



**MINISTÉRIO DA SAÚDE
GRUPO HOSPITALAR CONCEIÇÃO
GERÊNCIA DE ENSINO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM AVALIAÇÃO DE TECNOLOGIAS PARA O SUS
MESTRADO PROFISSIONAL EM AVALIAÇÃO E PRODUÇÃO DE TECNOLOGIAS PARA O
SUS**

CAROLINA OLIVEIRA PACHECO FERON

**GOVERNANÇA DE DADOS PESSOAIS NA SAÚDE PÚBLICA BRASILEIRA À
LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI 13.709/18:
UMA REVISÃO DE ESCOPO**

PORTO ALEGRE

2025



**MINISTÉRIO DA SAÚDE
GRUPO HOSPITALAR CONCEIÇÃO
GERÊNCIA DE ENSINO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM AVALIAÇÃO DE TECNOLOGIAS PARA O SUS
MESTRADO PROFISSIONAL EM AVALIAÇÃO E PRODUÇÃO DE TECNOLOGIAS PARA O
SUS**

CAROLINA OLIVEIRA PACHECO FERON

**GOVERNANÇA DE DADOS PESSOAIS NA SAÚDE PÚBLICA BRASILEIRA À
LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI 13.709/18:
UMA REVISÃO DE ESCOPO**

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Avaliação e Produção de Tecnologias para o SUS no Programa de Pós-Graduação em Avaliação de Tecnologias para o SUS do Grupo Hospitalar Conceição.

Orientador(a): Prof. Dr. Fernando Anschau

PORTO ALEGRE

2025



**MINISTÉRIO DA SAÚDE
GRUPO HOSPITALAR CONCEIÇÃO
GERÊNCIA DE ENSINO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM AVALIAÇÃO DE TECNOLOGIAS PARA O SUS
MESTRADO PROFISSIONAL EM AVALIAÇÃO E PRODUÇÃO DE TECNOLOGIAS PARA O
SUS**

Banca Examinadora

Prof^(a). Dr(a)/Me./ e nome completo

Prof^(a). Dr(a)/Me./ e nome completo

Prof^(a). Dr(a)/Me./ e nome completo

RESUMO

A digitalização dos sistemas de saúde pública intensificou a produção e circulação de grandes volumes de dados pessoais sensíveis, tornando urgente a adoção de modelos robustos de governança da informação. A gestão ética, segura e eficiente desses dados é estratégica para a qualificação das políticas públicas, da administração sanitária e do atendimento ao cidadão. Nesse contexto, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018; LGPD) estabeleceu um marco regulatório fundamental ao disciplinar o tratamento de dados pessoais no setor público e privado. Esta dissertação apresenta uma revisão de escopo sobre a governança de dados pessoais na saúde pública brasileira, à luz da LGPD, com o objetivo de sintetizar evidências científicas e institucionais produzidas entre 2018 e 2025, a fim de subsidiar a elaboração de um Programa de Governança em Privacidade (PGP) aplicável à Secretaria Estadual da Saúde do Rio Grande do Sul (SES/RS). A metodologia seguiu as diretrizes do *PRISMA Extension for Scoping Reviews*, com buscas em bases científicas e fontes institucionais. Foram incluídos 19 documentos — 10 artigos científicos e 9 documentos da literatura cinzenta. Os resultados apontaram avanços normativos importantes, como a nomeação de encarregados, elaboração de Relatórios de Impacto à Proteção de Dados e políticas internas de privacidade. No entanto, destacaram-se lacunas significativas, especialmente a ausência de padronização entre entes federativos, carência de estudos empíricos avaliativos e fragilidades na capacidade técnica de implementação das diretrizes da LGPD. Como produto técnico, foi elaborado um PGP voltado à realidade da SES/RS, estruturado em etapas preparatórias, executivas e operacionais, contendo inventários, planos, fluxogramas e indicadores. O produto técnico resultante oferece suporte prático à institucionalização da governança de dados sensíveis na saúde pública estadual, alinhando-se às diretrizes da Autoridade Nacional de Proteção de Dados. Espera-se que sua implementação contribua para consolidar uma cultura organizacional voltada à proteção de dados pessoais no Sistema Único de Saúde (SUS), com potencial de replicação em outros contextos da administração pública.

Palavras-chave: Governança de dados pessoais. Privacidade. Saúde pública. SUS. LGPD. Brasil.

ABSTRACT

The digitalization of public health systems has intensified the production and circulation of large volumes of sensitive personal data, making the adoption of robust information governance models urgent. The ethical, secure, and efficient management of this data is strategic for improving public policies, health administration, and citizen services. In this context, the General Data Protection Law (Law No. 13,709/2018; LGPD) established a fundamental regulatory framework by regulating the processing of personal data in the public and private sectors. This dissertation presents a scoping review of personal data governance in Brazilian public health, in light of the LGPD, with the aim of synthesizing scientific and institutional evidence produced between 2018 and 2025 to support the development of a Privacy Governance Program (PGP) applicable to the Rio Grande do Sul State Health Department (SES/RS). The methodology followed the PRISMA Extension for Scoping Reviews guidelines, with searches in scientific databases and institutional sources. Nineteen documents were included—10 scientific articles and 9 gray literature documents. The results highlighted important regulatory advances, such as the appointment of data protection officers, the preparation of Data Protection Impact Reports, and internal privacy policies. However, significant gaps were highlighted, particularly the lack of standardization across federal entities, the lack of empirical evaluation studies, and weaknesses in the technical capacity to implement LGPD guidelines. As a technical product, a PGP tailored to the SES/RS reality was developed, structured into preparatory, executive, and operational stages, containing inventories, plans, flowcharts, and indicators. The resulting technical product offers practical support for the institutionalization of sensitive data governance in the state's public health system, aligning with the guidelines of the National Data Protection Authority. Its implementation is expected to contribute to consolidating an organizational culture focused on personal data protection within the Unified Health System (SUS), with potential for replication in other public administration contexts.

Keywords: Personal data governance. Privacy. Public health. SUS. LGPD. Brazil.

LISTA DE FIGURAS

Figura 1 - Fluxograma da seleção dos estudos. PRISMA-ScR.....	31
Figura 2 - Linha do tempo dos marcos legais analisados.....	39

LISTA DE QUADROS

Quadro 1 - Caracterização dos estudos incluídos - artigos científicos (2018-2025).	33
Quadro 2 - Caracterização dos estudos incluídos - literatura cinzenta (2018-2025)	36
Quadro 3 - Descrição dos marcos legais analisados.....	41
Quadro 4 - Detalhamento dos artigos mapeados em cada normativa.....	43
Quadro 5 - Modelos de programas institucionais de governança em privacidade selecionados.....	51
Quadro 6 - Bases de dados da SES/RS, organizadas por finalidade.....	52
Quadro 7 - Conceitos mais citados, desafios apontados e lacunas evidenciadas por eixo temático.....	55
Quadro 8 - Desafios identificados por categoria.....	57
Quadro 9 - Diretrizes propostas para a governança de dados pessoais no contexto da saúde pública brasileira.....	59
Quadro 10 - Práticas e Estruturas para Programas de Governança em Privacidade.....	61

LISTA DE GRÁFICOS

Gráfico 1 - Distribuição dos documentos analisados por tipo de publicação.....	29
Gráfico 2 - Distribuição anual dos documentos incluídos (2018–2025).....	30
Gráfico 3 - Distribuição de estudos (científicos e literatura cinzenta) por tipo de estudo).....	32

LISTA DE ABREVIações E SIGLAS

ABRASECI - Associação Brasileira de Segurança Cibernética
AEPD - Assessoria Especial de Proteção de Dados da PGE/RS
ANPD - Autoridade Nacional de Proteção de Dados
CEP - Comitês de Ética em Pesquisa
CGPPSES - Comitê Gestor da Política de Pesquisa da SES/RS
CONEP - Comissão Nacional de Ética em Pesquisa
DATASUS - Departamento de Informação e Informática do SUS
DGTI - Departamento de Gestão de Tecnologias e Inovação da SES/RS
FIOCRUZ - Fundação Oswaldo Cruz
GDPR - *General Data Protection Regulation*
IA - Inteligência artificial
INPD - Instituto Nacional de Proteção de Dados
IoT - Internet das Coisas
JBI - *Joanna Briggs Institute*
LGPD - Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018
MAD - Metodologia de Administração de Dados
MDCS - Sistemas de Coleta de Dados *mHealth* - saúde móvel
PDS - Personal data stores (armazenamento pessoal de dados)
PGE/RS - Procuradoria Geral do Estado do Rio Grande do Sul
PGP - Programa de Governança em Privacidade
PIA - Avaliação de Impacto à Privacidade
PPPD/PGE - Política de Privacidade e Proteção de Dados da PGE/RS
PRI - Plano de Resposta a Incidentes
PRISMA-ScR - *PRISMA Extension for Scoping Reviews*
PROCERGS - Centro de Tecnologia da Informação e Comunicação do Estado do Rio Grande do Sul S/A
PSI/SES - Plano de Segurança da Informação da SES/RS
RIPD - Relatório de Impacto à Proteção de Dados
RNDS - Rede Nacional de Dados em Saúde
SEIDIGI - Secretaria de Informação e Saúde Digital - Ministério da Saúde
SES/RS - Secretaria Estadual da Saúde do Rio Grande do Sul
SGSI - Sistema de Gestão de Segurança da Informação

SUS - Sistema Único de Saúde

TAI - Termo de Autorização Institucional

TIC - Tecnologias de Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO.....	12
2 OBJETIVOS.....	15
2.1 Objetivo Geral.....	15
2.2 Objetivos Específicos.....	15
3 REVISÃO DA LITERATURA.....	16
4 METODOLOGIA.....	23
4.1 Tipo de estudo, questão de pesquisa e estratégica PCC.....	23
4.2 Estratégia de busca.....	23
4.3 Critérios de inclusão e exclusão.....	24
4.4 Extração dos dados.....	25
4.5 Análise dos dados.....	25
4.6 Justificativa para a ausência de avaliação da qualidade metodológica e do risco de viés dos estudos incluídos.....	26
5 RESULTADOS.....	27
5.1 Seleção dos Estudos.....	27
5.2 Descrição dos Estudos Incluídos.....	32
5.3 Legislações e Programas de Governança.....	38
5.4 Bases de Dados - SES/RS.....	52
5.5 Categorias Temáticas: Conceitos, Desafios e Lacunas.....	53
5.6 Síntese Integrativa: Diretrizes LGPD na Governança de Dados.....	58
6 DISCUSSÃO.....	63
6.1 Análise dos achados: desafios, diretrizes e lacunas da governança de dados pessoais na saúde pública.....	63
6.2. Implicações para a Política Pública e Gestão de Dados Pessoais.....	66
6.3. Limitações da Revisão.....	67
6.4. Contribuições para a Ciência e Pesquisa.....	68
6.5. Contribuições para a proposta da SES/RS.....	69
7 CONSIDERAÇÕES FINAIS.....	71
REFERÊNCIAS.....	73
APÊNDICE A - PRODUTO TÉCNICO - PROPOSTA DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE PARA A SES/RS.....	79
APÊNDICE B – SINTAXE DE BUSCA NAS BASES DE DADOS.....	103
APÊNDICE C - ÍNTEGRA DAS PLANILHA DE EXTRAÇÃO DE DADOS.....	107
APÊNDICE D - CHECKLIST PRISMA-ScR.....	113
APÊNDICE E - QUESTIONÁRIOS / FORMULÁRIOS.....	115
APÊNDICE F - MAPEAMENTO DOS BANCOS DE DADOS SES/RS.....	116
ANEXO A - APROVAÇÃO - COMISSÃO DE CONSULTORIA CIENTÍFICA - GHC.....	117

1 INTRODUÇÃO

O advento da era digital tem se expandido com rapidez e profundidade, impactando todos os setores da sociedade, inclusive os serviços públicos. No Brasil, a digitalização das operações e o tratamento de dados pessoais cresceram exponencialmente, tornando a proteção dessas informações uma necessidade estratégica para garantir a confiança nas instituições e a efetividade das políticas públicas.

No setor da saúde pública, onde a coleta e o uso de dados pessoais e sensíveis são frequentes, a boa governança dessas informações torna-se imprescindível para assegurar seu uso ético, seguro e eficiente. Neste cenário, a Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei 13.709/2018 — surgiu como marco regulatório essencial, estabelecendo regras claras sobre o tratamento de dados pessoais por pessoas naturais ou jurídicas, públicas ou privadas (Brasil, 2018). Cabe destacar que a própria LGPD instituiu a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Vinculada à Presidência da República, a ANPD tem competência para editar normas, aplicar sanções administrativas e promover a cultura da proteção de dados no país.

Ainda que a LGPD represente o principal referencial normativo, outras legislações brasileiras já indicavam preocupações com a proteção de dados, como a Constituição Federal de 1988 (Brasil, 1988), o Código Civil (Brasil, 2002), a Lei de Acesso à Informação (Brasil, 2011) e o Marco Civil da Internet (Brasil, 2014). Tais dispositivos compõem um arcabouço jurídico que fortalece a proteção de direitos fundamentais, como a privacidade e a liberdade individual.

A aplicação da LGPD no contexto da saúde pública brasileira, especialmente no Sistema Único de Saúde (SUS), representa um desafio adicional, uma vez que o setor envolve volumes massivos de dados sensíveis, interoperabilidade entre sistemas, e múltiplos atores institucionais. A transformação digital dos serviços de saúde vem intensificando a coleta e circulação dessas informações, exigindo mecanismos sólidos de governança que garantam eficiência, segurança e conformidade legal. Esse cenário demanda uma resposta estruturada por parte do

poder público, considerando as especificidades da saúde digital e os riscos associados ao uso inadequado desses dados.

A proteção de dados pessoais já está prevista no artigo 5º, inciso LXXIX da Constituição Federal (Brasil, 1988), o que confere ainda mais legitimidade e urgência à implementação de práticas eficazes de governança. No entanto, órgãos públicos continuam sendo alvos de sanções por incidentes de vazamento de dados, como demonstrado por registros oficiais do Governo Federal (Brasil, 2023; Brasil, 2024). Tais episódios reforçam a importância de mecanismos preventivos e estruturais, como programas institucionais de governança, capazes de mitigar riscos e assegurar direitos.

Apesar da centralidade da Administração Pública na coleta de dados pessoais, observa-se ausência de diretrizes claras, fragmentação de políticas, escassez de estudos sistematizados e desafios éticos e técnicos que dificultam a implementação de uma governança de dados eficaz no SUS. Na área da saúde, dados pessoais sensíveis demandam especial atenção quanto à segurança, interoperabilidade e respeito aos princípios da LGPD.

No âmbito da Secretaria Estadual de Saúde do Estado do Rio Grande do Sul (SES/RS), identificou-se que dados pessoais e sensíveis — tanto de usuários do SUS quanto de colaboradores — são tratados diariamente por diversos setores e servidores. Apesar da existência de legislações federais e estaduais que regulamentam a aplicação da LGPD nas Secretarias Estaduais do Estado do Rio Grande do Sul, constatou-se que a SES/RS ainda não possui um Programa institucionalizado de Governança em Privacidade, o que configura uma lacuna crítica para o cumprimento efetivo da LGPD.

O Programa de Governança em Privacidade, conforme se depreende da leitura do artigo 50 da LGPD (Brasil, 2018), representa o primeiro estágio a ser alcançado por instituições públicas que desejam proteger adequadamente os dados pessoais sob sua responsabilidade, considerando que acaba por se consubstanciar em um guia estruturado, que tem como objetivo orientar a implementação da proteção de dados pessoais e da privacidade de forma sistêmica, em conformidade com os princípios, direitos e obrigações estabelecidos pela LGPD.

Embora o Estado do Rio Grande do Sul já tenha estabelecido diretrizes gerais sobre a matéria, cabe a cada Secretaria vinculada ao Poder Executivo a responsabilidade pela implementação concreta dessas normas, ajustando-as à sua

realidade institucional. Assim, não é possível estabelecer um Programa de Governança único e padronizado para todas as pastas estaduais, uma vez que cada Secretaria possui estruturas, fluxos de dados, vulnerabilidades e prioridades distintas. Dessa forma, torna-se imprescindível que a SES/RS elabore um Programa próprio, que reflita suas particularidades e atenda de forma efetiva às exigências legais, técnicas e éticas da governança de dados pessoais no contexto da saúde pública. Trata-se de uma etapa essencial para consolidar práticas sustentáveis de proteção de dados e garantir segurança jurídica à atuação da secretaria.

Diante da escassez de estudos nacionais que sistematizem o conhecimento sobre governança de dados pessoais no SUS à luz da LGPD, justifica-se a realização de uma revisão de escopo como estratégia metodológica robusta, capaz de mapear conceitos, desafios e boas práticas na área. Conforme recomendado pelas diretrizes *PRISMA Extension for Scoping Reviews* (PRISMA-ScR) (Tricco *et al.*, 2018), esse tipo de revisão permite sintetizar evidências e apoiar decisões institucionais informadas.

Neste contexto, esta dissertação propõe a realização de uma revisão de escopo sobre a governança de dados pessoais na saúde pública brasileira, à luz da LGPD, com foco em sistematizar conceitos-chave, desafios enfrentados, práticas recomendadas e lacunas existentes. Como produto técnico, propõe-se ainda a elaboração de uma proposta de Programa de Governança em Privacidade para a SES/RS, a partir das evidências identificadas na revisão. Espera-se que este produto sirva como referência prática e aplicável à realidade da Secretaria, contribuindo para a institucionalização da proteção de dados no setor público da saúde.

2 OBJETIVOS

2.1 Objetivo Geral

Sintetizar as evidências disponíveis na literatura científica e institucional sobre governança de dados pessoais na saúde pública brasileira, à luz da LGPD, a fim de subsidiar a elaboração de uma proposta de Programa de Governança em Privacidade para a SES/RS.

2.2 Objetivos Específicos

2.2.1 Identificar os principais conceitos, desafios/lacunas e diretrizes aplicadas à governança de dados pessoais no contexto da saúde pública no Brasil.

2.2.2 Mapear modelos de programas de governança em privacidade adotados por instituições públicas.

2.2.3 Identificar os bancos de dados existentes na SES/RS.

2.2.4 Analisar a LGPD e os regramentos legais e normativos vinculados ao Estado do Rio Grande do Sul e à SES/RS para fins de elaboração de proposta de Programa de Governança em Privacidade para a SES/RS.

2.2.5 Elaborar uma proposta de Programa de Governança em Privacidade aplicável à SES/RS.

3 REVISÃO DA LITERATURA

O avanço das tecnologias de transmissão de dados, aliado à crescente valorização dos dados pessoais como ativos econômicos estratégicos, impulsionou a criação de marcos regulatórios que visam proteger os direitos dos titulares dessas informações. No contexto internacional, destaca-se a *General Data Protection Regulation* (GDPR), regulamentação da União Europeia em vigor desde 2018. Inspirado por essa normativa, o Brasil publicou, no mesmo ano, a Lei Federal nº 13.709/2018 (LGPD; Brasil, 2018), cuja vigência plena se iniciou em setembro de 2020, com a aplicação de sanções a partir de agosto de 2021.

A LGPD representou um divisor de águas ao estabelecer princípios, direitos e obrigações relacionados ao tratamento de dados pessoais no país, com o objetivo central de assegurar a privacidade e a autodeterminação informativa dos cidadãos. Posteriormente, a promulgação da Emenda Constitucional nº 115/2022 reforçou essa proteção ao incluir a tutela dos dados pessoais no rol dos direitos e garantias fundamentais da Constituição Federal - Art. 5º, LXXIX (Brasil, 1988), conferindo maior robustez e legitimidade ao tema no ordenamento jurídico brasileiro (Brasil, 2022).

No âmbito da Administração Pública, a coleta de dados pessoais ocorre de maneira ampla e contínua ao longo de toda a vida do indivíduo. Desde o nascimento até o falecimento, os cidadãos têm suas informações registradas em diversas bases, físicas e digitais. Esses registros constituem, por si só, um conjunto de dados pessoais de alta relevância e sensibilidade (Vale *et al.*, 2025). Exemplo emblemático dessa coleta é a emissão de documentos civis obrigatórios, como o Registro Geral (RG) e o Cadastro de Pessoas Físicas (CPF), cuja administração envolve diretamente o tratamento de dados identificáveis e sensíveis.

No contexto da saúde pública, o tratamento de dados pessoais vai além do simples armazenamento físico: a digitalização emergiu como uma estratégia central para a modernização e a eficiência dos sistemas. Tecnologias como prontuários eletrônicos, sistemas de informação em saúde, plataformas de análise de dados e serviços de telemedicina têm impulsionado avanços significativos na gestão, planejamento e prestação de cuidados. Essas ferramentas promovem o acesso equitativo, aprimoram a qualidade assistencial e favorecem a tomada de decisão baseada em evidências. Em cenários de crise sanitária, como pandemias, a

digitalização também viabiliza a vigilância epidemiológica em tempo real e a interoperabilidade entre sistemas. Dado que o SUS lida com volumes expressivos de dados sensíveis – definidos como tal pela LGPD – torna-se imprescindível estabelecer padrões robustos de segurança, anonimização e interoperabilidade. Contudo, essa transformação digital exige investimentos contínuos em infraestrutura, capacitação profissional e formulação de políticas específicas para proteção de dados, considerando que o uso indevido dessas informações pode gerar danos tão significativos quanto os benefícios que a digitalização propicia.

Conforme referenciam Vale *et al.* (2025), diversas são as situações que colocam em risco a proteção de dados, como por exemplo, acesso não autorizado, destruição indevida, e divulgação ou transmissão fora das hipóteses previstas pela LGPD (como por exemplo, caso de invasão *hacker*). Ainda, Fornazin (2023) reflete que os riscos tecnológicos, como a perda de privacidade, a manipulação e a coleta invasiva de dados pessoais, assumem especial relevância no campo da saúde, bem como aponta a emergência do surgimento de novas formas de discriminação, segregação e exclusão, que podem ser potencializadas pelo uso inadequado ou desregulado de tecnologias informacionais no tratamento de dados sensíveis.

A literatura revela que os efeitos da LGPD na saúde pública são múltiplos. Seus impactos atingem não apenas os usuários dos serviços, mas também gestores, profissionais e sistemas de informação, dada a crescente necessidade de interoperabilidade entre distintos atores do setor. A boa governança de dados nesse campo é essencial para garantir que a coleta, o armazenamento e o uso das informações ocorram de forma ética, segura e eficiente. Princípios como privacidade, transparência, interoperabilidade, qualidade da informação e responsabilização são fundamentais para promover a confiança dos cidadãos nas instituições públicas e assegurar o uso legítimo dos dados (Cavalieri, 2020). Uma governança de dados estruturada contribui para integrar sistemas de informação em saúde, elevar a qualidade das análises e embasar políticas públicas eficazes, em consonância com as exigências legais estabelecidas pela LGPD (Cavalieri, 2020).

Do ponto de vista conceitual, a governança de dados diz respeito a um conjunto de práticas, estruturas e políticas institucionais orientadas à gestão responsável de todo o ciclo de vida dos dados — desde a coleta até seu descarte — garantindo sua integridade, segurança, acessibilidade, conformidade legal e valor estratégico. O conceito de governança tem origem na ideia grega de direção ou

condução, e envolve quatro funções fundamentais: estabelecimento de metas, coordenação, implementação e avaliação baseada em feedback (Peters, 2013). Nesse sentido, a governança é compreendida como um processo contínuo de orientar a sociedade e as instituições rumo a objetivos coletivos.

No contexto da governança institucional, é pertinente destacar o entendimento apresentado por Dallari et al. (2021), segundo o qual a governança deve ser compreendida não apenas como um conjunto de normas, mas como um sistema articulado que envolve múltiplos agentes – internos e externos –, orientando condutas e promovendo o alinhamento de interesses institucionais. Tal sistema, de natureza dinâmica e autossustentável, revela-se essencial para a consolidação de padrões mínimos de comportamento, sobretudo em contextos marcados por elevada complexidade, como o setor da saúde pública.

A governança em privacidade, por sua vez, possui foco específico na proteção dos direitos dos titulares de dados pessoais, orientando-se por princípios como o consentimento, a limitação da finalidade, a minimização da coleta e a transparência. Trata-se de um conjunto de diretrizes ético-jurídicas voltadas à garantia da autodeterminação informativa e à integridade no tratamento dos dados pessoais (Cavalieri, 2020). Assim, compreende-se que os conceitos de governança de dados e governança em privacidade são complementares e se articulam no âmbito da proteção das informações pessoais.

Relativamente à delimitação da diferença e complementaridade entre os conceitos acima referidos, faço referência ao trecho do artigo que segue:

A governança em privacidade é, portanto, um programa que, além de promover o compliance e atuar na prevenção a sanções administrativas e judiciais, também (e principalmente) gera impactos positivos na operação da empresa e a valoriza. Como a governança de dados tem como um de seus pilares o compliance em matéria de privacidade e proteção de dados pessoais, acaba apresentando uma intersecção com a governança em privacidade. Ambas estão debaixo do guarda-chuva da governança corporativa, um sistema que dirige a organização por meio de boas práticas que contribuem para sua gestão e longevidade, bem como para o bem comum. (Cabella *et al.*, 2020, p. 5)

A LGPD, em seu artigo 50, §2º (Brasil, 2018), estabelece requisitos mínimos para a estruturação de um Programa de Governança em Privacidade. Entre esses requisitos, destaca-se a obrigação de o controlador demonstrar comprometimento com a implementação de políticas e práticas internas que assegurem a conformidade com a legislação e com as boas práticas de proteção de dados. Um programa efetivo deve fortalecer a confiança entre o titular e a instituição pública, por

meio de condutas transparentes e da promoção de mecanismos de participação da população, controle e responsabilização (Cavalieri, 2020).

Além disso, o Programa de Governança em Privacidade deve ser compreendido como um processo institucional contínuo, cíclico e transversal, que articula avaliação, direcionamento e monitoramento das ações relacionadas ao tratamento de dados. Sua implementação exige diagnóstico do grau de maturidade institucional, mapeamento e categorização das bases de dados, análise de riscos e definição de políticas adaptadas às necessidades da organização. Esses processos devem ser conduzidos à luz tanto da legislação vigente quanto de princípios éticos, com o objetivo de consolidar uma cultura organizacional orientada à proteção de dados e à valorização da informação como ativo estratégico. A consolidação dessa cultura demanda mudanças nas práticas de gestão, investimentos permanentes em capacitação, e o desenvolvimento de políticas de atualização, avaliação e revisão periódica (Cavalieri, 2020).

O caráter contínuo e permanente dos Programas de Governança em Privacidade é enfatizado no Guia de Elaboração de Programa de Governança em Privacidade, ao destacar que, diferentemente de um projeto, esses programas se constituem como metodologias abrangentes que influenciam de forma duradoura os processos decisórios institucionais, com base na gestão de riscos e no aprimoramento contínuo da maturidade organizacional (Brasil, 2024).

Segundo Costa (2021), o surgimento da LGPD ocorre em um contexto de transformações tecnológicas aceleradas, em que o uso intensivo de recursos digitais ampliou a eficiência dos serviços, mas também intensificou os riscos associados ao tratamento de dados pessoais. Na área da saúde, esses riscos são ainda mais sensíveis, dado o caráter delicado e protegido das informações dos pacientes. O autor aponta que esse cenário instaura uma tensão constante entre os benefícios proporcionados pela informatização — como os prontuários eletrônicos, a interligação de sistemas e a disponibilidade de dados em tempo real — e os desafios impostos à privacidade e à segurança da informação.

Rivelli (2022) reforça esse entendimento ao destacar a natureza sensível dos dados pessoais de saúde. Segundo o autor, o tratamento inadequado dessas informações pode comprometer direitos fundamentais, como a dignidade, a privacidade e a não discriminação. Por isso, a adoção de práticas robustas de proteção e governança de dados em saúde não se configura apenas como uma

exigência legal, mas como um imperativo ético e social, alinhado aos princípios estabelecidos na LGPD, artigo 6º (Brasil, 2018). Neste mesmo sentido, Cavalieri (2020) reflete sobre a integridade governamental que deve ser compreendida como uma missão estratégica nacional, que vai além do enfrentamento da corrupção, ao promover um modelo de desenvolvimento sustentado por valores como a ética, a transparência, a sustentabilidade e a probidade.

No campo das políticas públicas, Oliveira *et al.* (2021) analisam os impactos da LGPD na gestão de dados da saúde pública, com destaque para a Rede Nacional de Dados em Saúde (RNDS), sob coordenação do Departamento de Informática do SUS (DATASUS). Os autores enfatizam a importância de equilibrar, na implementação da LGPD, a proteção da privacidade dos cidadãos com os benefícios proporcionados pelas tecnologias da informação e comunicação. Nesse sentido, a RNDS tem se consolidado como uma estratégia promissora de integração de dados e fortalecimento das práticas institucionais voltadas à proteção e ao tratamento ético das informações em saúde, considerando ter sido concebida e desenvolvida para estar em conformidade com a LGPD (Dallari *et al.* 2021).

A Estratégia de Saúde Digital para o Brasil 2020–2028 (RNDS, 2020) reforça a conformidade com a LGPD, ao reconhecer o indivíduo como protagonista no processo de tratamento de seus dados em saúde. Nesse contexto, destaca-se a importância da participação ativa do titular dos dados e a centralidade da Governança e da Liderança como prioridades estratégicas. Tais diretrizes orientam o país quanto à formulação e ao desenvolvimento de ações institucionais voltadas à implementação da LGPD no setor da saúde (Dallari *et al.* 2021).

Dallari e Monaco (2021) chamam atenção para a necessidade de sensibilização e qualificação contínua dos agentes de tratamento de dados no setor público. Para os autores, não basta investir em soluções tecnológicas sofisticadas: é imprescindível garantir que os servidores públicos compreendam, com profundidade, suas responsabilidades legais e éticas quanto ao manuseio de dados pessoais. Treinamentos periódicos e ações educativas são essenciais para evitar violações à LGPD e fortalecer uma cultura institucional baseada na proteção de direitos e na gestão segura das informações.

No contexto da Administração Pública, o Programa de Governança em Privacidade configura-se como um conjunto estruturado de princípios, políticas, práticas e responsabilidades institucionais que visam assegurar o uso estratégico,

ético e seguro dos dados pessoais. Seu propósito abrange desde a formulação de políticas públicas até a prestação de serviços à população, promovendo a conformidade legal, a prevenção de riscos e a integridade no uso das informações. Tal programa deve orientar a gestão dos dados desde a sua coleta até seu descarte, fomentando uma cultura institucional pautada na proteção da privacidade e na valorização da informação como ativo estratégico, atendendo às regras estabelecidas pela LGPD relativamente ao tratamento de dados pessoais pelo poder público, nos termos do artigo 23 da referida lei (Brasil, 2018).

Nesse sentido, esta revisão de escopo teve como objetivo mapear os principais conceitos teóricos, modelos institucionais de governança em privacidade, dispositivos legais aplicáveis, desafios operacionais e boas práticas observadas no campo da saúde pública. Busca-se, com isso, não apenas sistematizar o conhecimento já disponível, mas também fornecer subsídios teóricos e práticos para orientar a construção do produto técnico desta dissertação — a proposta de um Programa de Governança em Privacidade aplicável à SES/RS.

O Estado do Rio Grande do Sul, por meio do Poder Executivo, instituiu sua Política Estadual de Proteção de Dados Pessoais por meio do Decreto Estadual nº 55.987/2021 (Rio Grande do Sul, 2021), complementado pelos Decretos nº 55.647/2020 (Rio Grande do Sul, 2020) e nº 55.986/2021 (Rio Grande do Sul, 2021). Tais normativos estabeleceram diretrizes, prazos e responsabilidades para a adequação dos órgãos públicos estaduais às exigências da LGPD, incluindo a obrigatoriedade de que cada secretaria desenvolva e implemente seu próprio Programa de Governança em Privacidade. Essa descentralização normativa reconhece que não é possível aplicar um modelo único e padronizado a todas as secretarias, uma vez que cada órgão possui especificidades operacionais, fluxos de dados distintos e necessidades próprias de tratamento da informação.

