MINISTÉRIO DA SAÚDE

GUIA RÁPIDO de GOVERNANÇA de DADOS

DISTRIBUIÇÃO GRATUITA
VENDA PROIBIDA

Brasília DF 2025

MINISTÉRIO DA SAÚDE
Secretaria de Vigilância em Saúde e Ambiente
Departamento de Análise Epidemiológica
e Vigilância de Doenças não Transmissíveis

GUIA RÁPIDO de GOVERNANÇA de DADOS

Brasília DF 2025

1ª edição – 2025 – versão eletrônica

Elaboração, distribuição e informações:
MINISTÉRIO DA SAÚDE
Secretaria de Vigilância em Saúde e Ambiente
Departamento de Análise Epidemiológica
e Vigilância de Doenças Não Transmissíveis
SRTVN 701, via W5 Norte, Edifício PO 700, 6º andar
CEP: 70719-040 – Brasília/DF
Site: www.saude.gov.br/svsa
E-mail: svsa@saude.gov.br

Fundação Oswaldo Cruz – Bahia
Centro de Integração de Dados e Conhecimentos para Saúde
Ed. Tecnocentro, rua Mundo, 121, Trobogy
CEP: 41745-715 – Salvador/BA
Site: https://cidacs.bahia.fiocruz.br/
E-mail: cidacs.comunicacao@fiocruz.br

Ministro de Estado da Saúde:
Alexandre Rocha Santos Padilha

Secretária de Vigilância em Saúde e Ambiente:
Mariângela Batista Galvão Simão

Organização:
Fundação Oswaldo Cruz:
Maíra Lima de Souza
Alayde Lopes Sarno Carvalho
Carlos Antonio de Souza Teles Santos
Maria Yury Travassos Ichihara
Maria Jenny Silva Araujo
Maurício Lima Barreto
Pablo Ivan Pereira Ramos

Ministério da Saúde:
Camila Arantes Ferreira Brecht D' Oliveira
Dayan Carvalho Ramos Salles de Oliveira
Fabiana Godoy Malaspina
Letícia de Oliveira Cardoso
Lucíola Santos Silva
João Ferreira Silva Junior

Revisão técnico-científica:
Paola Marchesini – CGEVSA/Daevs/SVSA

Diagramação:
Sabrina Lopes – CGEVSA/Daevs/SVSA

Normalização:
Valéria Gameleira da Mota – Editora MS/CGDI

Revisão textual:
Khamila Silva – Editora MS/CGDI
Tamires Felipe Alcântara – Editora MS/CGDI

Ficha Catalográfica

Brasil. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis.
Guia Rápido de Governança de Dados [recurso eletrônico] / Ministério da Saúde, Secretaria de Vigilância em Saúde e Ambiente, Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis. – Brasília : Ministério da Saúde, 2025.
75 p. : il.

Modo de acesso: World Wide Web:
http://bvsms.saude.gov.br/bvs/publicacoes/guia_rapido_governanca_dados.pdf
ISBN 978-65-5993-833-9

1. Gestão de Dados. 2.Segurança de Dados. 3. Lei de Proteção de Dados. I. Título.

CDU 004.65

Catalogação na fonte – Coordenação-Geral de Documentação e Informação – Editora MS – OS 2024/0250

Título para indexação:
Data Governance: A Straightforward Guide

SUMÁRIO

APRESENTAÇÃO

Os dados de saúde produzidos pelos sistemas de informação, sob a gestão da Secretaria de Vigilância em Saúde e Ambiente (SVSA), constituem elementos fundamentais tanto para as ações de monitoramento epidemiológico e sanitário de doenças, agravos e eventos relevantes para a saúde pública do País quanto para a produção de indicadores e conhecimento técnico-científico.

De caráter nacional, esses dados permitem traçar cenários relacionados à situação de saúde e delinear o perfil da linha da vida da população. Esse potencial é ampliado por meio de estratégias de integração (como o *linkage*) e interoperabilidade entre sistemas advindos de diferentes fontes.

O valor estratégico desses conjuntos de dados, o interesse público em acessá-los e utilizá-los, assim como as estratégias nacionais de governo aberto (Lei n.º 12.527, de 18 de novembro de 2011), governo digital (Lei n.º 14.129, de 19 de março de 2021) e saúde digital (Portaria n.º 1.434, de 28 de maio de 2020), reforçam a importância da implementação de uma estratégia de governança.

A governança de dados estabelece uma estrutura multifuncional voltada para a gestão eficaz e racional de dados, considerando seu ciclo de vida e sua importância para o modelo de negócio de uma organização (Abraham; Brocke; Schneider, 2019). Essa prática define políticas, processos, direitos e responsabilidades relacionados às decisões que envolvem o tratamento de dados.

No setor público, a governança de dados reforça o apelo ao desenvolvimento e à implementação de um modelo que favoreça a incorporação de uma cultura orientada à privacidade e à proteção de dados. Conforme sinaliza a Agência Nacional de Proteção de Dados (ANPD), o tratamento de dados pelo poder público apresenta peculiaridades que precisam ser bem geridas e governadas, especialmente no que se refere ao uso compartilhado de dados pessoais (Brasil, 2022). Além disso, ao definir

a atividade de tratamento com ações específicas[1], a Lei Geral de Proteção de Dados (LGPD) reforça a necessidade de uma boa gestão de dados e, por conseguinte, de uma boa governança.

As normas e as boas práticas em governança de dados do governo federal estão sob responsabilidade do Comitê Central de Governança de Dados (CCGD). O conteúdo deste documento foi elaborado de acordo com as recomendações e diretrizes do CCGD[2].

O *Guia Rápido de Governança de Dados* da Secretaria de Vigilância em Saúde e Ambiente (SVSA), baseado principalmente na estrutura proposta pelo *Data Management Body of Knowledge* (DAMA-DMBoK)[3] (Henderson *et al*., 2017), busca esclarecer os pontos essenciais sobre o tema e fornecer orientações para a melhoria dos processos de gestão do ciclo de vida dos dados[4] sob a responsabilidade do Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis (Daent). Apresenta os principais conceitos e princípios que podem ser aplicados no dia a dia e às bases de dados de vigilância em saúde, além de materiais complementares para a implementação das boas práticas de governança e gestão de dados em sua coordenação ou departamento.

Este Guia é um dos resultados da parceria entre o Daent e o Centro de Integração de Dados e Conhecimentos para a Saúde (Cidacs/Fiocruz Bahia) no âmbito do projeto TED 159/2019, que tem o objetivo de fortalecer a capacidade de desenvolvimento de metodologias e tecnologias, visando ao aprimoramento na qualidade da análise de informações e intervenções do Sistema Nacional de Vigilância em Saúde (SNVS) por meio da melhoria de seus fluxos de dados.

[1]De acordo com o art. 5.º, inciso X, da LGPD, o tratamento de dados refere-se a toda e qualquer operação de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[2]https://www.gov.br/governodigital/pt-br/governanca-de-dados.

[3]O DAMA propõe uma estrutura de governança de dados baseada em 11 diretrizes de conhecimento: governança de dados; arquitetura de dados; modelagem e projeto de dados; armazenamento e operações de dados; segurança de dados; integração e interoperabilidade de dados; documentação e conteúdo; gestão de dados mestres; armazenamento de dados e inteligência de negócios; metadados; e qualidade dos dados.

[4]A gestão orientada ao ciclo de vida dos dados abrange um conjunto de funções que, do ponto de vista técnico, envolve o planejamento, a aquisição, as estratégias de armazenamento, o uso, a preservação e o descarte de dados. As ações, ao longo de todo o ciclo de vida dos dados, podem ocorrer de forma contínua, sequencial ou ocasional. No contexto da SVSA, a consideração do ciclo de vida dos dados deve ser adaptada à infraestrutura de vigilância e à gestão de dados de saúde.

1 | ESTRUTURA DO GUIA

O Guia está dividido em dez seções, que incluem desde uma introdução conceitual básica até a disponibilização de documentos de apoio para o processo de implementação, monitoramento e avaliação da governança e gestão de dados em seu setor. Os itens disponíveis estão divididos da seguinte forma:

1 e 2. **Introdução à governança de dados e princípios da governança de dados:** apresentam os conceitos básicos sobre o tema e os princípios de governança de dados, como precisão e qualidade dos dados, segurança e privacidade, e transparência e responsabilidade.

3. **Marcos regulatórios, éticos e de segurança e privacidade na governança de dados:** aborda como os marcos regulatórios implicam as ações de tratamento de dados e quais medidas devem ser tomadas para estar em conformidade.

4. **Estrutura organizacional:** introduz a estrutura organizacional da governança de dados com definição dos papéis, das responsabilidades e das estratégias de capacitação.

5. **Gestão de dados:** apresenta técnicas de gerenciamento de dados, como a coleta, o armazenamento, a manutenção, a análise e o uso de dados.

6. **Compartilhamento de dados:** apresenta os aspectos de gestão relevantes para a troca segura de dados entre diferentes departamentos e instituições, e referencia a interoperabilidade como opção para o compartilhamento de dados relevantes no campo da saúde.

7. **Plano de governança de dados:** traz um conjunto de documentos capazes de auxiliar a implantação prática de uma estratégia de governança de dados.

8. **Recomendações finais:** discute os principais desafios na implementação de uma governança de dados e os aspectos relacionados ao campo da governança.

9. **Glossário:** apresenta os termos técnicos e jargões utilizados no manual para garantir uma compreensão unificada.

10. **Materiais complementares:** apresenta os documentos e os recursos práticos para apoiar o processo de governança.

2 | INTRODUÇÃO À GOVERNANÇA DE DADOS

A governança de dados pode ser compreendida como um conjunto de normas, diretrizes, indicadores de desempenho e atribuições que asseguram que estratégias, processos operacionais, colaboradores, tecnologia aplicada e dados estejam harmonizados. De uma maneira geral, traz os seguintes benefícios para instituições de qualquer porte e em qualquer área:

1. **Controle de riscos**, o qual garante a segurança, a integridade e a proteção de dados e sistemas.
2. **Captura de valor**, ao estabelecer regras e padrões técnicos para permitir transferência, combinação e troca de dados mais eficazes.
3. **Confiança** na forma como os dados são produzidos, coletados, processados e utilizados.
4. **Normatização**, por meio da definição de normas e regras sobre direitos, princípios e obrigações relacionados ao uso de dados.
5. **Melhorias na gestão**, ao apoiar a implementação de políticas, leis, regulamentos e padrões para o governo dos dados.
6. **Aprimoramento organizacional**, ao dar suporte para que as organizações usem dados para informar e orientar decisões estratégicas.
7. **Eficiência operacional**, ao melhorar a precisão, a qualidade e a consistência dos dados, o que leva a operações mais eficientes.
8. **Conformidade regulatória**, ao assegurar que a organização esteja em conformidade com as legislações e regulamentações de dados aplicáveis.
9. **Melhoria na tomada de decisões**, ao fornecer dados confiáveis e de alta qualidade que suportam a tomada de decisões baseadas em evidências.
10. **Facilita a colaboração** quando permite o compartilhamento seguro de dados entre diferentes departamentos, parceiros e partes interessadas.

Na Administração Pública, a governança de dados é essencial para estimular, melhorar e assegurar a eficácia das políticas públicas, assim como para a oferta de soluções e de serviços à população. Além disso, proporciona benefícios como maior transparência e eficiência no serviço público, custos otimizados, além de decisões mais assertivas.

Dados bem governados são a base para decisões fundamentadas em evidências, o que os torna essenciais nos processos relacionados à vigilância em saúde e à saúde pública como um todo.

FIQUE POR DENTRO

O governo brasileiro reconheceu a importância da governança de dados como base para a melhoria da oferta de serviços públicos ao cidadão. Com base nessa visão, o governo adotou a Estratégia de Governo Digital, que promove, entre outros aspectos, a integração e a interoperabilidade (Brasil, 2023) dos sistemas de dados.

3 | PRINCÍPIOS DA GOVERNANÇA DE DADOS

A governança de dados em organizações não acadêmicas é realizada em torno de três pilares: precisão e qualidade de dados, segurança e privacidade, transparência e responsabilidade.

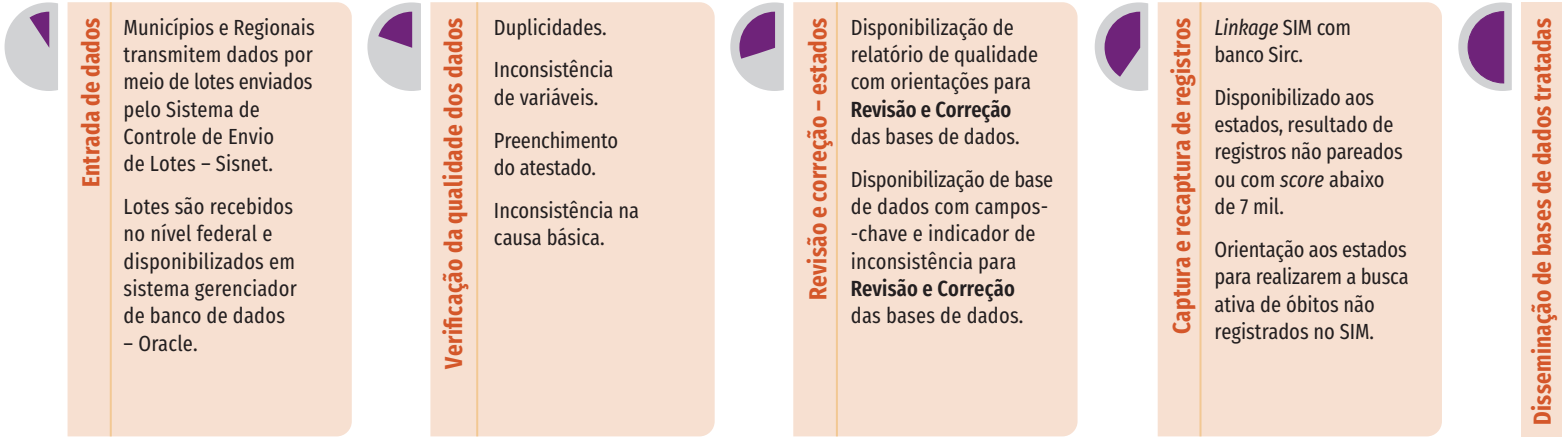
3.1 PRECISÃO E QUALIDADE DE DADOS

Refere-se à exatidão e à confiabilidade das informações registradas. Isso significa a aplicação de ações para mitigar erros, omissões e distorções, assegurando que os dados reflitam, da melhor forma, a realidade que pretendem representar, garantindo a integridade e a confiabilidade dos dados coletados e processados. Assim, em um sistema de registros de pacientes, a precisão dos dados garantiria que as informações pessoais, como nome, data de nascimento e histórico médico, estejam corretas e atualizadas. Igualmente, em um banco de dados de epidemiologia, a precisão dos dados é crucial para garantir a confiabilidade das estatísticas sobre incidência de doenças e monitoramento de surtos. A precisão dos dados é essencial para embasar decisões e formulação de políticas de saúde baseadas em evidências sólidas e confiáveis.

