substitui o Conselho de Transformação Digital, reunindo secretarias estratégicas como Controladoria, Planejamento, Ciência e Tecnologia e Centro de Operações do Recife (COP)
- **Padronização de dados:** publicação de minuta detalhada, com orientações para uniformizar campos como CPF, endereço, raça, para garantir a interoperabilidade entre sistemas. Acompanhada de oficinas itinerantes de capacitação de servidores.

A política se organiza em seis eixos principais: (i) Governança: estabelecimento de estruturas formais para gestão de dados; (ii) Qualidade: padronização de dados para permitir cruzamentos eficientes; (iii) Capacidade: reforço técnico e operacional das equipes envolvidas; (iv) Transparência: extensão do Portal da Transparência, com foco na experiência do usuário; (v) Definição de protocolos claros e aderentes à LGPD; e (vi) Segurança: implementação de certificações e medidas preventivas contra ameaças digitais.

A estratégia também inclui a criação de uma **sala de situação de indicadores**, voltadas para análises integradas e o **Farol**, uma página interna que centraliza informações sobre políticas públicas, programas e recursos municipais. Um piloto bem sucedido foi realizado na Secretaria da Mulher, com possível escalabilidade do modelo para outras áreas.

Foi destacado que a abordagem adotada em Recife é replicável, com adaptações mínimas para atender às particularidades locais de outros municípios. Além disso, a experiência acumulada pela Prefeitura foi enriquecida por projetos de aceleração como o da Bloomberg e agora serve de referência para cidades como Fortaleza.

Outro ponto mencionado foi sobre o processo de adequação à Lei Geral de Proteção de Dados (LGPD) da Prefeitura de Recife, iniciada em 2021 e liderado pela Controladoria. Após identificar práticas dispersas e possíveis vulnerabilidades nos portais municipais, foi realizada uma revisão emergencial de plataformas como o Portal da Transparência e o Portal de Compras para garantir a conformidade com a legislação. Como principais ações:

- **Capacitação de Servidores:** Produção de uma cartilha[23] com perguntas e respostas práticas para conscientizar os servidores públicos. Posteriormente, capacitações específicas foram realizadas para encarregados e ampliadas para alcançar mais setores.
- **Modelo Descentralizado:** Implementação de um modelo no qual cada secretaria designa um encarregado e assume a responsabilidade como controlador. A lista de encarregados foi publicada no Portal da Transparência e compartilhada com a ANPD[24].
- **Política Municipal de Proteção de Dados:** Criação de uma política que instituiu um conselho gestor e um grupo de trabalho para assessorar as ações de governança de dados.

A Prefeitura consultou práticas de outras cidades e participou de fóruns nacionais para ajustar seu modelo. Optou por contratar uma consultoria para fortalecer suas iniciativas. Um novo marco normativo, previsto para 2025, integrará proteção de dados pessoais, dados abertos e transformação digital.

O entrevistado afirmou que um dos maiores desafios na temática é conseguir organizar os dados, tentando chegar a uma estrutura de “mercado perfeito”, em termos de organização e interoperabilidade de dados, reconhecendo que padrões perfeitos são utópicos. Entretanto, ressaltou a importância de criar uma base funcional atualizada, como foi alcançada durante a pandemia por meio da vacinação digital, iniciativa onde houve o cadastro digital dos cidadãos para vacinação. Contudo, o desafio atual é manter a base de dados funcional, sem depender de outro evento extraordinário.

[23] https://www2.recife.pe.gov.br/sites/default/files/cartilha_lgpd_2022.pdf
[24] https://transparencia.recife.pe.gov.br//codigos/web/estaticos/estaticos.php?nat=TRA#filho

O entrevistado sugeriu que o Governo Federal assumisse o papel de base de dados central, integrando e disponibilizando informações para Estados e Municípios. Na prática, não atua dessa forma e acaba competindo na entrega de serviços já realizados pelos municípios, dificultando a interoperabilidade e eficiência operacional. Ele pontuou que essa mudança é essencial para operacionalizar serviços na ponta e garantir maior eficiência nas entregas de políticas públicas.