No caso da SES/RS, observa-se o tratamento contínuo e sistemático de dados pessoais e sensíveis relacionados a servidores públicos, prestadores de serviços e usuários do SUS. Tais dados são processados por diversos setores, com base em fundamentos legais diversos previstos na LGPD, tais como:

- o cumprimento de obrigações legais e regulatórias, como as atividades de vigilância em saúde e auditoria;
- o uso e o compartilhamento de dados no âmbito da administração pública para viabilizar a execução de políticas públicas;

- a realização de estudos e pesquisas com fins de planejamento, monitoramento e formulação de novas políticas;
- a proteção da vida e da integridade física dos indivíduos, exemplificada por ações de prevenção, notificação de doenças e análises epidemiológicas;
- a tutela da saúde, por meio de programas, políticas públicas e serviços assistenciais prestados pelo SUS.

Dada a amplitude e a sensibilidade desses dados, torna-se imperativa a adequação da SES/RS às exigências da LGPD, não apenas em termos normativos, mas sobretudo do ponto de vista técnico e operacional (Rio Grande do Sul, 2020). Isso implica a reestruturação de fluxos de trabalho, a capacitação contínua dos servidores, a revisão de contratos com terceiros e a atualização dos mecanismos de controle e segurança da informação. A adoção de medidas proativas visa assegurar a continuidade e a qualidade dos serviços públicos de saúde, ao mesmo tempo em que evita violações de direitos fundamentais e reduz os riscos institucionais decorrentes de eventuais falhas na proteção de dados pessoais.

4 METODOLOGIA

4.1 Tipo de estudo, questão de pesquisa e estratégica PCC

Este estudo trata-se de uma revisão de escopo, conduzida de acordo com as diretrizes metodológicas do PRISMA-ScR e os procedimentos estabelecidos pelo *Joanna Briggs Institute* (JBI). A escolha dessa abordagem se justifica por sua pertinência na exploração de temas emergentes e ainda pouco consolidados na literatura, como a governança de dados pessoais na saúde pública brasileira sob a ótica da LGPD.

O protocolo da revisão foi previamente registrado na plataforma *Open Science Framework*, assegurando transparência, rastreabilidade e rigor metodológico em todas as etapas da pesquisa (Registro DOI: <https://doi.org/10.17605/OSF.IO/BYM9N>). A pesquisa também foi cadastrada no Portal da Pesquisa na SES/RS (código da pesquisa - 441).

A estratégia metodológica foi delineada com base na estrutura PCC – População, Conceito e Contexto, conforme recomendação de Brun e Zuge (2015) para estudos não clínicos. Os elementos definidos foram:

População: saúde pública brasileira

Conceito: governança de dados pessoais

Contexto: implementação da LGPD

A articulação entre esses componentes, em consonância com os objetivos do estudo, permitiu a formulação da seguinte questão de pesquisa: "Quais são os conceitos, modelos institucionais e práticas de governança de dados pessoais aplicados à saúde pública brasileira, à luz da LGPD, descritos na literatura científica e nos repositórios institucionais?"

4.2 Estratégia de busca

A busca bibliográfica foi realizada nas bases científicas PubMed, SciELO, LILACS e BVS; além de consultados repositórios institucionais relevantes, como ANPD, Instituto Nacional de Proteção de Dados (INPD), Associação Brasileira de Segurança Cibernética (ABRASECI), Secretaria de Informação e Saúde Digital - Ministério da Saúde (SEIDIGI), DATASUS, Fundação Oswaldo Cruz (Fiocruz),

Procuradoria Geral do Estado do Rio Grande do Sul (PGE-RS) e Centro de Tecnologia da Informação e Comunicação do Estado do Rio Grande do Sul S/A (PROCERGS).

A construção da estratégia de busca envolveu a combinação de termos controlados e palavras-chave, utilizando operadores booleanos. Os principais descritores empregados foram: *“governança de dados pessoais”*, *“privacidade”*, *“saúde pública”*, *“SUS”*, *“LGPD”* e *“Brasil”*. A delimitação temporal compreendeu o período de 2018 a 2025, correspondente ao marco regulatório da LGPD.

Para a elaboração do produto técnico, realizou-se o mapeamento de modelos de Programas de Governança em Privacidade adotados por instituições públicas, por meio da análise dos sites das Secretarias Estaduais de Saúde (SES) dos 27 estados brasileiros. As buscas foram realizadas utilizando os termos *“LGPD”* e *“governança”*. Também foram analisados os programas do Ministério da Saúde e da PGE/RS, órgão responsável pela orientação da implementação da LGPD no Executivo estadual gaúcho. O mapeamento dos bancos de dados da SES/RS foi conduzido por meio de questionamento enviado aos respectivos setores institucionais via e-mail.

A pesquisa de legislação foi realizada nos sites do Poder Executivo e da Assembleia Legislativa do Estado do Rio Grande do Sul, utilizando os seguintes termos-chave: *“LGPD”*, *“governança”*, *“dados pessoais”*, *“informação em saúde”* e *“compartilhamento de dados”*.

A estratégia completa de pesquisa está disponível no Apêndice B.

4.3 Critérios de inclusão e exclusão

Os critérios de inclusão adotados nesta revisão contemplaram publicações veiculadas entre os anos de 2018 e 2025, redigidas nos idiomas português, inglês ou espanhol, que abordassem de forma direta a temática da governança de dados pessoais no contexto da saúde pública brasileira. Por outro lado, foram excluídas da análise todas as publicações duplicadas, os estudos voltados à saúde suplementar, à governança corporativa ou realizados fora do escopo nacional, bem como aqueles que abordavam exclusivamente a GDPR. Os trabalhos que tratavam apenas da governança de dados administrativos ou de gestão e os documentos cujo texto completo não pôde ser acessado também foram desconsiderados.

4.4 Extração dos dados

Os dados foram extraídos e organizados em planilhas de forma padronizada, separadas por espécie de achados (artigos, literatura cinzenta, legislações e modelos de Programas de Governança em Privacidade de outras instituições).

- **Bases científicas e literatura cinzenta:** Título, Autores, Ano, Tipo de Estudo, População/Contexto, Objetivo Principal, Contribuições para a Governança de Dados, Desafios Identificados, Propostas ou Soluções, Limitações do Estudo, Base de Dados de Origem, Inclusão/Exclusão (com justificativa), Notas Adicionais.
- **Legislação:** Tipo de Norma, Número, Ano, Órgão Emissor, Tema Central, Artigos-chave relacionados à governança de dados, Resumo do conteúdo, Comentários e Notas Adicionais
- **Programas de Governança em Privacidade de outras instituições:** Órgão, Ano, Tema Central, Principais tópicos, Conceitos-chave de governança de dados pessoais, Práticas e estruturas aplicáveis à SES/RS, Recomendações adicionais, Notas.

4.5 Análise dos dados

A análise dos dados foi conduzida em duas etapas complementares: análise descritiva e análise temática, com o objetivo de sistematizar as informações obtidas e alinhá-las aos objetivos do estudo. A categorização dos dados em temas centrais foi feita com base na recorrência e relevância dos conceitos e desafios apontados. A interpretação dos achados seguiu as cinco fases descritas por Yin (2016): compilação, decomposição, recomposição, interpretação e conclusão.

Os resultados da análise dos dados estão apresentados de forma integrada ao capítulo de resultados desta dissertação, sob a forma de quadros, gráficos e descrições narrativas. As visualizações apoiam a compreensão das tendências observadas na literatura e nos documentos institucionais, permitindo evidenciar as lacunas, desafios e avanços identificados no campo da governança de dados pessoais em saúde pública no Brasil.

4.6 Justificativa para a ausência de avaliação da qualidade metodológica e do risco de viés dos estudos incluídos

De acordo com o manual metodológico do JBI (2020), revisões de escopo têm como finalidade principal mapear e descrever a amplitude e a natureza das evidências disponíveis, não sendo obrigatória a avaliação crítica da qualidade metodológica ou do risco de viés dos estudos incluídos. Essa orientação é reforçada pela declaração PRISMA-ScR (Tricco *et al.*, 2018), que indica que tal avaliação só deve ser realizada quando os resultados da revisão forem utilizados como base para decisões clínicas ou de políticas públicas.

Como o objetivo deste estudo é identificar e sistematizar conceitos, diretrizes e práticas institucionais relacionados à governança de dados pessoais na saúde pública, à luz da LGPD, não se aplica a análise crítica da qualidade metodológica dos estudos, o que é coerente com os objetivos e com o delineamento metodológico da presente revisão.

5 RESULTADOS

5.1 Seleção dos Estudos

A busca realizada nas bases científicas resultou na identificação inicial de 111 registros nas plataformas PubMed, SciELO, LILACS e BVS. Após a aplicação dos critérios de elegibilidade e exclusão, e conforme demonstrado no fluxograma PRISMA-ScR (Figura 1), foram selecionados 10 artigos científicos que compõem o corpo da presente revisão de escopo. O processo de seleção seguiu as diretrizes metodológicas recomendadas, com base no fluxograma PRISMA-ScR e no checklist PRISMA-ScR para revisões de escopo (Apêndice D), a fim de assegurar transparência, rastreabilidade e rigor científico em todas as etapas da triagem. Foi conduzida, ainda, a análise das referências bibliográficas citadas nesses artigos, porém, não se verificou a inclusão de novos documentos, uma vez que os materiais referenciados não apresentavam aderência à pergunta de pesquisa, encontravam-se fora do recorte temporal estabelecido ou já faziam parte do conjunto inicial de estudos analisados.

Optou-se por manter a base LILACS na etapa de seleção, tendo em vista que, durante o processo de remoção de duplicatas, constatou-se que os registros dessa base não correspondiam integralmente aos encontrados na BVS, justificando sua permanência de forma autônoma.

O processo de seleção dos artigos científicos foi conduzido de acordo com os critérios de inclusão previamente estabelecidos e contou com o apoio da ferramenta Rayyan (<https://rayyan.ai/>). As etapas compreenderam: remoção de duplicatas, leitura dos títulos e resumos, leitura integral dos estudos potencialmente elegíveis e registro sistemático dos motivos de inclusão e exclusão. A seleção foi realizada de forma colaborativa por dois revisores (pesquisador e orientador), com decisões consensuais em todos os casos.

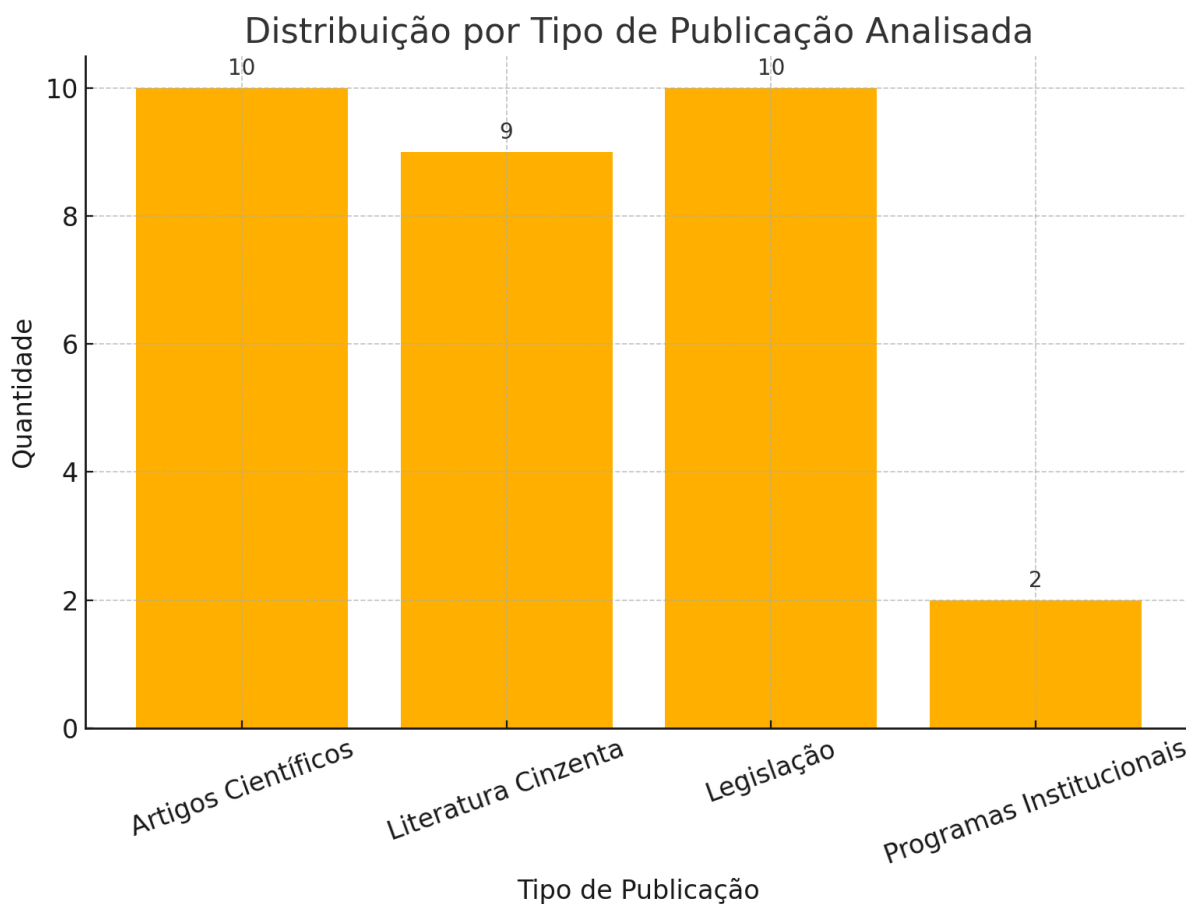
No que se refere à literatura cinzenta, foram selecionados 9 documentos que contribuíram de maneira significativa para o embasamento desta revisão. Os materiais foram obtidos nos portais da ANPD, do DATASUS, da Fiocruz e da PROCERGS. Apesar de também terem sido consultados os sites do INPD, da ABRASECI, da SEIDIGI e da PGE/RS, não foram encontrados documentos aderentes ao escopo da pesquisa.

A seleção dos documentos da literatura cinzenta seguiu os mesmos critérios de inclusão previamente definidos no protocolo metodológico, embora, nesta etapa, não tenha sido utilizada a ferramenta Rayyan. A triagem consistiu na exclusão de duplicatas, leitura de títulos e resumos, leitura integral dos documentos elegíveis e registro dos motivos de inclusão e exclusão. A análise foi conduzida por um único revisor.

No que tange à pesquisa normativa, foi realizada uma busca sistemática nos sites da Assembleia Legislativa do Estado do Rio Grande do Sul, ao portal institucional da SES/RS (seção de Portarias) e ao repositório de legislação disponível na página oficial do Governo Federal, com o uso das expressões-chave “*LGPD*”, “*governança*”, “*dados pessoais*”, “*informação em saúde*” e “*compartilhamento de dados*”. Como resultado, foram identificados 9 atos normativos estaduais pertinentes, além da própria LGPD, em âmbito federal, que compuseram o corpus documental analisado.

Para o mapeamento de programas institucionais de governança em privacidade, foram examinadas as páginas eletrônicas das secretarias estaduais de saúde das 27 unidades federativas do Brasil. No entanto, não foram localizadas publicações específicas sobre programas estruturados de governança em privacidade nas referidas instituições, mesmo com o uso dos termos de busca “*LGPD*” e “*governança*”. Diante disso, a formulação da proposta de Programa de Governança em Privacidade para a SES/RS baseou-se nos programas adotados pelo Ministério da Saúde e pela PGE/RS, esta última por sua função normativa e orientadora no processo de implementação da LGPD no âmbito do Poder Executivo estadual.

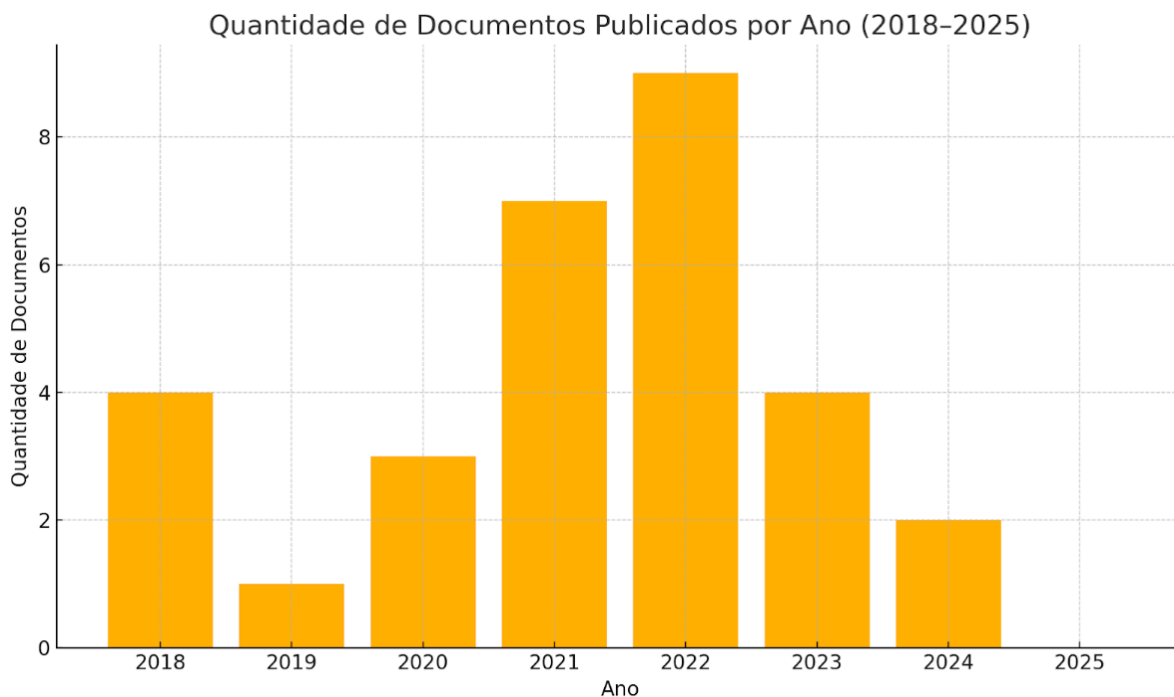
O gráfico a seguir (Gráfico 1) apresenta a distribuição quantitativa dos documentos analisados por categoria – artigos científicos, literatura cinzenta, atos normativos e programas institucionais –, evidenciando a representatividade proporcional dos achados entre as diferentes fontes consultadas.

Gráfico 1. Distribuição dos documentos analisados por tipo de publicação

Fonte: elaborado pela autora (2025)

No gráfico acima (Gráfico 1) podemos identificar que o conjunto de publicações analisadas foi composto por dez artigos científicos, nove documentos classificados como literatura cinzenta, dez publicações de natureza legislativa e dois programas institucionais.

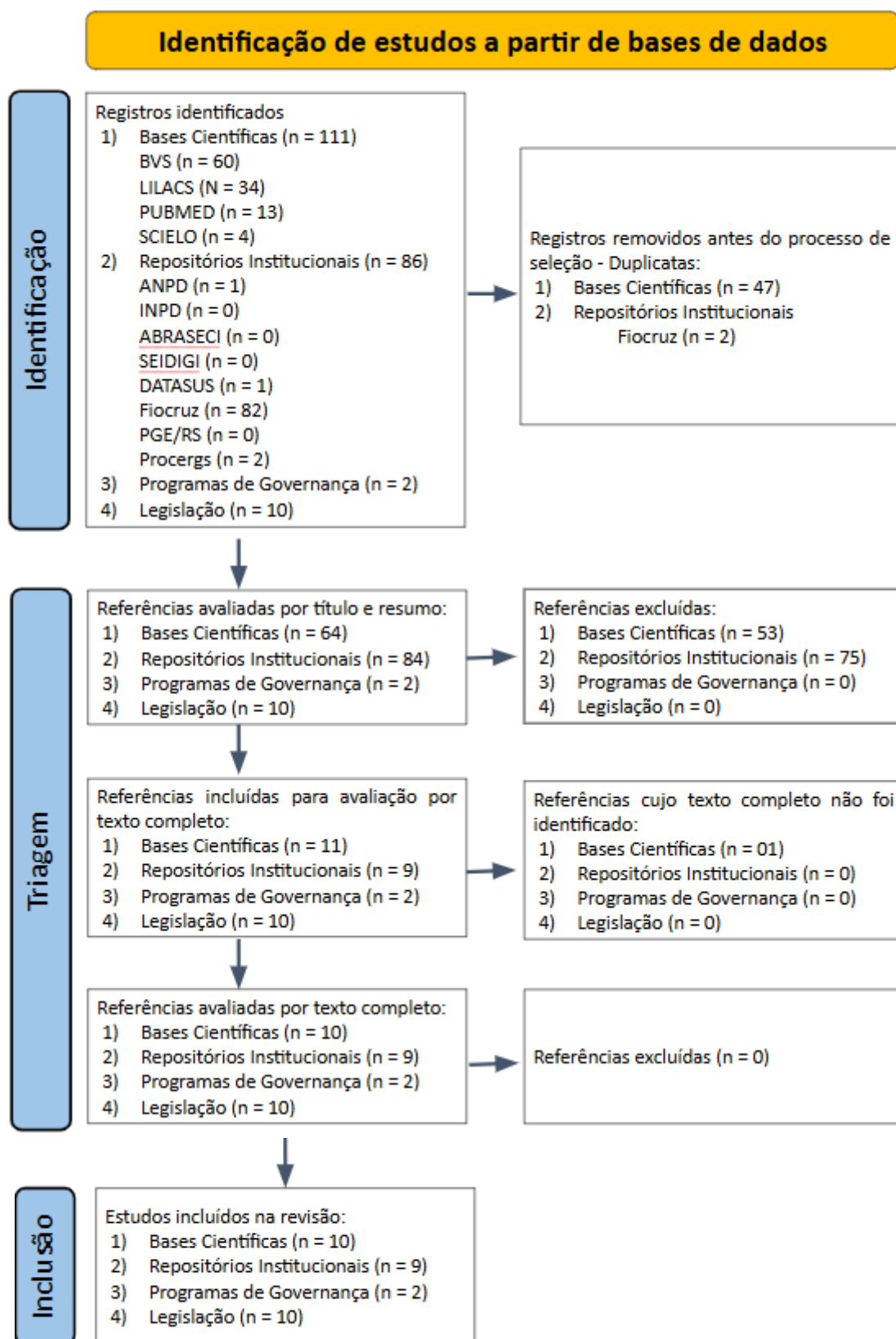
O gráfico a seguir (Gráfico 2) apresenta a distribuição temporal dos documentos incluídos nesta revisão, considerando o período de 2018 a 2025. Essa visualização permite observar a evolução da produção científica e institucional sobre governança de dados pessoais na saúde pública brasileira à luz da LGPD.

Gráfico 2. Distribuição anual dos documentos incluídos (2018–2025)

Fonte: elaborado pela autora (2025)

No gráfico 2 observamos o levantamento da quantidade de documentos publicados por ano, no período de 2018 a 2025, evidenciando que, em 2018, foram identificados quatro registros. No ano seguinte, 2019, observou-se apenas um documento, enquanto em 2020 houve um acréscimo para três publicações. Em 2021, registraram-se sete documentos, número que aumentou para nove em 2022. Já em 2023, verificou-se a presença de quatro documentos e, em 2024, dois registros. Para o ano de 2025, não foram identificadas publicações.

Figura 1. Fluxograma da seleção dos estudos. PRISMA-ScR¹.



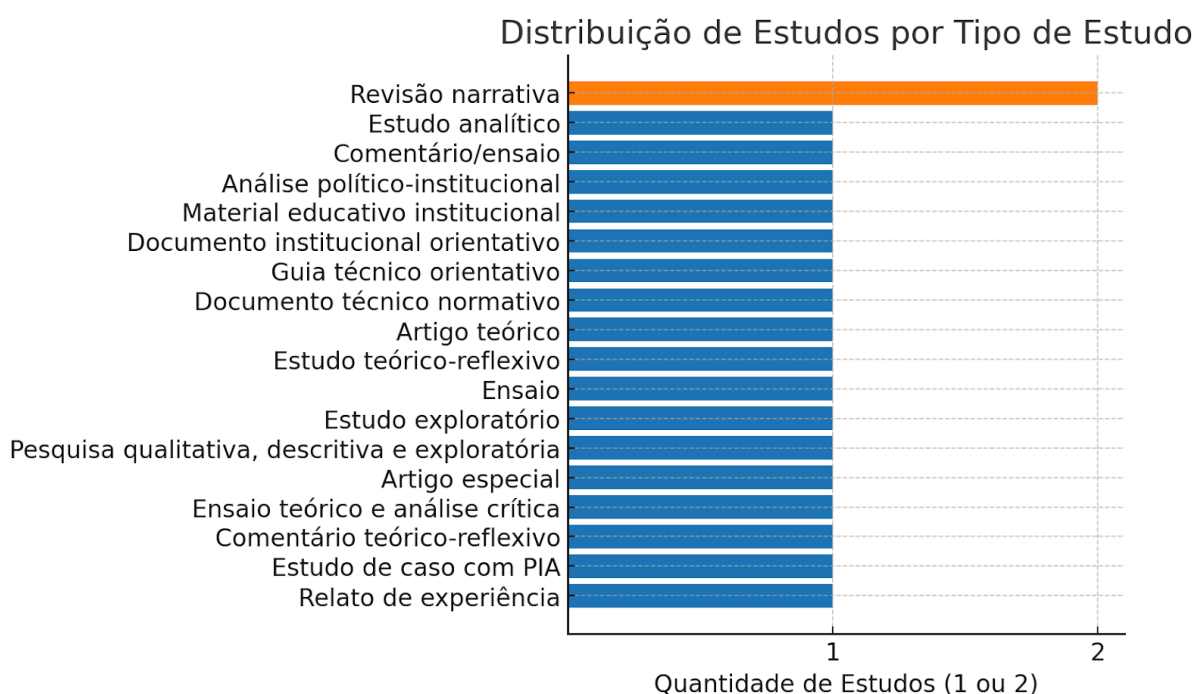
Fonte: elaborado pela autora (2025)

¹ Modelo obtido em:
<https://eme.cochrane.org/prisma-2020-checklist-para-relatar-uma-revisao-sistematica/>

5.2 Descrição dos Estudos Incluídos

Os 19 estudos selecionados para compor esta revisão foram classificados de acordo com sua natureza (artigos científicos ou literatura cinzenta) e caracterizados conforme o tipo de abordagem metodológica. O Gráfico 3, a seguir, ilustra essa distribuição, evidenciando a diversidade de formatos presentes entre os documentos analisados.

Gráfico 3. Distribuição de estudos (artigos científicos e literatura cinzenta) por tipo de estudo



Fonte: elaborado pela autora (2025)

O gráfico acima (Gráfico 3) apresenta a distribuição da quantidade de estudos por tipo. Observa-se que todos os tipos listados têm ocorrência de uma ou duas publicações no período analisado. Cada barra representa um tipo específico de estudo, identificado no eixo vertical, enquanto o eixo horizontal indica a quantidade correspondente. Essa representação permite visualizar de forma objetiva a presença quantitativa reduzida desses formatos de estudo na amostra levantada, evidenciando a proporção relativa de cada categoria dentro desse recorte específico.

Os quadros 1 e 2 apresentam uma síntese das principais informações extraídas dos estudos incluídos, separadas por tipo de publicação. A versão detalhada dos quadros encontra-se no Apêndice C.

Quadro 1. Caracterização dos estudos incluídos - artigos científicos (2018-2025)

ID	Autor (Ano)	Tipo de Estudo	Objetivo Principal	Contribuições para a Governança de Dados Pessoais
1	Dourado <i>et al.</i> (2022)	Comentário / ensaio	Discutir a abrangência do direito à explicação e à revisão de decisões automatizadas na regulação da inteligência artificial (IA) na saúde no Brasil a partir do marco da LGPD, considerando o debate internacional sobre o tema e os limites atualmente existentes para IA explicável na área da saúde.	Enfatiza o direito à explicação e a necessidade de estruturas regulatórias.
2	Zaganelli <i>et al.</i> (2022)	Estudo exploratório	Abordar os aspectos gerais da LGPD e uma perspectiva comparada em relação à GDPR. Apresentar associação entre o tratamento de dados sensíveis e a confidencialidade na assistência em saúde.	Propõe maior cuidado com dados sensíveis na saúde. Apresenta reflexão relativa aos conceitos de confidencialidade, enquanto um dever ético e profissional; e à privacidade enquanto uma criação da legislação moderna. Conclui sobre a importância da realização da Avaliação de Impacto em dados sensíveis.
3	Tietzmann <i>et al.</i> (2021)	Revisão narrativa	Abordar questões relativas ao sigilo, segredo, privacidade e confidencialidade; o compartilhamento de informações entre profissionais por meio de aplicativos ou redes sociais; e o compartilhamento de imagens.	Aponta os desafios da confidencialidade na saúde digital sob à luz da LGPD. Reflexão sobre bioética.
4	Corte-Real <i>et al.</i> (2024)	Estudo analítico	Realizar análise abrangente, considerando as propriedades da tecnologia <i>blockchain</i> na saúde digital, abordando considerações médico-legais, de privacidade e regulatórias.	Propõe soluções normativas para uso de <i>blockchain</i> na governança de dados.
5	Iwaya <i>et al.</i> (2019)	Estudo de caso com PIA	Apresentar uma Avaliação de Impacto à Privacidade (PIA) para Sistemas de Coleta de Dados mHealth - saúde móvel (MDCSs), fornecendo uma identificação e avaliação sistemáticas de potenciais riscos à privacidade, enfatizando particularmente controles e estratégias de mitigação para lidar com impactos negativos à privacidade.	Aponta falhas e recomendações práticas para proteger dados sensíveis, como, por exemplo, controles para gerenciar consentimento, transparência e minimização de dados.
6	Ventura <i>et al.</i> (2018)	Comentário teórico-reflexivo	Analisar a privacidade e os dados pessoais entre o público e o privado; bem como, a questão atinente à privacidade e governança de acesso a dados.	Propõe superação de dicotomias público/privado e defende governança voltada ao bem comum. Apresenta o modelo de governança de dados como uma alternativa que assegura o equilíbrio entre a preservação do direito à privacidade e os ganhos potenciais do uso dos dados na avaliação e pesquisa populacional.

7	Nina da Hora; Mariana Martins de Carvalho <i>et al.</i> (2023)	Ensaio teórico e análise crítica	Capítulo 3 - Analisar a privacidade e a ética enquanto conceitos fundamentais para a cidadania; Capítulo 7 - Contribuir para a compreensão das práticas de proteção de dados no ecossistema de digitalização dos serviços de saúde e fortalecer a cultura de proteção de dados pessoais, tendo como referência a LGPD.	Reflete sobre o papel da cidadania e dos conselhos de saúde na construção de políticas de governança de dados. Aponta a ausência dos usuários no debate como um dos problemas existentes para a consolidação do direito aos dados pessoais, demonstrando como tal problema está também atravessado por marcadores sociais da diferença, como classe, raça/etnia e geração.
8	Pinto <i>et al.</i> (2022)	Artigo especial	Refletir sobre a construção no Brasil de políticas e estratégias que combinem proteção e segurança dos dados pessoais, melhoria do sistema de saúde e desenvolvimento econômico-social sustentável e incluyente.	Aponta riscos, recomenda medidas normativas e sugere aprimoramento da LGPD na saúde.
9	Aragão <i>et al.</i> (2020)	Pesquisa qualitativa, descritiva e exploratória	Apontar em que medida a estrutura do sistema público de saúde brasileiro será impactada pela publicação da Lei e indicar eventuais caminhos a serem trilhados nesse sentido.	Relaciona diretamente o SUS com a necessidade de estrutura normativa e práticas de proteção de dados. Aborda questões relativas ao tratamento de dados sensíveis e consentimento; anonimização de dados sensíveis e hipóteses de compartilhamento; segurança dos dados e boas práticas de governança. Apresenta sugestões para harmonização do SUS à LGPD.
10	Camara <i>et al.</i> (2021)	Revisão narrativa	Apontar as fragilidades relativas à privacidade de usuários do SUS e propor uma solução teórica, a partir de uma infraestrutura pautada em armazenamento pessoal de dados – <i>personal data stores</i> (PDS), ou, a partir da segurança da <i>blockchain</i> .	Propõe alternativas tecnológicas e reflexões sobre a governança de dados sensíveis no SUS, como, por exemplo, o uso da tecnologia da <i>blockchain</i> ou armazenamento de dados em PDS.