Por outro lado, a qualidade de dados refere-se à adequação, à confiabilidade e à consistência das informações armazenadas em um sistema. Em outras palavras, dados de alta qualidade são aqueles que são precisos, completos, consistentes e atualizados.

No Daent, a precisão e a qualidade dos dados são asseguradas por um processo rigoroso de validações, com vistas à confiabilidade, dividido nas seguintes etapas: qualificação inicial, com remoção de duplicidades assegurada pelas áreas técnicas responsáveis; análise para verificar a forma de organização dos dados e para assegurar a presença das informações necessárias; e, após a homologação da qualidade, publicação dos dados em portais de transparência, como o OpenDataSUS, TabNet e o Tableau, que permitem acesso a dados agregados e a microdados anonimizados para fins de consulta e análise. A Figura 1 exemplifica a estratégia de qualidade de dados aplicada ao Sistema de Informações sobre Mortalidade (SIM).

FIGURA 1 Estratégia de garantia da qualidade de dados



Fonte: Daent/SVSA.

3.2 SEGURANÇA E PRIVACIDADE

A segurança dos dados envolve a proteção contra acessos não autorizados, garantindo que apenas pessoas autorizadas possam acessar as informações, assim como a precaução de utilizar a criptografia de dados em sistemas de informações em saúde para proteger as informações confidenciais dos usuários ou pessoas, evitando violações de segurança e vazamento de dados sensíveis.

De forma semelhante, a privacidade de dados pessoais e confidenciais dos indivíduos nos registros de saúde deve ser garantida por meio de armazenamento que assegure que apenas profissionais autorizados tenham acesso às informações nominais dos pacientes, respeitando as leis de privacidade de dados, como a LGPD no Brasil. As boas práticas de segurança e de privacidade de dados são essenciais para garantir o cumprimento de regulamentações e normas de proteção de dados, bem como para manter a confiança dos cidadãos no sistema de saúde.

O estado de segurança e privacidade no tratamento de dados pelo Daent é assegurado tanto pelo Departamento de Informação e Informática do Sistema Único de Saúde (DataSUS), responsável pelos sistemas, pela infraestrutura de rede e pela arquitetura de armazenamento de dados, quanto pelas normas que garantem a conformidade e a responsabilidade no acesso e no uso dos dados. Quando aplicados, esses princípios estipulam que, por exemplo, o acesso aos sistemas de dados seja baseado no princípio da necessidade, pelo qual os usuários acessam apenas as informações necessárias para suas tarefas. Assim, o acesso às pastas compartilhadas na rede interna (intranet) é restrito a computadores e logins autorizados, necessário para o fluxo interno de tratamento de dados.

3.3 TRANSPARÊNCIA E RESPONSABILIDADE

São aspectos essenciais da governança de dados na área de saúde pública. A transparência pressupõe, nesse contexto, fornecer acesso às informações sobre como os dados são coletados, processados e utilizados. Isso inclui comunicar, de forma acessível, as políticas de privacidade, segurança e compartilhamento de dados, tanto para os profissionais de saúde quanto para os usuários e o público em geral. Assim, o Daent/SVSA, ao elaborar o protocolo de acesso a dados e definir documentos que regulamentam e informam como os dados pessoais devem ser protegidos e utilizados, está demonstrando responsabilidade e transparência.

A responsabilidade envolve a atribuição de quem é responsável pelos diferentes aspectos da governança de dados, garantindo que todos os envolvidos compreendam e cumpram suas obrigações. Um exemplo disso

foi a criação do Núcleo de Governança de Dados (NGD), responsável por revisar e aprovar o uso dos dados de forma ética e garantir a conformidade com as regulamentações de proteção de dados.

FIQUE POR DENTRO

A governança da SVSA relaciona os seguintes elementos: a fonte de dados, o tratamento e armazenamento, e a finalidade de uso. Ela sublinha a importância de considerar o nível de sensibilidade dos dados de saúde, a necessidade e a forma como os dados serão utilizados.

3.4 PRINCÍPIOS DA GOVERNANÇA DE DADOS NO DEPARTAMENTO DE ANÁLISE EPIDEMIOLÓGICA E VIGILÂNCIA DE DOENÇAS NÃO TRANSMISSÍVEIS

Os princípios de gestão de dados no Daent são baseados em seis pilares, com destaque para a **segurança**, a **privacidade** e a **conformidade legal**, que asseguram a proteção de dados pessoais sensíveis relacionados à saúde. O Departamento tem investido na criação de uma cultura de boas práticas no tratamento de dados, definindo uma estrutura funcional e criando documentos que uniformizam procedimentos, garantindo a **responsabilidade pelos dados**, a **transparência** e a **qualidade de dados**.

- **Segurança da informação**: ao longo do tempo, o Departamento investiu em estratégias para assegurar a proteção de dados contra acesso não autorizado, uso indevido e divulgações indevidas. Isso se torna evidente na implementação da Sala de Acesso Restrito (SAR) para tratamento de dados identificados, no uso de ferramentas de criptografia para compartilhamento de dados, nas políticas de acesso restrito a informações confidenciais e no monitoramento constante dos sistemas.

- **Privacidade dos dados**: a proteção da privacidade dos indivíduos é primordial, com medidas para garantir que apenas pessoas autorizadas acessem dados pessoais para serem usados para fins legítimos e específicos, por exemplo, pesquisas em saúde, conforme o artigo 13 da LGPD. Busca-se, portanto, garantir que o uso de dados identificados siga as orientações de processamento em ambiente seguro e de acesso

conforme a legislação vigente, aplicando-se métodos de anonimização, pseudonimização e desidentificação, a depender da finalidade e da necessidade do tratamento de dados, bem como do nível de autorização de acesso do operador a esses dados.

- **Conformidade legal**: as ações são pautadas pelas leis e regulamentações brasileiras relacionadas à proteção de dados, incluindo a LGPD e a Lei de Acesso à Informação (LAI). Diferentes procedimentos vêm sendo adotados para garantir o cumprimento dessas leis, incluindo a gestão de solicitações de dados, a assinatura de termos de responsabilidade, a categorização dos dados para compartilhamento e a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados.

- **Responsabilidade pelos dados**: estruturas e processos transparentes para a gestão de dados vêm sendo estabelecidos, com funções e responsabilidades bem definidas, para garantir a tomada de decisões responsáveis em relação aos dados, tanto para o NGD quanto para os gestores de informação, guardiões dos sistemas e áreas técnicas.

- **Transparência**: o esforço pela transparência tem dois eixos principais: 1) a formalização e publicidade de informações dos seus sistemas, fluxos de dados e procedimentos para solicitação de acesso; e 2) a publicação de dados abertos anonimizados, assegurando o acesso público à informação.

- **Qualidade de dados**: os dados passam por processos de validação, consistência, completude e atualização a fim de assegurar sua qualidade.

4 MARCOS REGULATÓRIOS, ÉTICOS E DE SEGURANÇA E PRIVACIDADE NA GOVERNANÇA DE DADOS

Os marcos regulatórios, éticos, de segurança e privacidade orientam o uso apropriado e responsável de dados no setor público e no setor privado em geral. Eles abrangem ações como a criação de relatórios de impacto e risco, considerações sobre anonimização e controle de acesso, entre outras.

Esses marcos devem ser considerados pelos agentes públicos, pela sociedade e por aqueles que desejam estabelecer relações com o serviço público. Devem ser aplicáveis a todas as ações de tratamento de dados e estar alinhados à estratégia de governança de dados[5].

É preciso estar ciente das legislações específicas que se aplicam aos dados da SVSA, bem como das normativas que orientam a prevenção de discriminação, o compartilhamento e a reutilização de dados, os direitos autorais e a propriedade intelectual, a liberdade de informação, as análises estatísticas e a divulgação de informações.

Além da LGPD, é relevante referenciar outras normas internacionais pertinentes, tais como o Regulamento Geral de Proteção de Dados da União Europeia, que estabelece padrões semelhantes de proteção de dados. A adesão a essas normas internacionais não apenas fortalece a adequação, mas também demonstra o compromisso com a proteção dos dados pessoais em um contexto global.

Além disso, as melhores práticas recomendadas por entidades como a Organização Mundial da Saúde (OMS) e a *International Organization for Standardization* (ISO) podem oferecer orientações adicionais para a gestão de dados em saúde pública, proporcionando um referencial de excelência e conformidade para as organizações.

[5]As considerações sobre esses marcos devem acompanhar toda a estratégia de digitalização e inovação tecnológica da Secretaria.

Por fim, a ética dos dados envolve a responsabilidade e a sustentabilidade no uso de dados, seguindo os princípios e os valores baseados na justiça, na igualdade e no respeito ao ser humano, sobre os quais os direitos humanos e as leis de proteção de dados estão fundamentados.

Segundo Perez *et al*. (2021), os dez princípios de boas práticas de ética de dados no setor público são:

- Gerenciar dados com integridade.
- Estar ciente e observar os acordos relevantes em todo o governo para acesso, compartilhamento e uso confiáveis de dados.
- Incorporar considerações éticas de dados nos processos de tomada de decisão do governo, da organização e do setor público.
- Monitorar e manter o controle sobre os dados, em particular aqueles usados para informar o desenvolvimento e o treinamento de sistemas algorítmicos e inteligência artificial, adotando uma abordagem baseada em riscos no caso de automação de decisões.
- Ser específico sobre a finalidade do uso dos dados, especialmente no caso de dados pessoais.
- Definir limites e condições para acesso, compartilhamento e uso de dados.
- Ser claro, inclusivo e aberto.
- Publicar dados abertos e código-fonte.
- Ampliar o controle de indivíduos e coletivos sobre seus dados.
- Ser responsável e proativo no gerenciamento de riscos.

Ao incorporar práticas alinhadas com os marcos regulatórios, éticos, de segurança e privacidade[6], seguir as diretrizes do DAMA-DMBoK e referenciar normas internacionais e melhores práticas, as organizações de saúde pública podem assegurar uma sólida adequação às melhores práticas na gestão de dados, promovendo a confiança, a segurança e a integridade das informações em benefício da saúde da população.

[6]Com o intuito de apoiar a gestão em privacidade e segurança da informação, o governo brasileiro publicou uma série de guias, modelos e ferramentas para orientar as melhores práticas. Entre eles, há o *Guia do Framework de Privacidade e Segurança da Informação*, que pode ser acessado pelo link: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf.

Quais práticas de segurança da informação e autorização de acesso aos dados são propostos pelo DAMA-DMBoK?

A segurança da informação e a autorização de acesso aos dados são críticas na gestão de informações de saúde pública. Para proteger dados confidenciais, as organizações devem adotar medidas robustas, como criptografia, controle de acesso baseado em funções, monitoramento de atividades de usuários e políticas de segurança de dados.

A autorização de acesso deve ser gerenciada cuidadosamente, garantindo que apenas indivíduos autorizados possam acessar informações sensíveis. Políticas baseadas no princípio do menor privilégio e processos de auditoria e revisão de acessos ajudam a mitigar riscos e preservar a privacidade dos dados de saúde.

Estabelecendo sólidas práticas de segurança e privacidade da informação e autorização de acesso, as organizações mostram seu compromisso com a proteção de dados confidenciais, essenciais para promover saúde e bem-estar. Revisões e atualizações constantes das políticas de segurança, treinamentos para conscientização dos profissionais envolvidos e medidas de monitoramento e resposta a incidentes são essenciais para garantir a eficácia dessas práticas.

4.1 MARCOS REGULATÓRIOS, ÉTICOS, DE SEGURANÇA E PRIVACIDADE

A iniciativa de governança de dados no Daent é referenciada por dispositivos legais e regulatórios que, direta e indiretamente, delimitam a ética e os marcos de segurança e privacidade. Esses dispositivos, destacados a seguir, regulamentam os direitos dos cidadãos, a Administração Pública e a gestão da informação pública.

Constituição Federal de 1988: a Constituição é mencionada como a base legal primordial para o direito à informação e para a proteção da privacidade.

Leis

Lei n.º 14.289, de 3 de janeiro de 2022 (lei que trata da preservação do sigilo): importante no contexto da proteção de dados sensíveis e estigmatizantes.

Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD): base legal fundamental para a proteção de dados pessoais no Brasil, estabelecendo princípios, direitos e obrigações para o tratamento de dados, incluindo a coleta, o uso, o compartilhamento e a segurança das informações, especialmente para os dados de saúde classificados como sensíveis.

Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI): regula o acesso a informações públicas, garantindo o direito à informação e estabelecendo procedimentos para sua solicitação e fornecimento.

Lei n.º 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa): estabelece sanções para atos de improbidade administrativa, que incluem o uso indevido de informações sigilosas. Reflete no contexto da responsabilidade dos agentes públicos no tratamento de dados sensíveis, reforçando a importância do sigilo e da confidencialidade.

Decretos

Decreto n.º 11.491, de 12 de abril de 2023: promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

Decreto n.º 10.046, de 9 de outubro de 2019: estabelece regras para o compartilhamento de dados entre órgãos e entidades da Administração Pública Federal, com o objetivo de promover a integração de dados e a melhoria da qualidade dos serviços públicos.

Decreto n.º 7.724, de 16 de maio de 2012: regulamenta a Lei de Acesso à Informação (LAI), detalhando procedimentos para a solicitação e o fornecimento de informações públicas e estabelecendo prazos e requisitos específicos. É citado como referência para a assinatura de termos de responsabilidade para o acesso a dados pessoais, reforçando a necessidade de controlar e documentar o acesso a informações sensíveis.

4.2 CÓDIGO DE ÉTICA PROFISSIONAL DO SERVIDOR PÚBLICO CIVIL DO PODER EXECUTIVO FEDERAL

Decreto n.º 1.171, de 22 de junho de 1994: o Código de Ética é citado como um conjunto de normas que orientam o comportamento ético dos servidores públicos, incluindo o dever de proteger informações sigilosas.

Resoluções

Resolução CD/ANPD n.º 19, de 23 de agosto de 2024: aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.

Resolução CD/ANPD n.º 18, de 16 de julho de 2024: aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

Resolução CD/ANPD n.º 15, de 24 de abril de 2024: aprova o Regulamento de Comunicação de Incidente de Segurança.

Resolução n.º 738, de 1° de fevereiro de 2024: dispõe sobre o uso de banco de dados com finalidade de pesquisa científica envolvendo seres humanos.

Resolução CD/ANPD n.º 4, de 24 de fevereiro de 2023: aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Altera o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD n.º 1, de 28 de outubro de 2021, publicada no Diário Oficial da União de 29 de outubro de 2021.

Resolução CD/ANPD n.º 3, de 25 de janeiro de 2023: institui o Comitê de Governança Digital da Autoridade Nacional de Proteção de Dados.

Resolução CNS n.º 466/2012 e Resolução CNS n.º 510/2016: mencionadas como referência para a aprovação de pesquisas com dados sensíveis pelos Comitês de Ética em Pesquisa (CEP).

Portarias

Portaria GM/MS n.º 3.232, de 1º de março de 2024: altera a Portaria de Consolidação GM/MS n.º 5, de 28 de setembro de 2017, para instituir o Programa SUS Digital.