Por fim, apresentou o conceito de **"Governo Zero Cliques",** uma abordagem que inverte a lógica tradicional de solicitação de serviços. Nesse modelo, o governo automaticamente garante os direitos dos cidadãos. Por exemplo, ao completar 60 anos, o cidadão recebe automaticamente mensagens de felicitações acompanhadas de sua credencial para transporte público ou estacionamento, eliminando a necessidade de solicitação.

### Tribunal Superior Eleitoral (TSE)

No dia 18 de novembro de 2024, o GT 4 entrevistou representante do TSE, para coletar subsídios sobre os desafios e boas práticas na governança de dados no setor público. Tatiana destacou a complexidade devido a diversidade de estruturas e diferentes níveis de maturidade entre os órgãos, e entende ser necessário oferecer capacitação em diferentes níveis para conscientizar as áreas responsáveis.

A entrevistada afirmou que devido à burocracia e à falta de recursos nos órgãos públicos, muitas unidades enfrentam dificuldade na implementação de políticas de governança eficazes, especialmente na integração de conceitos técnicos e jurídicos. Ressaltando a necessidade de direcionamentos claros e replicáveis, tendo em vista que a LGPD define o que deve ser feito, mas não como. Neste contexto, sugeriu a realização da tradução de conceitos técnicos e jurídicos, como os das Normas ISO e NIST em diretrizes práticas para aplicação no setor público;

A entrevistada, entende ser interessante implementar auditorias internas como mecanismo de avaliação contínua, para avaliar a adequação e a proteção de dados nos órgãos públicos. Alguns órgãos estão mais avançados, como o TRE-Paraná, que criou equipes de apoio ao encarregado de proteção de dados, permitindo maior profundidade na implementação da LGPD.

Entende que a segurança da informação não deve ser limitada à TI. É um conceito mais amplo, essencial para a proteção de dados sensíveis e a continuidade dos serviços públicos. Assim, entende que a Política deve contemplar a estruturação dos temas: Governança de Dados, Segurança da Informação e Proteção de Dados Pessoais.

**Papel do Encarregado de Dados:**

- No TSE, a Ouvidoria desempenha papel da unidade encarregada de proteção de dados. No entanto, o papel se limita a uma função de "ponte", intermediando comunicações, sem autonomia técnica ou capacidade operacional. Afirmou que o ideal seria que o encarregado deveria contar com uma equipe técnica de apoio, especializada no tema;
- **Descentralização da função:** Defendeu que o encarregado não precisa ser centralizado em uma única pessoa. Dependendo da estrutura do órgão, pode haver auxiliares técnicos em áreas como TI ou gestão documental, complementando o trabalho do encarregado.
    - Citou o TRE-Paraná como referência por criar equipes de apoio ao encarregado, permitindo uma implementação mais robusta e eficaz da LGPD. Essas equipes são compostas por pessoas que auxiliam diretamente no cumprimento das responsabilidades do encarregado.

## Autoridade Nacional de Proteção de Dados (ANPD)

No dia 04 de fevereiro de 2025, o GT-4 entrevistou representante da ANPD. Durante a entrevista, o entrevistado abordou diversos tópicos importantes relacionados à segurança da informação e à proteção de dados pessoais. Foi destacada a disparidade de maturidade entre as esferas federal, estados e municípios mencionada na pesquisa do Nic.br sobre privacidade[25] e a importância da Autoridade Nacional de Proteção de Dados (ANPD) nesse contexto. O entrevistado acredita que a ANPD desempenha um papel crucial e desafiador pois mesmo que adote uma abordagem responsiva, eventualmente terá que abrir processos de fiscalização.

Também foi discutida a necessidade de separar governança e gestão, sugerindo que a ANPD deveria focar na governança enquanto outra entidade cuidaria da gestão. Atualmente essa função é em parte exercida pela SGD, ao menos no âmbito da administração pública federal. Enfatizou que, embora sejam distintos, a segurança da informação não pode ser discutida sem considerar a proteção de dados, mencionando o artigo 49 da LGPD como um auxílio nesse aspecto.

Outro ponto abordado foi a ausência de uma autoridade central para a segurança da informação, com diferentes entidades cuidando de aspectos distintos, o que dificulta a criação de um ambiente seguro. O entrevistado acredita que a ANPD tem um papel de conscientizar sobre a proteção de dados pessoais, mas que precisa ser complementado por alguém de dentro, como a Secretaria de Governo Digital (SGD).