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 1) reúne os dez estudos científicos selecionados, publicados entre 2018 e 2025, abrangendo distintas abordagens metodológicas, como revisões narrativas, comentário/ensaio, estudo exploratório, estudo analítico, estudo de caso com Avaliação de Impacto à Privacidade – PIA, comentário teórico-reflexivo, ensaio teórico com análise crítica, artigo especial e pesquisa qualitativa, descritiva e exploratória. Os objetivos dos estudos variaram desde a discussão sobre o direito à explicação e à revisão de decisões automatizadas na saúde (Dourado et al., 2022), passando pela análise dos aspectos gerais da LGPD e confidencialidade na assistência (Zaganelli et al., 2022), até reflexões sobre sigilo, segredo e compartilhamento de informações em saúde digital (Tietzmann et al., 2021) e proposições normativas para o uso de blockchain na governança de dados (Corte-Real et al., 2024). Outros trabalhos abordaram, por exemplo, avaliações de impacto à privacidade em sistemas mHealth (Iwaya et al., 2019), a relação entre privacidade e governança de dados voltada ao bem comum (Ventura et al., 2018), a cidadania e a cultura de proteção de dados no ecossistema de saúde (Nina da Hora; Carvalho et al., 2023), bem como políticas e estratégias para harmonizar proteção de dados, eficiência do SUS e desenvolvimento sustentável (Pinto et al., 2022; Aragão et al., 2020; Camara et al., 2021). As contribuições identificadas incluem desde a proposição de soluções normativas e alternativas tecnológicas, passando por recomendações práticas de mitigação de riscos à privacidade, até reflexões sobre inclusão social, participação cidadã e fortalecimento de práticas de governança de dados pessoais no contexto da saúde pública.

Quadro 2. Caracterização dos estudos incluídos - literatura cinzenta (2018-2025)

ID	Autores	Tipo de Estudo	Objetivo Principal	Contribuições para a Governança de Dados Pessoais
1	Zaganelli <i>et al.</i> (2023)	Ensaio	Discutir o tratamento de dados sensíveis na telemedicina sob a ótica da LGPD.	Reflexões sobre práticas seguras e conformidade normativa na telemedicina.
2	Guanaes <i>et al.</i> (2018)	Análise político-institucional	Analisar a repercussão da LGPD no âmbito das políticas públicas de saúde e os desafios para sua implementação no SUS.	Oferece diretrizes político-normativas para a implementação da LGPD no setor público da saúde.
3	Minghelli <i>et al.</i> (2023)	Relato de experiência	Discutir diretrizes para construção de um Relatório de Impacto à Proteção de Dados (RIPD) com enfoque na autodeterminação informativa e na humanização do tratamento de dados na telemedicina.	Promoção da autodeterminação informativa e conformidade com a LGPD por meio do RIPD.
4	Ramos <i>et al.</i> (2021)	Artigo teórico	Analisar a utilização de dados de seres humanos na ciência e na administração pública, à luz da LGPD e das decisões do Supremo Tribunal Federal.	Base normativa da LGPD, contribuições do Supremo Tribunal Federal e diretrizes éticas fortalecem a governança de dados no Brasil.
5	Ministério da Saúde (2024)	Documento técnico normativo	Estabelecer padrões e papéis para administração de dados no Ministério da Saúde, com foco na RNDS, LGPD, segurança e interoperabilidade usando HL7 FHIR.	Propõe uma Metodologia de Administração de Dados (MAD), contendo a regulamentação e a descrição dos padrões e procedimentos a serem adotados em relação à Administração de Dados no âmbito do Ministério da Saúde. Trata de questões relativas a modelos de interoperabilidade de dados e anonimização de dados.
6	ANPD (2023)	Guia técnico orientativo	Fornecer orientações práticas para agentes públicos sobre tratamento e proteção de dados pessoais conforme a LGPD.	Aborda a temática da LGPD em face do poder público, tratando das bases legais, princípios e questões relativas ao compartilhamento de dados pessoais pelo poder público.
7	PROCERGS (2022)	Documento institucional orientativo	Demonstrar a importância da cultura de privacidade e proteção de dados no ambiente institucional da PROCERGS.	Instrumentaliza a implementação de uma cultura de governança de dados pessoais na Administração Pública estadual.
8	PROCERGS (2022)	Material educativo institucional	Explicar os principais conceitos, princípios, bases legais e obrigações da LGPD em linguagem acessível para os colaboradores da PROCERGS.	Oferece um guia prático para implementação de governança em privacidade e conformidade legal.

9	Almeida <i>et al.</i> (2020)	Estudo teórico-reflexivo	Analisar os desafios éticos, legais e técnicos no uso de dados pessoais para enfrentamento da COVID-19 e propor novos modelos de governança.	Propõe princípios e diretrizes para governança ética e transparente em contextos de crise sanitária. Defende uma governança responsável, transparente e participativa para o uso de dados em saúde pública.
---	------------------------------	--------------------------	--	---

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 2) reúne informações referentes aos nove estudos da literatura cinzenta selecionados. Cada registro apresenta o nome dos autores e o ano de publicação, o tipo de estudo ou documento produzido, o objetivo principal e as contribuições específicas para a governança de dados pessoais. Entre os tipos de publicações incluídos, encontram-se ensaios, análises político-institucionais, relatos de experiência, artigos teóricos e documentos técnicos normativos. Os objetivos principais descrevem as finalidades centrais de cada estudo, variando desde discussões conceituais sobre o tratamento de dados sensíveis e implicações da LGPD até a proposição de diretrizes, metodologias e padrões para a gestão segura e eficiente dessas informações. Já a coluna dedicada às contribuições para a governança de dados pessoais apresenta elementos como reflexões sobre práticas seguras, diretrizes normativas, incentivo à autodeterminação informativa e propostas metodológicas para administração e proteção de dados no âmbito da saúde pública.

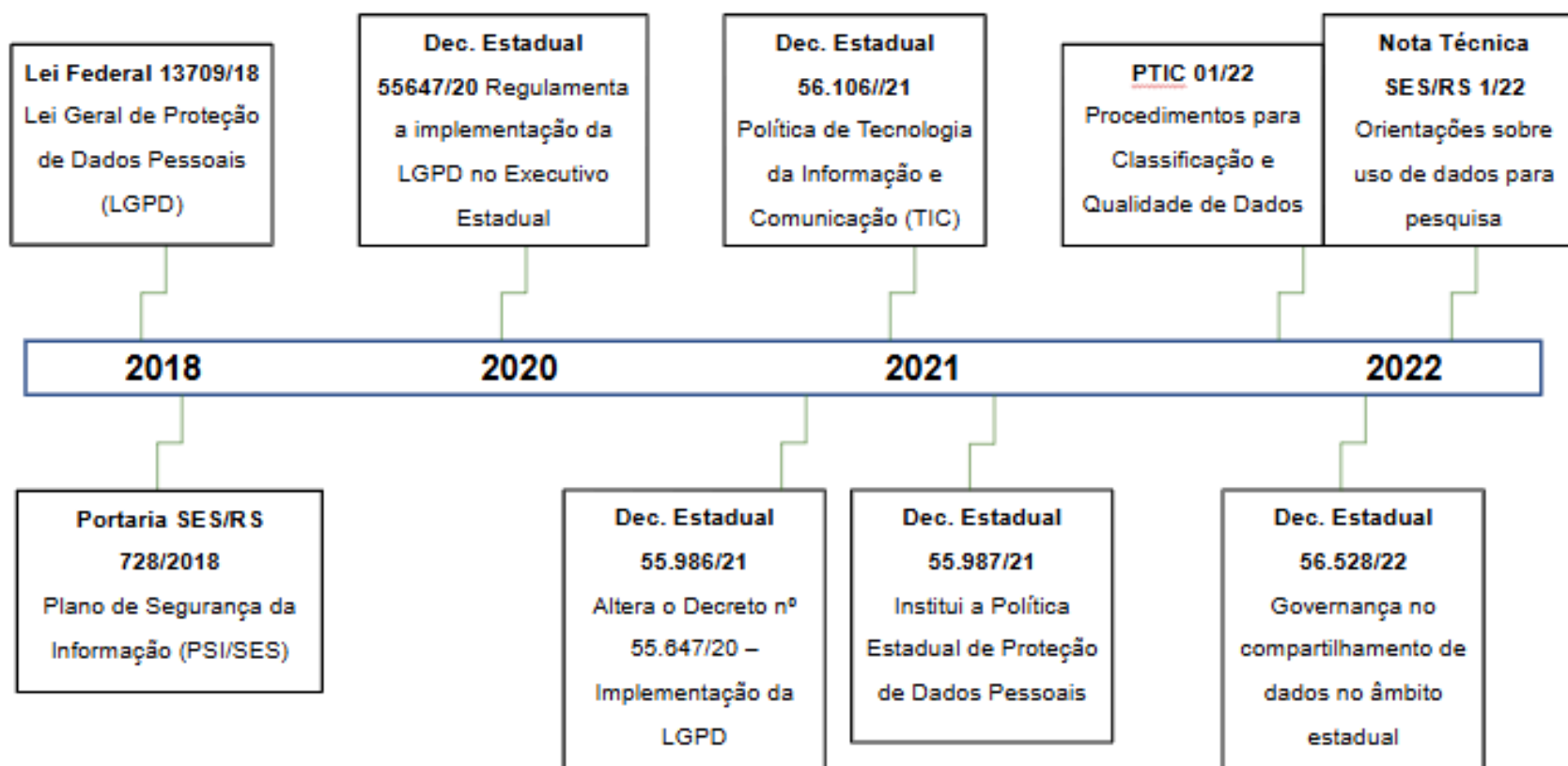
5.3 Legislações e Programas de Governança

A análise dos regramentos legais e normativos pertinentes ao Estado do Rio Grande do Sul e à SES/RS, necessária à fundamentação da proposta de Programa de Governança em Privacidade, foi conduzida por meio de consulta sistemática às plataformas da Assembleia Legislativa do Estado do Rio Grande do Sul, ao portal institucional da SES/RS (seção de Portarias) e ao repositório de legislação disponível na página oficial do Governo Federal.

Durante o processo de triagem, foram considerados os documentos cuja temática estivesse relacionada à proteção e à governança de dados, respeitando-se o marco temporal definido para a pesquisa (2018–2025). De forma excepcional, incluiu-se uma nota técnica emitida pela SES/RS em 2015, pela sua relevância estratégica, uma vez que regulamenta o uso das Tecnologias da Informação no âmbito da Secretaria e contribui para o histórico institucional da temática.

Como resultado, o mapeamento normativo contemplou a análise integral da LGPD (Lei nº 13.709/2018), cinco decretos e normativas estaduais, bem como três portarias e uma nota técnica emitidas pela SES/RS. A Figura 2 a seguir apresenta uma linha do tempo dos principais marcos legais relacionados à governança de dados pessoais, destacando os instrumentos normativos específicos do Estado do Rio Grande do Sul e da SES/RS, com a respectiva categorização por tipo de documento e tema central.

Figura 2. Linha do tempo dos marcos legais analisados.



Fonte: elaborado pela autora (2025)

No que se refere ao mapeamento dos modelos de programas institucionais de governança em privacidade, foram analisadas as plataformas digitais das secretarias estaduais de saúde dos 27 estados brasileiros. Contudo, não foram localizadas publicações públicas que explicitassem a existência de programas formais nessas instâncias. As buscas foram realizadas com os termos “*LGPD*” e “*governança*”, diretamente nos portais institucionais. Diante dessa lacuna, optou-se por adotar, como modelos referenciais, os programas desenvolvidos pelo Ministério da Saúde e pela PGE/RS — sendo esta última a entidade responsável pela orientação normativa da implementação da LGPD no âmbito do Poder Executivo Estadual (Rio Grande do Sul, 2020). A seguir, apresentam-se os quadros com os resultados dessa etapa (Quadros 3, 4 e 5).

Quadro 3. Descrição dos marcos legais analisados.

ID	Tipo de Norma	Tema Central	Contribuições
1	Lei Federal 13.709/18	Lei Geral de Proteção de Dados Pessoais (LGPD)	Estabelece princípios, direitos e deveres relacionados à proteção de dados pessoais. Define conceitos como controlador, operador, encarregado, tratamento de dados e estabelece a criação da ANPD.
2	Portaria SES/RS 740/15	Uso das Tecnologias da Informação na SES/RS	Regulamenta o uso de TIC no âmbito da SES/RS. Estabelece procedimentos e padrões para infraestrutura, segurança e acesso às informações institucionais.
3	Portaria SES/RS 728/18	Plano de Segurança da Informação (PSI/SES)	Estabelece diretrizes para a segurança dos ativos da informação da SES/RS. Define responsabilidades dos usuários quanto à confidencialidade, integridade e disponibilidade das informações.
4	Decreto Estadual 55.647/20	Regulamenta a implementação da LGPD no Executivo Estadual	Define prazos, fases e a figura do Encarregado pelo Tratamento de Dados. Cria Conselho e Grupo de Trabalho para implementação da LGPD no RS.
5	Decreto Estadual 55.986/21	Altera o Decreto nº 55.647/2020 – Implementação da LGPD	Permite que um mesmo encarregado atue em mais de um órgão. Estabelece parâmetros para relatórios de impacto e programas de governança em privacidade no RS.
6	Decreto Estadual 55.987/21	Institui a Política Estadual de Proteção de Dados Pessoais	Define princípios da proteção de dados pessoais no RS e diretrizes para sua implementação conforme a LGPD. Destaca o papel do controlador, operador, encarregado e a estrutura de governança.
7	Decreto Estadual 56.106/21	Política de Tecnologia da Informação e Comunicação (TIC)	Institui a Política de TIC no RS, define princípios, diretrizes e o Sistema de Governança e Gestão de TIC. Inclui governança de dados como um dos eixos estruturantes da política.
8	Decreto Estadual 56.528/22	Governança no compartilhamento de dados no âmbito estadual	Estabelece normas para o compartilhamento de dados entre órgãos públicos estaduais. Define níveis de compartilhamento (amplo, institucional, específico) e a figura dos Facilitadores de Dados.
9	Padrão Técnico (PTIC) 01/22	Procedimentos para Classificação e Qualidade de Dados	Estabelece padrões de TIC para classificação e qualidade de dados no RS, conforme Decreto 56.106/2021 e 56.528/2022. Define dados brutos, transformados, plataformas e produtos de dados. Reforça a atuação dos Facilitadores de Dados.
10	Nota Técnica SES/RS 01/22	Orientações sobre uso de dados para pesquisa na SES/RS	Define diretrizes éticas e legais para uso de dados pessoais e sensíveis em pesquisas científicas. Estabelece o fluxo de autorização via Termo de Autorização Institucional (TAI) e Comissão Nacional de Ética em Pesquisa (CONEP) / Comitês de Ética em Pesquisa (CEP), destacando o papel da anonimização e pseudoanonimização.

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 3) apresenta um levantamento dos marcos legais analisados. Cada registro está classificado de acordo com o tipo de norma, contemplando leis federais, decretos estaduais e portarias específicas da SES/RS. As colunas incluem a identificação do tema central, descrevendo o foco normativo de cada dispositivo, e o campo de contribuições, que sintetiza as principais disposições ou impactos da norma, abrangendo aspectos como princípios e direitos relacionados à proteção de dados pessoais, regulamentações sobre uso de tecnologias da informação, diretrizes de segurança da informação, bem como regras específicas para a implementação da LGPD no âmbito estadual.

Quadro 4. Detalhamento dos artigos mapeados em cada normativa

Normativa	Artigos	Tema Central	Relação com a Governança de Dados Pessoais	Aplicabilidade no SUS
Lei Federal 13.709/18 - LGPD	Art. 6º	Princípios do tratamento de dados pessoais	Define princípios como finalidade, necessidade, segurança e prestação de contas, que embasam políticas de governança.	Orienta práticas de tratamento ético e seguro de dados pessoais de pacientes e servidores públicos.
	Art. 13	Acesso a dados em estudos de saúde pública	Regulamenta o uso de dados para pesquisas com anonimização e proteção.	Viabiliza pesquisas em saúde com base em dados pessoais, com segurança e controle ético.
	Art. 23 a 27	Tratamento de dados pelo poder público	Dispõe sobre a obrigatoriedade de indicar encarregado e de manter dados acessíveis e controlados.	Normatiza o uso dos dados pelos órgãos do SUS e garante transparência e responsabilidade.
	Art. 32 e 50 §2º	Padrões de boas práticas e governança	Permite à ANPD sugerir padrões e a órgãos públicos criar mecanismos de avaliação e resposta.	Estimula a adoção de boas práticas por instituições públicas de saúde para proteção e confiança dos titulares.
	Art. 37 a 41	Agentes de tratamento e obrigações	Dispõe sobre o registro das operações de tratamento e o papel do encarregado de dados.	Exige controle e transparência na manipulação de dados sensíveis de saúde por órgãos públicos.
	Art. 46 a 49	Segurança e sigilo dos dados	Estabelece medidas de segurança e de notificação de incidentes.	Prevê obrigações para prevenir vazamentos e garantir a confidencialidade de dados de pacientes.
	Art. 50	Boas práticas e governança	Autoriza a criação de programas de governança em privacidade com regras claras e mecanismos internos de supervisão.	Permite que secretarias e instituições de saúde implementem programas internos de governança baseados na LGPD.
Portaria SES/RS 740/15	1	Regulamentação do uso da TI na SES/RS	Define o acesso e utilização de sistemas, redes e equipamentos de informática.	Fundamental para assegurar uma gestão segura e eficiente de dados de saúde.
	4	Canal de atendimento para serviços de TI	Estabelece normas de solicitação e priorização de serviços ao Departamento de Gestão de Tecnologias e Inovação (DGTI).	Organiza a governança de dados e serviços digitais na rede pública de saúde.

	5	Cadastramento de usuários	Define critérios para acesso a sistemas e dados.	Controla o acesso a informações sensíveis da saúde pública.
	7	Obrigações dos usuários	Estabelece normas de segurança e uso responsável.	Garante o sigilo e integridade das informações em saúde.
	8	Competência do DGTI	Define atribuições como elaboração de políticas, segurança e auditoria.	Coordena estratégias de governança digital na saúde pública.
	9	Uso da Internet	Restringe uso da rede exclusivamente para atividades laborais.	Evita riscos e garante integridade dos sistemas que armazenam dados de saúde.
	14	Instalação de novos sistemas	Estabelece controle técnico para novos softwares.	Previne vulnerabilidades nos sistemas de gestão em saúde.
	17	Regras para correio eletrônico	Define limites de espaço, tipos de arquivos e regras de envio.	Garante proteção contra vazamento de dados pessoais em saúde.
	27	Infrações e penalidades	Tipifica usos indevidos de sistemas e equipamentos.	Permite responsabilização por falhas na governança de dados.
Portaria SES/RS 728/18	1	Regulamentação da segurança da informação na SES	Estabelece mecanismos de proteção, controle e integridade da informação.	Fundamental para garantir confidencialidade e integridade dos dados de saúde.
	2	Princípios e fundamentos da segurança da informação	Define os pilares da governança como confidencialidade, integridade e disponibilidade.	Aplicação direta em sistemas de saúde com dados sensíveis.
	7	Responsabilidade dos usuários	Define deveres sobre proteção, uso correto e comunicação de incidentes.	Previne perdas de dados e responsabiliza agentes públicos na saúde.
	9	Responsabilidades dos gestores	Determina deveres de controle e adequação de acessos.	Gestores de unidades de saúde devem zelar pela governança de dados locais.
	10	Atribuições do DGTI	Responsável por elaborar e aplicar políticas de segurança.	Centraliza governança técnica dos dados da saúde no Estado.
	11	Comitê de Governança da TI	Coordenação estratégica para gestão de dados e tecnologia.	Fortalece a governança institucional da informação em saúde.
	17	Normas sobre controle de acesso	Estabelece critérios para autenticação, permissões e senhas.	Evita acessos indevidos aos sistemas e bancos de dados de saúde.

	24	Compartilhamento de dados	Orienta sobre sigilo, permissões e <i>backup</i> .	Essencial para evitar exposição indevida de informações de pacientes e servidores.
	27	Responsabilidade por perdas	Define obrigações em caso de perdas por má gestão de dados.	Reflete sobre a responsabilidade institucional por falhas de governança.
	29	Correio eletrônico institucional	Normas para uso seguro de e-mails	Evita vazamentos de dados pessoais por meios digitais.
	32	Aquisição de sistemas e equipamentos	Centraliza decisões no DGTI para controle e segurança.	Garante que soluções de TI na saúde estejam em conformidade com normas de dados.
	37	Cópias de segurança	Define rotinas de <i>backup</i> e recuperação de dados.	Garante continuidade do cuidado e integridade dos registros de saúde.
	39	Uso obrigatório de antivírus	Impede a circulação de <i>malwares</i> que comprometem dados.	Protege os sistemas de saúde pública contra ameaças digitais.
	43	Uso de equipamentos móveis	Normas para uso seguro de celulares, <i>notebooks</i> e <i>tablets</i> .	Evita extravio ou vazamento de dados em contextos móveis.
	45	Conscientização dos usuários	Criação de cartilhas e treinamentos.	Promove cultura de segurança de dados na rede pública de saúde.
	47	Classificação das informações	Baseada na LAI e outras normas estaduais.	Permite classificar dados sensíveis, como os da saúde, conforme seu grau de sigilo.
	50	Comissão de Avaliação de Documentos Sigilosos	Assessora a classificação correta de informações.	Fundamental para definir o que pode ou não ser exposto no âmbito da saúde pública.
Decreto Estadual 55.647/20	Art. 1º	Finalidade do Decreto	Estabelece procedimentos para implementação da LGPD no Executivo Estadual.	Orienta a aplicação da LGPD na SES/RS e outros órgãos públicos estaduais.
	Art. 2º a 5º	Indicação e atribuições do Encarregado de Dados	Define perfil, responsabilidades e garantias institucionais do Encarregado.	Exige que a SES/RS nomeie encarregado capacitado para gerir dados pessoais.
	Art. 6º e 7º	Conselho de Implementação da LGPD	Estabelece órgão responsável pelas diretrizes estratégicas de adequação à LGPD.	Integra a SES às ações estruturantes da política de proteção de dados estaduais.

	Art. 8º a 11	Grupo de Trabalho da LGPD	Organiza estrutura técnica para apoiar a governança e propor normativos.	Garante suporte técnico e jurídico à SES na implementação da LGPD.
	Art. 12	Capacitação de agentes públicos	Dispõe sobre treinamento e formação dos envolvidos com dados pessoais.	Exige que servidores da SES sejam capacitados em proteção e governança de dados.
	Art. 13 e 14	Política de proteção de dados e programa de governança	Define prazo e exigências para implementação de políticas e programas de privacidade.	Obriga a SES a instituir política própria e programa de governança em privacidade.
	Art. 15	Competência dos gestores públicos	Estabelece responsabilidades como medidas de segurança e comunicação de incidentes.	Responsabiliza os gestores da SES por implementar e supervisionar a governança de dados.
	Art. 16	Consultoria da PGE	Determina apoio jurídico da PGE na elaboração de atos normativos relacionados à LGPD.	Apoia tecnicamente a SES na criação de normas internas aderentes à LGPD.
	Art. 17	Empresas públicas e sociedades de economia mista	Exige que essas entidades adotem políticas próprias de proteção de dados.	Abrange autarquias da área da saúde que operem sob regime público ou misto.
Decreto Estadual 55.986/21	Art. 2º, §§ 3º e 4º	Designação de Encarregado compartilhado	Permite que órgãos com baixo volume de tratamento designem um mesmo encarregado de outra instituição pública.	Viabiliza compartilhamento de dados entre órgãos e autarquias da saúde pública com menor complexidade operacional.
	Art. 13	Parâmetros e orientações para programas de governança	Define que o Conselho sobre a LGPD estabelecerá parâmetros e orientações para os programas de governança em privacidade.	Fundamenta a construção de programas de governança de dados nas secretarias e órgãos estaduais de saúde.
	Art. 17-A	Estrutura permanente de governança	Estabelece o prazo e a responsabilidade pela proposição de uma estrutura permanente de governança da proteção de dados.	Pressupõe que a saúde pública estadual disponha de governança estável e institucionalizada em proteção de dados;
Decreto Estadual 55.987/21	Art. 1º	Instituição da Política Estadual de Proteção de Dados	Estabelece diretrizes e princípios fundamentais para o tratamento de dados pessoais no âmbito estadual.	Base normativa para adoção de políticas de proteção de dados na saúde pública;

	Art. 2º	Diretrizes estratégicas da Política de Proteção de Dados	Define parâmetros de governança e boas práticas para o tratamento de dados pessoais	Orienta a gestão estratégica da informação e governança de dados sensíveis da saúde
	Art. 4º	Programas de Governança em Privacidade (PGP)	Obrigatoriedade de elaboração de programas internos de governança com estrutura, documentos e planos	Fundamental para garantir estrutura de governança nas secretarias e instituições de saúde
	Art. 5º	Apoio técnico e orientações aos encarregados	Define apoio institucional e orientações aos encarregados de dados	Garante suporte técnico à governança de dados nas unidades públicas de saúde
	Art. 6º	Plataforma transversal para governança de dados	Estabelece sistema único para monitoramento da conformidade com a LGPD	Viabiliza gestão integrada e segura dos dados da saúde pública estadual
	Art. 7º	Contratação de consultorias para adequação à LGPD	Regulamenta exceções e condições para contratação de serviços de adequação à LGPD	Afeta diretamente as estratégias de implementação de governança em saúde
	Art. 8º	Política de privacidade e cookies nos sites públicos	Obrigatoriedade de veicular política de privacidade nos portais institucionais	Protege os dados de cidadãos usuários de serviços de saúde eletrônicos
	Art. 9º a 11	Atendimento aos titulares de dados	Regulamenta canal eletrônico, identificação, sigilo e acesso às informações pessoais	Assegura o direito do cidadão à consulta e controle sobre seus dados de saúde
	Art. 12 e 13	Registro de tratamento e anonimização	Exige que controladores mantenham registros e adotem técnicas de anonimização	Permite controle e segurança sobre os dados sensíveis da saúde pública
	Art. 14 e 15	Compartilhamento de dados	Estabelece regras e requisitos para uso compartilhado de dados pessoais	Garante segurança e finalidade legítima na troca de dados entre órgãos de saúde
Decreto Estadual 56.106/21	Art. 2º, IV, V, VI, VIII, IX	Definições e estrutura de governança de TIC	Define o Sistema de Governança e Gestão de TIC e menciona arquitetura digital e estruturas de decisão, essenciais para governança de dados.	Permite estruturar ações estratégicas em saúde baseadas em dados e decisões colegiadas de TIC nos órgãos da saúde pública.
	Art. 4º, VII	Áreas de abrangência da Política de TIC	Inclui expressamente Governança de Dados como área estratégica, ao lado de segurança da informação e arquitetura digital.	Direciona o uso de dados para tomada de decisão e aprimoramento de políticas públicas de saúde.

	Art. 15º, IV	Diretrizes gerais da Política de TIC	Promove o uso intensivo de melhores práticas de governança e gestão de TIC, incluindo governança de dados.	Aumenta a confiabilidade, integridade e governança sobre os dados produzidos no SUS.
	Art. 21, III, i	Conhecimento de TIC	Aponta 'governança e inteligência de dados' como área fundamental de conhecimento.	Capacita gestores e técnicos da saúde para tomada de decisão baseada em evidências.
	Art. 26	Diretrizes específicas para Governança de Dados	Estabelece objetivos, estruturas decisórias, cultura de dados, compartilhamento, padronização e segurança conforme a LGPD.	Viabiliza o uso ético, seguro e eficiente de dados de pacientes e serviços no SUS.
	Art. 31	Publicação das políticas específicas de segurança e governança de dados	Prevê a formalização das diretrizes da governança de dados por meio de decreto específico.	Assegura institucionalização e sustentabilidade das práticas de governança de dados em saúde.
Decreto Estadual 56.528/22	Art. 1º	Diretrizes para compartilhamento de dados	Estabelece a base normativa do compartilhamento de dados entre órgãos públicos estaduais.	Favorece integração entre sistemas de informação da saúde, viabilizando serviços mais eficazes e análise de dados para formulação de políticas públicas.
	Art. 3º	Definições relacionadas ao tratamento e governança de dados	Define atores como gestores de dados, facilitadores de dados e operadores de infraestrutura.	Estrutura o papel institucional de agentes responsáveis pelos dados em saúde pública.
	Art. 4º e 5º	Designação e responsabilidades dos facilitadores de dados	Institui a exigência de termo de responsabilidade e controle sobre os dados administrados.	Assegura <i>accountability</i> na gestão de dados de saúde, com responsabilidades claras.
	Art. 6º	Classificação dos dados por nível de compartilhamento	Define níveis de compartilhamento: amplo, institucional e específico.	Organiza a abertura dos dados em saúde conforme grau de sensibilidade, respeitando a LGPD.
	Art. 7º a 10	Qualidade dos dados e validação	Estabelece padrões técnicos e ações para garantir entrada, extração e uso qualificado dos dados.	Melhora a confiabilidade dos registros em saúde pública e sua utilização em decisões.
	Art. 11 a 16	Mecanismos e custos de compartilhamento de dados	Regula procedimentos para acesso e uso dos dados, conforme sua classificação.	Permite estruturação segura do acesso aos dados de saúde por diferentes entidades públicas.

	Art. 17 a 19	Padrões de TIC e catalogação das bases de dados	Impõe deveres aos órgãos públicos para catalogar e informar suas bases de dados e metadados.	Fundamental para mapear os bancos de dados da saúde e implementar governança eficaz.
Padrão Técnico (PTIC) 01/22	1.1	Objeto do PTIC	Estabelece os procedimentos para classificação e qualidade de dados.	Normatiza práticas de governança de dados no tratamento de informações da saúde no âmbito do Estado.
	1.3	Designação dos Facilitadores de Dados	Define papéis e responsabilidades na catalogação e classificação de dados.	Garante responsabilidade institucional na manipulação de dados de saúde sob gestão pública.
	2.1 a 2.4	Processos de Catalogação de Dados	Orienta a organização e classificação sistemática de dados conforme sua finalidade.	Viabiliza o mapeamento e o uso qualificado de dados clínicos, administrativos e epidemiológicos.
	2.5	Procedimentos de Catalogação	Define os campos obrigatórios e formatos para a catalogação estruturada.	Assegura o controle de ciclo de vida dos dados de pacientes, sistemas e serviços de saúde.
	2.6	Níveis de Compartilhamento de Dados	Classifica os dados em amplo, institucional ou específico conforme acesso permitido.	Fundamental para controlar o sigilo de dados sensíveis em saúde pública, conforme a LGPD.
	2.7	Validação dos Dados Catalogados	Estabelece fluxo de aprovação e revisão dos dados catalogados.	Garante qualidade, segurança e controle sobre os dados disponibilizados no SUS.
	2.8	Qualificação dos Dados	Estipula padrões para dados comuns e para desenvolvimento de novos sistemas.	Facilita integração entre bases e padronização de dados utilizados em ações de saúde.
	2.9	Qualidade e Proteção de Dados Pessoais	Dispõe sobre CPF como identificador, anonimização e conformidade com a LGPD.	Crucial para garantir o sigilo e a rastreabilidade dos dados dos cidadãos atendidos pelo SUS.
Nota Técnica SES/RS 01/22	Trecho integral	Orientações para uso de dados da SES-RS em pesquisas científicas	Estabelece critérios, vedações e fluxos de acesso aos dados sob gestão da SES-RS, incluindo requisitos de anonimização e pseudoanonimização, em conformidade com a LGPD.	Garante a proteção e o uso ético de dados sensíveis da saúde pública em projetos científicos, orientando pesquisadores e servidores quanto às responsabilidades legais.

O quadro acima (Quadro 4) apresenta um mapeamento estruturado das disposições normativas dos marcos legais analisados e descritos no quadro 3, com ênfase nos dispositivos diretamente relacionados à governança de dados pessoais no contexto da saúde pública. Cada linha contempla a identificação do artigo legal, a síntese do tema central abordado, a descrição da relação com a governança de dados pessoais e a aplicabilidade específica no âmbito do SUS. Entre os temas destacados, constam princípios para o tratamento de dados, regulamentações para uso em pesquisas, diretrizes para tratamento por órgãos públicos, padrões de boas práticas e governança, bem como obrigações atribuídas aos agentes de tratamento. A planilha organiza essas informações de modo a permitir a visualização integrada dos fundamentos legais e de sua tradução prática para o setor público de saúde, contemplando tanto aspectos de conformidade quanto de operacionalização das exigências legais.