Portaria GM/MS n.º 271/2017 (Política de Segurança da Informação e Comunicações do Ministério da Saúde): estabelece diretrizes para a segurança da informação no âmbito do Ministério da Saúde, incluindo a proteção de dados pessoais sensíveis.

FIQUE POR DENTRO

Com a observância dos marcos mencionados, foram delineados os fluxos de solicitação de dados no que tange a: solicitação de dados, segurança, manuseio e qualificação de dados, com definição de termos de responsabilidade.

5 | ESTRUTURA ORGANIZACIONAL

A estrutura organizacional e a definição do "negócio dos dados" são fundamentais para o estabelecimento de um plano de governança de dados institucionais. Para tal, é importante levar em consideração os seguintes passos:

1. Estabelecer o caso de negócio em governança de dados.

O caso de negócio em governança de dados é um argumento estruturado que justifica o investimento em governança de dados dentro de uma organização. Seu objetivo é convencer as partes interessadas da importância de adotar as práticas de governança de dados, promover o alinhamento estratégico e garantir apoio e recursos necessários para iniciativas nessa área. O caso de negócio detalha:

- Os benefícios esperados, que incluem a melhoria na qualidade dos dados, a eficiência operacional, a conformidade regulatória e o apoio à tomada de decisão.
- Os riscos e os custos associados, apresentando uma análise do retorno sobre o investimento.

2. Obter apoio para as iniciativas de governança e gestão de dados.
3. Definir papéis e a participação daqueles que lidarão com os dados. É importante elencar quais servidores e colaboradores estão responsáveis por cada etapa do ciclo de gestão de dados que veremos na próxima seção.
4. Uma vez definidos e conhecidos os papéis, é necessário listar as responsabilidades, evidenciando a descrição do que deve ser feito, ou seja, qual é a função de cada um. É preciso que haja atualização regular dessas informações, registrando a data em que foi realizada, assim como providenciar que os acessos e os privilégios também sejam atualizados.
5. Por último, avaliar a maturidade da estrutura organizacional delineada para a governança de dados. É importante manter o conhecimento atualizado para gerir e tratar adequadamente os dados, por meio de capacitação continuada da equipe. Ao final deste documento, é possível acessar um conjunto de treinamentos que podem apoiar essas capacitações.

DICA

Para alinhar sua estrutura organizacional, responda aos seguintes questionamentos:

Quem somos? Como estamos? Para onde queremos ir? E como chegaremos lá? **A partir daí, considere as necessidades mais urgentes e importantes e avalie sua capacidade e maturidade. Isso ajudará no entendimento e no delineamento da sua estrutura organizacional.**

5.1 ESTRUTURA ORGANIZACIONAL IMPLEMENTADA NO DEPARTAMENTO DE ANÁLISE EPIDEMIOLÓGICA E VIGILÂNCIA DE DOENÇAS NÃO TRANSMISSÍVEIS

A estrutura organizacional delineada para a governança de dados no Departamento é composta pelas seguintes instâncias:

- **Núcleo de Governança de Dados (NGD):** responsável por garantir a segurança e o uso responsável dos dados dentro do Departamento e o compartilhamento com colaboradores externos. O NGD atua como um filtro para os gestores de informação, analisando as solicitações de dados, verificando a conformidade legal e aplicando protocolos de segurança.

- **Gestores da Informação:** servidor responsável por autorizar o acesso e a disponibilização de bases de dados sob sua responsabilidade, observando a legislação em vigor. A direção do Daent é responsável pela gestão das informações, tomando decisões sobre o compartilhamento de dados, com base nas análises do NGD e pareceres das áreas técnicas. Cada sistema de informação possui um gestor responsável, que autoriza o acesso às suas bases de dados.

- **Gestores de Negócio:** servidor responsável por solicitar o desenvolvimento ou a manutenção de sistema de informação, acompanhar evoluções e realizar homologações de entregas sob sua responsabilidade.

No Ministério da Saúde, o gestor da informação e o gestor de negócios de cada Sistema de Informação em Saúde, no âmbito federal, são nomeados por portaria do DataSUS.

- **Guardiões dos Sistemas:** colaboradores do Departamento designados para realizar o tratamento de dados de forma contínua, bem como auxiliar na gestão da Sala de Acesso Restrito (SAR), de modo a permitir o acesso seguro de usuários(as) eventuais, além de realizar recortes, tratamento, anonimização e disponibilização segura das informações para os solicitantes autorizados.

- **Áreas Técnicas:** responsáveis pela vigilância e pela análise de diferentes agravos e doenças. Essas áreas participam do processo de solicitação de dados, realizando as devidas análises e emitindo pareceres sobre os projetos de pesquisa, avaliando sua relevância e seu alinhamento com a agenda de pesquisa dos seus respectivos departamentos. Além disso, manifestam-se quanto à utilização dos dados qualificados por eles. E, ainda, no caso de vinculação de dados com as bases dos sistemas sob gestão do Daent, são responsáveis por autorizar a utilização desses dados provenientes dos sistemas geridos por seus departamentos.

6 | GESTÃO DE DADOS

A gestão de dados é um componente essencial da governança, abrangendo a supervisão, a coordenação e o controle dos recursos para assegurar sua qualidade e aplicabilidade. As instituições de saúde pública devem adotar estratégias eficientes de gerenciamento de dados, incluindo a definição de metadados, a padronização de métodos de coleta e armazenamento, além da criação de políticas de segurança para proteger informações sensíveis. Adicionalmente, o gerenciamento de dados envolve a aplicação de práticas de privacidade e proteção de dados para garantir a conformidade com normas e legislações vigentes.

A geração de informações baseadas em dados é fundamental para a saúde pública, mas depende de um sistema de gestão que seja seguro, adaptável e escalável. Esse sistema deve possibilitar a obtenção, o armazenamento, a análise e o compartilhamento eficiente de dados relacionados à saúde. Dessa forma, é viável promover práticas mais eficazes, eficientes e assertivas no âmbito da saúde pública. As informações derivadas de dados confiáveis desempenham um papel crucial na melhoria da tomada de decisões e na elaboração de políticas de saúde fundamentadas em evidências. Essa abordagem fortalece o ciclo do conhecimento, garantindo que os dados sejam úteis, pertinentes e alinhados a objetivos claros. Ao adotar boas práticas de gestão de informações, as instituições de saúde pública conseguem obter percepções valiosas, que sustentam decisões estratégicas e facilitam a aplicação de políticas mais efetivas. Isso contribui diretamente para o aprimoramento da qualidade dos serviços de saúde prestados à sociedade.

6.1 COLETA DE DADOS

A coleta é uma etapa fundamental para garantir a qualidade e a confiabilidade das informações. Existem diversas técnicas e métodos para realizar a coleta de dados de forma sistemática e consistente. Uma das técnicas mais comuns é a utilização de formulários padronizados, garantindo que as informações sejam registradas de maneira uniforme e organizada. Além disso, a coleta de dados pode envolver a utilização de sistemas de informação, registradas de forma eletrônica, facilitando a análise e o compartilhamento entre diferentes setores da saúde pública.

Outra técnica importante é a validação dos dados coletados, que envolve a verificação da exatidão e da integridade das informações por meio de comparações com fontes confiáveis ou por meio de técnicas estatísticas. O processo de validação viabiliza bases de dados precisas e de qualidade, imprescindível para a elaboração e a extração de informações seguras e com o menor viés possível. Além disso, é fundamental assegurar a qualificação e o envolvimento contínuo dos profissionais de saúde, bem como de qualquer pessoa responsável pela coleta de dados ou pelo preenchimento de Sistemas de Informação em Saúde. Essa medida garante o registro correto das informações, evita a omissão de campos essenciais e assegura que os dados e eventos sejam descritos com o classificador mais adequado possível.

No próximo tópico, abordaremos o armazenamento e a manutenção dos dados, destacando a importância de soluções seguras e atualização periódica para garantir a integridade e a disponibilidade das informações.

6.2 ARMAZENAMENTO E MANUTENÇÃO DE DADOS

O armazenamento e a manutenção de dados consistem na garantia de que as informações coletadas sejam preservadas com segurança e estejam disponíveis quando necessárias. Portanto é essencial implementar soluções de armazenamento seguro, como bancos de dados protegidos por criptografia, *firewalls* e sistemas de becapes regulares. A escolha de plataformas de armazenamento que atendam aos padrões de segurança e privacidade é fundamental para proteger as informações confidenciais dos usuários e garantir a conformidade com regulamentações no âmbito da segurança da informação e da saúde.

Por outro lado, a manutenção periódica dos dados visa garantir que as informações estejam atualizadas e livres de erros. Isso envolve a realização de procedimentos de limpeza, correções de inconsistências, atualização de registros obsoletos e a revisão de metadados para garantir a solidez e a coerência das informações armazenadas.

A implementação de práticas eficazes de armazenamento e manutenção de dados contribui para a disponibilidade de informações confiáveis que podem ser utilizadas na tomada de decisões, na formulação de políticas de saúde e na realização de pesquisas para aprimorar os serviços de saúde pública.

Este tópico destaca a importância de garantir a segurança, a integridade e a disponibilidade dos dados por meio de práticas eficazes de armazenamento e manutenção, fundamentais para o sucesso da governança de dados na área de saúde pública.

6.3 ANÁLISE DOS DADOS

A análise de dados é essencial para produzir evidências, pois permite transformar dados brutos em *insights* significativos, contribuindo para uma compreensão mais profunda de fenômenos e para o avanço científico. Além disso, a análise de dados contribui para a identificação de problemas e melhorias nos próprios dados, planejamento de ações, programas e políticas de monitoramento e prevenção de problemas de saúde, bem como a alocação eficiente de recursos.

Para uma abordagem metodológica apropriada, a análise de dados na área de saúde pública adota ferramentas e técnicas que possam identificar padrões, tendências e correlações relevantes para aprofundar o conhecimento dos problemas. Assim, a utilização de software ou de plataformas especializadas em análise de dados, bem como a aplicação de métodos estatísticos, matemáticos e computacionais, pode facilitar o processamento e a interpretação de grandes conjuntos de informações, servindo para testagem e validação de hipóteses, previsão e inovação no campo da saúde.

Nesse sentido, é importante que os profissionais responsáveis pela análise dos dados possuam habilidades para aplicar as ferramentas e os métodos, assim como para interpretar os dados, transformando-os em informações úteis para explicar desfechos e agravos em saúde.

Ao compreender e adotar práticas de análise de dados, as organizações de saúde pública podem maximizar o valor dos dados coletados, transformando-os em conhecimento acionável e objetivo que impulsiona e aprimora teorias e práticas e fomenta a interdisciplinaridade.

6.4 PROCEDIMENTOS, PROCESSOS E FLUXOS DE GESTÃO DE DADOS

Como visto, a governança refere-se ao conjunto de políticas e processos em torno de gestão de dados, de recursos computacionais, de tecnologia da informação e de segurança, a fim de preservar, salvaguardar e garantir as boas práticas no uso tanto dos dados quanto da infraestrutura de dados. A política de dados diz respeito às regras e aos princípios gerais adotados pela SVSA para orientar os agentes públicos nas atividades de gestão de dados. Nesse sentido, ela deve incluir um conjunto de procedimentos, processos e fluxos necessários para lidar com as etapas de tratamento de dados.

Para organizar as ações de tratamento de dados, pode-se, por exemplo, criar uma planilha que relacione os processos, os estágios da documentação e as prioridades. Procedimentos como acesso e uso de dados, curadoria, processamento e aqueles relacionados à segurança da informação devem ser criados e documentados em formato padrão.

Estabelecidos os procedimentos, devem-se desenvolver regimentos internos com regras definidas para promover a cultura de governança e boas práticas de tratamento de dados.

Os documentos devem ser classificados conforme a confidencialidade e o sigilo da informação, discutidos e definidos pela SVSA ou pela política de segurança da informação, adotando-se, por exemplo, os seguintes níveis de acesso: "Interno", "Público", "Restrito" e "Confidencial".

6.5 A GESTÃO DE DADOS

A gestão de dados deve ser guiada por aspectos políticos, procedimentos e infraestrutura tecnológica para garantir a segurança e a privacidade das informações de saúde. As ações de gestão repousam nos seguintes critérios:

- **Transparência – art. 27, § 3.º, II + Capítulo IV da LAI**. O uso do Sistema Eletrônico de Informação (SEI) para formalizar as solicitações de acesso a dados pessoais sensíveis, assegurando a transparência e a rastreabilidade.
- **Publicidade – art. 7.º, I da LAI + art. 23 e 26 da LGPD**. Estabelecimento de diretrizes claras para a solicitação e o compartilhamento de dados, com procedimentos para diferentes tipos de solicitantes, os documentos necessários e as responsabilidades de cada parte envolvida.
- **Segurança e prevenção – art. 6.º, VII a IX, do Código de Defesa do Consumidor**. Adoção de instrumentos de controle para garantir rastreabilidade, confidencialidade e responsabilidade no uso dos dados. Eles abrangem uma vasta gama de obrigações, incluindo a utilização dos dados apenas para fins específicos, a proteção contra acessos não autorizados e a comunicação imediata de qualquer violação de segurança.

No Daent, por exemplo, foi criada uma estrutura interna com a missão de gerir o fluxo do conjunto de dados de toda a Secretaria. Essa estrutura alinha a criação do NGD e da SAR.

- O NGD tem como principal função proteger os dados pessoais dos cidadãos atendidos pelo Sistema Único de Saúde (SUS), limitando o acesso e o tratamento do conjunto de dados que está sob a responsabilidade da SVSA[7].
- A SAR tem a finalidade de restringir o acesso e promover um ambiente de trabalho seguro e controlado para o tratamento de dados; trata-se de um ambiente seguro projetado para garantir a segurança, a confidencialidade e a salvaguarda dos dados em posse do Departamento. O acesso a esse ambiente deve ser previamente aprovado pelo diretor do Daent.

[7] Cf. Protocolo de Acesso a Dados Identificados – DAENT_09_2022, documento interno.

Assim, cabe ao NGD aplicar a política de gestão de dados, visando à integridade, à qualidade, à disponibilidade e à segurança das informações. Nesse sentido, o núcleo é responsável por gerenciar a entrada à SAR; receber e analisar as demandas por dados advindos dos sistemas geridos pelo Daent; intermediar o processo de autorização de acesso junto ao gestor da informação (diretor do Daent); articular a preparação dos dados junto aos guardiões dos sistemas; e cuidar das boas práticas quanto aos procedimentos, aos fluxos e aos protocolos de acesso a dados, bem como para solicitar dados.

Um agente importante na gestão de dados de saúde é o DataSUS, responsável por facilitar o recebimento, o armazenamento e a disponibilização das informações geradas pelo Ministério da Saúde e pelas Secretarias Estaduais de Saúde. Assim, promove e gerencia a infraestrutura de dados, fornece suporte de informática e atua como repositório, sendo responsável pelo monitoramento da rede nacional de dados do SUS e pela segurança das transações.

Há um conjunto de procedimentos, processos e fluxos elaborados para garantir que os dados sejam coletados, armazenados, acessados e usados de forma segura, ética e eficiente. Eles envolvem diversas etapas referentes a: 1) Coleta e Armazenamento; 2) Tratamento e Curadoria; 3) Segurança e Privacidade; 4) Acesso e Compartilhamento de Dados; e 5) Transparência e Comunicação.