[25] https://nic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf

Ele também mencionou a importância de criar indicadores para aferição da maturidade dos diferentes entes. Também foi destacada a demanda por cursos na Escola Nacional de Administração Pública (Enap) e os desafios enfrentados pelo setor público em termos de segurança da informação e proteção de dados. Foi levantada a ideia de uma possível parceria entre a ANPD e a Enap para desenvolver e oferecer cursos específicos sobre segurança da informação e proteção de dados pessoais.

Foi discutida também a necessidade de gerar demanda que leve à ação e a importância de pensar em ferramentas de autoavaliação, monitoramento e rankings para melhorar a a aplicação efetiva da LGPD. Essas ferramentas permitiriam que os órgãos públicos avaliem seu próprio desempenho e identifiquem as áreas de melhoria.

Por fim, foi destacada a capacidade de investimento como um ponto crucial, mencionando que todos os órgãos públicos vão precisar de recursos financeiros para implementar soluções de larga escala. Foi mencionada a dificuldade de criar um ambiente seguro no setor público devido à falta de uma autoridade central e a necessidade de padrões e elementos que possam sobreviver a mudanças de governo.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

## ANEXO 03: TABELA DE ANÁLISE DAS ENTREVISTAS

| | Fonte/Entrevista | Nivel | Categoria | Problemas/ Desafios identificados | Ações/Boas Práticas | Avanços Realizados | Tendencias/Padrões |
|---|---|---|---|---|---|---|---|
| 2 | Executivo | Federal | Capacitação | Maturidade dos órgãos públicos brasileiros ainda em desenvolvimento | MGI promove o aculturamento e apoio técnico por meio de plataformas como gov.br. | Criação da figura do "Executivo de Dados" para liderar ações técnicas e estratégicas. | Necessidade de qualificação contínua para órgãos implementadores. |
| 3 | Executivo | Federal | Governança | Governança de dados limitada em órgãos de menor maturidade. | Criação de programas internos de governança nos órgãos implementadores. | Estrutura definida com Governança Central, Conselho Normatizador e Controle por CGU e TCU. | Governança centralizada como elemento conector do ecossistema. |
| 4 | Executivo | Federal | Interoperabilidade | Integração entre sistemas ainda em estágio inicial em diversos níveis de governo. | Exemplo do sistema de consulta do passe livre como modelo de interoperabilidade. | Integração entre bases como BPC, eSocial e CadÚnico para programas sociais. | Uso de APIs e integração de bases para eficiência nos serviços públicos. |
| 5 | Executivo | Federal | Segurança | Garantir confidencialidade e integridade dos dados em diferentes plataformas (nuvem pública e privada). | Estabelecimento de princípios de proteção de dados, como confidencialidade e integridade. | Elementos de segurança como pilares do ecossistema, incluindo nuvens públicas e privadas. | Segurança como prioridade no arcabouço de governança de dados. |
| 6 | Executivo | Federal | Recursos Financeiros | Pouca menção direta, mas dependência de recursos para implementar sistemas robustos. | Estruturação de controle por CGU e TCU para monitorar implementação e uso de recursos. | Suporte normativo para direcionar recursos, com inspirações no modelo federal para outros níveis. | Alinhamento normativo para otimizar recursos e melhorar maturidade. |
| 7 | Executivo | Federal | Tecnologia | Adoção de tecnologias como nuvens públicas e privadas ainda é limitada em alguns setores. | Estratégia Nacional de Governo Digital oferece diretrizes para o uso de tecnologias inovadoras. | Infraestrutura Nacional de Dados com elementos como catalogação, qualidade e inteligência para análise e projeções. | Crescente utilização de soluções tecnológicas integradas e padronizadas. |
| 8 | Executivo | Municipal | Capacitação | Lacuna na formação de agentes públicos para o setor público. | Criação de programas de capacitação e sensibilização para agentes municipais. | 96% dos órgãos municipais do Rio de Janeiro possuem encarregados nomeados, coordenados por um encarregado central. | ANPD deve assumir um papel mais ativo na capacitação. |
| 9 | Executivo | Municipal | Governança | Ambiguidade sobre a figura do controlador público na LGPD. | Abordagem descentralizada, com cada secretaria atuando como controlador público individual. | Rede de encarregados setoriais coordenada por um encarregado central. | Necessidade de flexibilidade para modelos de governança adaptados a realidades locais. |
| 10 | Executivo | Municipal | Interoperabilidade | Nenhuma referência direta neste relato. | Ferramentas como o Índice de Avaliação de Maturidade para mensurar a adequação dos órgãos. | Fórum de Proteção de Dados dos Municípios promove a discussão de consórcios intermunicipais para compartilhar recursos e responsabilidades. | Uniformização de critérios mínimos em nível nacional para promover integração. |
| 11 | Executivo | Municipal | Segurança | Identificação e mitigação de riscos no tratamento de dados. | Gerenciamento de riscos como eixo principal da política municipal. | Criação de instrumentos de governança e modelos disponíveis no site da Prefeitura do Rio para auxiliar na conformidade e segurança. | Incentivo a modelos simplificados que orientem a conformidade e a proteção. |
| 12 | Executivo | Municipal | Recursos Financeiros | Restrição de recursos nos municípios menores para a implementação da LGPD. | Proposta de consórcios intermunicipais para compartilhar funções e recursos de encarregado. | Fórum de Proteção de Dados dos Municípios liderado pela Frente dos Prefeitos como instância de apoio e colaboração. | Compartilhamento de recursos como solução para limitações financeiras. |