Quadro 5. Modelos de programas institucionais de governança em privacidade selecionados

ID	Órgão	Principais tópicos	Principais conceitos relacionados à governança de dados pessoais	Práticas ou estruturas que possam ser adaptadas ao contexto da SES/RS
1	Ministério da Saúde (2022)	Iniciação e Planejamento; Construção e Execução; Monitoramento	<i>Privacy by design</i> , cultura de proteção de dados, RIPD, política de privacidade, inventário de dados pessoais, encarregado de dados, indicadores de performance, plano de resposta a incidentes	Modelo de diagnóstico de maturidade, estrutura da Assessoria Especial de Proteção de Dados (AEPD), criação de comitês internos, instrumentos de avaliação contínua, modelo de RIPD e plano de conscientização
2	PGE/RS (2021)	Estrutura organizacional; Instrumentos operacionais; Cronograma de implantação	Inventário de dados, relatórios de impacto, plano de resposta a incidentes, política de privacidade, grupo de apoio ao encarregado, governança da informação e dos processos	Modelo escalonado de implantação com cronograma, definição clara dos instrumentos operacionais, estruturação do grupo de apoio ao encarregado, modelo de Política de Privacidade e Proteção de Dados da PGE (PPPD/PGE)

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 5) apresenta informações organizadas sobre os dois programas institucionais de governança em privacidade selecionados. Cada registro está estruturado pelo órgão responsável pela publicação, acompanhado do ano de referência. São descritos, para cada documento, os principais tópicos abordados, os conceitos centrais relacionados à governança de dados pessoais e as práticas ou estruturas com potencial de adaptação ao contexto da SES/RS. Entre os tópicos, destacam-se elementos de planejamento, execução e monitoramento de programas, aspectos organizacionais, instrumentos operacionais e metodologias de implantação. Já os conceitos centrais incluem abordagens como *privacy by design*, inventário e diagnóstico de dados, relatórios de impacto e planos de adequação. Por fim, são indicadas práticas e modelos estruturais, como diagnósticos de maturidade e cronogramas escalonados, que podem servir de referência para o desenvolvimento de políticas internas.

5.4 Bases de Dados - SES/RS

A identificação da natureza e da finalidade dos sistemas permitiu constatar a existência de um volume expressivo de operações de tratamento de dados pessoais, abrangendo tanto usuários do SUS quanto servidores públicos e colaboradores da SES/RS. Esses sistemas, em sua maioria, operam com dados pessoais sensíveis, frequentemente associados à saúde, à identificação funcional, à gestão administrativa e à prestação de serviços públicos essenciais.

A seguir, apresenta-se o Quadro 6, que sistematiza as bases de dados identificadas, organizadas segundo sua finalidade principal.

Quadro 6. Bases de dados da SES/RS, organizadas por finalidade

ID	Finalidade do Sistema	Sistemas
1	Financeiro	- FPE (Sistema de tecnologia da informação que permite o gerenciamento e controle da execução orçamentária, financeira e contábil da despesa e da receita do Estado) - SAIPS - Sistema de Apoio à Implementação de Políticas em Saúde - Captação de recursos
2	Monitoramento	- Sistema de Monitoramento Estratégico - SGE
3	Planejamento	- DIGISUS - Instrumentos de planejamento do MS
4	Tramitação de Processos Administrativos	- PROA (Sistema onde tramitam os processos administrativos)
5	Recursos Humanos	- RHE - Recursos Humanos do Estado; - RHS - Recursos Humanos da SES; - SIST - Sistema de Informação da Saúde do Trabalhador (notificações e investigações)
6	Políticas de Saúde	- SISAB - Produção da Atenção Básica; - SisPIM - Sistema da Primeira Infância Melhor; - SIVISA - Sistema de Informação da Vigilância Sanitária
7	Sistemas de Informação	- SIM - Sistema de Informação de Mortalidade; - SINASC - Sistema de Informação de Nascidos Vivos; - SIH - Sistema de Informações Hospitalares; - SIA - Sistema de Informações Ambulatoriais; - SINAN - Sistema de Informação de Agravos de Notificação; - SIVEP Gripe - Sistema de notificação de SRAG e SG; - Esus Notifica - Notificação COVID-19; - SIPNI - Sistema de Informação do Programa Nacional de Imunizações; - Sistema Nacional de Transplantes (SNT) - Central de Transplantes; - Hemovida;

8	Gestão	- SIGAH - Sistema de Gestão da Atenção Hospitalar; - SISMAC - Sistema de Controle de Limite Financeiro da Média e Alta Complexidade; - AME - Administração de Medicamentos; - GAL - Gestão de Laboratórios (LACEN); - VGS - Gestão de Doadores de sangue; - GERINT - Gestão da Regulação de Internações; - GERCON - Gestão da Regulação de Consultas; - GERPAC - Gestão da Regulação de procedimentos de Alto Custo; - SAPH - Gestão de Atendimento Móvel de Urgência e Emergência - SAMU;
9	Educacional	- Sistema de Gestão Acadêmica; - POPERS - Portal de Pesquisas na SES - Comitê Gestor da Política de Pesquisas na SES; - Gestão da Biblioteca - Pergamum;
10	Comunicação	- Gestão do Site da SES; - Instagram, Twitter, Youtube; - Ouvidor SUS; - LAI - Sistema de recebimento de demandas da Lei de Acesso à Informação

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 6) apresenta um inventário de sistemas utilizados na SES/RS, organizados em duas colunas principais. A primeira coluna, intitulada “Finalidade do Sistema”, descreve a função principal de cada sistema, abrangendo áreas como gestão financeira, monitoramento, planejamento, tramitação de processos administrativos, recursos humanos, políticas de saúde, sistemas de informação, gestão, atividades educacionais e comunicação institucional. A segunda coluna, “Sistemas”, relaciona nominalmente as ferramentas ou plataformas vinculadas a cada finalidade, detalhando desde sistemas internos de tramitação e controle até plataformas de monitoramento estratégico, gestão acadêmica, redes sociais e bases de dados utilizadas no âmbito da saúde pública.

5.5 Categorias Temáticas: Conceitos, Desafios e Lacunas

A partir da análise sistemática dos artigos científicos e documentos de literatura cinzenta incluídos nesta revisão, identificaram-se conceitos recorrentes e desafios relevantes relacionados à governança de dados pessoais no contexto da saúde pública brasileira. A categorização dos conteúdos foi conduzida com base em análise de conteúdo, permitindo uma sistematização robusta dos eixos temáticos predominantes, bem como das lacunas apontadas pelos estudos.

Entre os conceitos-chave mais frequentemente abordados nas publicações, destacam-se: confidencialidade, privacidade, dados pessoais e dados sensíveis, consentimento, governança, interoperabilidade, anonimização, *accountability*, *compliance*, minimização de dados, entre outros.

Quanto aos desafios e lacunas identificadas, os temas mais recorrentes envolvem: compartilhamento indevido de dados pessoais sensíveis; acesso descontrolado a dados entre diferentes instituições; utilização de dados pessoais sem base legal claramente definida; ausência de uma cultura institucional voltada à proteção de dados; falta de articulação entre entes federativos; dificuldades técnicas para a adequação das plataformas públicas; carência na formação de profissionais sobre governança de dados; e inexistência de diretrizes operacionais claras nos serviços públicos de saúde.

Os resultados foram organizados segundo três eixos analíticos principais: Pessoas, Processos e Tecnologias, com a respectiva frequência percentual de ocorrência dos conceitos e a síntese dos principais desafios e lacunas apontados. Essa categorização encontra-se detalhada no Quadro 7 a seguir.

Para aprofundar a análise dos desafios mapeados e facilitar sua incorporação em propostas práticas, elaborou-se o Quadro 8, que organiza os principais desafios por categoria temática transversal, consolidando os achados da literatura em quatro grupos analíticos.

Quadro 7. Conceitos mais citados, desafios apontados e lacunas evidenciadas por eixo temático

Eixo	Principais Conceitos Citados (%)	Principais Desafios Apontados	Principais Lacunas Evidenciadas
PESSOAS	* Privacidade (100%) * Dados pessoais e dados pessoais sensíveis (100%) * Consentimento (85%) * Confidencialidade (65%) * Desigualdades raciais na proteção de dados (10%)	* Acesso descontrolado e o uso indevido dos dados de saúde; * Banalização do direito à privacidade do indivíduo; * Respeito às pessoas e à sua vulnerabilidade, o respeito à autonomia dos pacientes e ao seu melhor benefício, bem como todos os cuidados relativos à segurança das diferentes informações	* Dados já coletados e armazenados nos equipamentos do SUS sem prévia solicitação de consentimento * Falta de conhecimento dos usuários sobre como seus dados estão sendo compartilhados * Integração entre proteção de dados e gestão pública com foco em cidadania
PROCESSOS	* Anonimização (85%) * Interoperabilidade / Compartilhamento (80%) * Governança (55%) * Monitoramento e tratamento de incidentes (50%) * Minimização de dados (45%) * <i>Compliance</i> (35%) * Integridade dos dados (30%) * <i>Accountability</i> (25%) * <i>Privacy by design</i> - privacidade desde a concepção (10%) * RIPD (10%)	* Segurança, confiabilidade e a proteção da integridade dos dados. * Regulamentação sobre o tema ainda limitada, fragmentada e instável. * Busca de proteção das informações sensíveis X as necessidades e dificuldades práticas de gestão * Variabilidade de modelos e vias de coleta não padronizadas e não normatizadas * Limitação de recursos orçamentários para a adaptação de todos os sistemas informatizados às regras da LGPD. * Falta de estrutura normativa e técnica para proteção de dados sensíveis no SUS * Falta de integração entre LGPD e práticas administrativas públicas * Falta de padronização, segurança e integração entre sistemas * Falta de conhecimento técnico sobre a LGPD no setor público * Governança responsável, transparente e participativa para o uso de dados em saúde pública. * Risco de vigilância excessiva, desigualdade no acesso à tecnologia e ausência de salvaguardas claras.	* Interoperabilidade / compartilhamento de dados sem prévio consentimento * Livre compartilhamento de informações entre instituições de igual ou distinta esfera federativa sem clara regulamentação * Ausência de uma política nacional única de segurança de dados de saúde * Implementação efetiva da LGPD * Fortalecimento da fiscalização * Aperfeiçoamento da legislação para que puna os agentes que comprarem/obterem, intermediarem, venderem e usarem indevidamente os dados acarretando prejuízos aos cidadãos. * Treinamentos, orientações e documentos normativos internos. * Estabelecimento de protocolos regulatórios claros * Participação social na governança de dados.

TECNOLOGIAS	* Telemedicina (40%) * Tecnologias de informação e comunicação (TIC) (35%) * Internet das Coisas (IoT) (30%) * E-Saúde (e-Health) (25%) * Blockchain (15%) * Sistema de Gestão de Segurança da Informação (SGSI) (5%) * MDCS (5%) * Population Data BC (PopData) (5%) * <i>Personal data storage</i> PDS - armazenamento pessoal de dados (5%)	* Conflitos entre as diretrizes regulatórias e as características do blockchain; * MDCS - obter e tratar o consentimento informado explícito dos titulares dos dados e permitir a retirada do consentimento / definir medidas para se opor ao processamento e permitir o bloqueio ou exclusão de dados / utilizar técnicas apropriadas de anonimização para o compartilhamento de dados	* Plataformas de interoperabilidade de dados com regras transparentes e sob governança pública * Adoção de protocolos rígidos de segurança e responsabilização clara
--------------------	--	--	---

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 7) apresenta os conceitos mais citados, desafios apontados e lacunas evidenciadas por eixo temático. A organização dos achados ocorre segundo três eixos principais — Pessoas, Processos e Tecnologias —, cada um deles acompanhado de um conjunto de informações estruturadas. Para cada eixo, são elencados os principais conceitos citados, expressos em termos percentuais de ocorrência nas fontes analisadas, seguidos dos principais desafios apontados, que indicam obstáculos ou barreiras associadas à temática, e das principais lacunas evidenciadas, que correspondem a aspectos ainda carentes de desenvolvimento ou aprofundamento. O eixo “Pessoas” concentra-se em elementos como privacidade, dados pessoais e sensíveis, além de direitos dos titulares. O eixo “Processos” contempla questões como anonimização, interoperabilidade e conformidade regulatória. Já o eixo “Tecnologias” aborda tópicos como telemedicina, tecnologias da informação e comunicação e infraestrutura digital.

Quadro 8: Desafios Identificados por Categoria Temática Transversal

Categoria	Desafios Relacionados
Compartilhamento Inadequado de Dados	* Compartilhamento indevido de dados pessoais sensíveis. * Acesso descontrolado a dados entre diferentes instituições.
Uso Indevido ou Tratamento Inadequado	* Tratamento inadequado de dados em sistemas informacionais de saúde. * Uso de dados pessoais sem base legal clara.
Desinformação e Falta de Transparência	* Falta de transparência na coleta e uso dos dados por parte das instituições públicas. * Baixo nível de conhecimento dos usuários sobre os seus direitos de proteção de dados.
Dados Sensíveis e Vulnerabilidades	* Risco de exposição de dados clínicos sensíveis sem mecanismos de proteção apropriados.
Outros (Desafios Diversos ou Não Classificados)	* Ausência de cultura institucional voltada à proteção de dados. * Falta de articulação entre entes federativos. * Dificuldade de adequação técnica das plataformas públicas. * Lacuna na formação de profissionais sobre governança de dados. * Falta de diretrizes operacionais claras nos serviços públicos de saúde. * Insegurança jurídica sobre os fluxos de dados em saúde pública. * Limitações técnicas para anonimização e pseudonimização dos dados. * Pouca integração entre os sistemas de informação em saúde. * Resistência institucional à implementação de políticas de proteção de dados.

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 8) apresenta um mapeamento de desafios organizados em categorias temáticas. Cada categoria agrupa um conjunto de dificuldades ou problemas recorrentes, como o compartilhamento inadequado de dados, o uso indevido ou tratamento inadequado das informações, a desinformação e a falta de transparência, as questões relacionadas a dados sensíveis e vulnerabilidades, e outros desafios diversos ou não classificados. Para cada categoria, são listados de forma descritiva os desafios específicos observados, contemplando aspectos como riscos à privacidade, fragilidades institucionais, insuficiência de políticas e procedimentos, e práticas que podem comprometer a segurança e a conformidade legal no tratamento de dados.

5.6 Síntese Integrativa: Diretrizes LGPD na Governança de Dados

A presente revisão de escopo possibilitou a construção de uma síntese integrativa sobre o estado atual da governança de dados pessoais na saúde pública brasileira, com base na LGPD, e com foco especial na aplicabilidade institucional dos achados à realidade da SES/RS. A análise cruzada entre documentos científicos, institucionais e normativos revelou um conjunto de conceitos operacionais recorrentes — como *privacy by design*, relatório de impacto à proteção de dados, minimização de dados, interoperabilidade e *accountability* — que funcionam como pilares conceituais essenciais para uma governança de dados eficaz, segura e juridicamente alinhada às exigências da LGPD.

Além dos conceitos estruturantes, a revisão identificou boas práticas concretas que podem ser adaptadas e implementadas no contexto da SES/RS, com vistas à elaboração de um Programa de Governança em Privacidade. Dentre essas práticas, destacam-se: (i) elaboração periódica de Relatórios de Impacto à Proteção de Dados (RIPD) nos projetos e sistemas estratégicos da Secretaria; (ii) mapeamento e classificação das bases de dados sob responsabilidade da instituição; (iii) designação formal de encarregado pelo tratamento de dados, com formação e capacitação técnica contínuas; (iv) definição de fluxos claros de governança, supervisão e auditoria da informação; (v) implementação de capacitações técnicas permanentes voltadas aos servidores públicos; e (vi) integração da temática da proteção de dados aos planos de integridade e *compliance* institucionais; (vii) adoção de estratégias de resposta a incidentes, com protocolos claros e auditáveis.

As principais diretrizes identificadas em cada documento analisado encontram-se sistematizadas no Quadro 9, que relaciona o título da obra, o ano de publicação e as diretrizes propostas. Na sequência, o Quadro 10 resume as práticas e estruturas com maior potencial de replicação, extraídas dessa síntese crítica e adaptadas à realidade dos serviços públicos de saúde.

Quadro 9. Diretrizes propostas para a governança de dados pessoais no contexto da saúde pública brasileira

Título do Estudo / Temática	Ano	Propostas de diretrizes para a Governança de Dados Pessoais
O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados	2023	Adoção de protocolos rígidos de segurança e responsabilização clara
Capítulo – Lei Geral de Proteção de Dados: desafios para o SUS e a cidadania	2018	Integração entre proteção de dados e gestão pública com foco na cidadania e no fortalecimento dos direitos fundamentais.
A autodeterminação informativa como contexto normativo para elaboração de diretrizes para a construção de um Relatório de Impacto à Proteção de Dados Pessoais	2023	Modelo de RIPD baseado em princípios legais. Criação de diretrizes com foco na preservação da dimensão humana no tratamento de dados pessoais.
Questões éticas e perspectiva jurídica da proteção de dados	2021	Fortalecimento da LGPD. Implementação de instrumentos legais que garantam privacidade sem inviabilizar pesquisa.
Metodologia de Administração de Dados (MAD)	2024	Padronização de processos, definição de papéis e segurança da informação. Implantação de padrões de administração e interoperabilidade de dados de saúde.
Guia Orientativo para o Poder Público – ANPD	2023	Mapeamento de dados, elaboração de RIPD, boas práticas de segurança da informação
Cartilha de Condutas voltadas à Privacidade e à Proteção de Dados	2022	Treinamentos, orientações e documentos normativos internos.
Cartilha LGPD PROCERGS – Lei Geral de Proteção de Dados	2022	Implantação de Programa de Governança em Privacidade (PGP), treinamentos e padronização.
Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global	2020	Estabelecimento de protocolos regulatórios claros e participação social na governança de dados. Identificação de riscos de uso indevido de dados e necessidade de salvaguardas robustas para garantir confiança social.
A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais	2022	Estabelecimento de estruturas regulatórias.
La Lei General de Protecció de Dades i les seves implicacions per a la salut	2022	Implementação de um Sistema de Gestão de Segurança da Informação (SGSI)

Privacidade e confidencialidade das informações clínicas em saúde mental: velhos desafios em um novo contexto	2021	Compartilhamento responsável de dados pessoais. Implementação de rotina de treinamentos sobre a temática da governança de dados
Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology	2024	Foco na segurança, na confiabilidade e na proteção da integridade dos dados. Capacitação dos gestores dos dados.
Mobile Health Systems for Community-Based Primary Care: Identifying Controls and Mitigating Privacy Threats	2019	Integrar os procedimentos organizacionais relacionados à privacidade em um sistema de gestão de segurança da informação. Estabelecer maneiras para lidar com vulnerabilidades e ataques desconhecidos. Estabelecer revisão contínua dos processos e procedimentos estabelecidos.
Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança	2018	Sugestão de adoção do Population Data BC (PopData) - modelo inovador para o acesso, tratamento e uso de bases de dados populacionais de interesse para a pesquisa em saúde.
Capítulo 3 – Privacidade, ética e transparência de dados na saúde Capítulo 7 – Onde estão os usuários neste debate?	2023	Inclusão dos usuários no debate relativo aos problemas existentes para a consolidação do direito aos dados pessoais.
Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais	2022	Plataformas de interoperabilidade de dados com regras transparentes e sob governança pública. Fortalecimento dos sistemas de fiscalização.
Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde	2020	Avaliação sobre o estágio de maturidade. Definição do plano a ser seguido para a efetiva proteção dos dados e para o atingimento dos requisitos da LGPD. Estabelecimento das políticas e diretrizes internas. Gestão de terceiros [prestadores contratados]. Monitoramento e tratamento de incidentes.
Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados	2021	Sugestão de adoção de Personal Data Storages (PDS) - armazenamento pessoal de dados, funciona como um cofre ou armário pessoal de dados.

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 9) apresenta diretrizes propostas para a governança de dados pessoais no contexto da saúde pública brasileira. A base de dados utilizada neste quadro compreende 19 registros (artigos científicos e literatura cinzenta), abrangendo publicações distribuídas no período de 2018 a 2024. O conjunto contempla títulos variados, cada um associado às propostas de diretrizes para a governança de dados pessoais. A planilha está organizada em três colunas principais, incluindo “Título do Estudo / Temática”, “Ano” e “Propostas de diretrizes para a Governança de Dados Pessoais”.

Quadro 10. Práticas e Estruturas para Programas de Governança em Privacidade

ID	Práticas ou estruturas recomendáveis para aplicação em Programas de Governança em Privacidade
1	Modelo de diagnóstico de maturidade
2	Criação de comitês internos
3	Padronização dos fluxos de tratamento
4	Classificação de bancos de dados
5	Revisão contínua dos processos e procedimentos estabelecidos
6	Modelo de RIPD e plano de conscientização
7	Modelo escalonado de implantação com cronograma
8	Definição clara dos instrumentos operacionais
9	Designação formal de encarregados pelo tratamento de dados
10	Estruturação do grupo de apoio ao encarregado
11	Capacitação técnica contínua
12	Participação Social
13	Implementação de um Sistema de Gestão de Segurança da Informação (SGSI)
14	Protocolo de resposta de incidentes
15	Adoção do conceito privacy by design

Fonte: elaborado pela autora (2025)

O quadro acima (Quadro 10) apresenta um conjunto de 15 práticas e estruturas recomendáveis para aplicação em Programas de Governança em Privacidade. Entre os elementos listados, destacam-se propostas voltadas à organização interna, como a criação de comitês específicos, a designação formal de encarregados pelo tratamento de dados e a estruturação de grupos de apoio.

Também são incluídas medidas técnicas e procedimentais, como a padronização dos fluxos de tratamento, a classificação de bancos de dados, a revisão contínua de processos, bem como a adoção de modelos de diagnóstico de maturidade e de RIPD aliados a planos de conscientização. Adicionalmente, contempla-se a definição de instrumentos operacionais claros e a implantação escalonada com cronograma, compondo um arcabouço de ações voltadas à consolidação de uma governança eficaz e alinhada às exigências legais e organizacionais.

6 DISCUSSÃO

6.1 Análise dos achados: desafios, diretrizes e lacunas da governança de dados pessoais na saúde pública

A análise dos 19 estudos incluídos nesta revisão de escopo (artigos científicos e literatura cinzenta) evidenciou que a implementação da LGPD no âmbito da saúde pública brasileira ainda se encontra em estágio incipiente, enfrentando entraves normativos, operacionais e institucionais que dificultam a consolidação de práticas eficazes de governança de dados.

No período de 2020 a 2021, observou-se um aumento expressivo na produção científica e institucional sobre o tema, reflexo do início da vigência da LGPD em 2020, bem como, do início da aplicação das sanções em 2021. Entretanto, após este período inicial de grande repercussão da lei, observa-se nova queda nas publicações - 2022 em diante - nos termos do que se demonstrou no gráfico 2.

Relativamente aos tipos de estudos encontrados, observou-se que grande parte concentrou-se em comentários, abordagens teóricas e jurídico-normativas da LGPD, enfatizando princípios como finalidade, necessidade, responsabilização e segurança como fundamentos da proteção de dados no contexto do SUS. No entanto, não foram identificados estudos que apresentaram propostas práticas de diagnóstico organizacional para aplicação da LGPD no setor público, revelando uma lacuna crítica de estudos empíricos e operacionais voltados à implementação institucional.

Entre alguns dos obstáculos identificados estão: (i) a diversidade de sistemas e plataformas de informação do SUS; (ii) a ausência de regulamentação mínima quanto ao fluxo de informações entre órgãos integrantes do SUS; (iii) escassez de debate acadêmico, teórico e prático acerca da necessidade de adaptação do SUS aos dispositivos da LGPD; (iv) ausência de uma cultura organizacional voltada à proteção de dados; (v) lacunas regulatórias específicas aplicáveis à saúde pública; (vi) baixa interoperabilidade entre sistemas informacionais; (vii) escassez de profissionais capacitados; e (viii) riscos decorrentes da exposição de dados sensíveis em ambientes digitais (Aragão *et al.*, 2020; Zaganelli *et al.*, 2022; Ventura *et al.*, 2018). Também foi evidenciada a invisibilidade de grupos vulneráveis nos

modelos institucionais de proteção de dados, com destaque para populações negras e em situação de vulnerabilidade social. Essa exclusão, apontada por Carvalho (2023), acarreta riscos éticos, jurídicos e operacionais, especialmente em um setor que lida com informações altamente sensíveis.

A literatura cinzenta complementou a análise ao fornecer diretrizes normativas, experiências institucionais e reflexões práticas oriundas da própria Administração Pública. Documentos como os guias da ANPD (2023), a Cartilha LGPD da PROCERGS (2022) e o MAD do Ministério da Saúde (2024) ofereceram subsídios operacionais relevantes — tais como mapeamento e classificação de bancos de dados, definição de papéis e fluxos, e elaboração de RIPD. No entanto, ainda são escassas as evidências sobre a efetividade dessas práticas no cotidiano das instituições públicas de saúde; bem como, observa-se que se tratam em grande parte de documentos institucionais localizados e sem aplicação direta à nível nacional.

Os principais conceitos recorrentes nos documentos analisados — como privacidade, confidencialidade, interoperabilidade, anonimização e consentimento — constituem pilares para a construção de uma política institucional alinhada à LGPD. A sistematização desses conceitos está apresentada no Quadro 7, que também indica a frequência de sua ocorrência nas fontes analisadas. Observa-se, nesse sentido, um movimento de incorporação progressiva da cultura de proteção de dados nas instituições públicas, especialmente a partir das discussões mais recentes sobre segurança da informação e justiça algorítmica (Cavalcante *et al.*, 2024).

As lacunas e os desafios mapeados também foram organizados em três eixos estratégicos — pessoas, processos e tecnologias — conforme categorização do Quadro 7. No eixo “pessoas”, destaca-se a ausência de cultura organizacional e a carência de formação técnica continuada entre os servidores. No eixo “processos”, evidencia-se a inexistência de fluxos institucionais de governança e auditoria, bem como a baixa articulação entre áreas técnicas e jurídicas. Já no eixo “tecnologias”, os principais entraves referem-se à obsolescência dos sistemas, à falta de interoperabilidade e às falhas na anonimização de dados sensíveis.

O Quadro 9 apresenta um conjunto de diretrizes propositivas extraídas da literatura científica, da literatura cinzenta e de documentos institucionais, com destaque para a elaboração de RIPD, a institucionalização de comitês de

governança, a capacitação técnica dos encarregados e a inserção da proteção de dados nos planos de integridade e *compliance*. A incorporação dessas boas práticas ao contexto da SES/RS pode contribuir para o fortalecimento de sua política de governança em privacidade.

Complementarmente, o Quadro 10 sistematiza práticas e estruturas com potencial de incorporação no Programa de Governança em Privacidade da SES/RS. Entre elas, destacam-se elementos estruturantes constantes no guia da ANPD (2023), na Cartilha de Condutas da PROCERGS (2022) e na Cartilha LGPD da PROCERGS (2022), como a padronização dos fluxos de tratamento, a classificação de bancos de dados, a definição de protocolos de resposta a incidentes e a designação formal de encarregados pelo tratamento de dados, com capacitação técnica contínua.

As evidências indicam que a proteção de dados pessoais sensíveis na saúde pública deve ser compreendida não apenas como uma exigência legal, mas como instrumento de fortalecimento da cidadania, da equidade, do controle social e da qualidade da atenção à saúde. Temas como interoperabilidade, segurança da informação, RIPD, justiça algorítmica, inclusão digital e *privacy by design* têm ganhado centralidade nas publicações mais recentes, ampliando o debate para além da conformidade normativa e incorporando dimensões éticas, sociais e tecnológicas da governança (Cavalcante *et al.*, 2024; PROCERGS, 2022; Camara *et al.*, 2021).

Apesar dos avanços observados, permanecem fragilidades importantes. Estudos como os de Zaganelli *et al.* (2022), Aragão *et al.* (2020), Guanaes (2018) e o MAD do Ministério da Saúde (2024) apontam para a ausência de padronização nacional na aplicação da LGPD no setor público e evidenciam a desproporcionalidade econômica relativa aos esforços de adequação e conformidade às novas diretrizes legais. A falta de investimentos contínuos em infraestrutura digital e em formação também compromete a sustentabilidade das ações em curso. Dessa forma, ainda que se observe uma evolução normativa e institucional relevante, a governança de dados no SUS segue em processo de amadurecimento, exigindo maior coordenação interinstitucional, mecanismos eficazes de avaliação e maior atenção às especificidades regionais na formulação de políticas públicas.

6.2. Implicações para a Política Pública e Gestão de Dados Pessoais

Os achados desta revisão fornecem subsídios relevantes e concretos para o aprimoramento das políticas públicas no campo da proteção de dados pessoais no setor da saúde pública brasileira. Em primeiro lugar, revela-se urgente a definição de diretrizes nacionais claras que promovam a harmonização das práticas relativas à saúde digital, assegurando níveis mínimos de segurança, interoperabilidade e responsabilização (Carvalho, 2023).

No nível subnacional, a revisão identificou a ausência de estruturas institucionais formais para a governança de dados, reflexo da escassez de diretrizes aplicáveis em âmbito nacional — como capacitações, comitês de proteção de dados, planos de resposta a incidentes, RIPDs e encarregados designados. Esse vácuo organizacional, aliado à limitada capacitação técnica dos servidores, compromete não apenas a conformidade legal, mas também a efetividade das ações em saúde, sobretudo nos serviços de atenção primária e vigilância em saúde.

Nesse contexto, torna-se imprescindível a formulação de políticas públicas que contemplem ações estruturantes como: (i) a formação técnica continuada e descentralizada sobre fundamentos legais e operacionais da LGPD; (ii) a criação de linhas de financiamento específicas para modernização da infraestrutura tecnológica; (iii) a disponibilização de soluções interoperáveis de baixo custo adaptadas à realidade local; e (iv) a definição de planos de ação intersetoriais que orientem desde o mapeamento e classificação dos bancos de dados até os fluxos de resposta a incidentes de segurança.

Outro ponto de destaque diz respeito à promoção da cultura de proteção de dados como eixo transversal da gestão pública. A elaboração de RIPDs, a adoção do princípio da minimização, o fortalecimento da responsabilização e a implementação de soluções baseadas no conceito de *privacy by design* devem ser incentivados e incorporados nos processos de planejamento, contratação, auditoria e avaliação de políticas públicas.

Foram identificados nos estudos analisados diversas ferramentas tecnológicas potencialmente capazes de contribuir para uma melhor governança dos dados pessoais, como por exemplo, uso da tecnologia blockchain, MDCS, population Data BC (PopData) e personal data storage PDS - armazenamento

peçoal de dados (Camara *et al.*, 2021; Ventura *et al.*, 2018; Iwaya *et al.*, 2019; Corte-Real *et al.*, 2024).

A revisão também alerta para a necessidade de políticas inclusivas, que garantam que grupos historicamente invisibilizados — como a população negra e pessoas em situação de vulnerabilidade social — sejam contemplados nos modelos de governança de dados. A ausência de salvaguardas específicas pode aprofundar desigualdades, sobretudo quando dados sensíveis são utilizados de forma indiscriminada por sistemas automatizados de triagem, atendimento ou fiscalização (Carvalho, 2023).

Dessa forma, os resultados desta revisão não apenas evidenciam lacunas normativas, operacionais e estruturais, mas também indicam caminhos estratégicos e adaptáveis para que a proteção de dados pessoais sensíveis seja compreendida como instrumento de fortalecimento da cidadania, do controle social, da equidade em saúde e da qualidade da atenção prestada pelo SUS.

6.3. Limitações da Revisão

Apesar da abrangência metodológica adotada e da busca intencional por múltiplas fontes, esta revisão apresenta limitações que devem ser consideradas na interpretação dos resultados. Observa-se uma predominância de estudos qualitativos, descritivos e de natureza teórica, com ênfase em análises jurídico-normativas, o que restringe a possibilidade de generalização dos achados. Esse cenário revela uma lacuna expressiva de investigações empíricas robustas capazes de avaliar, de forma sistemática e mensurável, a efetividade das medidas de proteção de dados implementadas nos serviços públicos de saúde. As principais limitações identificadas, tanto nos estudos científicos quanto na literatura cinzenta incluídos, concentram-se em: (i) predominância de abordagens descritivas e normativas; (ii) escassez de evidências empíricas; (iii) ausência de padronização conceitual e metodológica entre as pesquisas; e (iv) reduzida atualização e aplicabilidade prática de parte dos documentos institucionais analisados.