É importante salientar que cada coordenação pode estabelecer seus próprios fluxos e procedimentos para o tratamento de dados.

- **Coleta e armazenamento de dados:** dada a especificidade dos dados sob a responsabilidade do Daent, as atividades de coleta e tratamento do conjunto de dados são exclusivas e atribuídas às áreas técnicas específicas. Assim, cabe a cada área técnica, como parte de suas atividades cotidianas, coletar semanalmente os dados na plataforma DataSUS, realizar as etapas de curadoria e salvaguardar os dados curados em suas instalações.

No Daent, os dados são armazenados na Sala de Acesso Restrito, onde estão os recursos computacionais configurados e disponibilizados para a manipulação de dados identificados, além de dispor de becapes *off-line* regulares para prevenir perdas.

- **Tratamento e curadoria:** para garantir a qualidade dos dados, o Daent usa curadoria semanal e validação bimestral das informações que recebe. Assim, o tratamento e a curadoria de dados ocorrem em dois níveis e momentos distintos:

a. Semanalmente, os analistas da SVSA, após a coleta dos dados, realizam uma rotina de curadoria que envolve a padronização e o enriquecimento de algumas informações. Em seguida, os dados são curados conforme suas especificidades técnicas por cada equipe responsável, que também realiza um tratamento adicional para preparar os dados para a inclusão na base de informações anual. Esse tratamento inclui a verificação de duplicidades e inconsistências, como erros de preenchimento, além da análise de compatibilidade entre os dados.

b. A avaliação de completude, consistência e integridade dos dados estaduais ocorre a cada dois meses. Os resultados dessas validações são registrados em relatórios, acompanhados de observações críticas, para que os estados e municípios revisem seus registros.

O processo de tratamento e curadoria das bases de informação é contínuo até a sua consolidação. Usualmente, estima-se o período de um ano para se garantir o recebimento completo de dados de todos os municípios e estados da Federação e sua revisão e curadoria pelas áreas técnicas. Esse processo é feito considerando os diferentes níveis de acesso e graus de desidentificação, a fim de garantir a segurança e a privacidade das informações.

Após o fechamento do banco de dados para fins estatísticos, ele não é mais atualizado e as informações são disponibilizadas publicamente em plataformas como TabNet. Importante dizer que, embora o banco de dados seja denominado de "fechado", o sistema continua recebendo dados e atualizações de informações.

- **Segurança e privacidade:** o Departamento tem investido em ações para promover a cultura de segurança da informação, melhorar a comunicação com o público e garantir que os dados sejam usados para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Nesse sentido, a gestão da segurança e da privacidade envolve as seguintes prerrogativas:

a. O acesso aos dados é baseado em **papéis e responsabilidades** e envolve:

- **Acesso controlado e zonas de acesso:** o acesso é feito por meio de logins e senhas individuais fornecidos pelo DataSUS. A autorização vincula o usuário a um computador específico, por meio do ID da máquina, e a diretórios específicos. Embora os dados sejam armazenados em pastas que permitem o compartilhamento entre os computadores do Departamento, o acesso é restrito às áreas técnicas responsáveis e aos sistemas sob sua responsabilidade. Além disso, são adotadas medidas de segurança para rastrear as operações como logs de transações e proteção contra acessos não autorizados.

- **Uso responsável e confidencial dos dados:** todos os agentes públicos envolvidos no tratamento de dados assinam termos de responsabilidade, identificando-se como operadores de dados, enquanto seus superiores são identificados como controladores. Todos estão sujeitos a sanções de natureza civil, penal e administrativa.
- **Transferência segura de dados:** o compartilhamento de dados criptografados é uma prática padrão dentro do Daent. A SVSA está trabalhando para fortalecer a cultura de criptografia em todos os departamentos e instâncias de acesso e uso.

b. Provisão de um **ambiente seguro** para a manipulação de dados, incluindo sala de acesso restrito, monitoramento por câmeras de vigilância, computadores dedicados e mídias específicas para armazenamento, como HDs-cofre, com proibição de cópia, incluindo para pastas na nuvem.

c. O uso **ético**, **legal** e **protetivo** das informações dos cidadãos registrados baseia-se na implementação de ações para garantir os direitos dos titulares dos dados, zelando pela privacidade dos indivíduos registrados nos sistemas e assegurando que as informações não sejam utilizadas para decisões punitivas.

Acesso e compartilhamento de dados: por se tratar de base de dados contendo informações pessoais e sensíveis, de caráter restrito, conforme artigo 31 da Lei n.º 12.527/2011 (LAI), e sigiloso, conforme Lei n.º 14.289/2022, cujo acesso está discriminado na Lei n.º 13.709/2018 (LGPD) e o compartilhamento com órgãos da Administração Pública Federal obedece às regras gerais definidas pelo Comitê Central de Governança de Dados, instituído pelo Decreto n.º 10.046/2019, a avaliação de solicitações de acesso e compartilhamento deve considerar, além dos princípios da LGPD, o tipo de solicitante, os objetivos e o interesses de uso. Os pedidos de acesso, submetidos via Sistema Eletrônico de Informações (SEI), que chegam ao NGD são analisados, verificando o cumprimento de todos os requisitos exigidos pela legislação vigente de proteção de dados pessoais. Conforme estabelecido na Nota Técnica n.º 1/2025-Daent/SVSA/MS, podem solicitar acesso aos dados identificados os titulares, as unidades do Ministério da Saúde, os órgãos da Administração Pública, os órgãos de justiça, as instituições de ensino e pesquisa e os órgãos de pesquisa.

Todos os solicitantes, conforme sua especificidade, devem fornecer a documentação pertinente ao pedido, preencher formulários e acordos de acesso, incluindo um plano de vinculação, que é necessário para solicitar *linkage* entre conjuntos de dados. A autorização de compartilhamento passa pela instância do NGD e pela diretoria do Daent, além de, em casos específicos, pela regulação da Consultoria Jurídica no Ministério da Saúde (Conjur/MS).

O Ministério da Saúde utiliza o SEI para protocolar as demandas internas e externas, incluindo o registro de solicitações de acesso aos dados dos sistemas de informação sob sua custódia. Dessa forma, e segundo o artigo 37 da LGPD, mantém o registro das operações de tratamento de dados pessoais que realiza e controla o acesso aos dados pessoais sensíveis, garantindo que apenas usuários autorizados manipulem as informações. Além disso, o Decreto n.º 7.724/2012, no seu artigo 61, dita que o acesso à informação pessoal por terceiros será condicionado à assinatura de termos de responsabilidade, entre outros. No Quadro 1, encontra-se a relação de termos utilizados na gestão, com a descrição de sua finalidade e tipo de uso.

QUADRO 1 Termos e declaração de acesso aos dados identificados utilizados pelo Daent

DOCUMENTO	FINALIDADE	PÚBLICO
Termo de Responsabilidade e Confidencialidade	Formalizar a cessão de bases de dados identificadas dos Sistemas de Informação em Saúde (SIS). Controla a necessidade, a finalidade e as obrigações de uso.	Público externo e interno do Ministério da Saúde.
Plano de Vinculação de Dados	Definir os detalhes da vinculação de diferentes bases de dados, incluindo os recortes temporais e territoriais, variáveis a serem pareadas, estratégias de blocagem, softwares utilizados e variáveis da base final.	
Termo de Responsabilidade para Recepção de Bases de Dados	Formalizar a entrega de bases de dados geradas na Sala de Acesso Restrito do Daent. Controla a responsabilidade e os requisitos de uso da informação.	
Termo de Anuência	Registrar a concordância do Daent/SVSA/MS com a execução de um projeto de pesquisa, após aprovação ética.	
Declaração de Infraestrutura e Instalações	Declarar a disponibilização da infraestrutura da Sala de Acesso Restrito do Daent para a execução de um projeto de pesquisa específico, após aprovação ética.	

Fonte: Daent/SVSA.

Transparência e comunicação

- O Daent/SVSA/MS esclarece as dúvidas sobre segurança de dados por meio de contato direto com o NGD (**ngd@saude.gov.br**).
- Canais como o Fala.BR, o Serviço de Informação ao Cidadão (SIC) e a Ouvidoria do Ministério da Saúde estão disponíveis para que os cidadãos tirem dúvidas e façam solicitações relacionadas à privacidade e ao uso de seus dados.
- Para fins de transparência ativa, o Daent divulga microdados dos sistemas de informação sob sua gestão, disponibiliza e atualiza periodicamente suas bases anonimizadas (sem identificação pessoal no site do DataSUS (**https://datasus.saude.gov.br/**), em sua página (**https://svs.aids.gov.br/daent/**) e no Portal de Dados Abertos (**https://dados.gov.br/home**).

7 | COMPARTILHAMENTO DE DADOS

O compartilhamento de dados, tanto interno entre departamentos quanto externo com órgãos da Administração Pública Federal, exige a definição de requisitos específicos para essas operações, a ser realizada pelo gestor da informação responsável pelo sistema de informação. É fundamental avaliar os aspectos legais e regulamentares aplicáveis aos dados e às informações a serem compartilhados. Vale ressaltar que os requisitos de dados podem variar de acordo com o domínio e o tipo de informação envolvida.

O Decreto n.º 10.046/2019[8] estabelece um arcabouço legal para a governança no compartilhamento de dados no âmbito da Administração Pública Federal. A partir das disposições trazidas, compreende-se que a estrutura de governança deve considerar: os níveis de compartilhamento; os órgãos e as entidades responsáveis; os instrumentos e as condições de compartilhamento; e a política, os princípios e as diretrizes de dados da Administração. Nesse sentido, é necessário:

1. Definir quem será responsável pela estratégia e direção do compartilhamento.
2. Estabelecer quem cuidará da provisão dos dados solicitados.
3. Definir quais serão os possíveis solicitantes de dados.
4. Que todas as operações estejam em conformidade legal e ética[9].
5. O desenvolvimento de uma política de solicitação, troca ou compartilhamento de dados. Os acordos de partilha de dados devem especificar as condições de uso e o acesso previstos, bem como os tempos de resposta e de duração da operação. É preciso definir com quais organizações os dados serão compartilhados, como serão compartilhados e qual

[8]Ver mais no Decreto n.º 10.046, de 9 de outubro de 2019, que 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.

[9]Veja mais em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf.

a finalidade de uso. Além da política de compartilhamento, essa avaliação permitirá a criação de um plano de monitoramento e avaliação de risco de compartilhamento de dados.

6. A produção de uma estratégia que adeque os recursos e as competências para definição do fluxo e de compartilhamento. Assim, acordos de partilha de dados mais tradicionais e menos complexos podem ser geridos em processos-padrão, apoiados pelo agente de compartilhamento. Acordos mais elaborados, mais complexos ou de maior risco, devem ser atribuídos ao especialista estratégico. Lembre-se, uma política de compartilhamento de dados requer também uma política de categorização de dados.

7. O planejamento de pontos de controle para a transação de dados. Projetar uma arquitetura de transação; definir os serviços, os fluxos, os mecanismos de execução e os padrões de transação; escolher as ferramentas e tecnologias adequadas para essa arquitetura de transação, considerando fatores como escalabilidade, segurança e compatibilidade.

A observação dos pontos listados nesta seção constitui o quadro de governança para o compartilhamento de dados[10]**.** Esta estrutura reforça o cumprimento dos princípios da finalidade, da transparência e da necessidade da LGPD (parâmetros legais), assim como dos princípios da legalidade, da moralidade e da publicidade estabelecidos na Constituição Federal (parâmetros constitucionais)[11]. É essencial que os propósitos do compartilhamento sejam legítimos, específicos e explícitos, estejam em conformidade com as finalidades informadas e sejam transparentes.

No que diz respeito aos procedimentos para a criação e o compartilhamento do catálogo de dados, a estrutura de compartilhamento deve também abordar outras questões relacionadas à gestão e à administração técnica dos dados, incluindo sua **acessibilidade** e **usabilidade**, além da própria qualidade, transparência e rastreabilidade. No contexto da acessibilidade e da usabilidade, o setor de saúde tem adotado a interoperabilidade como meio de facilitar o compartilhamento e aumentar o uso dos dados. Essa estratégia permite a comunicação e a troca de informações entre sistemas distintos. Uma arquitetura consistente de sistema de informação é fundamental para alcançar a interoperabilidade de dados e informações. Em resumo, a interoperabilidade inclui processos relacionados à movimentação e à consolidação de dados dentro e entre organizações e estruturas de armazenamento.

[10]O compartilhamento de dados pelo setor público ocorre em todos casos previstos para a transferência e considera também as hipóteses mais amplas previstas no art. 7º, caput, I da LGPD. Observa-se que tanto a transferência quanto o uso compartilhado dependem de autorização (art. 5º, XVI) e informe (art. 27, caput) específicos à ANPD.

[11]O uso de dados pelo poder público é regido tanto pelos princípios da proteção de dados quanto pela própria Constituição, conforme indicado no Capítulo 3 deste documento.

A acessibilidade refere-se à disponibilidade de um conjunto de dados para pesquisa e à sua capacidade de ser descoberto. A usabilidade, entretanto, diz respeito à adequação dos dados para uso. Qualidade, transparência e rastreabilidade são princípios de governança, como discutido anteriormente. Qualidade enfatiza a adequação dos dados para seus usos pretendidos, destacando a necessidade de uma abordagem estruturada para compreender, documentar e mensurar a adequação dos dados. Transparência e rastreabilidade, por outro lado, medem a disponibilidade de informações sobre a origem dos dados e seus sistemas de processamento.

A estratégia de investir na acessibilidade e na usabilidade dos dados deve estar alinhada aos padrões definidos pela comunidade de saúde, no que tange a formatos e convenções de dados e informações. Isso tanto facilita a interoperabilidade dos conjuntos de dados quanto o reúso de dados relevantes para a saúde. A Rede Nacional de Dados em Saúde (RNDS), plataforma nacional de interoperabilidade em saúde, por exemplo, define para cada conjunto de dados os modelos de informação e computacional que normatizam as regras de uso e a padronização que serão suportadas pelos sistemas de informação que participam da troca de informações em saúde com a RNDS.

FIQUE DE OLHO

Avaliação de acessibilidade e usabilidade deve considerar aspectos como:
a disponibilidade de documentação (por exemplo, dicionário de dados, notas técnicas etc.), a existência de metadados, se os dados estão em um formato padronizado que permite interoperabilidade (independentemente de máquina e escalável), se estão anonimizados, se existem estratégias de visualização, e se há ferramentas disponíveis que suportem acesso e uso, entre outras questões.

7.1 A POLÍTICA DE SOLICITAÇÃO, TROCA E COMPARTILHAMENTO DE DADOS NO DAENT/SVSA/MS

A política de compartilhamento de dados do Daent é regida, em específico, pela Nota Informativa n.º 1/2025-Daent/SVSA/MS, desenvolvida a partir das Leis n.º 12.527/2011 (Lei de Acesso à Informação) e n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais); e pelos Decretos n.º 7.724/2012 (acesso à informação) e n.º 10.046/2019 (compartilhamento de dados). As decisões sobre o compartilhamento baseiam-se nos seguintes critérios:

I. **Proveniência dos dados**

II. **Organizações e finalidades do compartilhamento**

III. **Tipos de dados**

IV. **Condições de uso e duração do compartilhamento**

V. **Instrumentos de acesso aos dados**

VI. **Meios de compartilhamento**

VII. **Revisão da política**

I. Proveniência dos dados

A demanda deve tratar sobre uma base de dados sob a tutela e a gestão do Departamento.