Tabela_1

| | Fonte/Entrevista | Nivel | Categoria | Problemas/ Desafios identificados | Ações/Boas Práticas | Avanços Realizados | Tendencias/Padrões |
|---|---|---|---|---|---|---|---|
| 12 | Executivo | Municipal | Recursos Financeiros | Restrição de recursos nos municípios menores para a implementação da LGPD. | Proposta de consórcios intermunicipais para compartilhar funções e recursos de encarregado. | Municípios liderado pela Frente dos Prefeitos como instância de apoio e colaboração. | Compartilhamento de recursos como solução para limitações financeiras. |
| 13 | Executivo | Municipal | Tecnologia | Complexidade de modelos atuais, como os baseados na ISO, dificulta a implementação. | Desenvolvimento de listas básicas de conformidade e diretrizes práticas. | Modelos e instrumentos disponíveis online para orientação e suporte ao público e agentes municipais. | Simplicidade e acessibilidade nos modelos como tendência para pequenos municípios. |
| 14 | Executivo | Estadual | Governança | Governança em proteção de dados ainda em fase inicial no estado. | Criação do Comitê Gestor de Governança de Dados em SP, responsável pelo compartilhamento de dados. | Nomeação de encarregados em entidades estaduais. | Uso de gerências dedicadas para coordenar ações de governança e privacidade. |
| 15 | Executivo | Estadual | Interoperabilidade | Integração inconsistente no âmbito federal e inexistente nos municípios. | Criação da Central de Dados do Estado de SP (CDE/SP) para centralizar bases estaduais. | Integração de bases como CADÚnico e IRGD, promovendo políticas de catalogação e segurança. | Centralização como tendência para melhorar eficiência e acessibilidade. |
| 16 | Executivo | Estadual | Segurança | Vulnerabilidade de sistemas a ataques cibernéticos, como Sabesp e CPTM. | Investimentos em camadas de proteção e criação de políticas de controle para ambientes de teste e homologação. | Políticas de recuperação de desastres e acesso restrito implementadas na Prodesp. | Segurança fortalecida como pilar para continuidade dos serviços estaduais. |
| 17 | Executivo | Estadual | Recursos Financeiros | Custos crescentes de soluções em nuvem e tecnologias emergentes, como IA. | Programa Cidades SP oferece suporte básico, como digitalização de documentos e gestão de processos. | Apoio a municípios com baixa maturidade por meio do programa Cidades SP. | Sustentabilidade de modelos emergentes é uma prioridade em desenvolvimento. |
| 18 | Executivo | Estadual | Tecnologia | Pulverização de infraestruturas federais com 130 data centers na Esplanada. | Desenvolvimento da Nuvem Soberana como estratégia para centralização de dados federais. | Uso de tecnologias como digitalização, nuvens públicas e privadas para ampliar acessibilidade e eficiência. | Crescimento da adoção de IA e digitalização para melhorar processos. |
| 19 | Executivo | Municipal | Governança | Necessidade de maior organização e padronização de dados. | Criação de um Comitê de Governança para substituir o Conselho de Transformação Digital. | Diagnóstico de maturidade abrangente aplicado às secretarias municipais. | Governança estruturada como pilar para análise e políticas públicas. |
| 20 | Executivo | Municipal | Interoperabilidade | Dificuldade em integrar dados entre sistemas devido à falta de padrões uniformes. | Publicação de minuta detalhada com orientações para padronização de campos como CPF, endereço e raça. | Base de dados integrada, utilizada durante a vacinação digital, com potencial de replicação para outras áreas. | Abordagem replicável em outras cidades com adaptações mínimas. |
| 21 | Executivo | Municipal | Segurança | Vulnerabilidades identificadas em portais municipais, como o Portal da Transparência. | Implementação de certificações e medidas preventivas contra ameaças digitais. | Revisão emergencial de plataformas para garantir conformidade com a LGPD. | Segurança fortalecida como requisito para plataformas públicas municipais. |
| 22 | Executivo | Municipal | Capacitação | Falta de conscientização e treinamento contínuo para servidores públicos. | Produção de cartilhas práticas e capacitações específicas para encarregados e servidores. | Ampliação das capacitações e criação de grupos de trabalho para apoio técnico. | Capacitação contínua para servidores e maior engajamento no uso de dados. |
| 23 | Executivo | Municipal | Recursos Financeiros | Modelo atual depende de eventos extraordinários, como a vacinação, para organização de bases funcionais. | Contratação de consultorias para fortalecer iniciativas e assessorar políticas municipais. | Política Municipal de Proteção de Dados integrada com dados abertos e transformação digital, prevista para 2025. | Sustentabilidade de modelos como prioridade em planejamentos futuros. |