Adicionalmente, constatou-se a dificuldade em mapear de maneira abrangente e sistemática a totalidade das publicações institucionais disponíveis sobre o tema, sobretudo devido à sua dispersão em múltiplas plataformas digitais e à ausência de um repositório centralizado. Essa dispersão foi agravada pela

heterogeneidade dos documentos em termos de escopo, estrutura, formato e atualidade, dificultando a identificação de modelos consolidados de governança em privacidade e a comparação entre diferentes iniciativas.

A inclusão da literatura cinzenta — embora essencial para o enriquecimento da análise, por conter diretrizes práticas, experiências institucionais e orientações operacionais da própria Administração Pública — impõe desafios metodológicos relevantes. Tais fontes carecem, em geral, de revisão por pares, o que fragiliza sua validade científica e impõe atenção ao risco de viés de autoria ou de institucionalidade. A ausência de critérios uniformes de elaboração, bem como a falta de atualização em muitos desses documentos, compromete sua aplicabilidade prática no contexto atual.

Outro ponto limitante foi a distribuição temporal irregular das publicações analisadas, o que inviabilizou a realização de uma análise longitudinal mais consistente sobre a evolução das práticas de governança de dados pessoais na saúde pública brasileira desde a promulgação da LGPD. Além disso, a escassez de estudos comparativos entre instituições públicas e a ausência de avaliações formais de impacto — como RIPDs publicados — também limitaram a capacidade de análise sobre a efetividade e maturidade das políticas implementadas.

6.4. Contribuições para a Ciência e Pesquisa

Esta revisão de escopo apresenta uma contribuição original e abrangente ao sistematizar o conhecimento disponível sobre a governança de dados pessoais na saúde pública brasileira, com foco na aplicação da LGPD no SUS. Ao integrar marcos legais, normativos, científicos e institucionais, a análise proporcionou uma visão ampliada e intersetorial do tema, articulando as dimensões jurídica, técnica e administrativa que envolvem a proteção de dados sensíveis no setor público de saúde.

A pesquisa permitiu identificar lacunas relevantes que abrem caminhos promissores para investigações futuras. Entre essas lacunas, destacam-se: (i) a escassez de estudos empíricos avaliando a efetividade das práticas de governança de dados pessoais nos serviços públicos de saúde; (ii) a ausência de métricas padronizadas de conformidade com a LGPD; (iii) a sub exploração de tecnologias aplicadas à anonimização, segurança da informação e auditoria automatizada; e (iv)

a carência de conhecimento dos profissionais da saúde e usuários do SUS em relação à LGPD (Almeida *et al.*, 2020).

As evidências sistematizadas evidenciam que o campo da governança de dados pessoais no setor público de saúde encontra-se em processo de consolidação. Há uma mobilização normativa e institucional em curso, especialmente após a promulgação da LGPD (Brasil, 2018), mas ainda são limitados os avanços concretos na articulação entre diferentes níveis de governo, na estruturação de políticas coordenadas nacionalmente e no financiamento de pesquisas aplicadas que possam guiar práticas efetivas.

A descrição detalhada dos estudos incluídos nesta revisão oferece uma base empírica sólida para o delineamento de recomendações futuras. Além disso, pode auxiliar gestores públicos na estruturação de Programas de Governança em Privacidade, informar o desenho de políticas públicas alinhadas à realidade dos serviços de saúde, e subsidiar pesquisadores interessados na interseção entre saúde, direito e tecnologia. A sistematização aqui apresentada, portanto, contribui não apenas para o avanço da produção científica sobre o tema, mas também para a qualificação do debate público e institucional acerca da proteção de dados pessoais no contexto da saúde coletiva no Brasil.

6.5. Contribuições para a proposta da SES/RS

Os achados desta revisão de escopo oferecem subsídios concretos e estratégicos para a estruturação de um Programa de Governança em Privacidade aplicável à SES/RS. Ao mapear obstáculos, diretrizes e práticas institucionais, a análise permitiu identificar elementos que podem ser diretamente incorporados ao planejamento da política estadual de proteção de dados pessoais sensíveis no contexto do SUS.

Em primeiro lugar, destaca-se a necessidade de institucionalização de estruturas formais de governança, como comitês de privacidade, designação oficial de encarregado de dados, elaboração de RIPD e definição de fluxos padronizados de auditoria e resposta a incidentes. Tais medidas, recorrentes nos documentos analisados (ANPD, 2023; Ministério da Saúde, 2024; PROCERGS, 2022), podem ser adaptadas à realidade organizacional e territorial da SES/RS, considerando suas diferentes unidades e níveis de complexidade.

Além disso, a categorização dos desafios em três eixos estratégicos — pessoas, processos e tecnologias — fornece uma base sólida para a construção de planos de ação específicos. No eixo “pessoas”, recomenda-se a implementação de programas de formação continuada em proteção de dados para os servidores, com especial atenção à atenção primária e aos setores administrativos. No eixo “processos”, revela-se urgente a padronização de fluxos de tratamento de dados e a integração da proteção de dados aos planos de integridade e compliance da Secretaria, além de investimentos em treinamentos e conscientização dos agentes de tratamentos dos dados. No eixo “tecnologias”, devem ser priorizados investimentos em interoperabilidade, anonimização e segurança da informação, preferencialmente baseados nos princípios de *privacy by design* e *by default*.

A análise também evidencia a importância de incorporar o princípio da equidade à governança em privacidade, garantindo que os modelos adotados contemplem a diversidade socioterritorial da população atendida, com atenção às vulnerabilidades étnico-raciais, sociais e regionais. Nesse sentido, recomenda-se que a SES/RS implemente mecanismos de participação popular nas decisões relativas à proteção de dados pessoais.

Por fim, a sistematização apresentada nos Quadros 7 a 10 desta dissertação pode ser utilizada como referência prática para a formulação do Programa. Esses quadros oferecem: (i) conceitos-chave da LGPD adaptáveis à saúde pública; (ii) desafios organizados em eixos estratégicos; (iii) diretrizes extraídas da literatura científica e institucional; e (iv) estruturas e práticas com potencial de incorporação imediata. *raça*

Dessa forma, esta dissertação contribui não apenas com o campo científico, mas com a gestão pública, ao oferecer insumos analíticos e operacionais que poderão fundamentar a elaboração e a implementação de uma política de governança em privacidade sólida, contextualizada e alinhada aos princípios da LGPD no âmbito da SES/RS.

7 CONSIDERAÇÕES FINAIS

Esta revisão de escopo cumpriu o objetivo de sintetizar as evidências disponíveis sobre governança de dados pessoais na saúde pública brasileira, à luz da LGPD, com foco na formulação de uma proposta aplicável à realidade da SES/RS. A análise integrada de 31 documentos, entre artigos científicos, literatura cinzenta, atos normativos e programas institucionais, permitiu mapear conceitos-chave, desafios persistentes e diretrizes operacionais, compondo uma base robusta para o desenvolvimento do Programa de Governança em Privacidade.

Os resultados evidenciam um avanço progressivo na formalização de estruturas de conformidade, como a nomeação de encarregados, elaboração de RIPD e implementação de políticas internas. No contexto da SES/RS, a descrição técnica das bases de dados e a análise normativa estadual forneceram subsídios fundamentais para a construção de uma proposta customizada e juridicamente fundamentada, atendendo aos objetivos específicos do estudo.

Como resultado concreto e aplicável, esta dissertação apresenta o Produto Técnico: uma proposta de Programa de Governança em Privacidade estruturada em diretrizes, planos, inventários e instrumentos operacionais. Essa proposta se alinha às diretrizes da ANPD e responde às necessidades institucionais da SES/RS, oferecendo uma base prática, ética e tecnicamente qualificada para a gestão de dados sensíveis.

Apesar da escassez de estudos empíricos e da heterogeneidade dos enfoques institucionais, os achados reafirmam o papel estratégico da governança de dados na promoção da transparência, segurança jurídica e eficiência administrativa no SUS. Ao mesmo tempo, evidenciam a necessidade de padronização, fortalecimento técnico e criação de mecanismos de avaliação contínua.

Para pesquisas futuras, recomenda-se o aprofundamento de investigações sobre os impactos da LGPD nos diversos níveis de gestão do SUS, o desenvolvimento de métricas de conformidade e a adoção de tecnologias que viabilizem anonimização, interoperabilidade e auditoria automatizada.

Por fim, os resultados desta dissertação não apenas respondem aos objetivos propostos, como também fortalecem a base para a institucionalização de práticas de proteção de dados na SES/RS. O produto técnico desenvolvido — um Programa de Governança em Privacidade aplicável à SES/RS — traduz em diretrizes

operacionais e normativas as evidências sistematizadas, oferecendo uma base sólida, ética e tecnicamente qualificada para a implementação institucional. Este produto representa um avanço estratégico rumo a uma governança sólida, transparente e comprometida com os direitos fundamentais dos titulares.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 25, supl. 1, p. 2487–2492, 2020. DOI: 10.1590/1413-81232020256.1.11792020.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *Reciis – Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, Rio de Janeiro, v. 14, n. 3, p. 692–708, jul./set. 2020. Disponível em: <https://doi.org/10.29397/reciis.v14i3.2012>.

AROMATARIS E, Lockwood C, Porritt K, Pilla B, Jordan Z, editores. *Manual JBI para Síntese de Evidências*. JBI; 2024. Disponível em: <https://synthesismanual.jbi.global> . <https://doi.org/10.46658/JBIMES-24-01>. Acesso em: 23 jun. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia orientativo: tratamento de dados pessoais pelo Poder Público*. Versão 2.0. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 2 ago. 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 ago. 2025.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 2 ago. 2025.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 2 ago. 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 ago. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais – LGPD. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018.

BRASIL. Ministério da Saúde. *Programa de Governança em Privacidade do Ministério da Saúde*. Brasília: Ministério da Saúde, 2022. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/programa_governanca_privacidade.pdf. Acesso em: 2 ago. 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 2 ago. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD sanciona mais um órgão público*. [S.l.], 18 out. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-mais-um-orgao-publico>. Acesso em: 2 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. *Guia de elaboração de Programa de Governança em Privacidade (PPSI)*. Versão 2.3. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos, nov. 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 2 ago. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD*. [S.l.], 1 fev. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd>. Acesso em: 2 ago. 2025.

BRASIL. MINISTÉRIO DA SAÚDE. *Metodologia de Administração de Dados – MAD*. Brasília: Ministério da Saúde, 2024. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2025/06/MAD_240625.pdf. Acesso em: 2 ago. 2025.

BRUN, C. N.; ZUGE, S. S. Revisão sistemática da literatura: desenvolvimento e contribuição para uma prática baseada em evidências na enfermagem. In: LACERDA, M. R.; COSTENARO, R. G. S. (Org.). *Metodologias da pesquisa para a enfermagem e saúde*. Porto Alegre: Moriá, 2015. p. 77–98.

CABELLA, Daniela Monte Serrat; FERREIRA, Raíssa Moura; KAUER, Gisele Shinozaki; KAUER, Manoel Silvino. Afinal de contas: o que é a "Governança em Privacidade" da LGPD? *Migalhas*, São Paulo, 3 jul. 2020. Disponível em: <https://www.migalhas.com.br/depeso/330230/afinal-de-contas--o-que-e-a--governanca-em-privacidade--da-lgpd>. Acesso em: 5 ago. 2025.

CAMARA, Maria Amália Arruda et al. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de

Dados. *Cadernos Ibero-Americanos de Direito Sanitário*, Brasília, v. 10, n. 1, p. 93–112, jan./mar. 2021. Disponível em: <https://doi.org/10.17566/ciads.v10i1.657>.

CARVALHO, Marina Martins de. *et al.* Proteção de Dados Pessoais e Saúde: onde estão os usuários neste debate? In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedroza (org.). *Lei Geral de Proteção de Dados e o controle social da saúde*. Porto Alegre: Rede Unida, 2023. (Série Participação Social e Políticas Públicas, v. 13). Disponível em: <https://doi.org/10.18310/9786554620468>.

CAVALCANTE, Ailton Ferreira; OTA, Kleber da Cunha; OLIVEIRA, Valdivino José de. Governança Digital e Ética Pública: Construindo confiança em um mundo de algoritmos. *Revista Políticas Públicas & Cidades*, [S. l.], v. 13, n. 2, p. e 1445, 2024. DOI: 10.23900/2359-1552v13n2-392-2024. Disponível em: <https://journalppc.com/RPPC/article/view/1445>. Acesso em: 7 ago. 2025.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). *LGPD & Administração Pública: uma análise ampla dos impactos*. São Paulo: Thomson Reuters Brasil, 2020. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/68715532/Artigo_Governanca_de_Dados_e_Programa_de_Compliance_Digital-libre.pdf?1628795447=&response-content-disposition=inline%3B+filename%3DGOVERNANCA_DE_DADOS_E_PROGRAMA_DE_COMPLI.pdf&Expires=1754595972&Signature=gzqgl0mqHht0j4ZYilbeRU2JIS2u8~oukBTtux9IXkDneuacUxG-GXeUpX8HAyzG4yBASrY9cj3KH1OxyghGbKNQDFy4P65hpKtEvu57o~t-vjjBroV7DPndPE34gl~k9v19ZS~r3m05iLJTAU--3Elol1pySQXJbESWfd3R0sLkWEwLtFm1WXus68rYI1iYIf2zte9ky5UZIFW9CBQwngeLKi~Ot4LiFtAj090-3n1iluet5Bi95ppEGsd7eRD3dM5Wwd4aGUOhXigml~ZevmFdrLOLxjGGIRHMIre7fsQG6G1iHVrEFB9t1hV5eCiUyssgwI82cNKdTdWPu-YEA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 7 ago. 2025.

CORTE-REAL, Ana; NUNES, Tiago; CUNHA, Paulo Rupino da. Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology. *International Journal of Environmental Research and Public Health*, v. 21, n. 230, p. 1–19, 2024. Disponível em: <https://doi.org/10.3390/ijerph21020230>.

COSTA, José Augusto Fontoura. Tratamento e transferência de dados de saúde: limites ao compartilhamento de dados sensíveis. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos. *LGPD na Saúde*. Ed. Revista dos Tribunais, 2021. p. 89-102.

DALLARI, Analluza Bolivar. *et al.* Proteção e compartilhamento de dados entre profissionais e estabelecimentos de saúde. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos. *LGPD na Saúde*. Ed. Revista dos Tribunais, 2021. p. 117-138.

DOURADO, Daniel de Araujo; ALTH, Fernando Mussa Abujamra. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. *Revista de Saúde Pública*, 2022; 56:80. Disponível em: <https://doi.org/10.11606/s1518-8787.2022056004461>.

FORNAZIN, Marcelo. Saúde Digital: origens e proposta de governança. In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedroza (org.). *Lei Geral de Proteção de Dados e o controle social da saúde*. Porto Alegre: Rede Unida, 2023. p. 258-277. Disponível em: <https://doi.org/10.18310/9786554620468>.

GUANAES, Paulo Cezar Vieira (Org.). *Marcos legais nacionais em face da abertura de dados para pesquisa em saúde: dados pessoais, sensíveis ou sigilosos e propriedade intelectual*. Rio de Janeiro: Fiocruz, 2018. 123 p. Disponível em: <https://arca.fiocruz.br/handle/iciict/28838>. Acesso em: 2 ago. 2025.

IWAYA, Leonardo Horn et al. Mobile Health Systems for Community-Based Primary Care: Identifying Controls and Mitigating Privacy Threats. *JMIR mHealth and uHealth*, v. 7, n. 3, e11642, 2019. Disponível em: <https://doi.org/10.2196/11642>.

MINGHELLI, Marcelo. *et al.* A autodeterminação informativa como contexto normativo para elaboração de diretrizes para a construção de um Relatório de Impacto à Proteção de Dados Pessoais: a proposta de um modelo humanizador para a telemedicina. *Reciis – Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, Rio de Janeiro, v. 17, n. 4, p. 938-961, out./dez. 2023. Disponível em: <https://doi.org/10.29397/reciis.v17iAhead-of-Print.3602>.

NINA, da Hora. Privacidade, Ética e Transparência de Dados na Saúde. In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedroza (org.). *Lei Geral de Proteção de Dados e o controle social da saúde*. Porto Alegre: Rede Unida, 2023. (Série Participação Social e Políticas Públicas, v. 13). Disponível em: <https://doi.org/10.18310/9786554620468>.

OLIVEIRA, Thais Lucena de. et al. LGPD e Saúde Pública: A rede nacional de dados em saúde e a proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos. *LGPD na Saúde*. Ed. Revista dos Tribunais, 2021. p. 159-169.

PETERS, Brainard Guy. O que é Governança?. *Revista do TCU*, Brasília, n. 127, p. 28–33, 2013. Disponível em: <https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/87>. Acesso em: 3 ago. 2025.

PINTO, Hêider Aurélio; SANTANA, José Santos Souza; CHIORO, Arthur. Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais. *Revista Saúde em Redes*, v. 8, n. 2, p. 361–371, 2022. Disponível em: <https://doi.org/10.18310/2446-4813.2022v8n2p361-371>.

PROCERGS. *Lei Geral de Proteção de Dados: Cartilha PROCERGS. v. 1.0*. Porto Alegre: PROCERGS, 2022. Disponível em: <https://www.procergs.rs.gov.br/upload/arquivos/202301/12065932-cartilha-lgpd-proce-rgs.pdf>. Acesso em: 2 ago. 2025.

PROCERGS. *Cartilha de Condutas voltadas à Privacidade e à Proteção de Dados. v. 1.0*. Porto Alegre: PROCERGS, 2022. Disponível em:

<https://www.procergs.rs.gov.br/upload/arquivos/202301/12065930-cartilha-condutas-procergs-1.pdf>. Acesso em: 2 ago. 2025.

RAMOS, Edith Maria Barbosa *et al.* Questões éticas e perspectiva jurídica da proteção de dados. *Cadernos Ibero-Americanos de Direito Sanitário*, Brasília, v. 10, n. 3, p. 172–190, jul./set. 2021. DOI: 10.17566/ciads.v10i3.796.

REDE NACIONAL DE DADOS EM SAÚDE (RNDS). *Estratégia de Saúde Digital para o Brasil 2020–2028*. Ministério da Saúde, 2020. Disponível em https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 6 ago. 2025.

RIO GRANDE DO SUL. Secretaria da Saúde. *Portaria nº 740, de 2015*. Regulamenta o uso das Tecnologias da Informação no âmbito da Secretaria Estadual de Saúde do Rio Grande do Sul. Porto Alegre: SES/RS, 2015. Disponível em <https://saude.rs.gov.br/upload/arquivos/carga20170441/13054154-1448286590-740-dgti.pdf>. Acesso em: 2 ago. 2025.

RIO GRANDE DO SUL. Secretaria da Saúde. *Portaria nº 728, de 2018*. Regulamenta o Plano de Segurança da Informação (PSI/SES). Porto Alegre: SES/RS, 2018. Disponível em <https://saude.rs.gov.br/upload/arquivos/carga20180825/03162500-728.pdf>. Acesso em: 2 ago. 2025.

RIO GRANDE DO SUL. *Decreto nº 55.647, de 14 de dezembro de 2020*. Regulamenta os procedimentos gerais, os prazos e as fases para implementação da Lei Federal no 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Poder Executivo do Estado do Rio Grande do Sul. Diário Oficial do Estado do Rio Grande do Sul, nº 256, de 16 de dezembro de 2020.

RIO GRANDE DO SUL. *Decreto nº 55.986, de 07 de julho de 2021*. Altera o Decreto no 55.647, de 14 de dezembro de 2020, que regulamenta os procedimentos gerais, os prazos e as fases para implementação da Lei Federal no 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Poder Executivo do Estado do Rio Grande do Sul. Diário Oficial do Estado do Rio Grande do Sul, nº 137, de 8 de julho de 2021.

RIO GRANDE DO SUL. Procuradoria-Geral do Estado. *Programa de Governança em Privacidade – PGP/PGE-RS*. Porto Alegre: PGE-RS, dez. 2021. Disponível em: <https://www.pge.rs.gov.br/upload/arquivos/202112/29083040-pgp-pge.pdf>. Acesso em: 2 ago. 2025.

RIO GRANDE DO SUL. *Decreto nº 55.987, de 07 de julho de 2021*. Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual, em conformidade com a Lei Federal no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD. Diário Oficial do Estado do Rio Grande do Sul, nº 137, de 8 de julho de 2021.

RIO GRANDE DO SUL. *Decreto nº 56.106, de 24 de setembro de 2021*. Institui a Política de Tecnologia da Informação e Comunicação. Diário Oficial do Estado do Rio Grande do Sul, nº 193, de 27 de setembro de 2021.

RIO GRANDE DO SUL. *Decreto nº 56.528, de 25 de maio de 2022*. Dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública Estadual. Diário Oficial do Estado do Rio Grande do Sul, nº 100, de 26 de maio de 2022.

RIO GRANDE DO SUL. Secretaria da Saúde. *Nota Técnica nº 1/2022 – Comitê Gestor da Política de Pesquisa*. Orientações sobre o uso de dados da Secretaria de Estado da Saúde do RS. Diário Oficial do Estado do Rio Grande do Sul, nº 199, de 18 de outubro de 2022.

RIO GRANDE DO SUL. Secretaria de Planejamento, Governança e Gestão. *PTIC Nº 01/2022*. Disponível em: <https://planejamento.rs.gov.br/upload/arquivos/202301/09103253-ptic-01-2022-classificacao-e-qualidade-de-dados-site.pdf>. Acesso em: 2 ago. 2025.

RIVELLI, Fábio. Aplicação e conformidade dos dados sensíveis na saúde digital e os preceitos da LGPD. In: AITH, Fernando; DALLARI, Analluza. *LGPD na Saúde Digital*. Ed. Revista dos Tribunais, 2022. p. 183-197.

TIETZMANN, Ana Cristina et al. Privacidade e confidencialidade das informações clínicas em saúde mental: velhos desafios em um novo contexto. *Revista Brasileira de Psicoterapia*, Porto Alegre, v. 23, n. 3, p. 165–175, 2021. Disponível em: <https://doi.org/10.5935/2318-0404.20210050>.

TRICCO, Andrea C. et al. PRISMA *Extension for Scoping Reviews* (PRISMA-ScR): *Checklist and Explanation*. *Annals of Internal Medicine*, [s. l.], v. 169, n. 7, p. 467–473, 2 out. 2018. DOI: 10.7326/M18-0850.

UNIÃO EUROPEIA. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, p. 1-88, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 8 ago. 2025.

VALE, Luís Manoel Borges do; OLIVEIRA, Rafael Carvalho Rezende. *LGPD na administração pública*. Ed. Forense, 2025.

VENTURA, Miriam; COELI, Cláudia Medina. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. *Cadernos de Saúde Pública*, v. 34, n. 7, 2018. Disponível em: <https://doi.org/10.1590/0102-311X00106818>.

YIN, Robert K. *Pesquisa qualitativa do início ao fim*. Disponível em: Minha Biblioteca – Escola GHC, Grupo A, 2016.

ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis. La Llei General de Protecció de Dades i les seves implicacions per a la salut: Avaluacions d'Impacte sobre el tractament de dades en el context clínic i hospitalari. *Revista de Bioética y Derecho*, n. 54, p. 215–232, 2022. Disponível em: <https://doi.org/10.1344/rbd2021.54.36005>.

ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis. O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados. *Reciis – Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, Rio de Janeiro, v. 17, n. 3, p. 729-740, jul./set. 2023. Disponível em: <https://doi.org/10.29397/reciis.v17i3.3689>.

APÊNDICE A - PRODUTO TÉCNICO - PROPOSTA DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE PARA A SES/RS

SECRETARIA ESTADUAL DA SAÚDE DO RIO GRANDE DO SUL (SES/RS) PROGRAMA DE GOVERNANÇA EM PRIVACIDADE (PGP)

Versão 1.0 | Agosto de 2025

1. APRESENTAÇÃO

A transformação digital e a intensificação do uso de dados pessoais nos serviços públicos de saúde impõem desafios crescentes à gestão da informação e à proteção da privacidade dos cidadãos. Nesse contexto, a Lei nº 13.709, de 14 de agosto de 2018 — conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) — estabelece princípios, direitos e deveres que demandam respostas estruturadas por parte das instituições públicas. A legislação orienta a formulação de políticas e diretrizes voltadas à governança dos dados pessoais, tanto em meios físicos quanto digitais, tratados por pessoas naturais ou jurídicas, de direito público ou privado.

A LGPD foi criada com o objetivo de garantir a privacidade, a segurança da informação e os direitos fundamentais dos titulares, estabelecendo regras claras sobre a coleta, armazenamento, processamento e compartilhamento de dados pessoais. A lei também reforça a necessidade de transparência, responsabilização e prestação de contas por parte dos agentes de tratamento.

Diante dessa realidade, este documento propõe um conjunto de diretrizes técnicas voltadas à estruturação do Programa de Governança em Privacidade (PGP) da Secretaria Estadual da Saúde do Rio Grande do Sul (SES/RS). Trata-se de um instrumento normativo, estratégico e operacional, destinado a apoiar gestores, equipes técnicas e demais responsáveis pelo tratamento de dados na adoção de práticas alinhadas à LGPD, respeitando as especificidades organizacionais e federativas da SES/RS.

As diretrizes aqui apresentadas visam articular conformidade legal e efetividade institucional, por meio da definição de etapas de implementação, atribuições claras, recursos mínimos necessários e indicadores sugeridos de monitoramento. O objetivo central é consolidar uma cultura organizacional baseada

na ética, na segurança e na transparência no uso dos dados pessoais no setor público da saúde.

Neste sentido, em consonância com o §2º do artigo 50 da LGPD, apresentam-se as diretrizes preliminares para o PGP da SES/RS, alinhadas aos Decretos Estaduais nº 55.647/2020, nº 55.986/2021, nº 55.987/2021 e demais normativas correlatas aplicáveis ao contexto estadual.

2. OBJETIVOS

O presente documento tem por objetivo orientar e subsidiar a SES/RS na implementação estruturada de ações voltadas à proteção de dados pessoais e à promoção da privacidade, em conformidade com os requisitos da LGPD (Lei nº 13.709/2018), especialmente no que se refere ao disposto no art. 50, inciso I.

São objetivos específicos do PGP:

- **Orientar** a implementação de mecanismos de proteção de dados pessoais e sensíveis no âmbito da SES/RS, com base nos princípios, direitos e deveres estabelecidos pela LGPD;
 - **Garantir** a integridade, a confidencialidade e a disponibilidade dos dados pessoais tratados pela instituição, assegurando o respeito aos direitos dos titulares;
 - **Estabelecer** diretrizes de governança e condutas éticas para o uso de dados pessoais em atividades de saúde pública, pesquisa, gestão e planejamento;
 - **Promover** a transparência, a segurança e a qualidade das informações, incentivando boas práticas na coleta, no tratamento e no compartilhamento de dados;
 - **Estimular** a consolidação de uma cultura organizacional comprometida com a privacidade, a proteção de dados e a responsabilização institucional;
 - **Assegurar** a observância dos princípios da **finalidade, necessidade, minimização, segurança, responsabilização e prestação de contas**, conforme definidos pela LGPD.
-

3. ABRANGÊNCIA

O PGP da SES/RS aplica-se a todos os dados pessoais e dados pessoais sensíveis coletados, armazenados, compartilhados, processados ou tratados por qualquer meio físico ou digital no âmbito da SES/RS, abrangendo:

- Dados de usuários do Sistema Único de Saúde (SUS);
- Dados de servidores públicos, colaboradores, profissionais terceirizados e estagiários vinculados à SES/RS;
- Dados tratados por meio dos sistemas e bases de dados institucionais, conforme listagem apresentada no Anexo I;
- Dados utilizados para fins de pesquisa, planejamento, gestão, avaliação, auditoria, regulação ou formulação de políticas públicas de saúde.

A abrangência deste programa se estende a todas as unidades administrativas, assistenciais, técnicas e estratégicas da SES/RS, independentemente da área finalística, garantindo a aplicação transversal das diretrizes de privacidade e proteção de dados em toda a estrutura institucional.

4. JUSTIFICATIVA

A crescente digitalização dos serviços de saúde e o tratamento massivo de dados pessoais pela SES/RS exigem diretrizes claras e estruturadas para garantir conformidade com a LGPD. A ausência de normativas internas específicas, aliada à diversidade de bases de dados e fluxos informacionais, amplia os riscos de uso inadequado, vazamentos e responsabilizações legais.

A criação deste PGP visa preencher essa lacuna, promovendo práticas padronizadas, seguras e transparentes, alinhadas aos princípios legais e às demandas operacionais da Secretaria. Trata-se de um instrumento estratégico para qualificar a gestão dos dados pessoais tratados no âmbito da SES/RS, com foco em proteção, responsabilidade e eficiência.

5. FUNDAMENTOS NORMATIVOS

Este PGP está fundamentado em dispositivos legais e normativos que orientam o tratamento de dados pessoais no setor público, em especial no âmbito da SES/RS. As principais normas e instrumentos considerados são:

- **Lei nº 13.709/2018 – LGPD:** Estabelece os princípios, direitos e obrigações referentes ao tratamento de dados pessoais por pessoas naturais ou jurídicas, de direito público ou privado;
- **Decreto Estadual nº 55.647/2020:** Regulamenta, no âmbito do Poder Executivo do RS, os procedimentos gerais, os prazos e as fases para implementação da LGPD;
- **Decreto Estadual nº 55.986/2021:** Altera dispositivos do Decreto nº 55.647/2020, adequando prazos e procedimentos;
- **Decreto Estadual nº 55.987/2021:** Institui a Política Estadual de Proteção de Dados Pessoais no Poder Executivo do RS, conforme a LGPD;
- **Decreto Estadual nº 56.106/2021:** Institui a Política de Tecnologia da Informação e Comunicação no Estado;
- **Decreto Estadual nº 56.528/2022:** Dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública estadual;
- **Padrão Técnico (PTIC) 01/2022:** Define procedimentos para classificação e qualidade dos dados;
- **Portaria SES/RS nº 740/2015:** Regulamenta o uso das Tecnologias da Informação no âmbito da SES/RS;
- **Portaria SES/RS nº 728/2018:** Regulamenta o Plano de Segurança da Informação – PSI/SES;
- **Nota Técnica SES/RS nº 01/2022:** Orienta sobre o uso de dados da SES/RS para fins de pesquisa científica.

Esses fundamentos asseguram a conformidade jurídica e técnica do programa, proporcionando respaldo normativo às diretrizes propostas para a proteção e o uso ético de dados pessoais no contexto da saúde pública.