II. Organizações e finalidades do compartilhamento

De forma geral, o Daent compartilha seus dados com:

- **Órgãos da Administração Pública Federal**: para subsidiar políticas públicas, ações de vigilância em saúde, estudos epidemiológicos, planejamento e avaliação de programas de saúde. É importante ressaltar que, para a transferência de dados nominais, o órgão deve dispor de uma infraestrutura segura para o armazenamento desses dados.

É importante notar que os pedidos feitos por pessoas físicas e os pedidos que se enquadrem nas exceções listadas no artigo 4º da LGPD, como tratamento de dados para fins jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, entre outros, são dirigidos aos canais de amplo compartilhamento.

III. Tipos de dados

Os dados podem ser plenamente compartilhados internamente entre as instâncias da SVSA, desde que justificada a necessidade. Já os compartilhamentos com instituições externas ocorrem mediante formalização de acordos e análise de pedidos caso a caso. Estabelece-se que:

- Dados brutos identificados têm, a princípio, acesso restrito às equipes técnicas internas do Ministério da Saúde responsáveis pela curadoria dos dados.
- Dados não identificados estão disponíveis publicamente por meio da transparência ativa, após a curadoria e a validação pelas áreas técnicas.
- Dados curados e identificados são de uso interno do Ministério da Saúde, podendo ser compartilhados para fins de pesquisa, conforme o art. 13 da LGPD, que ratifica a autorização para disponibilização de acesso a dados pessoais para realização de estudos e pesquisas, estipulando, em acréscimo, medidas específicas de prevenção e de segurança a serem observadas no campo dos estudos de saúde pública. No entanto, vale ressaltar, que após a manipulação justificada e necessária de dados nominais, eles são anonimizados e compartilhados para fins de pesquisa.

IV. Condições de uso e duração do compartilhamento

O compartilhamento de dados nominais para colaboradores internos será durante o período necessário para a manipulação, com a utilização justificada aos gestores da informação. Os solicitantes externos que necessitarem manipular dados nas instalações do Ministério da Saúde terão acesso restrito ao período em que estão realizando o procedimento. Recomenda-se também que a segurança dos dados anonimizados que sejam disponibilizados seja garantida por tempo indeterminado.

V. Instrumentos de acesso aos dados

O Daent reconhece a importância da formalização para o compartilhamento de dados, conforme previsto na LGPD e no Decreto n.º 10.046/2019. Assim, o compartilhamento dos seus dados se dará por meio de instrumentos como:

- **Acordos de cooperação técnica**: é um instrumento jurídico utilizado para formalizar uma parceria entre órgãos e entidades da Administração Pública para a realização de ações conjuntas. O objetivo é alcançar um propósito comum, voltado para o interesse público, por meio da troca de conhecimentos, experiências, recursos humanos e materiais. O acordo de cooperação diferencia-se de convênios, contratos de repasse e termos de execução descentralizada pelo simples fato de não existir a possibilidade de transferência de recursos entre os partícipes (Decreto n.º 11.531, de 16 de maio de 2023).

- **Decisões administrativas**: as autorizações para o compartilhamento de dados classificados como específicos são expedidas pelo agente competente no Daent/SVSA e pelo gestor da informação do(s) sistema(s) após a protocolização de um pedido.

Todas as solicitações, provenientes de entidades externas e internas, precisam ser submetidas pelo sistema SEI para fins de rastreabilidade, controle e registro de cadeia de custódia.

VI. Meios de compartilhamento

O compartilhamento de dados será realizado por meio de plataformas digitais seguras, como o QWare e/ou o OneDrive (com a opção de encriptação ponta a ponta e link de acesso restrito a usuários autorizados), que garantem a segurança e a rastreabilidade das informações. O QWare é utilizado para o envio de bases do Ministério da Saúde para colaboradores externos, enquanto o OneDrive é utilizado para a recepção de dados destinados ao Ministério da Saúde.

O compartilhamento de dados identificados, classificados como sensíveis e de acesso restrito, é realizado por meio da ferramenta de criptografia VeraCrypt, que transforma as informações em um formato ilegível para indivíduos não autorizados.

VII. Revisão da política

O Daent/SVSA reserva-se o direito de revisar e atualizar periodicamente a sua política, para mantê-la válida e adequada às novas demandas e legislações.

8 | PLANO DE GOVERNANÇA DE DADOS

O Plano de Governança de Dados apoia o planejamento, a implementação, a avaliação e o monitoramento de uma estratégia de governança aplicada, além de auxiliar na adaptação da estrutura institucional à sua prática. Conforme indicado na literatura, o caminho para a governança começa com a definição de seu escopo e princípios (do propósito à conformação) e prossegue com a estipulação de padrões, estruturas e processos. Isso envolve ações estratégicas, táticas e operacionais, e pode requerer a construção ou a melhoria de capacidades organizacionais (World Bank, 2021; NAO, 2022)[12].

No âmbito dessa estratégia, instituição, pessoas, processos e dados são os principais focos de avaliação, ajudando a entender o cenário atual, a identificar barreiras e a propor soluções.

Para delinear, implantar e avaliar a estratégia de governança de dados, a **etapa inicial** consiste em alinhar estrategicamente os propósitos institucionais e os objetivos a serem alcançados. Para isso, é necessário avaliar as expectativas da Secretaria com um processo independente e autoavaliativo.

A avaliação da situação atual da instituição requer mapear o estágio dos processos relacionados ao tratamento de dados, toda a estrutura envolvida e os marcos regulatórios, éticos, de segurança e privacidade pertinentes, visando projetar um cenário futuro. Essa iniciativa permite compreender os interesses institucionais e o ambiente, incluindo toda a estrutura que compõe o quadro funcional da SVSA. Nessa fase, deve-se:

- Avaliar os interesses da instituição e a estrutura atual para lidar com os dados em saúde (considerando parceiros e expectativas legais e de conformidade que desejam satisfazer etc.).
- Identificar pontos fortes e fracos.

[12]Para o caso brasileiro, ver exemplo da Petrobrás: https://www.gov.br/governodigital/pt-br/governanca-de-dados/petrobras-maturidade_dados_analytics_.pdf.

- Articular o escopo e os princípios-chave de governança que se deseja incorporar.

Esse alinhamento inicial abre caminho para o planejamento, fase que deve delinear o modelo de governança que será implementado. É importante definir as iniciativas mais relevantes para a instituição. O tema escolhido deve ser avaliado, abordando os principais pontos que o impactam e as questões a serem resolvidas. Essa fase pode requerer a formação de grupo de debate ou comitê de governança. Ao concluir a etapa de planejamento e elaborar as propostas que guiarão as decisões finais, é necessário avançar para o registro das definições gerais da estratégia de governança. Isso ajudará a estabelecer diretrizes e a estruturar as definições e orientações estratégicas do modelo de governança a ser implementado. As definições devem apresentar:

- A visão da estratégia de governança de dados, sua direção, seus objetivos e métricas, princípios e benefícios.
- A projeção da estrutura necessária para a governança (considerando os pontos fortes e fracos identificados).
- Definição de papéis e responsabilidades (estratégico).
- Definição final do modelo e das funções de governança que serão implementados.

FIQUE DE OLHO

A política de dados nacional da saúde influencia a definição das diretrizes do modelo de governança adotado. Nesse sentido, o alinhamento estratégico deve certificar-se de que há clareza quanto ao sentido, aos propósitos e aos resultados que se deseja obter com o modelo de governança.

A **etapa seguinte** consiste no delineamento do plano e na definição do escopo das ações de governança a serem incorporadas. Essa fase avalia a capacidade de governança e o estágio de maturidade atual da instituição, classificando-o conforme a fase de incorporação e desenvolvimento. Deve-se observar a situação geral da instituição, e depois o foco deve ser voltado para setores específicos. A abordagem analisa as pessoas, a presença ou a ausência de gestão de dados, os desafios e riscos, e as ações necessárias para melhoria e amadurecimento. Devem ser considerados: a existência de processos para tratamento de dados, a compreensão dos elementos que apoiam a governança e garantem sua funcionalidade, e os fatores críticos que impactam e contribuem para a competência

organizacional. Segundo a estratégia definida na fase de planejamento e alinhamento estratégico, a maturidade também pode ser avaliada por componentes de interesse, assim como a necessidade de aperfeiçoamento da gestão, fluxo de dados, qualidade de dados, metadados, competência e capacidades das equipes.

A partir dessas observações, deve-se definir o escopo do conhecimento ou ações necessárias para a governança, conforme sugerido pelo modelo DAMA-BOK.

FIQUE POR DENTRO

Para a saúde pública, o DAMA-BOK enfatiza a importância do conhecimento em governança de dados, arquitetura, modelagem e qualidade. Por exemplo, na Rede Nacional de Saúde, a definição da arquitetura de dados visa facilitar a interoperabilidade entre diferentes sistemas de informação e a integração eficaz de dados provenientes de diversas fontes. Além disso, a modelagem precisa e a garantia da qualidade dos dados são fundamentais para assegurar a confiabilidade das informações usadas na tomada de decisões e na formulação de políticas de saúde.

A fase de delineamento do plano de governança conduzirá a:

- Avaliação do estágio de maturidade dos componentes do modelo de governança em que se quer investir, bem como avaliação das condições de escalabilidade e melhorias desses componentes.
- Definição de um plano de ação com projeção de entregas, prazos, resultados e métricas.
- Definição de papéis e responsabilidades (táticos e operacionais).

Caso a SVSA deseje implementar uma estratégia institucional de compartilhamento de dados voltada para a interoperabilidade, a execução dessa estratégia será respaldada por objetivos que promovam a capacitação da equipe em modelagem, processamento e integração de dados, definição de normas e interfaces, além de desenvolver uma estrutura para abertura e padronização de dados. A estratégia também deverá adotar uma abordagem focada no ciclo de vida dos dados, o que envolve a criação de estratégias para garantir a qualidade e a gestão adequada dos dados.

O uso de ferramentas para gerenciar as atividades facilita o desenvolvimento do plano de governança, bem como permite documentar e avaliar a sua jornada de implementação. Os documentos podem ser organizados por orientação temática e distribuídos da seguinte forma:

- **O Quadro de Governança de Dados** – V.1.0 (New South Wales, 2021) (Apêndice A), documento principal, que deve registrar a trajetória de implantação e desenvolvimento do plano de governança.
- **O Modelo de Avaliação da Maturidade de Gestão** – V.1.0 (Dun *et al*., 2021; Pen, 2015) (Apêndice B), que propõe uma forma de avaliação e quantificação do nível de maturidade das ações de gestão de dados aplicadas a conjuntos de dados individuais da SVSA. A avaliação parte de uma escala de maturidade graduada para cada elemento essencial que compõe a administração de dados de saúde.
- **O Quadro de Conhecimento em Governança de Dados** – V.1.0 (Scholtens, 2019) (Apêndice C) que relaciona as competências necessárias para a prática de gestão de dados. Esse documento, juntamente com a planilha de papéis e responsabilidades de dados (material auxiliar), apoia as estratégias de capacitação continuada da equipe.

Todos esses três instrumentos avaliativos devem ser revisados e atualizados conforme a necessidade da SVSA.

É importante acompanhar o progresso e a eficácia da estrutura de governança delineada, avaliando os resultados em relação aos objetivos estabelecidos, bem como a flexibilidade e a escalabilidade do modelo. É essencial, também, criar mecanismos para a aprendizagem e a melhoria contínua do processo, incorporando os resultados e as propostas obtidos das avaliações periódicas e fazendo ajustes necessários.

9 | RECOMENDAÇÕS FINAIS

A implantação da governança de dados pode variar em termos de propósito (ou seja, a melhoria de uma questão técnica específica), de alcance (curto, médio e longo prazo), de foco (estratégico, tático ou operacional), de escopo (interna ou externa) e de abordagem (distribuída, centralizada, compartilhada, em rede ou de plataforma, ou até por domínio de dados). Independentemente do modelo a ser adotado, é necessário propiciar uma cultura, um ambiente institucional e técnico adequado para a implantação.

A trilha de governança de dados adotada pelo governo brasileiro tem priorizado iniciativas que ampliam a maturidade digital da sociedade e do governo federal, protegem a privacidade e a segurança dos dados, promovem a cultura e a gestão de dados e desenvolvem tecnologias como inteligência artificial e *blockchain*. Plataformas digitais têm sido lançadas para simplificar a interação do governo com a sociedade, fortalecer a interoperabilidade de sistemas e fomentar dados abertos. Um exemplo dessas iniciativas é a Estratégia de Saúde Digital para o Brasil 2028, que expande a Política Nacional de Informação em Saúde e inclui programas como o DigiSUS e o Conecte SUS, melhorando a qualidade dos serviços de saúde e facilitando a interoperabilidade dos sistemas de informação. Ressalta-se que as ações para a saúde digital também estimulam a formação de confederações e redes, segundo uma perspectiva de compartilhamento de dados que envolve atores distintos.

Dessa forma, cabe às Secretarias de Saúde, atores-chave, e, especificamente, à Secretaria de Vigilância em Saúde e Ambiente (SVSA), diante da importância dos sistemas de informação sob sua gestão para o Sistema Único de Saúde (SUS), adotarem um modelo de governança que promova o suporte às melhores práticas de gestão, por meio de serviços e processos de tratamento de dados, além de se incorporarem à estratégia de saúde digital para criar um ecossistema de governança de dados que aproveite o ambiente de interconectividade em desenvolvimento.

A jornada para a adoção da governança de dados é desafiadora e começa com o entendimento do negócio e dos objetivos que a Secretaria deseja alcançar na gestão de seus dados. Alguns tipos de indicadores de um programa de governança de dados são relacionados às métricas de negócios, compreensão dos processos de governança, integração de informações, qualidade e operações de dados, além da segurança e da privacidade.

Do ponto de vista da qualidade (e da acessibilidade e usabilidade dos dados), um levantamento dos perfis das bases de dados produzidas pela SVSA revelou limitações e desafios heterogêneos em termos de atualizações de sistemas e suas versões, qualidade e cobertura, coleta e processamento de dados, além das práticas de acesso e uso. Evidenciou-se uma diversidade de estágios de maturidade, marcada por baixa capacidade de interoperabilidade entre eles e diversificadas estratégias de abertura de dados (Brasil, 2023). Esse cenário reflete a experiência nacional na implementação do sistema de saúde, caracterizada pela incorporação federada, distribuída e diversificada (não padronizada) de sistemas de informação.

No que diz respeito aos mecanismos e às metodologias para as ações de gestão e administração de dados, focadas no estabelecimento de procedimentos e fluxos de dados, a experiência da parceria entre o Daent/Cgiae e o Centro de Integração de Dados e Conhecimentos para a Saúde (Cidacs/Fiocruz Bahia) no projeto TED 159/2019 destacou a importância de ter processos e regras bem definidos para o uso, acesso, recebimento, armazenamento, tratamento e compartilhamento de dados, bem como para garantir a segurança da informação, a privacidade e a proteção de dados.