| 1 | Fonte/Entrevista | Nivel | Categoria | Problemas/ Desafios identificados | Ações/Boas Práticas | Avanços Realizados | Tendencias/Padrões |
|---|---|---|---|---|---|---|---|
| | | | | dados. | Conselho de Transformação Digital. | aplicado às secretarias municipais. | para análise e políticas públicas. |
| 20 | Executivo | Municipal | Interoperabilidade | Dificuldade em integrar dados entre sistemas devido à falta de padrões uniformes. | Publicação de minuta detalhada com orientações para padronização de campos como CPF, endereço e raça. | Base de dados integrada, utilizada durante a vacinação digital, com potencial de replicação para outras áreas. | Abordagem replicável em outras cidades com adaptações mínimas. |
| 21 | Executivo | Municipal | Segurança | Vulnerabilidades identificadas em portais municipais, como o Portal da Transparência. | Implementação de certificações e medidas preventivas contra ameaças digitais. | Revisão emergencial de plataformas para garantir conformidade com a LGPD. | Segurança fortalecida como requisito para plataformas públicas municipais. |
| 22 | Executivo | Municipal | Capacitação | Falta de conscientização e treinamento contínuo para servidores públicos. | Produção de cartilhas práticas e capacitações específicas para encarregados e servidores. | Ampliação das capacitações e criação de grupos de trabalho para apoio técnico. | Capacitação contínua para servidores e maior engajamento no uso de dados. |
| 23 | Executivo | Municipal | Recursos Financeiros | Modelo atual depende de eventos extraordinários, como a vacinação, para organização de bases funcionais. | Contratação de consultorias para fortalecer iniciativas e assessorar políticas municipais. | Política Municipal de Proteção de Dados integrada com dados abertos e transformação digital, prevista para 2025. | Sustentabilidade de modelos como prioridade em planejamentos futuros. |
| 24 | Executivo | Municipal | Tecnologia | Governo Federal compete com serviços municipais, dificultando eficiência operacional. | Introdução do conceito "Governo Zero Cliques", eliminando a necessidade de solicitações manuais para alguns serviços. | Portal de transparência ampliado com foco na experiência do usuário e automação de processos públicos. | Crescimento da adoção de tecnologias que garantem serviços proativos. |
| 25 | Judiciário | Judiciário Federal | Governança | Diversidade de estruturas e níveis de maturidade entre os órgãos públicos. | Sugeriu a tradução de conceitos técnicos e jurídicos (ISO, NIST) para diretrizes práticas. | TRE-Paraná criou equipes de apoio ao encarregado de proteção de dados, promovendo maior profundidade na implementação da LGPD. | Capacitação e suporte técnico como pilares para governança eficiente. |
| 26 | Judiciário | Judiciário Federal | Segurança | Segurança vista de forma limitada, concentrada em TI. | Ampliação do conceito de segurança para incluir proteção de dados sensíveis e continuidade de serviços públicos. | Propôs a estruturação integrada de Governança de Dados, Segurança da Informação e Proteção de Dados Pessoais nas políticas públicas. | Segurança ampliada como elemento estratégico para políticas públicas. |
| 27 | Judiciário | Judiciário Federal | Capacitação | Falta de capacitação contínua e direcionamentos claros nos órgãos públicos. | Necessidade de capacitação em diferentes níveis para conscientizar áreas responsáveis pela LGPD. | TRE-Paraná como referência em capacitação ao criar equipes especializadas de apoio ao encarregado de proteção de dados. | Capacitação adaptada às especificidades de cada órgão público. |
| 28 | Judiciário | Judiciário Federal | Recursos Financeiros | Burocracia e falta de recursos dificultam a implementação de políticas eficazes. | Implementação de auditorias internas como mecanismo de avaliação contínua e suporte. | Auditorias propostas como ferramenta para acompanhar adequação e proteger dados. | Auditorias como componente essencial para garantir conformidade e melhoria. |
| 29 | Judiciário | Judiciário Federal | Governança/Encarregado | Falta de autonomia técnica e capacidade operacional na função de encarregado de dados. | Proposta de descentralização do papel do encarregado com apoio técnico especializado em áreas como TI e gestão documental. | Ouvidoria do TSE desempenha papel de encarregado, mas com limitações operacionais. | Descentralização e equipes especializadas como tendência para a função do encarregado. |