6. DIRETRIZES OPERACIONAIS

A seguir, apresentam-se as diretrizes operacionais recomendadas para a estruturação do PGP no âmbito da SES/RS. Essas diretrizes devem ser incorporadas progressivamente pelas áreas gestoras e técnicas, conforme suas atribuições, capacidades e prioridades institucionais:

- Mapeamento e registro das atividades de tratamento - Realizar o inventário contínuo de todas as operações de tratamento de dados pessoais realizadas pela SES/RS, conforme disposto no art. 37 da LGPD;
 - Catálogo e classificação de dados - Classificar os dados tratados conforme critérios de sensibilidade, criticidade e finalidade, utilizando como base o Padrão Técnico PTIC 01/2022;
 - Plano de resposta a incidentes de segurança - Estruturar um protocolo institucional para detecção, resposta, comunicação e remediação de incidentes de segurança envolvendo dados pessoais;
 - Procedimentos para atendimento dos direitos dos titulares - Estabelecer fluxos internos para atender às solicitações dos titulares de dados (acesso, correção, exclusão, oposição, portabilidade, entre outros), com prazos e responsabilidades definidos;
 - Critérios de minimização, conservação e descarte de dados - Aplicar o princípio da minimização na coleta e uso de dados, estabelecer políticas claras de retenção e descarte, observando prazos legais e finalidades específicas;
 - Avaliação de riscos e relatórios de impacto à privacidade (PIA) - Implantar processos periódicos de avaliação de riscos e elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, especialmente para atividades de alto risco;
 - Políticas de anonimização e pseudoanonimização - Adotar técnicas de anonimização ou pseudoanonimização dos dados pessoais sempre que possível, especialmente para fins de pesquisa, análise e compartilhamento de informações;
 - Gestão de consentimento quando aplicável - Criar mecanismos de obtenção, registro e gestão do consentimento do titular, quando este for a base legal aplicável ao tratamento, garantindo clareza e possibilidade de revogação.
-

7. ETAPAS DA IMPLANTAÇÃO DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A implementação do PGP da SES/RS está organizada em três fases sequenciais — **preparatória**, **executiva** e de **operação contínua** — adaptadas a partir do modelo da Procuradoria-Geral do Estado (PGE/RS). Cada fase contempla ações estratégicas e operacionais necessárias à conformidade com a LGPD, conforme descrito a seguir:

Etapas preparatórias	i. Designação de um Encarregado pelo Tratamento de Dados Pessoais e a definição de uma estrutura organizacional para coordenação das atividades; ii. Consolidação do Inventário de Processos Organizacionais; iii. Elaboração do Inventário de Dados Pessoais; iv. Consolidação do Inventário de Convênios e Ajustes; v. Consolidação do Inventário de Ativos de Informação;
Etapas de execução	vi. Elaboração de uma Política de Privacidade para a instituição; vii. Inclusão de Avisos de Privacidade, nos termos dispostos pela Política de Privacidade; viii. Adequação dos contratos, convênios e ajustes cujo objeto impacte sobre questões afetas à proteção da privacidade e segurança da informação; ix. Elaboração de um Plano de Conscientização e Treinamento em Privacidade e Segurança da Informação; x. Elaboração de um Plano de Resposta a Incidentes;
Operação	xi. Elaboração do Relatório de Impacto de Proteção de Dados; xii. Monitoramento e aperfeiçoamento.

Fonte: Programa de Governança em Privacidade – PGP/PGE-RS (2021)

8. ETAPAS PREPARATÓRIAS

As etapas preparatórias do PGP da SES/RS visam consolidar a estrutura institucional necessária para o cumprimento da LGPD, garantindo alinhamento estratégico, técnico e normativo desde o início da implementação.

8.1 ESTRUTURA DE GOVERNANÇA

8.1.1 Comitê Gestor do PGP/SES-RS:

Será instituído um Comitê Gestor do PGP no âmbito da SES/RS, como instância colegiada responsável pela articulação, deliberação e acompanhamento

das ações do programa. O comitê será composto por representantes das seguintes unidades:

- Gabinete do Secretário;
- Procuradoria Setorial da PGE/RS junto à SES/RS;
- Diretoria de Tecnologia da Informação;
- Diretoria de Planejamento e Pesquisa;
- Diretoria de Gestão e Desenvolvimento de Pessoas;
- Representantes de Departamentos técnicos e assistenciais;
- Representantes do Comitê de Ética em Pesquisa

Sugere-se a definição de reuniões periódicas e a criação de um canal institucional para comunicação e deliberação.

8.1.2 Encarregado pelo Tratamento de Dados Pessoais:

O Encarregado será nomeado conforme o Decreto Estadual nº 55.647/2020 e exercerá suas atribuições nos termos do art. 41 da LGPD, com independência funcional, autonomia técnica e suporte administrativo adequados.

Atribuições principais:

- Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e dos titulares, adotando as providências cabíveis.;
- Esclarecer dúvidas e orientar sobre os direitos dos titulares e as obrigações da instituição, promovendo ações corretivas quando necessário;
- Atuar como referência técnica junto a servidores, colaboradores, terceirizados e parceiros, disseminando boas práticas de proteção de dados;
- Coordenar, com apoio do Grupo de Trabalho Estadual, o mapeamento dos fluxos de tratamento de dados pessoais, incluindo os compartilhamentos internos e externos;
- Sugerir e propor adequações nos processos organizacionais com base na LGPD, garantindo conformidade legal e mitigação de riscos;
- Cumprir as demais funções determinadas pelo controlador institucional ou definidas por normas complementares

Os dados de contato do Encarregado são públicos e estão disponíveis em:
<https://saude.rs.gov.br/lgpd>

8.1.3 Facilitadores de Dados:

Nos termos do Decreto Estadual nº 56.528/2022, os Facilitadores de Dados são agentes públicos formalmente indicados por seus órgãos ou entidades, com atribuições específicas relacionadas ao tratamento de dados, atuando como referência técnica para subsidiar a tomada de decisão, a execução e a melhoria de processos administrativos e políticas públicas. Devem possuir domínio sobre as bases de dados sob sua gestão, bem como conhecimento das respectivas regras de negócio. Sua designação se dará por meio de portaria, conforme previsto no PTIC nº 01/2022 e no referido decreto.

8.1.4 Grupos de Trabalho Temáticos (GTs):

Poderão ser constituídos Grupos de Trabalho Temáticos (GTs), de caráter técnico-consultivo, para apoiar a implementação do Programa de Governança em áreas específicas como:

- qualidade de dados;
- anonimização e pseudoanonimização;
- segurança da informação;
- interoperabilidade de sistemas;
- entre outras temáticas estratégicas relacionadas à proteção de dados pessoais.

8.2 INVENTÁRIO DE PROCESSOS ORGANIZACIONAIS

O inventário de processos organizacionais corresponde à documentação resultante da catalogação e mapeamento das atividades realizadas pelos diferentes órgãos e unidades que compõem a estrutura da SES/RS. Seu principal objetivo é viabilizar o controle sistemático das operações de tratamento de dados, constituindo uma etapa essencial na consolidação da governança em privacidade.

Esse instrumento proporciona uma visão integrada das operações institucionais e permite identificar riscos, gargalos, interdependências e pontos críticos que possam comprometer a conformidade com a LGPD.

No contexto da SES/RS, o inventário permitirá compreender com precisão como os dados pessoais e sensíveis circulam entre setores, unidades e sistemas. Essa compreensão subsidia o desenvolvimento de medidas de segurança, a definição de políticas de acesso e a elaboração de planos de resposta a incidentes. Trata-se, portanto, de uma ferramenta estratégica para ampliar a transparência, a eficiência e a *accountability* no tratamento de dados pessoais.

8.3 INVENTÁRIO DE DADOS PESSOAIS

O Inventário de Dados Pessoais corresponde ao mapeamento completo do ciclo de vida dos dados pessoais tratados pela SES/RS. É composto pelos registros das atividades de tratamento de dados realizadas pela instituição, incluindo as seguintes informações: tipos de dados pessoais tratados, ativos de informação envolvidos e demais atributos necessários à avaliação de risco e conformidade com a legislação vigente.

Devem constar nesse inventário, quando aplicável: a classificação dos dados, informações que subsidiem a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), e dados sobre eventuais compartilhamentos.

A coordenação do Inventário ficará sob responsabilidade do Encarregado pelo Tratamento de Dados Pessoais. A atualização será realizada pelos responsáveis diretos por cada processo organizacional inventariado, a quem caberá comunicar quaisquer alterações ocorridas.

O modelo de Inventário de Dados Pessoais adotado pela SES/RS seguirá o padrão estabelecido pela Procuradoria-Geral do Estado do Rio Grande do Sul (PGE/RS).

8.4 INVENTÁRIO DE CONTRATOS, CONVÊNIOS E AJUSTES COM TERCEIROS

Os contratos, convênios e ajustes celebrados com terceiros deverão observar as minutas-padrão definidas pela PGE/RS, conforme disposto no art. 1º, § 1º, do Decreto Estadual nº 55.717, de 12 de janeiro de 2021.

Nos casos em que se fizer necessária a alteração das minutas-padrão, a proposta será submetida à apreciação do Procurador-Geral do Estado, respeitando-se, quando aplicável, as disposições do referido Decreto, que

regulamenta os modelos-padrão de editais de licitações, contratos e outros instrumentos administrativos no âmbito da Administração Pública Estadual.

Para os instrumentos jurídicos elaborados com modelo próprio da SES/RS, deverão constar cláusulas específicas referentes às responsabilidades decorrentes da LGPD. Nesses casos, a redação será definida mediante consulta à Procuradoria Setorial da PGE/RS junto à SES/RS, garantindo adequação legal e segurança jurídica no tratamento de dados pessoais.

8.5 INVENTÁRIO DE ATIVOS DE INFORMAÇÃO

O Inventário de Ativos de Informação corresponde ao levantamento sistemático e à catalogação dos sistemas e demais ativos tecnológicos utilizados na execução dos processos organizacionais da SES/RS. Esse inventário deverá conter, de forma detalhada, as bases que armazenam dados pessoais, as medidas de segurança aplicadas, os responsáveis pela gestão das informações e os perfis com acesso autorizado.

Trata-se de um instrumento fundamental para a implementação da governança e da segurança da informação, pois oferece uma visão integrada sobre a infraestrutura tecnológica disponível, permitindo a identificação de vulnerabilidades e a tomada de decisões estratégicas em conformidade com a LGPD.

Atualmente, com base no mapeamento mais recente, a SES/RS possui 37 sistemas catalogados, incluindo aqueles alimentados, acessados e/ou geridos internamente, os quais tratam dados pessoais sensíveis de usuários do SUS e de colaboradores da Secretaria. A lista completa desses sistemas encontra-se no Anexo I deste documento.

9. ETAPAS DE EXECUÇÃO

As etapas de execução do PGP da SES/RS têm como objetivo viabilizar a aplicação prática e contínua dos instrumentos de governança em privacidade e proteção de dados. Buscam assegurar a efetividade das diretrizes estabelecidas, promovendo a transparência, a responsabilização institucional e a conformidade com a LGPD no cotidiano das operações da Secretaria.

9.1 ELABORAÇÃO DE POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS (PPPD-SES/RS)

A Política de Privacidade e Proteção de Dados (PPPD-SES/RS) será um documento orientador, voltado ao público interno da SES, e terá como objetivo estabelecer diretrizes claras sobre a conduta esperada no tratamento de dados pessoais.

Conforme o art. 50 da Lei nº 13.709/2018 (LGPD), a PPPD servirá como referência institucional para garantir que todas as atividades de coleta, uso, armazenamento, compartilhamento e descarte de dados pessoais estejam em conformidade com a legislação vigente. O documento também sistematizará princípios, processos e responsabilidades relacionados à proteção da privacidade dos titulares de dados.

Além disso, a PPPD definirá, com maior detalhamento, a arquitetura operacional e os fluxos internos necessários para a aplicação dos instrumentos previstos neste Programa de Governança, sem prejuízo de atualizações que venham a ser determinadas por normativas futuras.

A elaboração da PPPD-SES/RS será coordenada pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio de grupo de trabalho interdisciplinar a ser instituído por ato da Secretária de Estado da Saúde.

9.2 AVISO DE PRIVACIDADE

O Aviso de Privacidade tem por finalidade informar, de maneira clara e acessível, os titulares de dados sobre a existência de coleta e tratamento de suas informações pessoais pela SES/RS, nos diferentes contextos institucionais. Esse documento representa um instrumento essencial de transparência e *accountability*, reforçando o compromisso da instituição com a proteção dos dados e o respeito aos direitos dos titulares. A estrutura, os conteúdos e a forma de disponibilização do Aviso de Privacidade serão definidos na PPPD-SES/RS.

9.3 ADEQUAÇÃO DOS INVENTÁRIO DE CONTRATOS, CONVÊNIOS E AJUSTES COM TERCEIROS

Conforme detalhado no item 8.4 deste Programa, os instrumentos celebrados com terceiros deverão seguir os modelos estabelecidos pela PGE/RS, contemplando

cláusulas específicas de proteção de dados pessoais e alinhamento à LGPD, com suporte da Procuradoria Setorial da SES/RS.

9.4 PLANO DE CONSCIENTIZAÇÃO E TREINAMENTO

Será desenvolvido um Plano de Conscientização e Treinamento em Privacidade e Segurança da Informação, com calendário periódico de capacitações sobre temas como segurança da informação, direito à privacidade, gestão de riscos e tratamento adequado de dados pessoais. Campanhas de treinamento e comunicação devem informar leis e políticas aplicáveis e as consequências por violá-las, identificar possíveis violações, explicar como abordar reclamações e incluir procedimentos de denúncia.

As ações educativas incluirão cursos presenciais, boletins, e-mails institucionais, treinamentos on-line e informativos no portal da SES/RS, podendo ser conduzidas por profissionais internos ou externos. O Programa de Saúde do Servidor (PROSER) poderá atuar como parceiro na promoção de uma cultura de privacidade entre os colaboradores.

9.5 PLANO DE RESPOSTA A INCIDENTES

A SES/RS instituirá um Plano de Resposta a Incidentes (PRI) para garantir o cumprimento do art. 48 da LGPD, com foco na mitigação de danos e na comunicação adequada à ANPD e aos titulares afetados. O PRI deverá contemplar:

- Fluxograma de resposta a incidentes envolvendo dados pessoais;
- Procedimentos para comunicação à ANPD e aos titulares;
- Medidas operacionais para contenção e diagnóstico do incidente, incluindo eventual bloqueio ou restrição de acesso a sistemas.

O plano será elaborado pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio da Diretoria de Tecnologia da Informação (DGTI), e deverá prever responsabilidades, fluxos decisórios e mecanismos de resposta em conformidade com a legislação vigente.

10. OPERAÇÃO

A fase de operação do PGP da SES/RS compreende a execução contínua e sistemática das medidas definidas nas etapas anteriores, com foco no

monitoramento, na avaliação e no aprimoramento das práticas de proteção de dados pessoais. Trata-se do momento em que os instrumentos regulatórios, como políticas internas, inventários, planos e diretrizes operacionais, passam a ser efetivamente aplicados no cotidiano institucional. Essa fase exige integração entre setores, definição clara de responsabilidades, atualização periódica das informações mapeadas e constante vigilância quanto a riscos emergentes, assegurando a conformidade com a LGPD e a efetividade da governança em privacidade.

10.1 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Nos termos do art. 38 da Lei nº 13.709/2018 (LGPD), o RIPD é um instrumento técnico elaborado pelo controlador que documenta os processos de tratamento de dados pessoais que possam representar riscos relevantes aos direitos fundamentais e às liberdades civis dos titulares.

No âmbito da SES/RS, o RIPD será elaborado nas seguintes situações:

- Por solicitação expressa da ANPD; ou
- De ofício, sempre que a análise integrada dos Inventários de Processos Organizacionais, de Dados Pessoais e de Ativos de Informação indicar a existência de atividades de tratamento com potencial de alto risco à privacidade dos titulares.

O conteúdo mínimo do RIPD abrangerá:

- i. A descrição dos tipos de dados pessoais coletados e tratados;
- ii. A metodologia utilizada para a coleta, o tratamento e a segurança das informações;
- iii. A análise crítica das medidas técnicas e organizacionais adotadas para mitigação dos riscos identificados;
- iv. Outras informações exigidas por normativas complementares ou diretrizes expedidas pela ANPD.

A elaboração do RIPD caberá ao Encarregado pelo Tratamento de Dados Pessoais, com apoio técnico dos setores responsáveis pelos processos mapeados, devendo seguir modelo institucional definido pela PGE/RS.

10.2. MONITORAMENTO E APERFEIÇOAMENTO

O monitoramento do Programa de Governança em Privacidade da SES/RS será implementado após a consolidação das etapas iniciais de estruturação e execução. Tem como finalidade mensurar o grau de conformidade institucional com a LGPD, garantir a efetividade das ações adotadas e promover o aprimoramento contínuo dos instrumentos de governança, com base em evidências e resultados práticos.

Esse monitoramento será orientado por dois marcos principais: Indicadores de Performance definidos pelo Programa; Plano de Resposta a Incidentes de Privacidade e Segurança, que permitirá a avaliação de falhas, tempos de resposta e melhorias aplicadas.

Indicadores para monitoramento inicialmente sugeridos:

- Relatórios anuais de governança e conformidade;
- Indicadores de qualidade e segurança dos dados;
- Revisão periódica das políticas e dos procedimentos, incluindo atualização periódica dos inventários elaborados nas etapas preparatórias;
- Auditorias internas e externas;
- Capacitação continuada de servidores e gestores.

11. OUTRAS CONDUTAS APLICÁVEIS À SES/RS

11.1 DAS CONDUTAS A SEREM OBSERVADAS QUANDO DO COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

Com base nas disposições legais estaduais, em especial o Decreto Estadual nº 56.528/2022, bem como, Guia Orientativo “Tratamento de Dados pelo Poder Público” da ANPD², as condutas a serem observadas quando do compartilhamentos de dados entre os órgãos da Administração Pública são os seguintes:

- Formalização e registro:
 - Apontamento dos facilitadores de dados;

² Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_el-eitoral.pdf/view

- Delimitação do conjunto de dados objeto do compartilhamento, com limitação ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III da LGPD);
 - Informação quanto à conclusão da catalogação dos dados que se pretende sejam compartilhados, conforme Padrão de Tecnologia da Informação e Comunicação (PTIC 01/2022);
 - Autorização expressa da Secretária da Saúde no que respeita ao compartilhamento dos dados proposto;
 - Indicação dos mecanismos tecnológicos que permitirão o compartilhamento dos dados
- Indicação do objeto do compartilhamento e da finalidade;
 - Indicação da Base legal aplicável ao compartilhamento;
 - Indicação da duração do tratamento, esclarecendo, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento.
 - Transparência e direitos dos titulares com definição expressa das formas de atendimento ao princípio da transparência (art. 6º, VI e art. 23, I da LGPD) e garantia dos direitos dos titulares dos dados.
 - Prevenção e segurança: estabelecimento das medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII, e 46, da LGPD).

11.2 DAS CONDUTAS A SEREM OBSERVADAS QUANDO DO COMPARTILHAMENTO DE DADOS PARA USO EM PESQUISAS

O compartilhamento de dados da SES/RS para uso em pesquisas observará as disposições constantes na Nota Técnica SES/RS nº 01/2022, que esclarece e orienta gestores, servidores da SES/RS e pesquisadores da comunidade sobre o acesso e uso de dados da SES/RS para pesquisas científicas conforme a LGPD.

Projetos de pesquisa que utilizam dados e/ou informações da SES/RS deverão exclusivamente e obrigatoriamente ser inseridos no sistema informatizado no Portal da Pesquisa na SES - POPE/SES.

11.3 ATENDIMENTO A DEMANDAS DE TITULARES

Conforme dispõe o Decreto 55.647/2020, cada órgão e entidade da administração pública estadual designou um encarregado próprio para tratar da proteção de dados pessoais no âmbito de suas competências. Não obstante, o Estado do Rio Grande do Sul é o controlador único dos dados (Decreto 55.987/2021), e, nesta qualidade, responde perante os titulares e a ANPD.

Tal circunstância impõe o desafio de estruturar um sistema transversal de atendimento às demandas dos titulares, capaz de abranger todos os órgãos e entidades do Poder Executivo do Estado do Rio Grande do Sul. A contratação desse serviço transversal está em andamento, a cargo da Secretaria de Planejamento, Governança e Gestão Estratégica. Enquanto não houver implementação de um sistema transversal de atendimento, devidamente validado pelas instâncias competentes, demandas dos titulares serão recebidas via ouvidoria, ou por e-mail encaminhado ao Encarregado pelo Tratamento de Dados Pessoais, no endereço eletrônico divulgado no site oficial da SES/RS.

12. SUGESTÕES DE ADEQUAÇÕES PARA MELHORIA NA PROTEÇÃO DA PRIVACIDADE E SEGURANÇA

12.1 PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO – *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*

Privacidade desde a Concepção - ***privacy by design*** - significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e perdurar por todo o ciclo de tratamentos dos dados pessoais.

Privacidade por Padrão - ***privacy by default*** - garante que as configurações mais favoráveis à privacidade sejam aplicadas automaticamente, minimizando a coleta e o processamento de dados por padrão.

Sobre esta temática, cabe referir três pilares: (i) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (ii) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente, e (iii) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos.

Exemplos de medidas técnicas e organizacionais:

- Uso de criptografia para proteção de bases de dados e meios de comunicação.
- Anonimização e pseudoanonimização de bases de dados.
- Controle de acesso baseado em funções.
- Mecanismo de respostas a requisições e reclamações dos titulares de dados.
- Plano de respostas a incidentes e remediação de segurança e privacidade.
- Segurança física.
- Políticas de privacidade para aquisição de produtos/serviços.
- Políticas de gerenciamento da segurança da informação.
- Política de retenção e eliminação de dados pessoais.

12.2 MEDIDAS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sugestões de medidas de segurança a serem adotadas pela SES/RS:

- Regras de firewall de redes para filtro de pacotes e bloqueio de portas de acesso.
- Firewall de aplicação web para proteção contra ataques como falsificação de solicitações entre sites, cross-site-scripting (XSS), inclusão de arquivos e SQL Injection.
- Software de proteção antivírus e antimalware para servidores.
- Rotinas de proteção de dados.
- Segurança das comunicações, com a utilização de protocolos de comunicação seguros – como TLS/HTTPS – e aplicativos com criptografia fim a fim.
- Processo de Gerenciamento de Vulnerabilidade, no qual as atividades são gerenciadas em três ciclos: detecção, remediação e monitoramento. Cada atividade é composta por uma lista de ações a serem realizadas.
- Processo de Gestão de Continuidade do Negócio que identifica ameaças potenciais para a organização e os possíveis impactos nas operações de negócio, fornecendo uma estrutura capaz de responder efetivamente e salvaguardar os interesses da organização.
- Processo de Gestão de Acessos que busca garantir o uso de serviços a usuários autorizados e, ao mesmo tempo, prevenir que usuários não autorizados tenham acesso a esses serviços. Além disso, as concessões deverão ser aplicadas respeitando o princípio de privilégios mínimos e apenas

pela duração de tempo necessário. O processo é implementado para decidir quem deverá ter direitos de acesso sobre os ativos de TI.

- Contrato de acordo de nível de serviço (Service Level Agreement – SLA) para os serviços de nuvem, que contemplem a segurança dos dados armazenados e o uso de autenticação com múltiplos fatores, para acesso aos serviços e dados pessoais que estão na nuvem.
- Processo de resposta e remediação a incidentes de segurança.
- Processo de Conscientização e Treinamento de segurança da informação para todos os colaboradores da Secretaria.

13. DISPOSIÇÕES FINAIS

Este PGP da SES/RS constitui instrumento orientador das ações voltadas à conformidade com a LGPD e à promoção de uma cultura organizacional comprometida com a proteção de dados pessoais. A sua aplicação será progressiva e adaptativa, sendo complementada por planos, portarias, manuais, guias operacionais e outros instrumentos normativos ou orientativos, elaborados conforme a evolução da maturidade da governança de dados no âmbito da Secretaria.

A atualização deste Programa ocorrerá de forma periódica, considerando:

- As avaliações de desempenho e os indicadores de monitoramento;
- As diretrizes da ANPD;
- As políticas públicas estaduais aplicáveis;
- A dinâmica institucional e os avanços regulatórios.

A efetiva implementação e manutenção do Programa dependerão do compromisso contínuo da alta gestão, dos servidores e dos parceiros institucionais, sendo responsabilidade compartilhada a garantia da conformidade, da ética no uso dos dados e da transparência perante a sociedade.

14. ANEXOS

ANEXO I: Glossário de termos em proteção de dados pessoais

- **Dado pessoal:** informação relacionada à pessoa natural identificada ou identificável;

- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos ou biométricos;
- **Dado pessoal sensível de saúde:** dado relativo à saúde de um titular de dados ou à atenção à saúde a ele prestada que revele informações sobre sua saúde física ou mental no presente, passado ou futuro;
- **Titular:** pessoa natural a quem se referem os dados pessoais;
- **Controlador:** órgão da administração responsável pelas decisões referentes ao tratamento de dados;
- **Operador:** pessoa natural ou jurídica que realiza o tratamento em nome do controlador;
- **Encarregado:** pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.
- **ANPD:** Autoridade Nacional de Proteção de Dados.
- **Facilitador de Dados:** agentes públicos autorizados e indicados por seus respectivos órgãos ou entidades como recursos humanos que tenham em suas atribuições às finalidades de trabalhar com o tratamento de dados, para o suporte à tomada de decisão, execução ou melhoria de atividades administrativas e de políticas públicas, que sejam conhecedores das bases de dados geridas por seus respectivos órgãos ou entidades e de suas regras de negócio.
- **Privacy by design** - privacidade e a proteção de dados devem ser consideradas desde a concepção e perdurar por todo o ciclo de tratamentos dos dados pessoais.
- **Privacy by default** - garante que as configurações mais favoráveis à privacidade sejam aplicadas automaticamente, minimizando a coleta e o processamento de dados por padrão.
- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- **Incidente de segurança:** qualquer evento que comprometa a segurança dos dados pessoais, resultando em acesso não autorizado, perda, alteração, destruição ou tratamento inadequado ou ilícito.
- **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;
- **Pseudoanonimização:** tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
- **Inventário de Dados Pessoais:** mapeamento do ciclo de vida de todos os dados pessoais tratados pela SES/RS.

ANEXO II – Cronograma de Implementação do PGP/SES-RS

Fase	Atividades	Responsável	Início Previsto	Término Previsto
Planejamento e Institucionalização	Criação do Comitê Gestor e designação de Encarregado e Facilitadores	Gabinete da SES/RS	01/10/2025	31/10/2025
Diagnóstico e Mapeamento	Inventário de sistemas e fluxos de dados pessoais e sensíveis	Encarregado de Dados e Departamentos	01/11/2025	30/11/2025
Classificação e Qualidade de Dados	Classificação de bases segundo o PTIC 01/2022 e definição de padrões mínimos de qualidade	Facilitadores de Dados	01/12/2025	31/01/2026
Elaboração de Instrumentos	Criação de políticas internas, planos de resposta a incidentes e modelos de PIA	Encarregado de Dados e GT	01/02/2026	28/02/2026
Capacitação Institucional	Treinamento de servidores e gestores sobre proteção de dados e LGPD	Escola de Saúde Pública	01/03/2026	31/03/2026
Monitoramento e Revisão	Avaliação contínua, indicadores, auditorias e revisão das práticas	Comitê Gestor / Encarregado	01/04/2026	Permanente

ANEXO III: Lista de base de dados que tratam dados pessoais e sensíveis**BASES - TRATAM DIRETA OU INDIRETAMENTE DE DADOS PESSOAIS E PESSOAIS SENSÍVEIS, SEJA DE USUÁRIOS DO SUS OU DE COLABORADORES**

- FPE
- Sistema de Monitoramento Estratégico - SGE
- DIGISUS - Instrumentos de planejamento do MS
- SAIPS - Sistema de Apoio à Implementação de Políticas em Saúde - Captação de recursos
- Gestão do Site da SES
- Redes sociais da secretaria (Instagram, Twitter, Youtube e etc)
- PROA
- RHE - Recursos Humanos do Estados
- RHS - Recursos Humanos da SES
- SISAB - Produção da Atenção Básica
- SIM - Sistema de Informação de Mortalidade
- SINASC - Sistema de Informação de Nascidos Vivos
- SisPIM - Sistema da Primeira Infância Melhor
- SIGAH - Sistema de Gestão da Atenção Hospitalar (Contratos, pagamentos)
- SIH - Sistema de Informações Hospitalares
- SIA - Sistema de Informações Ambulatoriais
- SISMAC - Sistema de Controle de Limite Financeiro da Média e Alta Complexidade
- AME - Administração de Medicamentos
- Sistema de Gestão Acadêmica
- POPERS - Portal de Pesquisas na SES - Comitê Gestor da Política de Pesquisas na SES
- Gestão da Biblioteca - Pergamum
- SINAN - Sistema de Informação de Agravos de Notificação
- SIVEP Gripe - Sistema de notificação de SRAG e SG
- Esus Notifica - Notificação COVID-19
- SIPNI - Sistema de Informação do Programa Nacional de Imunizações
- GAL - Gestão de Laboratórios (LACEN)
- SIST - Sistema de Informação da Saúde do Trabalhador (notificações e investigações)
- SIVISA - Sistema de Informação da Vigilância Sanitária
- VGS - Gestão de Doadores de sangue
- Ouvidor SUS
- LAI - Sistema de recebimento de demandas da Lei de Acesso à Informação
- GERINT - Gestão da Regulação de Internações
- GERCON - Gestão da Regulação de Consultas
- GERPAC - Gestão da Regulação de procedimentos de Alto Custo
- SAPH - Gestão de Atendimento Móvel de Urgência e Emergência - SAMU
- Sistema Nacional de Transplantes (SNT) - Central de Transplantes
- Hemovida

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia orientativo: tratamento de dados pessoais pelo Poder Público*. Versão 2.0. Brasília: ANPD, 2023.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Senado Federal, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018.

BRASIL. Ministério da Saúde. *Programa de Governança em Privacidade do Ministério da Saúde*. Brasília: Ministério da Saúde, 2022.

PROCERGS. Lei Geral de Proteção de Dados: Cartilha PROCERGS. v. 1.0. Porto Alegre: PROCERGS, 2022.

PROCERGS. Cartilha de Condutas voltadas à Privacidade e à Proteção de Dados. v. 1.0. Porto Alegre: PROCERGS, 2022.

RIO GRANDE DO SUL. Secretaria da Saúde. Portaria nº 740, de 2015. Regulamenta o uso das Tecnologias da Informação no âmbito da Secretaria Estadual de Saúde do Rio Grande do Sul. Porto Alegre: SES/RS, 2015.

RIO GRANDE DO SUL. Secretaria da Saúde. Portaria nº 728, de 2018. Regulamenta o Plano de Segurança da Informação (PSI/SES). Porto Alegre: SES/RS, 2018.

RIO GRANDE DO SUL. Decreto nº 55.647, de 14 de dezembro de 2020. Regulamenta os procedimentos gerais, os prazos e as fases para implementação da Lei Federal no 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Poder Executivo do Estado do Rio Grande do Sul. Diário Oficial do Estado do Rio Grande do Sul, nº 256, de 16 de dezembro de 2020.

RIO GRANDE DO SUL. Decreto nº 55.986, de 07 de julho de 2021. Altera o Decreto no 55.647, de 14 de dezembro de 2020, que regulamenta os procedimentos gerais, os prazos e as fases para implementação da Lei Federal no 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Poder Executivo do Estado do Rio Grande do Sul. Diário Oficial do Estado do Rio Grande do Sul, nº 137, de 8 de julho de 2021.

RIO GRANDE DO SUL. Decreto nº 55.987, de 07 de julho de 2021. Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual, em conformidade com a Lei Federal no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD. Diário Oficial do Estado do Rio Grande do Sul, nº 137, de 8 de julho de 2021.

RIO GRANDE DO SUL. Decreto nº 56.106, de 24 de setembro de 2021. Institui a Política de Tecnologia da Informação e Comunicação. Diário Oficial do Estado do Rio Grande do Sul, nº 193, de 27 de setembro de 2021.

RIO GRANDE DO SUL. Procuradoria-Geral do Estado. *Programa de Governança em Privacidade – PGP/PGE-RS*. Porto Alegre: PGE-RS, dez. 2021.

RIO GRANDE DO SUL. Decreto nº 56.528, de 25 de maio de 2022. Dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública Estadual. Diário Oficial do Estado do Rio Grande do Sul, nº 100, de 26 de maio de 2022.

RIO GRANDE DO SUL. Secretaria da Saúde. Nota Técnica nº 1/2022 – Comitê Gestor da Política de Pesquisa. Orientações sobre o uso de dados da Secretaria de Estado da Saúde do RS. Diário Oficial do Estado do Rio Grande do Sul, nº 199, de 18 de outubro de 2022.

RIO GRANDE DO SUL. Secretaria de Planejamento, Governança e Gestão. PTIC Nº 01/2022.

APÊNDICE B – SINTAXE DE BUSCA NAS BASES DE DADOS

B.1 - Estratégias de Busca Utilizadas nas Bases de Dados e Fontes Institucionais

B.1.1 Bases de Dados:

PUBMED

(public health[mh] OR public health[tiab] OR health systems[tiab] OR health information systems[tiab] OR SUS[tiab] OR Sistema Único de Saúde[tiab] OR Brazilian public health[tiab])

AND

(data governance[tiab] OR information governance[tiab] OR data stewardship[tiab] OR data responsibility[tiab] OR data strategy[tiab] OR data protection[tiab] OR data privacy[tiab] OR data security[tiab] OR data ethics[tiab] OR LGPD[tiab] OR Lei Geral de Proteção de Dados[tiab] OR knowledge governance[tiab] OR information policy[tiab] OR health information governance[tiab] OR health data protection[tiab] OR governance in privacy[tiab] OR health information security[tiab] OR General Personal Data Protection Law[tiab] OR Brazilian Data Protection Law[tiab] OR National Data Protection Authority[tiab] OR data-driven governance[tiab])

AND

(Brazil[mh] OR Brazil*[tiab] OR Brasil*[tiab])

AND

(2018:2025[pdat])

BVS (completa da BVS) - <https://bvssalud.org/>

(mh:(H02.403.720 OR N01.400.550 OR N06.850 OR SP1.852.900) OR tw:("public health" OR "public health" OR "Saúde Pública" OR "Salud Pública" OR "health systems" OR "Sistemas de Saúde" OR "Sistemas de Salud" OR "health information systems" OR "Sistemas de Informação em Saúde" OR "Sistemas de Información en Salud" OR SUS OR "Sistema Único de Saúde" OR "Brazilian public health"))

AND

(mh:(L01.224.134 OR N04.452.910.200) OR tw:("data governance" OR "governança de dados" OR "gobernanza de datos" OR "information governance" OR "governança da informação" OR "gobernanza de la información" OR "data stewardship" OR "administração de dados" OR "administración de datos" OR "data responsibility" OR "responsabilidade de dados" OR "responsabilidad de datos" OR "data strategy" OR "Estratégia de Dados" OR "estrategia de datos" OR "data protection" OR "proteção de dados" OR "protección de datos" OR "data privacy" OR "privacidade de dados" OR "privacidad de datos" OR "data security" OR "segurança de dados" OR "seguridad de datos" OR "Segurança Computacional" OR "Seguridad Computacional" OR "data ethics" OR "ética de dados" OR "ética de los datos" OR "knowledge governance" OR "governança do conhecimento" OR "gobernanza del conocimiento" OR "information policy" OR "política informacional" OR "política de información" OR "health information governance" OR "governança de dados em saude" OR "gobernanza de la información sanitaria" OR "health data protection" OR

"proteção de dados de saude" OR "proteção de dados em saude" OR "protección de datos de salud" OR "governance in privacy" OR "governança em privacidade" OR "gobernanza en la privacidad" OR "health information security" OR "segurança de dados em saude" OR "seguridad de la información de salud" OR "General Personal Data Protection Law" OR "LGPD" OR "Lei Geral de Proteção de Dados" OR "Ley General de Protección de Datos Personales" OR "Brazilian Data Protection Law" OR "Ley Brasileña de Protección de Datos" OR "National Data Protection Authority" OR "Autoridade Nacional de Proteção de Dados" OR "Autoridad Nacional de Protección de Datos" OR "data-driven governance" OR "governança baseada em dados" OR "gobernanza basada en datos"))

AND

(mh:(Z01.107.757.176) OR tw:(brazil* OR Brasil*))

AND

year_cluster:[2018 TO 2025]

LILACS (coleção completa da BVS) - <https://lilacs.bvsalud.org/>

(mh:(h02.403.720 OR n01.400.550 OR n06.850 OR sp1.852.900) OR tw:("public health" OR "public health" OR "Saúde Pública" OR "Salud Pública" OR "health systems" OR "Sistemas de Saúde" OR "Sistemas de Salud" OR "health information systems" OR "Sistemas de Informação em Saúde" OR "Sistemas de Información en Salud" OR sus OR "Sistema Único de Saúde" OR "Brazilian public health"))

AND

(mh:(l01.224.134 OR n04.452.910.200) OR tw:("data governance" OR "governança de dados" OR "gobernanza de datos" OR "information governance" OR "governança da informação" OR "gobernanza de la información" OR "data stewardship" OR "administração de dados" OR "administración de datos" OR "data responsibility" OR "responsabilidade de dados" OR "responsabilidad de datos" OR "data strategy" OR "Estratégia de Dados" OR "estrategia de datos" OR "data protection" OR "proteção de dados" OR "protección de datos" OR "data privacy" OR "privacidade de dados" OR "privacidad de datos" OR "data security" OR "segurança de dados" OR "seguridad de datos" OR "Segurança Computacional" OR "Seguridad Computacional" OR "data ethics" OR "ética de dados" OR "ética de los datos" OR "knowledge governance" OR "governança do conhecimento" OR "gobernanza del conocimiento" OR "information policy" OR "política informacional" OR "política de información" OR "health information governance" OR "governança de dados em saude" OR "gobernanza de la información sanitaria" OR "health data protection" OR "proteção de dados de saude" OR "proteção de dados em saude" OR "protección de datos de salud" OR "governance in privacy" OR "governança em privacidade" OR "gobernanza en la privacidad" OR "health information security" OR "segurança de dados em saude" OR "seguridad de la información de salud" OR "General Personal Data Protection Law" OR "LGPD" OR "Lei Geral de Proteção de Dados" OR "Ley General de Protección de Datos Personales" OR "Brazilian Data Protection Law" OR "Ley Brasileña de Protección de Datos" OR "National Data Protection Authority" OR "Autoridade Nacional de Proteção de Dados" OR "Autoridad Nacional de Protección de Datos" OR "data-driven governance" OR "governança baseada em dados" OR "gobernanza basada en datos"))

AND

(mh:(z01.107.757.176) OR tw:(brazil* OR brasil*))

AND

year_cluster:[2018 TO 2025]
 AND
 db:("LILACS")
 AND instance:"regional"

SciELO - <https://search.scielo.org/>

("public health" OR "public health" OR "Saúde Pública" OR "Salud Pública" OR "health systems" OR "Sistemas de Saúde" OR "Sistemas de Salud" OR "health information systems" OR "Sistemas de Informação em Saúde" OR "Sistemas de Información en Salud" OR sus OR "Sistema Único de Saúde" OR "Brazilian public health")

AND

("data governance" OR "governança de dados" OR "gobernanza de datos" OR "information governance" OR "governança da informação" OR "gobernanza de la información" OR "data stewardship" OR "administração de dados" OR "administración de datos" OR "data responsibility" OR "responsabilidade de dados" OR "responsabilidad de datos" OR "data strategy" OR "Estratégia de Dados" OR "estrategia de datos" OR "data protection" OR "proteção de dados" OR "protección de datos" OR "data privacy" OR "privacidade de dados" OR "privacidad de datos" OR "data security" OR "segurança de dados" OR "seguridad de datos" OR "Segurança Computacional" OR "Seguridad Computacional" OR "data ethics" OR "ética de dados" OR "ética de los datos" OR "knowledge governance" OR "governança do conhecimento" OR "gobernanza del conocimiento" OR "information policy" OR "política informacional" OR "política de información" OR "health information governance" OR "governança de dados em saude" OR "gobernanza de la información sanitaria" OR "health data protection" OR "proteção de dados de saude" OR "proteção de dados em saude" OR "protección de datos de salud" OR "governance in privacy" OR "governança em privacidade" OR "gobernanza en la privacidad" OR "health information security" OR "segurança de dados em saude" OR "seguridad de la información de salud" OR "General Personal Data Protection Law" OR "LGPD" OR "Lei Geral de Proteção de Dados" OR "Ley General de Protección de Datos Personales" OR "Brazilian Data Protection Law" OR "Ley Brasileña de Protección de Datos" OR "National Data Protection Authority" OR "Autoridade Nacional de Proteção de Dados" OR "Autoridad Nacional de Protección de Datos" OR "data-driven governance" OR "governança baseada em dados" OR "gobernanza basada en datos")

AND

(brazil* OR brasil*)

AND

(publication_year:2018/2025)

B.1.2 Repositórios Institucionais

ANPD: <https://www.gov.br/anpd/pt-br>

Pesquisa feita no campo geral de busca com os seguintes termos: "saúde" / "governança".

Também analisados os documentos constantes no repositório de "Centrais de Conteúdo" disponível no site (<https://www.gov.br/anpd/pt-br/centrais-de-conteudo>). Da busca foi selecionado 1 achado - Guia orientativo Tratamento de dados pessoais pelo Poder Público - disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>

DATASUS: <https://datasus.saude.gov.br/>

Da análise dos documentos disponíveis no site, foi selecionado o seguinte material: Metodologia de Administração de Dados MAD - disponível em https://datasus.saude.gov.br/wp-content/uploads/2025/06/MAD_240625.pdf

Fiocruz - ARCA - Repositório Institucional da Fiocruz:
<https://arca.fiocruz.br/home>

("governança de dados" OR "proteção de dados") AND "saude publica" AND "LGPD"

PGE / RS

"lgpd"

- Programa de Governança em Privacidade disponível em <https://www.pge.rs.gov.br/upload/arquivos/202112/29083040-pgp-pge.pdf>

PROCERGS

"lgpd"

- Cartilha LGPD Procergs disponível em <https://www.procergs.rs.gov.br/upload/arquivos/202301/12065932-cartilha-lgpd-procergs.pdf>

- CARTILHA_CONDUTAS_PROCERGS disponível em <https://www.procergs.rs.gov.br/upload/arquivos/202301/12065930-cartilha-condutas-procergs-1.pdf>

B.1.3 Programas de governança para nortear o desenvolvimento do produto

MS -

https://bvsms.saude.gov.br/bvs/publicacoes/programa_governanca_privacidade.pdf

PGE RS -

<https://www.pge.rs.gov.br/upload/arquivos/202112/29083040-pgp-pge.pdf>

B.1.4 Legislação

Busca sistemática no site do Governo do RS e da Assembleia Legislativa do RS, utilizando palavras-chave como "LGPD", "governança de dados", "dados pessoais", "informação em saúde" e "compartilhamento de dados".

APÊNDICE C - ÍTEGRA DAS PLANILHA DE EXTRAÇÃO DE DADOS

C.1 Artigos Científicos

(Disponível em: <https://drive.google.com/file/d/1K4IUvJP0v2XNuXQjtlD0mGqK-kK1AcBv/view?usp=sharing>)

ID	Título do Artigo	Autores	Ano	Tipo de Estudo	População / Contexto	Objetivo Principal	Contribuições para a Governança de Dados	Desafios identificados	Propostas ou Soluções	Limitações do Estudo	Base de Dados de Origem	Inclusão / Exclusão (com justificativa)	Notas Adicionais
1	A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais	Daniel de Araujo Dourado, Fernando Mussa Abujamra Aith	2022	Comentário / ensaio	Sistema de saúde brasileiro	Discutir a abrangência do direito à explicação e à revisão de decisões automatizadas na regulação da IA na saúde no Brasil a partir do marco da LGPD, considerando o debate internacional sobre o tema os limites atualmente existentes para a explicação e a necessidade de estruturas regulatórias.	Enfatiza o direito à explicação (A importância do direito à explicação é dar aos pacientes a possibilidade de compreender a lógica de decisões automatizadas que impactem condutas tomadas nos seus cuidados de saúde.) e a necessidade de estruturas regulatórias.	Direito à explicação na saúde: contemplar complexidades específicas da regulação da IA para uso clínico. Os obstáculos para desenvolver uma IA explicável na saúde devem ser reconhecidos e bem ponderados na construção de mecanismos regulatórios que considerem os limites da explicabilidade e consequentemente a abrangência do direito à explicação e à revisão de decisões automatizadas na assistência à saúde.	Além da atuação da ANPD, deve haver intervenção de outros órgãos reguladores, como a Agência Nacional de Vigilância Sanitária e das autoridades reguladoras de profissões regulamentadas, como os conselhos de medicina.	Teórico sem dados empíricos.	Revista de Saúde Pública	Incluso – relevante para a LGPD na saúde.	DOI: 10.11606/s1518-8787.2022056004461
2	La Lei General de Protección de Datos y sus implicaciones para la salud	Margareth Vettes Zaganelli, Douglas Luis Binda Filho	2022	Estudo exploratório	Contexto clínico-hospitalar	Abordar os aspectos gerais da LGPD e uma perspectiva comparada em relação à GDPR. Apresentar associação entre o tratamento de dados sensíveis e a confidencialidade na assistência em saúde.	Propõe maior cuidado com dados sensíveis na saúde. Apresenta reflexão relativa aos conceitos de confidencialidade, enquanto um dever ético e profissional; e à privacidade enquanto uma criação da legislação moderna. Conclui acerca da importância da realização da Avaliação de Impacto em dados sensíveis. Conceitos: A confidencialidade é principalmente um dever ético e profissional (muitas vezes imposto pela legislação), enquanto a privacidade é uma criação da legislação moderna. Em um ambiente médico, a confidencialidade é imposta ao médico em uma relação terapêutica médico-paciente e o dever de confidencialidade antecede em cerca de 2.200 anos a noção de privacidade. Essa engloba direitos para controlar informações sobre si mesmo e o direito de excluir outros de acesso às.	(1) O acesso descontrolado e o uso indevido dos dados de saúde. (2) Estabelecer melhores estratégias para a gestão, mantendo critérios de segurança da informação, como confidencialidade, integridade e disponibilidade. (3) Desproporcionalidade - LGPD apresenta alto custo de conformidade, o que beneficia grandes empresas e afasta pequenas e médias empresas; (4) LGPD - Falta de menção à necessidade de formalização de vínculo entre operador e controlador; não são explicitados os casos em que relatórios de impacto são necessários; não há prazos detalhados no que se refere à comunicação em casos de incidente de segurança que possa acarretar risco ou dano aos titulares dos dados; não há menção expressa a respeito do que seria "melhor interesse" no que se refere ao tratamento dos dados de menores; não há um prazo definido no que se refere à notificação do risco de vazamento de dados à autoridade; não há definição do que constitui nível "razoável" de proteção para dados pessoais, o que entrega aos reguladores flexibilidade significativa na avaliação de muitas por violações de dados e/ou não conformidade.	Recomenda-se que a instituição implemente um Sistema de Gestão de Segurança da Informação (SGSI), sistema organizacional que visa à proteção dos dados dentro dos critérios de confidencialidade, integridade e disponibilidade da organização.	Teórico sem dados empíricos.	Revista de Bioética y Derecho	Incluso – trata diretamente da LGPD na saúde.	DOI: 10.13144/rbd2021.54.36005
3	Privacidade e confidencialidade das informações clínicas em saúde mental: novos desafios em um novo contexto	Ana Cristina Tietzmann, Jane Iandora Herlinger, Márcia Santana Fernandes, José Roberto Goldim	2021	Revisão narrativa	Pacientes e profissionais de saúde mental	Abordar questões relativas ao sigilo, segredo, privacidade e confidencialidade; o compartilhamento de informações entre profissionais por meio de aplicativos ou redes sociais; e o compartilhamento de imagens.	Aponta os desafios da confidencialidade na saúde digital sob a luz da LGPD. Reflexão sobre bioética. Conceitos: Apenas conceitos de privacidade e confidencialidade.	Apesar dos novos contextos e tecnologias, os direitos, deveres éticos e valores envolvidos na relação terapêutica devem continuar a ser respeitados. São aspectos que compõem a reflexão bioética, devendo levar em consideração as particularidades de cada caso, o respeito às pessoas e à sua vulnerabilidade, o respeito à autonomia dos pacientes e ao seu melhor benefício, bem como todos os cuidados relativos à segurança das diferentes informações. Essa reflexão precisa estar presente no dia a dia dos profissionais de saúde mental.	(1) O compartilhamento de imagens deve merecer especial resguardo, visando não expor o paciente e outras pessoas incluídas nestes arquivos. Todas as fotos compartilhadas devem ter sido autorizadas previamente pelos seus titulares, sejam pacientes e/ou outros profissionais. (2) Enfatizar importância da privacidade dos dados pessoais e a necessidade de treinamento profissional a fim de evitar má prática.	Revisão narrativa sem dados empíricos.	Revista Brasileira do Psicoterapia	Incluso – diretamente alinhado com a LGPD na saúde.	DOI: 10.5935/2318-0404.20210050
4	Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology	Ana Cortie Real, Tiago Nunes, Paulo Rupino da Cunha	2024	Estudo analítico	Sistemas de saúde globais	Realizar análise abrangente, considerando as propriedades da tecnologia blockchain (BT) na saúde digital, abordando considerações legais, de privacidade e regulatórias.	Propõe soluções normativas para uso de blockchain na governança de dados. Conceitos: O conceito fundamental da tecnologia blockchain será discutido – registros de dados descentralizados que melhoram o compartilhamento e a interoperabilidade no acesso à informação, promovendo uma melhor comunicação entre as partes interessadas e reduzindo as disparidades de informação em linha com a imutabilidade e a integridade dos dados.	(1) A imutabilidade do blockchain pode entrar em conflito com a exigência do GDPR, PIPEDA e LGPD de excluir dados pessoais mediante retificação. (2) No contexto do blockchain, onde múltiplos participantes contribuem e validam dados, determinar a base legal para o processamento e obter o consentimento apropriado de todas as partes envolvidas pode ser um desafio, o que se reflete na governança de dados. (3) Uma estrutura de governança eficaz inclui o estabelecimento de políticas, diretrizes e protocolos para acesso, armazenamento e compartilhamento de dados, bem como mecanismos para resolução de disputas, aplicação de conformidade e gerenciamento de atualizações e aprimoramentos do sistema. Este processo de monitoramento de rede pode implementar controles de acesso e mecanismos de permissão, seguindo diferentes níveis de acesso por nós com base em suas funções e responsabilidades. Isso garante que entidades autorizadas com as permissões necessárias possam acessar dados pessoais. A proteção ou os padrões regulatórios devem ser garantidos. (4) Existem conflitos entre as diretrizes regulatórias e as características do blockchain, ressaltando a necessidade de discussões e colaborações contínuas entre especialistas jurídicos e técnicos. Soluções potenciais, incluindo revisões regulatórias e estruturas de governança, precisam ser exploradas para abordar preocupações relacionadas à conformidade com as leis e direitos humanos. Um design de sistema criterioso é necessário para equilibrar os direitos de privacidade, os requisitos de proteção de dados e as características únicas da tecnologia blockchain.	(1) Prioridade - segurança, a confiabilidade e a proteção da integridade dos dados. Além disso, deve capacitar os indivíduos na gestão de seus dados. (2) No contexto da saúde, os provedores de saúde podem acessar e contribuir para a blockchain com segurança, utilizando chaves criptográficas. Isso facilita o estabelecimento de um histórico médico transparente, auditável, confiável e à prova de adulteração, além da possibilidade de conceder ou revogar o acesso seletivo às informações de saúde. A BT também pode ser usada para atribuir identidades digitais seguras e portáteis, principalmente a indivíduos sem documentos oficiais. (3) A auditabilidade interna e externa deve ser destacada, garantindo transparência e controle das transações ou prestação de contas. O cumprimento regular dos padrões de qualidade está sujeito a auditorias para identificar vulnerabilidades e garantir medidas de qualidade adequadas. Contratos inteligentes, um recurso exclusivo da tecnologia blockchain, e tokens não fungíveis (NFTs) oferecem recursos avançados para o estabelecimento de mecanismos de conformidade e processos de auditoria. Contratos inteligentes, autoexecutáveis e à prova de violação, podem registrar e aplicar de forma autônoma permissões de acesso, modificações de dados e histórico de transações na rede blockchain. Tokens não fungíveis, ao representarem ativos digitais únicos, fornecem um meio de verificar e autenticar as identidades dos usuários e suas ações correspondentes no sistema. Juntas, essas ferramentas fornecem uma estrutura abrangente para rastrear e verificar de forma transparente o acesso, as modificações e as transações de dados, reforçando assim a responsabilidade e garantindo o estrito cumprimento dos padrões legais e éticos, incluindo aqueles relacionados aos direitos humanos.	Teórico sem dados empíricos.	International Journal of Environmental Research and Public Health	Incluso – relevante para governança de dados em saúde.	DOI: 10.3390/ijerph21020230

5	Mobile Health Systems for Community Based Primary Care: Identifying Controls and Mitigating Privacy Threats	Leonardo H. Iwaya, Simone Fischer Hübner, Rose Mharie Ahlfeldt, Leonardo A. Marlucci	2019	Estudo de caso com PIA	Agentes comunitários de saúde e pacientes do SUS	Apresentar uma Avaliação de Impacto à Privacidade (PIA) para MDSCs (Sistemas de Coleta de Dados mHealth - aplicativos de saúde móvel), fornecendo uma identificação e avaliação sistemáticas de potenciais riscos à privacidade, enfatizando particularmente controles e estratégias de mitigação para lidar com impactos negativos à privacidade.	Aponta falhas e recomendações práticas para proteger dados sensíveis, como por exemplo controles para gerenciar consentimento, transparência, intervenibilidade e minimização de dados.	(1) Embora tenha havido pesquisas significativas que abordam questões de segurança de dados, a atenção à privacidade em suas múltiplas dimensões ainda é escassa para os MDSCs em geral. Novos sistemas têm a oportunidade de incorporar privacidade e proteção de dados desde o projeto. Os sistemas existentes terão que abordar suas questões de privacidade para cumprir com as novas e futuras regulamentações de proteção de dados. No entanto, pesquisas adicionais ainda são necessárias para identificar soluções viáveis e econômicas. (2) Os principais desafios de privacidade para os MDSCs incluem os seguintes: (2.1) acesso individualizado a dados pessoais para fornecer transparência e intervenibilidade, (2.2) obter e tratar o consentimento informado explícito dos titulares dos dados e permitir a retirada do consentimento, (2.3) definir medidas para se opor ao processamento e permitir o bloqueio ou exclusão de dados, (2.4) empregar mecanismos de segurança e (2.5) utilizar técnicas apropriadas de anonimização para o compartilhamento de dados. (3) Resolver questões de privacidade e proteção de dados é fundamental para a implantação bem sucedida de tais sistemas. (4) Princípios importantes de privacidade poderiam ser aprimorados, como minimização de dados, obtenção de consentimento, transparência no processamento de dados e intervenibilidade. Para ser justo, as pesquisas existentes podem não considerar principalmente a privacidade, visto que recursos de preservação da privacidade são considerados requisitos não funcionais ou mesmo porque tais considerações estão além do escopo de muitos artigos. No entanto, os sistemas já implantados, especialmente na área da saúde, devem estar em conformidade com os princípios de privacidade desde a concepção.	(1) Abordagem mista de procedimentos técnicos e organizacionais que deveriam ser implementados para garantir a privacidade e a proteção de dados. (2) Integrar os procedimentos organizacionais relacionados à privacidade em um sistema de gestão de segurança da informação. (3) Estabelecer manuais para lidar com vulnerabilidades e ataques desconhecidos. (4) Estabelecer revisão contínua dos processos e procedimentos estabelecidos.	Estudo de caso único com aplicação limitada. Escrito quanto a LGPD ainda era um projeto de lei.	JMIR MHealth and UHealth	Incluso – aborda diretamente proteção de dados no SUS.	DOI: 10.2196/11642
6	Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança	Miriam Ventura, Cláudia Medina Coeli	2018	Comentário teórico-reflexivo	Saúde pública brasileira	Analisar a privacidade e dados pessoais entre o público e o privado; bem como, a questão atinente à privacidade e governança de acesso a dados.	Propõe superação de dicotomias público/privado e defende governança voltada ao bem comum. Apresenta o modelo de governança de dados como uma alternativa que assegura o equilíbrio entre a preservação do direito à privacidade e os ganhos potenciais do uso dos dados na avaliação e pesquisa populacional. Conceitos: A governança entendida como meio que a sociedade busca coletivamente assegurar as condições para alcançar determinado objetivo acontece principalmente, mas não exclusivamente, no domínio governamental.	(1) Dificuldades identificadas: conceitual, em torno da noção de público e privado, para definir bens e interesses objeto da regulamentação; outra relacionada à operacionalização desses conceitos na formulação de um modelo normativo de regulamentação e de governança em relação aos dados pessoais, que abrange, inclusive, a cessão de dados e seu tratamento. (2) Essa dinâmica ressignificação do direito à privacidade e à informação na saúde requer uma regulamentação e governança que articule virtuosamente proteção da privacidade e promoção do acesso à informação em compasso com as referidas necessidades coletivas e as possibilidades tecnológicas disponíveis. (3) Crescimento do volume e da variedade de dados que podem ser combinados, aumentando o risco de reidentificação mesmo após a anonimização ou desidentificação de bases isoladas. (4) A Saúde Pública conta com larga experiência na produção de informações a partir de dados pessoais e sensíveis, mas o setor conta com uma regulamentação sobre o tema ainda limitada, fragmentada e instável.	(1) Population Data BC (PopData), que representa um modelo inovador para o acesso, tratamento e uso de bases de dados populacionais de interesse para a pesquisa em saúde. O centro funciona como um terceiro confiável que faz a mediação entre pesquisadores e gestores das bases de dados da província de British Columbia (Canadá), cabendo a esses últimos a aprovação final de cada requisição para o uso dos dados sob sua custódia. (2) Pesquisadoras do PopData vêm sugerindo a adoção de um modelo de governança de dados que busca adequar os princípios legais de privacidade a uma avaliação de riscos das demandas de acesso às bases de dados populacionais proporcional ao nível de risco envolvido na solicitação de acesso.	Teórico sem dados empíricos.	Cadernos de Saúde Pública	Incluso – aborda governança e proteção de dados na saúde pública.	DOI: 10.1590/0102-311X00106818
7	Capítulo 3 – Privacidade, ética e transparência de dados na saúde Capítulo 7 – Onde estão os usuários neste debate?	Nina da Hora; Mariana Martins de Carvalho et al.	2023	Ensaio teórico e análise crítica	Usuários do SUS e sociedade civil organizada	Capítulo 3 - Analisar a privacidade e a ética enquanto conceitos fundamentais para a cidadania; Capítulo 7 - Contribuir para a compreensão das práticas de proteção de dados no ecossistema de digitalização dos serviços de saúde e fortalecer a cultura de proteção de dados pessoais, tendo como referência a LGPD.	Reflete sobre o papel da cidadania e dos conselhos de saúde na construção de políticas de governança de dados. Aponta ausência dos usuários no debate como um dos problemas existentes para a consolidação do direito aos dados pessoais, demonstrando como tal problema está também atravessado por marcadores sociais de diferença, como classe, raça/etnia e geração.	Críticas e preocupações relativamente à coleta de dados pelas Bigs Techs na área da saúde no Brasil; armazenamento de dados de saúde fora do país; divulgação responsável e acessível das informações relevantes sobre a saúde dos pacientes; pouca atenção à opinião dos usuários na percepção sobre os benefícios e os riscos da adoção das tecnologias de informação e comunicação (TICs) e, em especial, aquelas que coletam dados pessoais; ausência do foco no usuário invisibiliza também marcadores de diferença relacionados a gênero, sexualidade, raça/etnia, classe, geração e território.	(1) Soberania digital para desenvolvimento da sociedade. (2) Governança democrática da informação, informática e saúde no Brasil. (3) Estado regulador das práticas de saúde digital e que atue sobre o conjunto da sociedade não apenas para desenvolver soluções digitais, mas que regule todo o sistema de saúde e o conjunto do mercado, considerando a ausência de um marco legal de saúde digital, que, por exemplo, determine padrões para criação de ferramentas de mediação entre sistemas de saúde e usuários, como no caso dos prontuários eletrônicos e de sistemas informacionais mais amplos. (3) Estimular pesquisas que abordem a percepção dos/as usuários/as neste debate, bem como fomentar boas práticas e ações que promovam uma cultura de proteção de dados entre a população geral.	Teórico sem dados empíricos.	Livro 'Lei Geral de Proteção de Dados e o Controle Social da Saúde'	Incluso – capítulos centrais sobre governança de dados e saúde pública.	Rede UNIDA, ISBN: 978-65-5462-04-6 6.8, DOI: 10.18310/9786-554620468

8	Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais	Héider Aurélio Pinto, José Santos Souza Santana, Arthur Chioro	2022	Artigo especial	Sector público e privado da saúde brasileira, com foco em processos digitais	Refletir sobre a construção no Brasil de políticas e estratégias que combinem proteção e segurança dos dados pessoais, melhoria do sistema de saúde e desenvolvimento econômico social sustentável e incluyente.	Aponta riscos, recomenda medidas normativas e sugere aprimoramento da LGPD na saúde.	Considerando tanto o direito à proteção de dados pessoais quanto a importância da transformação digital na garantia do direito à saúde, é fundamental que a discussão sobre o uso de TIC na saúde seja articulada, e não oposta, à de governança e proteção de dados.	(1) Construir plataformas de interoperabilidade de dados com regras transparentes e sob governança pública, implementar efetivamente a LGPD e fortalecer a sua fiscalização, aperfeiçoar esta lei para que puna os agentes que comparem/obtem, intermediarem, venderem e usarem indevidamente os dados acarretando prejuízos aos cidadãos. (2) Uso de TIC na promoção de inovações no processo de trabalho em saúde, ao proporcionar ganhos de efetividade e eficiência, é cada vez mais essencial tanto para a segurança e melhoria da qualidade do cuidado, como para o planejamento, a gestão e a própria resiliência dos sistemas de saúde. Em função de sua complexidade e do amplo leque de interesses envolvidos no processo de transformação digital na saúde, torna-se fundamental dar centralidade ao tema da qualificação e fortalecimento da governança pública dos sistemas de informações em saúde. Da mesma forma, urge elevar e garantir a proteção de dados pessoais por meio da implementação e aprimoramento da LGPD, em busca de garantir privacidade dos dados dos cidadãos usuários de serviços de saúde e proteção quanto ao uso comercial inadequado e lesivo.	Teórico sem dados empíricos.	Revista Saúde em Redes	Incluso – central para discussão sobre transformação digital e proteção de dados na saúde.	DOI: 10.18310/2446-4813.2022v8n2p361-371
9	Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde	Sudilyn Mattos de Aragão, Taysa Schiocchet	2020	Pesquisa qualitativa, descritiva e exploratória	Sistema Único de Saúde (SUS)	Apontar em que medida a estrutura do sistema público de saúde brasileiro será impactada pela publicação da Lei e indicar eventuais caminhos a serem trilhados nesse sentido.	Relaciona diretamente o SUS com a necessidade de estrutura normativa e práticas de proteção de dados. Aborda questões relativas ao tratamento de dados sensíveis e consentimento; anonimização de dados sensíveis e hipóteses de compartilhamento; segurança dos dados e boas práticas de governança. Apresenta sugestões para harmonização do SUS à LGPD. Conceitos: (1) Remete aos artigos da LGPD. (2) O uso de tecnologias de informação e comunicação (TIC) para mediar a atenção à saúde é denominado e Saúde (e-Health).	(1) Dicotomia entre a legítima busca de proteção das informações sensíveis e as necessidades e dificuldades práticas de gestão, contradição aparentemente insuperável. (2) Uma das principais dificuldades de adequação do SUS à LGPD – variabilidade de modelos e vias de coleta não padronizadas e não normatizadas. Para além disso, há milhares de bytes já coletados e armazenados nos equipamentos do SUS para os quais não foi solicitado consentimento. A depender de eventual necessidade de utilização, o consentimento e/ou a anonimização serão mandatórios. (3) Outro ponto de crítica que se vive na relação SUS/LGPD é a questão do livre compartilhamento de informações entre instituições de igual ou distinta esfera federativa. Não há, até o momento, uma clara regulamentação acerca do intercâmbio de informações entre instituições componentes ou correlatas ao SUS. Assim, por exemplo, nos casos de pedidos de informação advindos do Judiciário, Defensorias Públicas e Ministérios Públicos, habitualmente procurados por pacientes do SUS que não têm seu direito à saúde assegurado; e entre as próprias instâncias do Executivo (Secretarias Municipais, Estaduais e Ministério da Saúde). Com relação à segurança dos dados, a principal limitação a ser enfrentada pelo sistema público de saúde brasileiro no atendimento à LGPD diz respeito à: a) ausência de uma política nacional única de segurança de dados de saúde; b) limitação de recursos orçamentários (desfinanciamento do SUS) para a adaptação de todos os sistemas informatizados mencionados às regras da LGPD. Como se tratam de sistemas com diferentes finalidades, atributos técnicos e riscos, torna-se ainda mais dispendiosa a tarefa.	(1) Exercício de compreensão sobre as normas trazidas pela LGPD, seus impactos e alcance sobre a estrutura da tecnologia da informação do SUS, a revisão do modelo de governança até então adotado e o levantamento das instituições integrantes e contratualizadas que serão afetadas. (2) Avaliação sobre i) o estágio de maturidade em que se encontra a atual estrutura de informação do SUS, ii) os fluxos de dados existentes, iii) os setores do SUS que serão mais fortemente impactados, iv) o alcance das medidas a serem planejadas (nacional, estadual, municipal), v) os responsáveis pela definição e implantação do plano estratégico a ser desenvolvido, vi) as metodologias processuais, físicas, tecnológicas e humanas fundamentais para a aderência aos requisitos da LGPD. (3) Definição: i) do plano a ser seguido para a efetiva proteção dos dados e para o atingimento dos requisitos da LGPD, ii) das políticas e diretrizes internas, iii) da organização do ambiente tecnológico e do modelo de governança a ser empregado, iv) das soluções propostas, v) da gestão de terceiros (prestadores contratados pelo SUS, vi) do monitoramento e tratamento de incidentes, vii) da dotação orçamentária e de recursos humanos. (4) Implementação dos componentes do modelo de governança de proteção de dados delineado nas fases anteriores, com finalidade de alinhar adequadamente as camadas do sistema e a tecnologia da informação para garantir, ao fim e ao cabo, desempenho, capacidade, maior eficiência do sistema público de saúde e garantia aos direitos fundamentais de privacidade e dignidade humana. (Sugestões específicas constantes no quadro 02 - fl. 703).	Teórico sem dados empíricos.	Revista Eletrônica de Comunicação, Informação e Inovação em Saúde (Recis)	Incluso – aborda diretamente os impactos da LGPD no SUS.	DOI: 10.29397/recis.v14i3.2012
10	Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados	Maria Amália Arruda Camara et al.	2021	Revisão narrativa	Sistema Único de Saúde e usuários	Apontar as fragilidades relativas à privacidade de usuários do SUS e propor uma solução teórica, a partir de uma infraestrutura paduana em armazenamento pessoal de dados – personal data stores (PDS), ou, a partir da segurança da blockchain.	Propõe alternativas tecnológicas e reflexões sobre a governança de dados sensíveis no SUS, como por exemplo o uso da tecnologia da blockchain ou armazenamento de dados em personal data stores (PDS). Conceitos: (1) A regulamentação sobre a Internet das Coisas, mais conhecida pelo acrônimo IoT (Internet of Things, em inglês) foi instituída no Brasil pelo art. 2º, I do Decreto no 9.854/2019. (2) A tecnologia da blockchain consiste apenas em uma cadeia de blocos, mas não no sentido tradicional dessas palavras. Nesse contexto, a palavra bloco significa uma informação digital, que está armazenada em um banco de dados público, a cadeia. A blockchain são compostos de informações digitais, que se organizam em três partes: os blocos que armazenam informações sobre as transações, ou compartilhamento de dados; os blocos que armazenam informações sobre quem está participando das transações; e os blocos que armazenam informações que os distinguem de outros blocos, ou metadados diferenciados.	(1) O compartilhamento de dados pessoais com os provedores de diferentes serviços representa um risco real à privacidade contemporânea. Isso se dá devido a problemas corriqueiros, tais quais o tratamento inadequado dos dados, a falta de conhecimento dos usuários sobre como seus dados estão sendo compartilhados, o compartilhamento incorreto e o excesso de dados que os próprios usuários finais expõem inadvertidamente. O compartilhamento de informações pessoais, na era da IoT, nos obriga a considerar não apenas dados pessoais, mas também o compartilhamento de dispositivos pessoais. Torna-se fundamental considerar a consentirização e a centralidade dos usuários no compartilhamento, bem como resiliência quanto terceiros mal-intencionados. (2) O uso da blockchain tem sido central na discussão a respeito da segurança dos dados sensíveis sanitários. Parte da doutrina diz que, por causa de seu próprio desenho, apresenta um risco em si à privacidade, na mesma medida que promove a transparência e o accountability. (3) O compartilhamento de dados no ambiente distribuído representa um desafio. Se, por um lado, existe a oportunidade de estruturar uma ferramenta tecnológica para gerenciar dados pessoais capaz de incorporar o paradigma de privacy by design, por outro lado, ainda existem muitos problemas que devem ser abordados para estar em compliance total com as leis protetivas dos dados pessoais. (4) Proposta teórica de uso de personal data storage PDS como possível solução para a redução dos riscos à privacidade e a identificação das fragilidades na implementação dessa solução pelo SIS/SUS, pois não foram encontrados artigos científicos que trabalhassem sobre essa abordagem e escopo no Brasil.	(1) Personal Data Storages (PDS) ou, em português, armazenamento pessoal de dados, funciona como um cofre ou armário pessoal de dados. É um serviço que permite armazenar, gerenciar e implantar dados pessoais importantes de maneira altamente segura e estruturada. Cada usuário não tem apenas controle sobre seus dados. Eles são reais proprietários, detentores da posse dos dados e, portanto, podem decidir quais serviços podem acessar o armazenamento de dados pessoais e, eventualmente, que tipo de dados. (2) A aplicabilidade da blockchain e como ela pode se aproximar da conformidade com a LGPD é amplamente estudada e prevista em muitos campos, mesmo que ainda não tenha alcançado uma abordagem pacífica. Isso mostra que existe um forte entendimento em torno da blockchain e de seu potencial de lidar com informações sensíveis, fornecendo até sugestões de conformidade de uma perspectiva legal.	Teórico sem dados empíricos.	Cadernos Ibero-americanos de Direito Sanitário	Incluso – aborda diretamente a proteção e governança de dados no SUS.	DOI: 10.17566/ciads.v10i1.657

C.2 Repositórios Institucionais

(Disponível em: <https://drive.google.com/file/d/1V9AYX-xpaMPv3H2IWE6LdRLbOPFT4Gul/view?usp=sharing>)

ID	Título do Artigo	Autores	Ano	Tipo de Estudo	População / Contexto	Objetivo Principal	Contribuições para a Governança de Dados	Desafios Identificados	Propostas ou Soluções	Limitações do Estudo	Base de Dados de Origem	Inclusão / Exclusão (com justificativa)	Notas Adicionais
1	O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados	Margareth Vets Zaganelli, Douglas Luis Binda Filho	2023	Ensaio jurídico-reflexivo com base em revisão normativa e doutrinária	Serviços de telemedicina	Discutir o tratamento de dados sensíveis na telemedicina sob a ótica da LGPD	Reflexões sobre práticas seguras e conformidade normativa na telemedicina	Risco de vazamento de dados sensíveis e divergência sobre responsabilidade jurídica	Adoção de protocolos rígidos de segurança e responsabilização clara	Teórico sem dados empíricos.	FIOCRUZ (Recis – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde)	Incluso – foco em governança de dados na telemedicina	https://doi.org/10.29397/recis.v17i3.3689
2	Capítulo – Lei Geral de Proteção de Dados: desafios para o SUS e a cidadania	Paulo Guanaes (Org.), diversos colaboradores	2018	Análise político-institucional	Sistema Único de Saúde (SUS)	Analisar a repercussão da LGPD no âmbito das políticas públicas de saúde e os desafios para sua implementação no SUS	Oferece diretrizes político-normativas para a implementação da LGPD no setor público da saúde.	Falta de integração entre LGPD e práticas administrativas públicas	Integração entre proteção de dados e gestão pública com foco em cidadania e no fortalecimento dos direitos fundamentais.	Análise política institucional sem dados empíricos	FIOCRUZ (Livro – Marcos legais nacionais em face da abertura de dados para pesquisa em saúde: dados pessoais, sensíveis ou sigilosos e propriedade intelectual)	Incluso – análise relevante sobre implementação da LGPD no SUS	Publicação impressa/digital – sem DOI
3	A autodeterminação informativa como contexto normativo para elaboração de diretrizes para a construção de um Relatório de Impacto à Proteção de Dados Pessoais	Marcelo Minghelli, Nathalia Berger Werlang, Barbara Balbis Garcia	2023	Pesquisa qualitativa, exploratória e relato de experiência	Núcleo Telessaúde UFSC, Telemedicina / Saúde pública	Discutir diretrizes para construção de um RIPD com enfoque na autodeterminação informativa e na humanização do tratamento de dados na telemedicina.	Promoção da autodeterminação informativa e conformidade com a LGPD por meio do RIPD.	Falta de regulamentação do RIPD; ausência de normatização completa para elaboração;	Modelo de RIPD baseado em princípios legais. Criação de diretrizes com foco na preservação da dimensão humana no tratamento de dados pessoais.	Pesquisa teórico-empírica com escopo limitado ao Núcleo Telessaúde UFSC.	FIOCRUZ (Recis – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde)	Inclusão – relevante para a governança de dados em saúde pública sob LGPD.	https://doi.org/10.29397/recis.v17i4bhe-ad-of-Print.3602
4	Questões éticas e perspectiva jurídica da proteção de dados	Edith Maria Barbosa Ramos, Amanda Silva Madureira, Jaqueline Prazeres de Sena, Pastora do Socorro Teixeira Leal	2021	Revisão bibliográfica e documental, método dedutivo e descritivo	Pesquisas científicas e Administração Pública no Brasil	Analisar a utilização de dados de seres humanos na ciência e na administração pública, à luz da LGPD e das decisões do STF.	Base normativa da LGPD, contribuições do STF e diretrizes éticas fortalecem a governança de dados no Brasil.	Dificuldade de anonimização total; riscos éticos na manipulação de dados em pesquisa; ausência de diretrizes éticas uniformes.	Fortalecimento da LGPD; revisão de resoluções do CNS. Implementação de instrumentos legais que garantam privacidade sem inviabilizar pesquisa.	Teórico sem dados empíricos.	FIOCRUZ (Cadernos Ibero-Americanos de Direito Sanitário)	Inclusão – base conceitual e normativa fundamental para a governança de dados pessoais no Brasil.	https://doi.org/10.17566/ciads.v10i3.796
5	Metodologia de Administração de Dados (MAD)	Ministério da Saúde	2024	Documento técnico normativo	Órgãos e profissionais do SUS envolvidos na gestão de dados	Estabelece padrões e papéis para administração de dados no MS, com foco na RNDs, LGPD, segurança e interoperabilidade usando HL7 FHIR	Propõe uma Metodologia de Administração de Dados (MAD), contendo a regulamentação e a descrição dos padrões e procedimentos a serem adotados em relação à Administração de Dados no âmbito do Ministério da Saúde. Trata de questões relativas a modelos de interoperabilidade de dados e anonimização de dados.	Falta de padronização, segurança e integração entre sistemas	Padronização de processos, definição de papéis e segurança da informação. Implantação de padrões de administração e interoperabilidade de dados de saúde.	Documento institucional técnico	DATASUS	Incluso – fornece diretrizes de governança de dados para o SUS	https://datasus.sau.gov.br/wp-content/uploads/2025/06/MAD_240625.pdf
6	Guia orientativo: Tratamento de dados pessoais pelo Poder Público	Autoridade Nacional de Proteção de Dados (ANPD)	2023	Guia técnico orientativo	Órgãos e entidades da Administração Pública	Fornecer orientações práticas para agentes públicos sobre tratamento e proteção de dados pessoais conforme a LGPD	Aborda a temática da LGPD em face do poder público, tratando das bases legais, princípios e questões relativas ao compartilhamento de dados pessoais pelo poder público.	Falta de conhecimento técnico sobre a LGPD no setor público	Mapeamento de dados, elaboração de RIPD, boas práticas de segurança da informação	Documento institucional técnico	ANPD	Incluso – fornece orientação prática de implementação da LGPD na esfera pública	https://www.gov.br/anpd/pt-br/central-s-de-conteudo/mat-eriais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf
7	Cartilha de Condutas voltadas à Privacidade e à Proteção de Dados	José Antonio Costa Leal, César Melchior Silveira da Luz, Cristiano Goulart Borges	2022	Documento institucional orientativo	Servidores e colaboradores da PROCERGS	Demonstrar a importância da cultura de privacidade e proteção de dados no ambiente institucional da PROCERGS.	Instrumentaliza a implementação de uma cultura de governança de dados pessoais na administração pública estadual.	Risco de desconhecimento ou descumprimento de princípios da LGPD pelos colaboradores.	Treinamentos, orientações e documentos normativos internos.	Documento institucional técnico	PROCERGS	Incluso – fornece diretrizes práticas e institucionais para a governança de dados pessoais.	https://www.procergs.rs.gov.br/upload/arquivos/202301/12065930-cartilha-condutas-procergs-1.pdf
8	Cartilha LGPD PROCERGS – Lei Geral de Proteção de Dados	José Antonio Costa Leal, César Melchior Silveira da Luz, Cristiano Goulart Borges	2022	Material educativo institucional	Colaboradores da PROCERGS e demais interessados em LGPD	Explicar os principais conceitos, princípios, bases legais e obrigações da LGPD em linguagem acessível para os colaboradores da PROCERGS.	Oferece um guia prático para implementação de governança em privacidade e conformidade legal.	Desconhecimento técnico-jurídico dos colaboradores; riscos de sanções legais.	Implantação de Programa de Governança em Privacidade (PGP), treinamentos e padronização.	Documento institucional técnico	PROCERGS	Incluso – documento institucional estruturado com foco direto na governança de dados pessoais.	https://www.procergs.rs.gov.br/upload/arquivos/202301/12065930-cartilha-lgpd-procergs.pdf
9	Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global	Almeida, B. A. et al.	2020	Estudo teórico-reflexivo	Governança de dados pessoais em emergências de saúde pública	Analisar os desafios éticos, legais e técnicos no uso de dados pessoais para enfrentamento da COVID-19 e propor novos modelos de governança.	Propõe princípios e diretrizes para governança ética e transparente em contextos de crise sanitária. Defende uma governança responsável, transparente e participativa para o uso de dados em saúde pública.	Risco de vigilância excessiva, desigualdade no acesso à tecnologia e ausência de salvaguardas claras.	Estabelecimento de protocolos regulatórios claros e participação social na governança de dados. Identificação de riscos de uso indevido de dados e necessidade de salvaguardas robustas para garantir confiança social.	Teórico sem dados empíricos.	FIOCRUZ (Ciência & Saúde Coletiva)	Incluso – aborda diretamente governança de dados e LGPD em contexto de saúde pública.	DOI: 10.1590/1413-8123.2020256.1.11792020

C.3 Legislação

(Disponível em: https://drive.google.com/file/d/1awsIhLSw_wJINfxAIP1O3cNRi14oV8p/view?usp=sharing)

ID	Tipo de Norma	Número	Ano	Órgão Emissor	Tema Central	Principais artigos relacionados à governança de dados e breve resumo	Comentário	Notas Adicionais
1	Lei Federal	13.709	2018	Presidência da República	Lei Geral de Proteção de Dados Pessoais (LGPD)	Artigos: 6º, 37 a 41, 46 a 49, 50, 13, 23 a 27, 32 e 50§2º Estabelece princípios, direitos e deveres relacionados à proteção de dados pessoais. Define conceitos como controlador, operador, encarregado, tratamento de dados e estabelece a criação da ANPD.	Marco legal da proteção de dados no Brasil, fundamento das normas estaduais.	https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
2	Padrão Técnico (PTIC)	1	2022	Comitê de Governança de TIC - RS	Procedimentos para Classificação e Qualidade de Dados	Itens: 1.1, 1.3, 2.1 a 2.4, 2.5 a 2.9 Estabelece padrões de TIC para classificação e qualidade de dados no RS, conforme Decreto 56.106/2021 e 56.528/2022. Define dados brutos, transformados, plataformas e produtos de dados. Reforça a atuação dos Facilitadores de Dados.	Documento técnico complementar aos decretos de governança e TIC do RS.	https://planejamento.rs.gov.br/upload/arquivos/202301/09103253-ptic-01-2022-classificacao-e-qualidade-de-dados-site.pdf
3	Decreto Estadual	56.528	2022	Governo do Estado do RS	Governança no compartilhamento de dados no âmbito estadual	Artigos: 1º, 3º ao 19º Estabelece normas para o compartilhamento de dados entre órgãos públicos estaduais. Define níveis de compartilhamento (amplo, institucional, específico) e a figura dos Facilitadores de Dados.	* Estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública estadual direta, autárquica e fundacional; * o compartilhamento de dados pressupõe a indicação ao sistema de Governança e Gestão de TIC do Estado, dos servidores que atuarão como facilitadores de dados e do conjunto de dados sujeitos à sua administração; * designação dos facilitadores de dados que farão a catalogação dos dados envolvidos no compartilhamento, classificando e informando o nível de compartilhamento dos dados; * O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública exige o atendimento dos seguintes requisitos: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); d) formalização e registro (art. 37); e) indicação objetiva e detalhada dos dados; f) indicação da base legal; g) estabelecimento do período de duração do uso compartilhado dos dados, bem como definição acerca da possibilidade de conservação ou eliminação dos dados após o término do tratamento; h) atendimento ao princípio da transparência (artigos 6º, VI, e 23, I); i) previsão de medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. INDICAÇÃO DE FACILITADORES DE DADOS / CATALOGAÇÃO DE DADOS	https://www.al.rs.gov.br/legis
4	Decreto Estadual	56.106	2021	Governo do Estado do RS	Política de Tecnologia da Informação e Comunicação (TIC)	Artigos: 2º IV, V, VI, VIII e IX; 4º VII, 15 IV, 21 III i, 26, 31 Institui a Política de TIC no RS, define princípios, diretrizes e o Sistema de Governança e Gestão de TIC. Inclui governança de dados como um dos eixos estruturantes da política.	Base legal para os padrões técnicos e para a governança digital do Estado.	https://www.al.rs.gov.br/legis
5	Decreto Estadual	55.986	2021	Governo do Estado do RS	Altera o Decreto nº 55.647/2020 – Implementação da LGPD	Artigos: 2º § 3º e 4º, 13, 17-A Permite que um mesmo encarregado atue em mais de um órgão. Estabelece parâmetros para relatórios de impacto e programas de governança em privacidade no RS.	Aprimora a estrutura de governança e facilita a implementação da LGPD no Estado.	https://www.al.rs.gov.br/legis

ID	Tipo de Norma	Número	Ano	Órgão Emissor	Tema Central	Principais artigos relacionados à governança de dados e breve resumo	Comentário	Notas Adicionais
6	Decreto Estadual	55.987	2021	Governo do Estado do RS	Institui a Política Estadual de Proteção de Dados Pessoais	Artigos: 1º, 2º, 4º ao 15 Define princípios da proteção de dados pessoais no RS e diretrizes para sua implementação conforme a LGPD. Destaca o papel do controlador, operador, encarregado e a estrutura de governança.	Documento estruturante da adequação do Executivo Estadual à LGPD.	https://www.al.rs.gov.br/legis
7	Decreto Estadual	55.647	2020	Governo do Estado do RS	Regulamenta a implementação da LGPD no Executivo Estadual	Artigos: 1º, 2º a 5º, 6º a 7º, 8º a 11, 12, 13 a 17 Define prazos, fases e a figura do Encarregado pelo Tratamento de Dados. Cria Conselho e Grupo de Trabalho para implementação da LGPD no RS.	Primeira regulamentação estadual sobre a LGPD. Base para estruturação institucional.	https://www.al.rs.gov.br/legis
8	Portaria Estadual	728	2018	Secretaria Estadual de Saúde do RS	Plano de Segurança da Informação (PSI/SES)	Itens: 1, 2, 7, 9, 10, 11, 17, 24, 27, 29, 32, 37, 39, 43, 45, 47 e 50 Estabelece diretrizes para a segurança dos ativos da informação da SES-RS. Define responsabilidades dos usuários quanto à confidencialidade, integridade e disponibilidade das informações.	Instrumento fundamental para o tratamento e proteção de dados sensíveis na SES-RS.	https://saude.rs.gov.br/upload/arquivos/carga20180825/03162500-728.pdf
9	Portaria Estadual	740	2015	Secretaria Estadual de Saúde do RS	Uso das Tecnologias da Informação na SES-RS	Itens: 1, 4, 5, 7, 8, 9, 14, 17 e 27 Regulamenta o uso de TIC no âmbito da SES-RS. Estabelece procedimentos e padrões para infraestrutura, segurança e acesso às informações institucionais.	Base normativa para infraestrutura de TIC e gestão da informação na SES-RS.	https://saude.rs.gov.br/upload/arquivos/carga20170441/13054154-1448286590-740-dgti.pdf
10	Nota Técnica	1	2022	Comitê Gestor da Política de Pesquisa – SES/RS	Orientações sobre uso de dados para pesquisa na SES-RS	Itens: Trecho integral Define diretrizes éticas e legais para uso de dados pessoais e sensíveis em pesquisas científicas. Estabelece o fluxo de autorização via TAI e CEP/CONEP, destacando o papel da anonimização e pseudoanonimização.	Instrumento orientador para pesquisadores e gestores em conformidade com a LGPD.	https://saude.rs.gov.br/upload/arquivos/202008/14092611-republicacao-438-esp.pdf

C.4 Modelos de programas de governança em privacidade adotados por instituições públicas

(Disponível em: <https://drive.google.com/file/d/1RYKSiCvjp4-1P4hUGvIwaS-WAZL3TC7A/view?usp=sharing>)

ID	Órgão	Ano	Tema Central	Principais tópicos	Principais conceitos relacionados à governança de dados pessoais	Práticas ou estruturas que possam ser adaptadas ao contexto da SES/RS	Recomendações Adicionais	Notas Adicionais
1	Ministério da Saúde (MS)	2022	Programa de Governança em Privacidade	Iniciação e Planejamento; Construção e Execução; Monitoramento	Privacy by design, cultura de proteção de dados, RIPD, política de privacidade, inventário de dados pessoais, encarregado de dados, indicadores de performance, plano de resposta a incidentes	Modelo de diagnóstico de maturidade, estrutura da AEPD, criação de comitês internos, instrumentos de avaliação contínua, modelo de RIPD e plano de conscientização	Adoção de modelo de maturidade LGPD e uso de indicadores de desempenho conforme o PGP/MS	https://bvsmis.saude.gov.br/bvsmis/publicacoes/programa_governanca_privacidade.pdf
2	Procuradoria-Geral do Estado do RS (PGE-RS)	2021	Programa de Governança em Privacidade	Estrutura organizacional; Instrumentos operacionais; Cronograma de implantação	Inventário de dados, relatórios de impacto, plano de resposta a incidentes, política de privacidade, grupo de apoio ao encarregado, governança da informação e dos processos	Modelo escalonado de implantação com cronograma, definição clara dos instrumentos operacionais, estruturação do grupo de apoio ao encarregado, modelo de PPPD-PGE	Incorporação de cronograma e matriz de responsabilidades conforme modelo PGE-RS	https://www.pge.rs.gov.br/upload/arquivos/202112/29083040-pgp-pge.pdf

APÉNDICE D - CHECKLIST PRISMA-ScR

Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) Checklist

SECTION	ITEM	PRISMA-ScR CHECKLIST ITEM	REPORTED ON PAGE #
TITLE			
Title	1	Identify the report as a scoping review.	FL. 02
ABSTRACT			
Structured summary	2	Provide a structured summary that includes (as applicable): background, objectives, eligibility criteria, sources of evidence, charting methods, results, and conclusions that relate to the review questions and objectives.	FLS. 04/05
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of what is already known. Explain why the review questions/objectives lend themselves to a scoping review approach.	FLS. 12/14
Objectives	4	Provide an explicit statement of the questions and objectives being addressed with reference to their key elements (e.g., population or participants, concepts, and context) or other relevant key elements used to conceptualize the review questions and/or objectives.	FL. 15
METHODS			
Protocol and registration	5	Indicate whether a review protocol exists; state if and where it can be accessed (e.g., a Web address); and if available, provide registration information, including the registration number.	FL. 23
Eligibility criteria	6	Specify characteristics of the sources of evidence used as eligibility criteria (e.g., years considered, language, and publication status), and provide a rationale.	FL. 24
Information sources*	7	Describe all information sources in the search (e.g., databases with dates of coverage and contact with authors to identify additional sources), as well as the date the most recent search was executed.	FLS. 23/24
Search	8	Present the full electronic search strategy for at least 1 database, including any limits used, such that it could be repeated.	FLS. 103/106
Selection of sources of evidence†	9	State the process for selecting sources of evidence (i.e., screening and eligibility) included in the scoping review.	FLS. 27/28
Data charting process‡	10	Describe the methods of charting data from the included sources of evidence (e.g., calibrated forms or forms that have been tested by the team before their use, and whether data charting was done independently or in duplicate) and any processes for obtaining and confirming data from investigators.	FL. 25
Data items	11	List and define all variables for which data were sought and any assumptions and simplifications made.	FLS. 103/106
Critical appraisal of individual sources of evidence§	12	If done, provide a rationale for conducting a critical appraisal of included sources of evidence; describe the methods used and how this information was used in any data synthesis (if appropriate).	NAO

SECTION	ITEM	PRISMA-ScR CHECKLIST ITEM	REPORTED ON PAGE #
Synthesis of results	13	Describe the methods of handling and summarizing the data that were charted.	FLS. 32/62
RESULTS			
Selection of sources of evidence	14	Give numbers of sources of evidence screened, assessed for eligibility, and included in the review, with reasons for exclusions at each stage, ideally using a flow diagram.	FL. 31
Characteristics of sources of evidence	15	For each source of evidence, present characteristics for which data were charted and provide the citations.	FLS. 32/62
Critical appraisal within sources of evidence	16	If done, present data on critical appraisal of included sources of evidence (see item 12).	NÃO
Results of individual sources of evidence	17	For each included source of evidence, present the relevant data that were charted that relate to the review questions and objectives.	FLS. 32/62
Synthesis of results	18	Summarize and/or present the charting results as they relate to the review questions and objectives.	FLS. 32/62
DISCUSSION			
Summary of evidence	19	Summarize the main results (including an overview of concepts, themes, and types of evidence available), link to the review questions and objectives, and consider the relevance to key groups.	FLS. 63/67
Limitations	20	Discuss the limitations of the scoping review process.	FLS. 67/68
Conclusions	21	Provide a general interpretation of the results with respect to the review questions and objectives, as well as potential implications and/or next steps.	FLS. 71/72
FUNDING			
Funding	22	Describe sources of funding for the included sources of evidence, as well as sources of funding for the scoping review. Describe the role of the funders of the scoping review.	NAO HA

JB1 = Joanna Briggs Institute; PRISMA-ScR = Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews.

* Where sources of evidence (see second footnote) are compiled from, such as bibliographic databases, social media platforms, and Web sites.

† A more inclusive/heterogeneous term used to account for the different types of evidence or data sources (e.g., quantitative and/or qualitative research, expert opinion, and policy documents) that may be eligible in a scoping review as opposed to only studies. This is not to be confused with information sources (see first footnote).

‡ The frameworks by Arksey and O'Malley (6) and Levac and colleagues (7) and the JBI guidance (4, 5) refer to the process of data extraction in a scoping review as data charting.

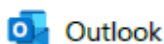
§ The process of systematically examining research evidence to assess its validity, results, and relevance before using it to inform a decision. This term is used for items 12 and 19 instead of "risk of bias" (which is more applicable to systematic reviews of interventions) to include and acknowledge the various sources of evidence that may be used in a scoping review (e.g., quantitative and/or qualitative research, expert opinion, and policy document).

From: Tricco AC, Lillie E, Zarin W, O'Brien KK, Colquhoun H, Levac D, et al. PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Ann Intern Med*. 2018;169:467-473. doi: 10.7326/M18-0850.



St. Michael's
Inspired Care.
Inspiring Science.

APÊNDICE E - QUESTIONÁRIOS / FORMULÁRIOS



Atualização de listagem de bases de dados administradas pela SES

De LGPD SES - [SES] <lgpd@saude.rs.gov.br>
Data Sex, 15/03/2024 15:39
Para SES - Diretores <diretores@saude.rs.gov.br>
Cc Maria Claudia Mulinari <maria-mulinari@saude.rs.gov.br>

1 anexo (33 KB)

Bases de dados SES por Departamento.pdf;

Prezados, boa tarde.

Na qualidade de Encarregada de Dados da SES, para fins de subsidiar o trabalho de implementação da LGPD na Secretaria, solicito aos Srs. Diretores análise e retorno com complementação da listagem das bases de dados administradas pela SES que segue em anexo.

Assim, solicito que cada Diretor analise os sistemas sob sua administração, indicando se no documento anexo consta algum lançamento incorreto ou eventual necessidade de complementação com a indicação de outras bases.

Desde já agradeço a atenção, solicitando, se possível, retorno até o final do mês de março do corrente ano, considerando a necessidade de finalização do Programa de Governança em Privacidade da SES.

Atenciosamente,

Carolina Pacheco Feron

Especialista em Saúde - Assessor Jurídico
Núcleo de Consultoria Administrativa e de Pessoal - NUCONSP/AJ
Secretaria da Saúde do RS

APÊNDICE F - MAPEAMENTO DOS BANCOS DE DADOS SES/RS

BASES - TRATAM DIRETA OU INDIRETAMENTE DE DADOS PESSOAIS E PESSOAIS SENSÍVEIS, SEJA DE USUÁRIOS DO SUS OU DE COLABORADORES

- FPE
- Sistema de Monitoramento Estratégico - SGE
- DIGISUS - Instrumentos de planejamento do MS
- SAIPS - Sistema de Apoio à Implementação de Políticas em Saúde - Captação de recursos
- Gestão do Site da SES
- Redes sociais da secretaria (Instagram, Twitter, Youtube e etc)
- PROA
- RHE - Recursos Humanos do Estados
- RHS - Recursos Humanos da SES
- SISAB - Produção da Atenção Básica
- SIM - Sistema de Informação de Mortalidade
- SINASC - Sistema de Informação de Nascidos Vivos
- SisPIM - Sistema da Primeira Infância Melhor
- SIGAH - Sistema de Gestão da Atenção Hospitalar (Contratos, pagamentos)
- SIH - Sistema de Informações Hospitalares
- SIA - Sistema de Informações Ambulatoriais
- SISMAC - Sistema de Controle de Limite Financeiro da Média e Alta Complexidade
- AME - Administração de Medicamentos
- Sistema de Gestão Acadêmica
- POPERS - Portal de Pesquisas na SES - Comitê Gestor da Política de Pesquisas na SES
- Gestão da Biblioteca - Pergamum
- SINAN - Sistema de Informação de Agravos de Notificação
- SIVEP Gripe - Sistema de notificação de SRAG e SG
- Esus Notifica - Notificação COVID-19
- SIPNI - Sistema de Informação do Programa Nacional de Imunizações
- GAL - Gestão de Laboratórios (LACEN)
- SIST - Sistema de Informação da Saúde do Trabalhador (notificações e investigações)
- SIVISA - Sistema de Informação da Vigilância Sanitária
- VGS - Gestão de Doadores de sangue
- Ouvidor SUS
- LAI - Sistema de recebimento de demandas da Lei de Acesso à Informação
- GERINT - Gestão da Regulação de Internações
- GERCON - Gestão da Regulação de Consultas
- GERPAC - Gestão da Regulação de procedimentos de Alto Custo
- SAPH - Gestão de Atendimento Móvel de Urgência e Emergência - SAMU
- Sistema Nacional de Transplantes (SNT) - Central de Transplantes
- Hemovida

ANEXO A - APROVAÇÃO - COMISSÃO DE CONSULTORIA CIENTÍFICA - GHC



PARECER DA COMISSÃO DE CONSULTORIA CIENTÍFICA DO GHC

A Comissão de Consultoria Científica do Grupo Hospitalar Conceição avaliou o seguinte projeto de pesquisa:

Projeto: 25096

Versão do Projeto:

Versão do TCLE:

CAAE:

Workflow: 4640889

Pesquisadores:

CAROLINA OLIVEIRA PACHECO FERON

FERNANDO ANSCHAU

Título: Governança de Dados na Saúde Pública Brasileira: uma revisão de escopo.

Parecer: A Comissão de Consultoria Científica do GHC avaliou os aspectos metodológicos e de infraestrutura do projeto de pesquisa apresentado, bem como a anuência dos coordenadores e gerentes das áreas, via Workflow, considerando os pontos adequados. Sendo assim, o estudo proposto recebeu parecer FAVORÁVEL ao prosseguimento do fluxo na instituição.

Considerações finais: Caso necessário apreciação ética pelo CEP-GHC este parecer deverá ser anexado na Plataforma Brasil (Observar as Resoluções do CNS/MS sobre pesquisas e tramitação em CEP). A Gerência onde será realizada a Pesquisa deverá ser comunicada quando do seu início.

Porto Alegre, 07 de julho de 2025.


MONICA VINHAS DE SOUZA
Presidente - Comissão de Consultoria Científica do GHC