Quando se considera todo o cenário mencionado sob a ótica do ciclo de vida dos dados, nota-se que cada fase desse ciclo enfrenta desafios específicos que exigem medidas distintas. Por exemplo, as diferentes estratégias de acesso e disponibilidade de dados para uso secundário entre os sistemas de informação podem requerer investimentos na uniformização de painéis de visualização, estrutura de dados, e na disponibilização de equipe técnica especializada em análise de dados, entre outros. Isso se baseia nos resultados do processamento de dados em cada estágio.

Portanto investir na formalização e na consolidação de estratégias e instâncias de governança de dados deve ser uma prioridade estratégica, que envolve o desenvolvimento de capacidades institucionais, a implementação de padrões de qualidade e segurança, a ampliação do ciclo de valor e a promoção de uma cultura de responsabilidade, transparência e ética no uso dos dados.

10 | MATERIAIS COMPLEMENTARES

10.1 LINKS E REFERÊNCIAS PARA FERRAMENTAS E LEITURAS ADICIONAIS SOBRE O TEMA (ESCOLA DE GOVERNO DA ENAP/ESCOLA VIRTUAL DO GOVERNO)

CURSOS

Governança de Dados

- Governança de Dados
- Governança de Dados na Transformação Digital

Integração e Interoperabilidade

- Governo Integrado: Como Construí-lo?

Ciência e Análise de Dados

- Estatística
- Análise de Dados como suporte à tomada de decisão
- Aprendendo com Python
- Análise de Dados em Linguagem R
- Aplicação do Power BI para Aprimoramento da Gestão

Dados Aplicados à Vigilância em Saúde

- Análise de dados para a vigilância em saúde – curso básico
- Análise espacial de dados para a vigilância em saúde
- Linkage de bases de dados de saúde
- Visualização de dados de interesse para a vigilância em saúde

- Construção de diagramas de controle na vigilância em saúde
- Construção de painéis (*dashboards*) para monitoramento de indicadores de saúde
- Produção automatizada de relatórios na vigilância em saúde

10.2 CHECKLIST – QUALIDADE DE DADOS

Definição de Metadados e Padrões de Dados

[ ] Estabelecer padrões claros para formatos de dados.
[ ] Documentar metadados para cada tipo de dado.

Avaliação de Precisão

[ ] Verificar a correta correspondência dos dados com fontes confiáveis.
[ ] Assegurar que os dados precisos tenham mecanismos para que sejam consistentemente capturados.

Verificação de Completude

[ ] Certificar-se de que todos os conjuntos de dados estejam completos.
[ ] Identificar informações ausentes quando possível.

Consistência e Conformidade

[ ] Garantir que os dados sejam consistentes entre diferentes sistemas.
[ ] Checar a aderência às regras e aos regulamentações relevantes.

Manutenção da Atualidade

[ ] Estabelecer procedimentos para atualização regular dos dados.
[ ] Remover ou corrigir dados desatualizados ou irrelevantes.

Integridade Referencial

[ ] Validar relações e dependências entre conjuntos de dados.
[ ] Corrigir referências quebradas ou inválidas.

Validação de Formatos e Unidades de Medida

[ ] Confirmar se os formatos e as unidades de medida estão corretos.
[ ] Converter dados para os formatos-padrão, conforme necessário.

Acessibilidade e Proteção

[ ] Garantir que os dados sejam acessíveis para usuários autorizados.
[ ] Proteger dados contra acessos não autorizados ou vazamentos.

Usabilidade dos Dados

[ ] Avaliar se os dados estão em um formato que suporte seu uso pretendido.
[ ] Certificar-se de que os dados estejam prontos para análise.

Exclusividade e Não Duplicidade

[ ] Verificar se os registros são únicos e não duplicados.

[ ] Eliminar ou mesclar informações duplicadas, conforme necessário.

Monitoramento e Feedback dos Usuários

[ ] Implementar mecanismos para monitorar a qualidade dos dados continuamente.

[ ] Estabelecer um sistema para receber e integrar feedback sobre a qualidade dos dados dos usuários.

Avaliação de Impacto de Qualidade de Dados

[ ] Realizar avaliações de impacto acerca das implicações de dados de baixa qualidade no negócio.

[ ] Planejar a mitigação de riscos para tratar as áreas identificadas.

Governança e Responsabilidade

[ ] Atribuir responsabilidades claras para a gestão da qualidade de dados.

[ ] Integrar a qualidade de dados na governança e nos processos de gestão, treinamento e conscientização.

[ ] Assegurar que a equipe receba treinamento adequado em qualidade de dados.

[ ] Promover a conscientização sobre a importância da qualidade dos dados.

Ferramentas e Tecnologias de Suporte

[ ] Implementar e utilizar ferramentas adequadas para auxiliar na manutenção da qualidade dos dados.

[ ] Atualizar tecnologias, conforme necessário, para manter o alinhamento com as melhores práticas de qualidade de dados.

Documentação e Procedimentos Operacionais

[ ] Manter documentação completa dos procedimentos de qualidade de dados.

[ ] Certificar-se de que os procedimentos estejam acessíveis e sejam seguidos pela equipe.

Validação e Testes Regulares

[ ] Implementar processos de validação e limpeza de dados regulares.

[ ] Conduzir testes periódicos para garantir a manutenção da qualidade.

Relatórios de Qualidade de Dados

[ ] Desenvolver relatórios periódicos para acompanhar a qualidade dos dados ao longo do tempo.

[ ] Utilizar relatórios para tomar decisões informadas e orientadas por dados.

REFERÊNCIAS

ABRAHAM, R.; BROCKE, J. vom; SCHNEIDER, J. Data governance: a conceptual framework, structured review, and research agenda. **International Journal of Information Management**, v. 49, 2019. Disponível em: https://doi.org/10.1016/j.ijinfomgt.2019.07.008. Acesso em: 10 abr. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. **Tratamento de dados pessoais pelo poder público: guia orientativo**. Brasília, DF: ANTP, 2022. 28 p. Disponível em: https://bit.ly/3gXPEBR. Acesso em: 15 maio 2024.

BRASIL. Governo Digital. **Governança de dados**. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/IND/governanca-de-dados. Acesso em: 13 dez. 2024.

BRASIL. Governo Digital. **Infraestrutura Nacional de Dados**. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados. Acesso em: 13 dez. 2024.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis. **Dados para vigilância**: perfis das bases de dados produzidas pela Vigilância em Saúde no Brasil. Brasília, DF: MS, 2023. 127 p.: il. color.

DUNN, R. *et al.* Ferramentas de avaliação de maturidade de gestão para modernização da gestão de dados climáticos. **Data Science Journal**, 2021. Disponível em: https://doi.org/10.5334/dsj-2021-007. Acesso em: 3 fev. 2024.

HENDERSON, D.; EARLEY, S.; SEBASTIAN-COLEMAN, L. (ed.). **DAMA-DMBOK**: Data Management Body of Knowledge. 2. ed. Bradley Beach, NJ: Technics Publications, 2017. 628 p.

NATIONAL AUDIT OFFICE. **Improving government data**: a guide for senior leaders. London: NAO, 2022. 36 p. Disponível em: https://www.nao.org.uk/wp-content/uploads/2022/07/Improving-government-data-a-guide-for-senior-leaders.pdf. Acesso em: 26 maio 2024.

NEW SOUTH WALES. **NSW Data Governance Toolkit V1.1**. Sydney: Government of New South Wales, 2021. 25 p. Disponível em: https://data.nsw.gov.au/sites/default/files/inlinfiles/NSW%20Data%20Governance%20Toolkit%20V1.1.pdf. Acesso em: 3 fev. 2024.

PENG, G. **Modelo de avaliação de maturidade de administração de dados científicos**. Versão: NCDC-CICS-SMM-0001-Rev.1 v4.0. Asheville, NC: NOAA, 2015. Disponível em: https://doi.org/10.6084/m9.figshare.1211954. Acesso em: 3 fev. 2024.

RIVERA PEREZ, J. A.; BITAR, O.; DOMAGALA, N. **Good practice principles for data ethics in the public sector**. Zenodo, 2021. Disponível em: https://doi.org/10.5281/zenodo.5218703. Acesso em: 20 jun. 2024.

SCHOLTENS, S. *et al.* **Life sciences data steward function matrix (V1.1).** Zenodo, 2019. Disponível em: https://doi.org/10.5281/zenodo.2561723. Acesso em: 14 maio 2024.

WORLD BANK. Institutions for data governance: building trust through collective action. In: WORLD BANK. **World development report 2021**: data for better lives. Washington, D.C.: World Bank, 2021. p. 265–296. Disponível em: https://doi.org/10.1596/978-1-4648-1600-0_ch8. Acesso em: 14 fev. 2024.

GLOSSÁRIO

Termos técnicos e jargões utilizados dentro do Guia, a fim de garantir uma compreensão unificada.

Agente público ▸ Aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na Administração Pública e que possui condição pessoal – inerente ao efetivo exercício de cargo, função, emprego ou atividade – indispensável para o acesso ou a cessão das bases de dados com informações pessoais em saúde (Lei n.º 8.429/1992).

Agentes de tratamento de dados ▸ Controlador e operador (art. 5.º da LGPD).

Anonimização ▸ Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5.º, XI, da LGPD).

Bancos de dados sob gestão do Daent ▸ Sistema de Informação sobre Nascidos Vivos (Sinasc), Sistema de Informação de Agravos de Notificação (Sinan), Sistema de Informações sobre Mortalidade (SIM), Sistema de Registro de Eventos em Saúde Pública (Resp) e Sistema de Notificação dos Casos de Síndrome Respiratória Leve (e-SUS Notifica).

Chefia imediata ▸ Servidor investido em cargo ou função de chefia, atuando como superior hierárquico direto de outros servidores.

Controlador ▸ Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5.º, VI, da LGPD).

Criptografia ▸ Cifração com o emprego de algoritmos matemáticos e parâmetros de controle chamados de chaves criptográficas. Busca tornar a mensagem incompreensível e inútil para todos os efeitos, enquanto não for submetida ao processo inverso de decifração. São dois os mecanismos básicos de cifração/decifração hoje em utilização: (i) criptografia simétrica (ou de chave secreta); e (ii) criptografia assimétrica (ou de chave pública).

Dado pessoal ▸ Informação relacionada à pessoa natural identificada ou identificável (art. 5.º, I, da LGPD).

Dado sensível ▸ Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político; dado referente à saúde ou à vida sexual; dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5.º, II, da LGPD).

Ecossistema de dados ▸ Conjunto de relações complexas que se formam entre os atores ou as entidades que interagem, direta ou indiretamente, consomem, produzem, fornecem dados e outros recursos relacionados.

Ética de dados ▸ Ramo da ética que estuda e avalia problemas morais e descreve os julgamentos de valor relacionados a dados (incluindo geração, registro, curadoria, processamento, disseminação, compartilhamento e uso), algoritmos (incluindo inteligência artificial, agentes artificiais, aprendizado de máquina e robôs) e práticas correspondentes (incluindo inovação responsável, programação, *hacking* e códigos profissionais), a fim de formular e dar suporte a soluções. A ética de dados abrange um conhecimento sólido da lei de proteção de dados e de outras legislações relevantes, bem como o uso apropriado de novas tecnologias.

Gestão ▸ Planejar, executar, controlar e agir para atingir os objetivos direcionados pela governança.

Governança de dados orientada à Administração Pública brasileira ▸ Conjunto de princípios, políticas, padrões, métricas e responsabilidades que permitem o alinhamento da estratégia, processos, pessoas, uso de tecnologia e dados com o objetivo de fomentar, aprimorar e garantir a efetividade do uso dos dados para o desenvolvimento de políticas públicas e entrega de soluções e serviços ao cidadão.

Guardião(ã) ▸ Colaborador(a) do Daent designado(a) para realizar o tratamento de dados de forma contínua, bem como auxiliar na gestão da Sala de Acesso Restrito (SAR), de modo a permitir o acesso seguro de usuários(as) eventuais.

Integridade ▸ Medidas de segurança da informação tomadas com vistas a salvaguardar a veracidade, evitar a adulteração e garantir seus métodos de processamento.

Interoperabilidade ▸ Capacidade das aplicações e dos sistemas de trocar dados de maneira segura e automática, independentemente dos limites geográficos, políticos ou organizacionais.

Modelo computacional ▸ Representação em linguagem computacional de uma estrutura de informações.

Modelo de informação ou modelo informacional ▸ Representação humana conceitual e contextual de uma estrutura de informações que se quer representar, com a definição semântica de todos os seus elementos.

Operador ▸ Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5.º, VII, da LGPD).

Política de dados ▸ Conjunto de princípios amplos e estratégicos que formam o quadro orientador para a gestão dos ativos de dados no Daent. Mais especificamente, as políticas de dados governam a gestão de dados, a interoperabilidade e os padrões de dados, a qualidade dos dados, a proteção de dados e a segurança da informação.

Princípio ▸ Essência do valor, caráter geral da organização que atua como guia para o entendimento das funções e relações, dando sentido ao seguimento de políticas e instruções normativas.

Programa Conecte SUS ▸ No âmbito do Ministério da Saúde, trata-se do programa voltado à informatização da atenção à saúde e à integração dos estabelecimentos de saúde públicos e privados e dos órgãos de gestão em saúde dos entes federativos, para garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão.

Qualidade dos dados ▸ Estado da qualidade da informação no que tange à adequação, à confiabilidade e à precisão, garantindo que seja completa, consistente e atualizada.

Rede Nacional de Dados em Saúde (RNDS) ▸ Componente do Sistema Nacional de Informações em Saúde (Snis), de que trata o artigo 47 da Lei n.º 8.080, de 19 de setembro de 1990, que consiste em uma plataforma nacional voltada à integração e à interoperabilidade de informações em saúde entre estabelecimentos de saúde públicos e privados e órgãos de gestão em saúde dos entes federativos, para garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão.

Sala de Acesso Restrito (SAR) ▸ Sala utilizada para tratamento de dados pessoais e sensíveis, que conta com dispositivos de segurança para manutenção da confidencialidade.

Segurança da informação ▸ Atividades que buscam reduzir o risco, aumentar a proteção e manter a qualidade dos dados e das informações.

Solicitante de dados ▸ Pessoa física ou jurídica que solicita acesso às bases de dados diversas, incluindo aquelas provenientes de órgãos da Administração Pública Federal, órgãos de pesquisa e universidades.

Transparência ▸ Garantia de acesso a toda e qualquer informação dos atos praticados pelo governo e de como os recursos públicos são aplicados.

Transparência ativa ▸ Divulgação de dados por iniciativa do próprio setor público, ou seja, quando são tornadas públicas informações, independentemente de requerimento, utilizando principalmente a internet.

Transparência passiva ▸ Disponibilização de informações públicas em atendimento a demandas específicas de uma pessoa física ou jurídica, seja de forma presencial ou eletrônica.