# ANEXO 04: Estudo Práticas Nacionais

## 1. Introdução

O presente estudo tem como objetivo analisar as práticas de governança de dados em órgãos públicos brasileiros para mapear o estado atual dessa temática no Brasil, fornecendo embasamento para as recomendações direcionadas à Política Nacional de Proteção de Dados. Por meio de uma análise detalhada de políticas e iniciativas governamentais existentes, frameworks implementados e normativas aplicáveis, buscando ampla compreensão das dinâmicas que permeiam a governança de dados no setor público.

Para tal propósito, será realizada uma revisão bibliográfica e documental, além da análise de estudos de caso e relatórios oficiais. Com objetivo de identificar boas práticas, lacunas e oportunidades de desenvolvimento que contribuam para uma governança de dados mais eficaz e alinhada às necessidades da administração pública brasileira.

Buscando maior aproveitamento dos estudos, foram elaboradas as seguintes questões para o levantamento: (i) O que a Administração Pública entende por Governança de Dados? (ii) Quais são os órgãos que compõem a macroestrutura e como os atores interagem; e como está estruturado; (iii) O que existe em termos de legislação sobre governança de dados? (iv) Em termos de governança de proteção de dados pessoais no poder público, o que existe hoje?

## 2. Administração Pública e Governança de Dados

Em um contexto de crescente digitalização e modernização, a administração pública enfrenta desafios para melhorar a eficiência, transparência e prestação de serviços à sociedade, buscando implementar estratégias eficazes de governança de dados. Neste contexto, este capítulo busca examinar as bases normativas, papéis e responsabilidades institucionais que sustentam a governança de dados na administração pública brasileira.

Governança de Dados no contexto da Administração Pública é compreendida como o "conjunto de princípios, políticas, padrões, métricas e responsabilidades que permitem o alinhamento da

estratégia, processos, pessoas e uso de tecnologia de dados"[26]. Segundo a Cartilha de Governança de Dados do Poder Executivo Federal, a governança é fundamental para o planejamento e a tomada de decisões baseadas em evidências, para uma administração pública mais transparente e responsiva.

Governança de Dados é definida como o conjunto de políticas, processos, estruturas e papéis que garantem a gestão ética, eficiente e segura dos ativos de dados de uma organização. Na administração pública, ocorre uma expansão do conceito para assegurar que os dados sejam usados estrategicamente na formulação de políticas públicas, no aprimoramento da prestação de serviços e na transparência governamental.[27]

De forma complementar, o Acórdão 390/2024 do Tribunal de Contas da União (TCU) aponta que a governança de dados deve incluir um enfoque na segurança, privacidade e transparência, além de fomentar o uso estratégico de informações confiáveis para a formulação de políticas públicas. Também enfatiza a necessidade de frameworks robustos, como o DAMA-DMBoK, para avaliar e aprimorar a maturidade dos processos de gestão de dados.

É imperioso destacar que tanto o Acórdão do TCU[28] quanto as Cartilhas do Poder Executivo Federal fazem clara diferenciação entre Governança de Dados e Gestão de Dados. Governança define diretrizes, políticas e supervisiona a execução, enquanto a Gestão de Dados executa as diretrizes estabelecidas. Já a gestão inclui planejamento e controle, enquanto a governança foca na conformidade e mitigação de riscos.

### 2.1. Papéis e responsabilidades

De acordo com a *Cartilha de Governança de Dados - Volume III*, os principais papéis e responsabilidades na administração pública são os chamados Agentes de Governança. Estes, são organizados em diferentes níveis para promover a eficiência e a segurança no uso de dados, são eles:

---

[26] https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/forum-governanca-de-dados/cartilha-de-governanca-de-dados-volume1-8-12.pdf

[27] Cartilhas de Governança de Dados e Acórdão 390 do TCU

[28] O Acórdão do TCU usa o termo " processo de governança" para se referir ao processo de "identificação de problemas a serem solucionados por uma organização ou entidade como um todo e não por um indivíduo ou por um grupo isolado de pessoas dentro dela".

1. **Executivo de Dados**: Coordena o programa de governança de dados no órgão; Representa a instituição em questões de governança de dados e Implementa políticas e monitora indicadores de desempenho.
2. **Curadores de Dados**: Gerem ativos de dados, garantem a qualidade e promovem seu reuso; e Monitoram o ciclo de vida dos dados e asseguram conformidade com a LGPD. São agentes públicos responsáveis pela gestão de ativos de dados, internos ou externos ao órgão ou entidade, designados por liderança na estrutura organizacional.
3. **Instância Estratégica de Governança de Dados**: colegiado composto por representantes de diferentes áreas que supervisionam diretrizes e resolvem conflitos relacionados à gestão de dados; e aprova o programa de governança e políticas internas de dados.

Esses agentes operam sob a estrutura regulamentar de normativos como a Lei de Acesso à Informação (LAI), a LGPD e decretos relacionados ao compartilhamento e à segurança de dados

### 2.2. Desafios e Maturidade Institucional

De acordo com o Tribunal de Contas da União (TCU), no Acórdão 390/2024, a governança de dados da administração pública federal ainda está em fase de consolidação. Segundo o levantamento feito pelo Tribunal sobre a macroestrutura atual de Governança de Dados no âmbito da administração pública federal, muitos órgãos ainda estão em estágios iniciais de maturidade em governança de dados, com ausência de processos formalizados, indicadores de desempenho e equipes capacitadas para gerenciar os ativos de dados. Essa realidade impede a adoção de uma cultura orientada a dados, que é essencial para modernizar a administração pública e responder aos desafios do cenário digital.

O Tribunal aponta ainda a insuficiência de programas estruturados de capacitação para servidores públicos como um obstáculo. A ausência de formação adequada limita a capacidade das equipes de lidar com as complexidades da gestão de dados, desde o planejamento até a execução de políticas voltadas para sua governança.