Tratamento de dados ▸ Qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração, conforme a Lei Geral de Proteção de Dados (LGPD).

Trilha de governança de dados ▸ Trajetória de implementação da cultura de dados, a partir da legislação vigente e das diretrizes de privacidade, transparência, proteção de dados, criação de valor, ética, melhora da atuação estatal e eficiência, no uso dos dados em benefício do cidadão.

APÊNDICES

APÊNDICE A
Quadro de Governança de Dados – V.1.0

COMO USAR O DOCUMENTO

Este documento permite definir as metas e os objetivos para cada tema a ser tratado, avaliando os pontos que o impactam e as principais questões a serem resolvidas. Durante a discussão, são detalhados os desafios e as perguntas que surgem em relação aos pontos mencionados. O documento possibilita tanto a enumeração da equipe responsável pelo tema quanto a identificação dos recursos necessários, como materiais, ferramentas e informações. Por fim, disponibiliza espaço para emissão de observações opinativas das propostas para orientar as decisões finais.

São quatro etapas contempladas:

1. **PLANEJAMENTO E DEBATE:** delimitam o cenário para a governança, sendo a primeira etapa do plano de governança de dados.
2. **DEFINIÇÕES GERAIS DE GOVERNANÇA:** após a definição do cenário, esta seção apresenta uma visão geral da governança para o setor, assim como suas metas e seus objetivos.
3. **MATURIDADE:** realiza uma avaliação diagnóstica do estágio dos processos de governança e define o plano de ação.
4. **COMPONENTES DE GOVERNANÇA:** definem os elementos a serem incorporados às boas práticas de governança.

PLANEJAMENTO E DEBATE					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Introdução	A governança de dados é essencial para a Secretaria? Liste as vantagens, as perspectivas de eficiência e eficácia. Liste os envolvidos, os departamentos e os gestores, incluindo aqueles gerenciados pela Secretaria. Liste quais expectativas legais e da comunidade podem ser atendidas com a governança de dados.	Crie um documento que fundamente e apoie a sua Política de Dados.	Liste os envolvidos no debate.	Escreva aqui as leis e as regulamentações que embasam e justificam a estratégia escolhida. Escreva todos os meios usados para as práticas, considerando as pessoas, os equipamentos, a infraestrutura e quaisquer outras ferramentas necessárias.	Utilize esse espaço para anotar as opiniões que orientem as decisões finais.
Propósito	O objetivo deste quadro é: (a) fornecer à SVSA um instrumento para gerir seus ativos de dados de forma eficaz, consistente e coordenada; (b) fornecer um modelo de boas práticas para desenvolver maturidade em governança de dados em suas agências; e (c) avaliar a maturidade das estratégias de governança de dados. O quadro pode estabelecer: princípios-chave da boa governança de dados; organizações de governança de dados; funções e responsabilidades de governança de dados; componentes de governança de dados; e atividades de implementação recomendadas.	Para cada estratégia de dados, considerando as opções de tratamento de dados, delineie um modelo de governança e gestão com o objetivo de definir as melhores práticas. Sugerimos a criação de um modelo-base a partir do funcionamento da Secretaria e de suas instâncias.	Liste os envolvidos no debate.	Escreva aqui as leis e as regulamentações que embasam e justificam a estratégia escolhida.	Utilize esse espaço para anotar as opiniões que orientem as decisões finais.

continua

continuação

PLANEJAMENTO E DEBATE					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Requisitos de conformidade	Identifique com quais estatutos, regulamentos e políticas governamentais relevantes relacionados à governança de dados a estrutura de governança está em conformidade. Lembre-se de considerar os domínios de negócio da sua Secretaria, bem como as atividades de tratamento de dados nas quais ela está envolvida.	Existe alguma outra legislação, política ou regulamento relevante?	Liste os envolvidos no debate.	Liste os requisitos.	Utilize esse espaço para anotar as opiniões que orientem as decisões finais.
Melhores práticas e padrões	Avalie se essa estrutura também está alinhada com padrões de melhores práticas aceitos, como o *DAMA-DMBoK, os padrões de gerenciamento de dados* ou o *padrão de interoperabilidade RNDS*.	Existem outros padrões relevantes?	Liste os envolvidos no debate.	Liste os padrões relevantes para o debate, a exemplo do *padrão de interoperabilidade do governo brasileiro.*	Utilize esse espaço para anotar as opiniões que orientem as decisões finais.
Escopo	Questione-se: o quadro se aplica a todas as formas e tipos de dados criados e gerenciados pelo setor? O quadro se aplica a todas as unidades da Secretaria? Quem terá acesso a esse documento?	O quadro deverá ser aplicado a todos os dados oriundos dos sistemas de informação da SVSA? Os dados de valor central são aqueles alinhados aos objetivos estratégicos da Secretaria e necessários para apoiar funções e serviços da SVSA?	Liste os envolvidos no debate.	N/A	Utilize esse espaço para anotar as opiniões que orientem as decisões finais.

continua

continuação

DEFINIÇÕES GERAIS DE GOVERNANÇA					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Governança de dados	Apresente aqui o conceito final de governança de dados definido para a SVSA. Informe a visão da governança e descreva as políticas, os processos, as funções, as responsabilidades e os procedimentos que compõem e comporão a estrutura.	Utilize estes espaços para anotar as decisões finais, os ajustes ou pontos de controle mencionados na seção anterior.			
Benefícios da governança de dados	Elabore sobre os benefícios da adoção dessa estratégia.				
Princípios de governança de dados	Apresente quais são os princípios da governança de dados da SVSA.				
Estrutura de governança de dados, incluindo organização para gestão de dados	Como a Secretaria deve ter uma estrutura de governança de dados claramente definida, deixe em evidência papéis e responsabilidades em todos os níveis.				

continua

continuação

DEFINIÇÕES GERAIS DE GOVERNANÇA					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Papéis e responsabilidades	Liste as funções e as responsabilidades relacionadas à custódia de dados; por exemplo, quem será o gestor de dados, o custodiante e os guardiões. Identifique também quem será responsável pela realização das atividades, quem terá autoridade para tomar as decisões, quem será consultado e quem precisará ser informado sobre o andamento do plano e o progresso das atividades.				
Funções de governança de dados – visão geral	Entre o grupo de conhecimentos atuais para a implementação da estrutura de governança proposta pelo DMBoK, liste aqueles que mais se adequam. Lembre-se de que a proposta do DAMA inclui: estratégia e planejamento; gerenciamento de qualidade de dados; segurança e privacidade de dados; armazenamento e operação de dados; referência e gerenciamento de dados mestres; integração e interoperabilidade de dados; *business intelligence* e análise; gerenciamento de metadados; e modelagem e design de dados.				

continua

continuação

MATURIDADE						
TEMA		**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Avaliação de maturidade		Uma vez definidos os sentidos da governança para a Secretaria, avalie o estágio de governança em que ela se encontra, classificando-o em fases. Essa avaliação deve estar alinhada com a visão do fluxo de tratamento de dados.	Aplique a matriz de avaliação de maturidade em gestão de dados de saúde e debata sobre os pontos de melhoria.			
Processos de gestão	Considerações sobre os processos de tratamento de dados e a evolução desses processos em relação a questões como qualidade, acessibilidade e interoperabilidade.	O modelo de governança pode ser expandido? Existem mecanismos de mensuração de eficiência? Existem mecanismos de gerenciamento de riscos?	Aplique o quadro de conhecimento em governança de dados e debata sobre os pontos de melhoria. Considere questões como escalabilidade e ampliação do escopo da gestão.			
Pessoas	Considerações sobre as habilidades para lidar com dados, escalabilidade do setor etc.	De quais treinamentos e capacitações as pessoas necessitam?	Aplique o quadro de conhecimento em governança de dados e debata sobre os pontos de melhoria.			
Decisões sobre ampliação e melhoria da governança de dados		Defina o escopo de melhoria, incluindo, por exemplo, o grupo de conhecimento DAMA-DMBoK, funcionalidades, políticas etc. Liste também o que mais se adequa.				

continua

continuação

COMPONENTES DE GOVERNANÇA					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Função 1 de Governança de Dados: Estratégia e Planejamento	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 2 de Governança de Dados: Gerenciamento de Qualidade de Dados	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 3 de Governança de Dados: Privacidade e Segurança	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 4 de Governança de Dados: Gerenciamento de Metadados	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 5 de Governança de Dados: Referência e Gerenciamento de Dados Mestre	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			

continua

conclusão

COMPONENTES DE GOVERNANÇA					
TEMA	**PONTOS A ENDEREÇAR**	**DISCUSSÃO E QUESTÕES**	**EQUIPE**	**RECURSOS**	**OPINIÃO**
Função 6 de Governança de Dados: Armazenamento e Operação de Dados	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 7 de Governança de Dados: Integração e Interoperabilidade de Dados	Questione a forma de aplicação e de melhoria desse componente e defina: princípio, justificativa de melhoria/ aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			
Função 8 de Governança de Dados: *Business Intelligence* e Análise	Questione a forma de aplicação e melhoria desse componente e defina: princípio, justificativa de melhoria/aplicação, elementos-chave e as atividades de implementação recomendadas.	Questione a forma de aplicação e melhoria dessa função.			

APÊNDICE B
Matriz de Avaliação de Maturidade na Gestão de Dados de Saúde – V.1.0

PROPOSTA

O processo de verificação deve ser aplicado a cada conjunto de dados geridos pela Secretaria. Sugere-se que a avaliação seja realizada por caso de uso, seguindo as estratégias de dados delineadas para o respectivo conjunto de dados. Essa iniciativa ajudará a identificar possíveis lacunas no processo. Os critérios definidos em cada nível de maturidade podem ser utilizados para: a) definir os requisitos de governança; b) monitorar o progresso do projeto e/ou demonstrar conformidade com práticas específicas de governança; ou c) criar um roteiro para aprimorar a maturidade da governança no nível do conjunto de dados.

Por exemplo, se um projeto exige que o Sistema de Informação sobre Mortalidade (SIM) atinja o Nível 3 para o componente-chave de Usabilidade, a disponibilização pública dos documentos do produto e do código-fonte deve ser um dos requisitos do projeto e integrar a lista de verificação de conformidade do conjunto de dados.

ORIENTAÇÃO

O processo de avaliação envolve:

1. identificar o conjunto de dados;
2. preencher a seção de metadados;
3. realizar a avaliação;
4. criar um diagrama de classificação de maturidade com base nos elementos avaliados; e
5. preencher o quadro avaliativo com conclusões e direcionamentos, quando pertinente.

MATRIZ DE AVALIAÇÃO DE MATURIDADE EM GESTÃO DE DADOS DE SAÚDE

IDENTIFICAÇÃO DO DOCUMENTO: XXXX; **VERSÃO:** V. XX

AVALIADO EM <DD/MM/AAAA> **PARA** <NOME DO CONJUNTO DE DADOS>

SEÇÃO DE METADADOS DO MODELO

Preencha as informações do conjunto de dados e crie a versão de sua avaliação:

Título do conjunto de dados	
Sistema de origem do conjunto de dados	
Recorte do conjunto de dados	
Identificação do provedor de dados (nome; e-mail; afiliação)	
Versão da avaliação (ID do documento e número da versão)	
Avaliador (nome; e-mail; afiliação)	
Versão de avaliação (v< nn >r<mm>, por exemplo, v01r00)	
Data da avaliação (MM/DD/AAAA)	
Categoria da maturidade avaliada	
Classificação da maturidade	
Caso de uso da avaliação (componente de governança do Quadro de Governança)	

CASO DE USO DA AVALIAÇÃO							
A categoria Acesso a Dados refere-se à capacidade de localizar (Descoberta) e obter o conjunto de dados em questão (Acessibilidade). A maturidade deve ser mensurada com base na facilidade de acesso e uso, incluindo tanto os dados quanto todos os seus metadados.							
Categorias	**Nível 1**	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**	**Considera:** 1) política de disponibilização de dados e metadados, e catálogo de dados; 2) protocolo de padrões; 3) padrão e qualidade dos metadados; 4) detecção de metadados; 5) conformidade com padrões nacionais e internacionais para acesso a dados e metadados; 6) serviços de visualização; 7) disponibilidade de dados e metadados por meio de protocolos de acesso livre e aberto.	
	▸ Por finalidade ▸ Não gerenciado	▸ Mínimo ▸ Gerência básica	▸ Intermediário ▸ Gerenciou ▸ Definido, parcialmente implementado	▸ Avançado ▸ Bem gerenciado ▸ Bem definido, totalmente implementado	▸ Ótimo ▸ Nível de excelência ▸ Medir, controlar, auditar		
Acesso a Dados						**Classificação**	**Observações**
Descoberta Condições de acesso e utilização dos dados, incluindo licenças.	Informação não difundida; informações do conjunto de dados não detectáveis.	Informações do conjunto de dados limitadas e básicas.	Metadados mínimos catalogados; conjunto de dados pesquisável on-line.	Conjunto abrangente de metadados catalogados e pesquisáveis + metadados granulares mínimos.	Disponível em catálogo internacional, exibido com destaque on-line e atualizado rotineiramente.	Nível	
Acessibilidade Disponibilização de serviços on-line, incluindo, no mínimo, download direto e outros serviços para acesso, visualização e análise.	Dados não disponíveis publicamente.	Serviços on-line básicos disponíveis para acesso a dados e metadados (por exemplo, download direto via FTP/HTTP).	Serviços simples de acesso a dados por meio de metadados, com arquitetura de acesso não padronizada.	Serviços de dados de interoperabilidade baseados em padrões.	Capacidade total de configuração, agregação e visualização.	Nível	

CASO DE USO DA AVALIAÇÃO							
A categoria Portabilidade e Usabilidade descreve a facilidade com que o conjunto de dados e seus metadados podem ser compreendidos e utilizados, sendo orientada para o compartilhamento automatizado de dados.							
Categorias	**Nível 1**	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**	**Considera:** 1) adoção de padrões para interoperabilidade; 2) uso de vocabulário controlado; 3) interoperabilidade semântica e sintática; 4) compartilhamento; e 5) modelo mínimo de qualidade dos dados.	
	▸ Por finalidade ▸ Não gerenciado	▸ Mínimo ▸ Gerência básica	▸ Intermediário ▸ Gerenciou ▸ Definido, parcialmente implementado	▸ Avançado ▸ Bem gerenciado ▸ Bem definido, totalmente implementado	▸ Ótimo ▸ Nível de excelência ▸ Medir, controlar, auditar		
Portabilidade e Usabilidade						**Classificação**	**Observações**
Codificação de dados Estruturação e codificação de dados	Dados não estruturados. Formato de dados não padronizado ou proprietário, ou mal documentado. Formato de arquivo padrão.	Esquema básico para uso automatizado de dados. Dados em formato de arquivo padrão documentado; nomenclatura fora do padrão. Notação das convenções utilizadas.	Uso de codificação padrão. Padrão documentado e utilizado pela comunidade científica.	Codificações de padrões adotados pela agência reguladora ou por organismos internacionais para interoperabilidade. Dados em formato de arquivo padrão bem documentado. Vocabulário e nomenclatura convencionais.	Padrões de codificação semântica aceitos edisponíveis para interoperabilidade. Os dados e metadados utilizam vocabulários compatíveis com os princípios FAIR. Padrão de dados prontos para análise.	Nível	

continua

conclusão

CASO DE USO DA AVALIAÇÃO							
A categoria Portabilidade e Usabilidade descreve a facilidade com que o conjunto de dados e seus metadados podem ser compreendidos e utilizados, sendo orientada para o compartilhamento automatizado de dados.							
Portabilidade e Usabilidade						**Classificação**	**Observações**
Documentação Registro de informação, atividades e processos.	Informações sobre o conjunto de dados.	Documentação limitada.	O documento sobre como o produto de dados foi criado e como usá-lo está disponível on-line.	Documentação abrangente baseada em um modelo padrão e disponível on-line.	Tutorial on-line sobre a utilização e a análise do conjunto de dados; informações completas do sistema de produção disponíveis on-line.	Nível	
Validação de qualidade Os dados serão controlados quanto à qualidade, e os resultados do controle de qualidade serão indicados nos metadados.	Sem verificação. Sem indicador de qualidade nos metadados. Sem documentação de procedimentos.	Controle básico de qualidade dos dados e verificação de monitoramento. Conjunto mínimo de procedimentos de controle de qualidade, documentados e disponíveis.	Indicador de qualidade. Procedimentos documentados de avaliação de qualidade.	Qualidade de dados monitorada e incrementada. Qualidade de metadados assegurada. Padrão mínimo de qualidade definido.	Nível de excelência. Histórico de indicadores de qualidade.	Nível	

CASO DE USO DA AVALIAÇÃO

A categoria Gestão da Qualidade abrange procedimentos de garantia de qualidade, incluindo monitoramento, controle e avaliação da qualidade, bem como comunicação sobre confiabilidade.

Categorias	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5	Considera:	
	▸ Por finalidade ▸ Não gerenciado	▸ Mínimo ▸ Gerência básica	▸ Intermediário ▸ Gerenciou ▸ Definido, parcialmente implementado	▸ Avançado ▸ Bem gerenciado ▸ Bem definido, totalmente implementado	▸ Ótimo ▸ Nível de excelência ▸ Medir, controlar, auditar	1) métodos e práticas de qualificação de dados; 2) divulgação e adoção de procedimentos; e 3) avaliação da completude, unicidade, consistência, validade, acurácia e usabilidade.	
Gestão da Qualidade						**Classificação**	**Observações**
Procedimento de garantia e controle de qualidade Conjunto de práticas e processos implementados.	Procedimento de área ou nenhum procedimento de garantia de qualidade (GQ) e controle de dados (CD).	Os procedimentos de GQ/CD são definidos, documentados e minimamente implementados.	Os procedimentos de GQ/CD são bem definidos de acordo com as melhores. Os procedimentos de GQ/CD são documentados e podem ser aplicados e replicados.	Estatísticas de erros são publicadas e há procedimentos para resposta e priorização de melhorias.	Relatório sobre historicidade dos procedimentos GQ/CD.	Nível	
Avaliação de qualidade Análise e medição da conformidade, segundo critérios e padrões definidos.	Avaliação da qualidade do produto não realizada ou realizada, mas os resultados da avaliação não estão documentados ou não estão disponíveis.	Qualidade do produto avaliada; avaliação documentada e publicada.	Indicador de qualidade e incerteza. Há procedimentos documentados de avaliação de qualidade.	Qualidade de dados monitorada e incrementada. Qualidade de metadados assegurada. Padrão mínimo de qualidade definido.	Método de avaliação da qualidade do produto disponível, validado e divulgado. Nível de excelência. Histórico de indicadores de qualidade.	Nível	

continua

conclusão

CASO DE USO DA AVALIAÇÃO							
A categoria Gestão da Qualidade abrange procedimentos de garantia de qualidade, incluindo monitoramento, controle e avaliação da qualidade, bem como comunicação sobre confiabilidade.							
Gestão da Qualidade						**Classificação**	**Observações**
Integridade de dados Precisão, consistência e confiabilidade dos dados ao longo de seu ciclo de vida.	Verificação de integridade de dados desconhecida ou inexistente.	Verificação básica de integridade de dados.	A integridade dos dados foi verificada sistematicamente, mas a metodologia não é comumente conhecida.	Integridade dos dados verificada sistematicamente com trilhas de auditoria e/ou rastreabilidade e seguindo práticas bem conhecidas, mas não necessariamente consistentes entre plataformas.	Todas as etapas da verificação da integridade dos dados são verificadas sistematicamente e aderem a práticas bem conhecidas.	Nível	

CASO DE USO DA AVALIAÇÃO

A categoria Gestão de Dados refere-se aos processos realizados para garantir que os dados e os metadados sejam bem administrados, de acordo com a política da Secretaria. Abrange não apenas a preservação dos dados e metadados com as salvaguardas adequadas, mas também a definição, a comunicação e a aplicação efetiva da política de dados.

Categorias	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5	Considera: 1) política de dados e política de becape; e 2) política de preservação, descarte e transferência.	
	▸ Por finalidade ▸ Não gerenciado	▸ Mínimo ▸ Gerência básica	▸ Intermediário ▸ Gerenciou ▸ Definido, parcialmente implementado	▸ Avançado ▸ Bem gerenciado ▸ Bem definido, totalmente implementado	▸ Ótimo ▸ Nível de excelência ▸ Medir, controlar, auditar		
Gestão de Dados						**Classificação**	**Observações**
Armazenamento e preservação Definição de políticas.	Qualquer local de armazenamento; sem política de becape.	Repositório não designado; dados com becape sistemático.	Arquivo designado. Política básica de preservação definida.	Política de becape e preservação definidas, implementadas em conformidade com os padrões de arquivamento.	Auditoria, monitoramento e melhoria das políticas.	Nível	
Metadados Criação, validação e verificação para garantir integridade, autenticidade e legibilidade.	Metadados das coleções de dados não disponíveis publicamente e/ou não utilizáveis. Não há avaliação.	Metadados das coleções de dados disponíveis. Características básicas do conjunto de dados. Adequação para uso da comunidade interessada no dado.	Em conformidade com os padrões nacionais e internacionais na maioria dos aspectos; metadados de qualidade e proveniência limitados.	Totalmente compatível com os padrões internacionais. Conteúdo rico de metadados. Metadados básicos em nível de grânulo. Proveniência do conjunto de dados de suporte.	Metadados mais abrangentes em nível granular. Qualidade dos metadados controlada e atualizada regularmente.	Nível	

continua

conclusão

CASO DE USO DA AVALIAÇÃO							
A categoria Gestão de Dados refere-se aos processos realizados para garantir que os dados e os metadados sejam bem administrados, de acordo com a política da Secretaria. Abrange não apenas a preservação dos dados e metadados com as salvaguardas adequadas, mas também a definição, a comunicação e a aplicação efetiva da política de dados.							
Gestão de Dados						**Classificação**	**Observações**
Governança Papéis e responsabilidades; habilidade.	A responsabilidade em relação ao conjunto de dados não está definida; nenhuma pessoa é designada.	A responsabilidade e a competência têm pouca delimitação. Pouca delimitação do escopo de administração do conjunto de dados.	Estão definidos mecanismos de responsabilidade/ prestação de contas e adequação. Ciência e adesão aos requisitos de competência e habilidade para gerenciar o conjunto de dados. Escopo de administração do conjunto de dados delimitado.	Regras e responsabilidades para gestão do conjunto de dados; possibilidade de realizar correções e atualizações de acordo com as revisões.	Regras e responsabilidades para gestão do conjunto de dados transparente. Monitorado e auditado.		

QUADRO DE MATURIDADE DO CONJUNTO DE DADOS

CONJUNTO DE DADOS															
ESCALA DE MATURIDADE				Acesso de Dados		Portabilidade e Uso			Gestão da Qualidade			Gestão de dados			
				Descoberta	Acessibilidade	Codificação de dados	Documentação	Avaliação de qualidade	Procedimento de garantia e controle de qualidade	Avaliação de qualidade	Integridade de dados	Armazenamento e preservação	Metadados	Governança
NÍVEL 1	Por finalidade	Não gerenciado												
NÍVEL 2	Mínimo	Gerência básica	Não definido											
NÍVEL 3	Intermediário	Gerenciou	Definido, parcialmente implementado											
NÍVEL 4	Avançado	Bem gerenciado	Bem definido, totalmente implementado											
NÍVEL 5	Ótimo	Nível 4 +	Medir, controlar, auditar											
Conclusões, justificativa e comentários:														
Plano de ação:														

APÊNDICE C
Quadro de Conhecimento em Governança de Dados – V.1.0

PROPOSTA

Este documento propõe um quadro para a avaliação de habilidades e conhecimentos em governança de dados. Esse quadro pode servir como base para a criação de descrições de trabalho comuns para uma futura equipe de dados, além de orientar a escolha de papéis e responsabilidades no escopo de governança e gestão de dados. Ele resume os conhecimentos, as competências e as habilidades necessárias.

O documento também mapeia práticas de gestão de dados e uma relação de competências, baseando-se nas atividades do Centro de Integração de Dados e Conhecimento para Saúde (Cidacs), considerando as etapas do ciclo de vida dos dados e as áreas de conhecimento propostas pelo DAMA.

Ciclo de vida dos dados:

❶ produção de dados; ❷ processamento de dados; ❸ análise de dados; ❹ preservação de dados; ❺ acesso de dados; e ❻ reúso de dados.

Competências na área de dados:

❶ bancos de dados e formato de dados; ❷ gestão de dados; ❸ validação e avaliação de qualidade de dados; ❹ pré-processamento e vinculação (*linkage*) de dados; ❺ interoperabilidade; ❻ produção de metadados; ❼ anonimização; ❽ preservação de dados; ❾ análise; ❿ visualização de dados; ⓫ domínio de dados; e ⓬ ética, privacidade e proteção de dados.

Áreas de conhecimento do DAMA:

❶ governança de dados; ❷ arquitetura de dados; ❸ modelagem e projeto de dados; ❹ armazenamento e operações de dados; ❺ segurança de dados; ❻ integração e interoperabilidade de dados; ❼ documentação e conteúdo; ❽ gestão de dados mestres; ❾ armazenamento de dados e inteligência de negócios; ❿ metadados; e ⓫ qualidade dos dados.

QUADRO DE CONHECIMENTO EM GOVERNANÇA DE DADOS

Área	Destinada a	Conhecimento		
		Ciclo de vida	Competência com dados	DAMA
1. Política/estratégia de dados	Desenvolver, implementar e monitorar uma política e estratégia de dados.	❶, ❷, ❸, ❹, ❺, ❻	❸, ❽, ⓫, ⓬	❶, ❽, ⓫
2. Marcos legais, éticos e de segurança e privacidade	Alinhamento contínuo com as normas legais e com os padrões éticos, e de segurança, proteção e privacidade para o tratamento de dados.	❶, ❷, ❸, ❹, ❺, ❻	❷, ❸, ⓫, ⓬	❶, ❺, ❽, ⓫, ⓬
3. Serviços	Suporte e disponibilidade de serviços de dados.	❶, ❷, ❸, ❹, ❺, ❻	❷, ❻, ❽	❺, ❻, ❾
4. Infraestrutura	Suporte e disponibilidade de infraestrutura de dados.	❶, ❷, ❸, ❹, ❺, ❻	❶, ❷, ❻	❶, ❷, ❹, ❺, ❾
5. Curadoria e metadados	Gestão da informação e do conhecimento mais adequada ao estágio do ciclo de vida dos dados.	❶, ❷, ❸, ❹, ❺, ❻	❶, ❷, ❸, ❻, ❼, ❽, ⓫, ⓬	❶, ❼, ❿, ⓫
6. Processamento e integração de dados	Desenho, engenharia e tratamento de dados para compartilhamento e integração.	❶, ❷, ❸, ❹, ❺, ❻	❶, ❹, ❾	❷, ❸
7. Arquivamento de dados	Infraestrutura de dados e ferramentas adequadas para o arquivamento interno e/ou externo de longo prazo dos dados.	❶, ❷, ❸	❶, ❷, ❸, ❽, ⓬	❶, ❽, ❾
8. Engajamento	Aplicação da cultura e disseminação da política de dados, além do envolvimento com áreas-chave.	❶, ❷, ❸, ❹, ❺, ❻	❷, ❾, ❿	❶, ⓫
9. Alinhamento com estratégias da RNDS	Desenho, engenharia e tratamento de dados para interligação de dados.	❶, ❷, ❸, ❹, ❺, ❻	❶, ❺, ⓫	❷, ❻, ❿, ⓫

APÊNDICE D
Planilha de papéis e responsabilidades de dados

Item	Definição	Exemplo de preenchimento
Papel	Defina o papel desempenhado pela pessoa no processo de governança de dados.	Pode ser subdividido entre estratégico, tático ou operacional, considerando governança de dados, gestão de dados, administrador de dados, guardião de dados, analista de dados etc.
Filiação	Indique a filiação daquele que deve desempenhar o papel.	Diretor e agentes públicos.
Autoridade	Defina o nível de responsabilidade na tomada de decisão.	**Liderança:** liderança, monitoramento de tendências, definição de estratégia e política, alocação de recursos e desenvolvimento de relacionamentos com parceiros-chave, órgãos de normalização e grupos de partes interessadas. **Suporte:** ligação com membros da equipe, gestores de dados para monitoramento e avaliação de desempenho.
Política/ estratégia de dados	Qual a responsabilidade desse papel com a definição da política e da estratégia de dados.	Considere ações de compartilhamento; mapa de dados; retenção, disposição e arquivamento de dados etc.
Marcos legais, éticos e de segurança e privacidade	Qual a responsabilidade desse papel com a definição dos marcos legais, éticos e de segurança e privacidade?	A responsabilidade pode ser subdividida entre estratégica, tática ou operacional.
Serviços	Qual a responsabilidade desse papel com os serviços?	A responsabilidade pode ser subdividida entre estratégica, tática ou operacional.
Infraestrutura	Qual a responsabilidade desse papel com a infraestrutura?	A responsabilidade pode ser subdividida entre estratégica, tática ou operacional.
Tratamento de dados	Qual a responsabilidade desse papel com o tratamento de dados?	Considere as habilidades pertinentes às ações de tratamento de dados.

PAPÉIS E RESPONSABILIDADES NA GESTÃO DE DADOS						
Papel	**Filiação**	**Autoridade**	**Política/ estratégia de dados**	**Marcos legais, éticos e de segurança e privacidade**	**Serviços**	**Infraestrutura**
Governança de Dados						
Guardião Geral de Dados						
Guardião de Dados						
Administrador de Dados						
...						

PAPÉIS E RESPONSABILIDADES DA EQUIPE TÉCNICA					
Papel	**Filiação**	**Tratamento dos dados**			
		Validação dos Dados	**Qualidade dos Dados**	**Integração dos Dados**	**Visualização dos Dados**
Curador de Dados					
Analista de Dados					
Engenheiro de Dados					
...					

Conte-nos o que pensa sobre esta publicação.
CLIQUE AQUI e responda a pesquisa.

Biblioteca Virtual em Saúde do Ministério da Saúde
bvsms.saude.gov.br