Baixa

## 3. Panorama Legislativo sobre Governança de Dados

A governança de dados no Brasil advém de diversos marcos legais, este capítulo apresenta os principais dispositivos legais e regulamentações que fundamentam a governança no contexto da administração pública.

| Marco histórico | Descrição |
|---|---|
| **Constituição Federal de 1988** | Reconhece o acesso à informação como um direito fundamental e assegura a proteção de dados pessoais, inclusive em meios digitais (Emenda Constitucional nº 115/2022) |
| **Lei 8.159/91** | Lei da Política Nacional de Arquivos Públicos e Privados |
| **Lei 9.507/97** | Lei do Habeas Data |
| **Decreto 4.829/03** | Criação do Comitê Gestor da Internet no Brasil (CGIbr) |
| **Lei 12.527/11** | Lei de Acesso à Informação |
| **Lei 12.682/12** | Elaboração e arquivamento de documentos em meios eletromagnéticos. Art. 3º tem pertinência com a Governança de Dados pela Administração |
| **Decreto 7.845/12** | Tratamento de informação classificada em qualquer grau de sigilo |
| **Lei 12.965/14** | Marco Civil da Internet |
| **Decreto 8.777/16** | Política de Dados Aberto do Poder Executivo Federal |
| **Decreto 8.789/16** | Dispõe sobre o compartilhamento de bases de dados na administração pública federal |
| **Decreto 8.936/16** | Plataforma de Cidadania Digital |
| **Decreto 9.094/17** | Dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos, institui o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo para a apresentação de dados do cidadão no exercício de obrigações e direitos e na obtenção de benefícios |
| **Decreto 9.637/18** | Política Nacional de Segurança da Informação |
| **Lei 13.444/17** | Identificação Civil Nacional (ICN), centralizando informações de identificação do cidadão. |
| **Lei 13.709/18** | Lei Geral de Proteção de Dados Pessoais. Define regras para o tratamento de dados pessoais, visando à proteção da privacidade e à promoção de transparência e segurança no uso |

| Marco histórico | Descrição |
|---|---|
| | de informações. |
| **Instrução Normativa SGD/ME 1/19** | Contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. |
| **Decreto 10.046/19** | Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, regula especificamente os art.s 23 a 32 da LGPD e o art. 11 da lei n. 13.444/17 |
| **Decreto 10.047/19** | Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. |
| **Lei 14.129/21** | Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública |

## 4. Governança de dados e proteção de dados pessoais no Poder público

A ANPD, estabelecida pela Lei nº 13.709/2018 (LGPD), iniciou suas operações em 2020 como a autoridade federal responsável por zelar pela aplicação da LGPD e pela proteção de dados pessoais no Brasil. Suas atribuições incluem a regulamentação, fiscalização e orientação de práticas relacionadas ao tratamento de dados, além de promover a defesa dos direitos dos titulares. A estrutura da ANPD conta com conselhos e comitês que garantem sua autonomia e capacidade de ação, como o Conselho Diretor e o Comitê de Fiscalização.

A proteção de dados pessoais no poder público brasileiro é regulamentada por diversos marcos legais e iniciativas institucionais que visam garantir a privacidade, a segurança e o uso ético dos dados. Por essa razão, este capítulo busca apresentar os principais elementos que estruturam a governança de dados, relacionados à proteção de dados pessoais no poder público.

### 4.1. Marcos Legais

| Marco Legal | Descrição |
|---|---|
| **Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)** | Define regras para o tratamento de dados pessoais,garantindo direitos como privacidade e definindo princípios. Aplica-se ao setor público quanto ao privado. |
| **Decreto nº 10.046/2019** | Estabelece diretrizes para a governança no compartilhamento de dados no âmbito da administração pública federal, criando o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. |
| **Resolução CD/ANPD nº 20 de 3 de outubro de 2024** | Institui a Política Interna de Proteção de Dados Pessoais na ANPD, com diretrizes sobre tratamento de dados, direitos dos titulares e capacitação. |

### 4.2. Iniciativas institucionais

| Iniciativa | Descrição |
|---|---|
| **Programa de Privacidade e Segurança da Informação (PPSI) 2.0** | Inclui cursos e trilhas de aprendizado em privacidade e segurança, atingindo mais de 20.000 inscritos em 2024. |
| **Cartilhas de Governança de Dados** | Os volumes publicaram diretrizes sobre papéis e responsabilidades relacionados à proteção de dados pessoais e à governança de dados no poder público. |
| **Acórdão 390/2024 do TCU** | Fornece diretrizes para boas práticas de governança e proteção de dados pessoais no setor público |
| **Guia de Elaboração de Programa de Governança em Privacidade**[29] | Orienta a elaboração de um Programa de Governança em Privacidade por órgãos e entidades da Administração Pública Federal |

[29] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos