



FORMAÇÃO
**SAÚDE
DIGITAL
NO SUS**

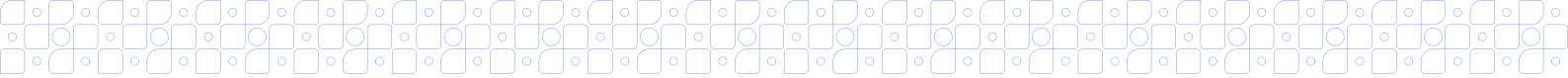
Segurança da Informação em Saúde Digital

Organizadoras

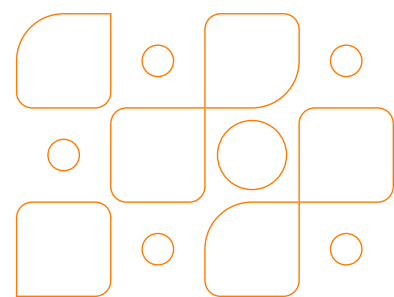
Paola Trindade Garcia
Ana Estela Haddad
Ana Emilia Figueiredo de Oliveira
Deysianne Costa das Chagas
Elza Bernardes Ferreira



EDLIFMA



Segurança da Informação em Saúde Digital





Reitor
Vice-Reitor

UNIVERSIDADE FEDERAL DO MARANHÃO

Prof. Dr. Fernando Carvalho Silva
Prof. Dr. Leonardo Silva Soares



Diretor

SISTEMA INTEGRADO DE BIBLIOTECAS

Prof. Dr. César Augusto Castro



EDUFMA

EDITORIA DA UFMA

Coordenadora

Irenilma Cadête Lima

Conselho Editorial

Prof.^a Dr.^a Andréa Katiane Ferreira Costa
Prof.^a Dr.^a Débora Batista Pinheiro Sousa
Prof. Dr. Edson Ferreira da Costa
Prof. Dr. José Carlos Aragão Silva
Prof.^a Dr.^a Jussara Danielle Martins Aires
Prof.^a Dr.^a Karina Almeida de Sousa
Prof. Dr. Luís Henrique Serra
Prof. Dr. Luiz Eduardo Neves dos Santos
Prof.^a Dr.^a Luma Castro de Souza
Prof. Dr. Márcio José Celeri
Prof.^a Dr.^a Maria Áurea Lira Feitosa
Prof.^a Dr.^a Raimunda Ramos Marinho
Prof.^a Dr.^a Rosângela Fernandes Lucena Batista
Bibliotecária Iole Costa Pinheiro



Associação Brasileira das Editoras Universitárias



All the contents of this work, except where otherwise noted, is licensed under a Creative Commons Attribution 4.0 International license.

Todo o conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença Creative Commons Atribuição 4.0.

Todo el contenido de esta obra, excepto donde se indique lo contrario, está bajo licencia de la licencia Creative Commons Reconocimiento 4.0.

Paola Trindade Garcia
Ana Estela Haddad
Ana Emília Figueiredo de Oliveira
Deysianne Costas das Chagas
Elza Bernardes Ferreira
(ORGS)

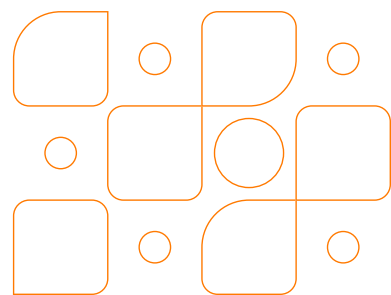
Segurança da Informação em Saúde Digital

São Luís



EDUFMA

2025



© 2025 EDUFMA - Todos os direitos reservados.

Projeto Gráfico, Diagramação e Capa

Jackeline Mendes Pereira

Clara Terra Rayol Santos

Revisão textual

Vitória Regina de Alencar Araújo

Dados Internacionais de Catalogação na Publicação (CIP)

Segurança da informação em saúde digital / Paola Trindade Garcia... *[et al.]*
(orgs.) . — São Luís: EDUFMA, 2025.
68 p.: il.

ISBN: 978-65-5363-530-2

1. Saúde digital – Segurança da informação. 2. Saúde digital – Regulação -
Brasil. 3. Programa SUS Digital. 4. Lei Geral de Proteção de Dados Pessoais.
5. Rede Nacional de Dados em Saúde. I. Garcia, Paola Trindade. II. Haddad,
Ana Estela. III. Oliveira, Ana Emília Figueiredo de. IV. Chagas, Deysianne
Costas da. V. Ferreira, Elza Bernardes.

CDD 614.005 8
CDU 614:004.056

Ficha catalográfica elaborada pela bibliotecária Marcia Cristina da Cruz Pereira
CRB 13 / 418

COMO CITAR ESTE MATERIAL

GARCIA, Paola Trindade *et al.* (org.); SILVA, Glenda Pereira Costa. Segurança da Informação em Saúde Digital. São Luís: EDUFMA, 2025. 68 p.

©2025. Secretaria de Informação e Saúde Digital (SEIDIGI) do Ministério da Saúde & Universidade Federal do Maranhão (UFMA).

Esta obra é disponibilizada nos termos da Licença Creative Commons – Atribuição – Não Comercial – Compartilhamento pela mesma licença 4.0 Internacional. É permitida a reprodução parcial ou total desta obra, desde que citada a fonte.

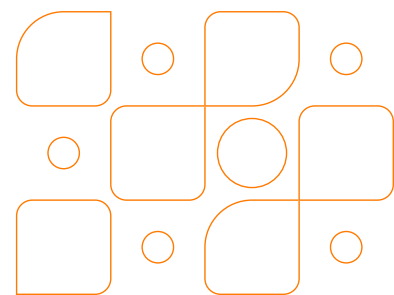
EDUFMA | EDITORA DA UNIVERSIDADE FEDERAL DO MARANHÃO

Av. dos Portugueses, 1966 – Vila Bacanga

CEP: 65080-805 | São Luís | MA | Brasil

Telefone: (98) 3272-8157

www.edufma.ufma.br | edufma@ufma.br



Ficha Técnica

Presidência da República

Luiz Inácio Lula da Silva

Presidente

Ministério da Saúde

Alexandre Rocha Santos Padilha

Ministro da Saúde

Secretaria de Informação de Saúde Digital - SEIDIGI

Ana Estela Haddad

Secretária de Informação e Saúde Digital

Maria Aparecida da Silva

Secretária Adjunta da Secretaria de Informação e Saúde Digital

Departamento de Saúde Digital e Inovação – DESD

Antônio Ferreira Lima Filho

Substituto eventual

Departamento de Informação e Informática do Sistema Único de Saúde – DataSUS

Paula Xavier dos Santos

Diretora do Departamento de Informação e Informática do Sistema Único de Saúde

Departamento de Monitoramento, Avaliação e Disseminação de Informações Estratégicas em Saúde – DEMAS

Paulo Eduardo Guedes Sellera

Diretor do Departamento de Monitoramento, Avaliação e Disseminação de Dados e Informações Estratégicas em Saúde

Grupo de trabalho – Ação Estratégica TransForma SUS Digital

Ana Estela Haddad

Secretária de Informação e Saúde Digital

Maria Aparecida da Silva

Secretária Adjunta da Secretaria de Informação e Saúde Digital

Naomar Almeida Filho

Cláudia Marques

Camila Huanca

Luiz Alves

Francisco Campos

Thaís Campos

Isabela Pinto

Consultores da SEIDIG

Universidade Aberta do Sistema Único de Saúde – UNA-SUS/UFMA

Coordenação do Projeto

Paola Trindade Garcia

Coordenadora do Projeto

Coordenação-Geral da UNA-SUS/UFMA

Elza Bernardes Ferreira

Coordenadora Geral da UNA-SUS/UFMA

Vice-Coordenação da UNA-SUS/UFMA

Ana Emilia Figueiredo de Oliveira

Vice-coordenadora da UNA-SUS/UFMA

Coordenação de Gestão de Projetos da UNA-SUS/UFMA

Deysianne Costa das Chagas

Coordenadora de Gestão de Projetos da UNA-SUS/UFMA

Coordenação de Produção Pedagógica da UNA-SUS/UFMA

Paola Trindade Garcia

Coordenadora de Produção Pedagógica da UNA-SUS/UFMA

Coordenação de Ofertas Educacionais da UNA-SUS/UFMA

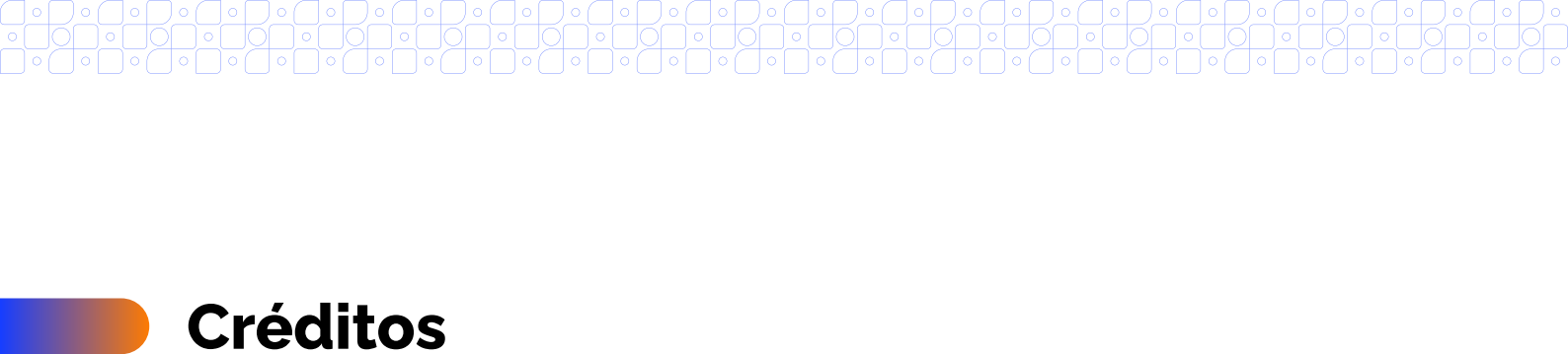
Juan Magalhães Paiva

Coordenador de Ofertas Educacionais da UNA-SUS/UFMA

Coordenação de Tecnologia da Informação da UNA-SUS/UFMA

Osvaldo Silva de Sousa Junior

Coordenador de Tecnologia da Informação da UNA-SUS/UFMA



Créditos

Secretaria de Informação e Saúde Digital - SEIDIGI

Ana Estela Haddad

Coordenação de Projeto

Paola Trindade Garcia

Coordenação Geral da UNA-SUS/UFMA

Elza Bernardes Ferreira

Elaboração conteúdos e atividades

Glenda Pereira Costa Silva

Validação Pedagógica

Isabelle Aguiar Prado

Validação Técnica - SEIDIGI

Ana Estela Haddad

Maria Aparecida da Silva

Identidade Visual

Jackeline Mendes Pereira

Design Instrucional

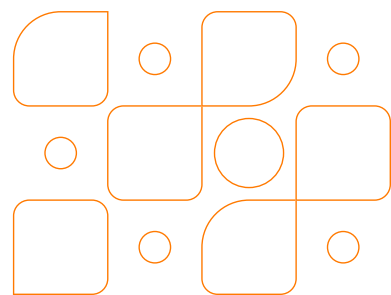
Donny Wallesson dos Santos

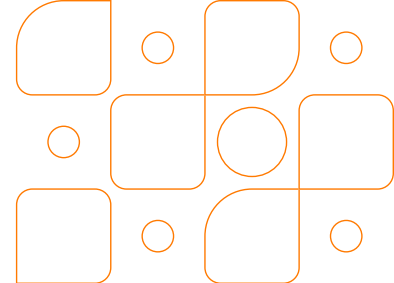
Design Gráfico

Clara Terra Rayol Santos

Revisão Textual

Vitória Regina de Alencar Araújo





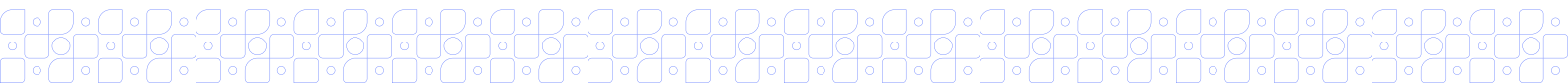
Sobre a autora

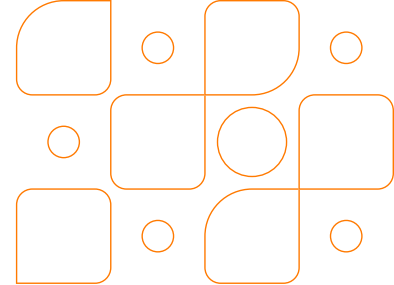


Glenda Pereira Costa Silva

Graduada em Nutrição pela Universidade Federal do Maranhão – UFMA, mestre em Saúde Coletiva pelo Programa de Pós-Graduação em Saúde Coletiva – PPGSC/UFMA, residente multiprofissional em Saúde da Família pela Universidade Estadual do Maranhão – UEMA, especialista em Nutrição Clínica, Fitoterápica e Funcional pela IDAAM e em Gestão em Saúde pela UFMA. Atualmente é doutoranda em Saúde Coletiva pelo PPGSC/UFMA. Possui experiência na área de Saúde Coletiva, com ênfase

em Gestão, Avaliação e Planejamento das Políticas Públicas em Saúde e Nutrição e Saúde Coletiva





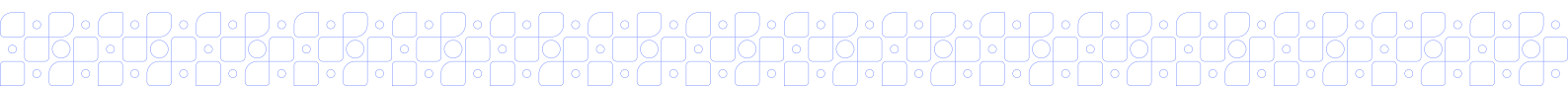
Sobre as organizadoras

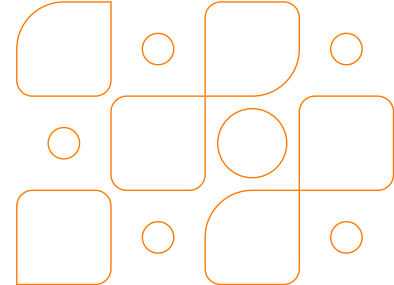


Paola Trindade Garcia

Fisioterapeuta, Doutora em Saúde Coletiva, Mestra em Saúde Coletiva e Residente Multiprofissional em Saúde pela Universidade Federal do Maranhão – UFMA. Especialista em Processos Educacionais na Saúde pelo Instituto de Ensino e Pesquisa do Hospital Sírio-Libanês, em Saúde da Família pelo Centro Universitário Santa Terezinha – CEST e em Gestão do Trabalho e Educação na Saúde pela UFMA. Docente do Departamento de Saúde Pública da UFMA e coordenadora de Produção Pedagógica da

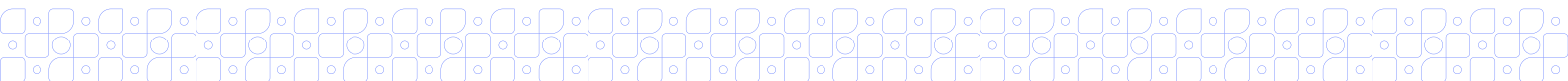
UNA-SUS/UFMA. Professora permanente do Programa de Mestrado Profissional em Saúde da Família da Rede da Rede Nordeste de Formação em Saúde da Família – RENASF/UFMA. Docente convidada do Programa de Pós-Graduação em Saúde Coletiva da UFMA. Integrante do Grupo de pesquisa Saúde, Tecnologia e Educação – SAITE (CNPq/UFMA) e Vice-líder do grupo de pesquisa Políticas Públicas de Saúde e Controle Social (CNPq/UFMA). Possui experiência em Educação a Distância – EaD e em metodologias ativas de ensino. Tem experiência na produção de Massive Open Online Courses – MOOCs na área da saúde. Coordena ações de extensão de cursos na modalidade de ensino a distância na UFMA, entre eles o curso de aperfeiçoamento Produção de Recursos Educacionais para EaD – PRAEAD e o curso de aperfeiçoamento Políticas Informadas por Evidências – PIE: possibilidades, desafios e ferramentas.

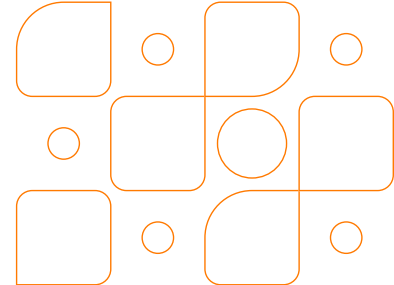




Ana Estela Haddad

Graduada em Odontologia, Mestre e Doutora em Ciências Odontológicas e Livre-Docente pela Universidade de São Paulo – USP, além de especialista em Odontopediatria pela Fundação para o Desenvolvimento Científico e Tecnológico da Odontologia – FUNDECTO da Faculdade de Odontologia da Universidade de São Paulo – FOUSP. Professora titular do Departamento de Ortodontia e Odontopediatria e docente permanente do Programa de Pós-Graduação em Ciências Odontológicas da FOUSP. Foi assessora do Ministro da Educação (2003-2005) e uma das idealizadoras e participantes da implementação do Programa Universidade para Todos – PROUNI. Atuou nos trabalhos relacionados à promulgação da Lei n.º 10.861/2004, que criou o Sistema Nacional de Avaliação da Educação Superior – SINAES e a Comissão Nacional de Avaliação da Educação Superior – CONAES. Ocupou no Ministério da Saúde o cargo de Diretora de Gestão da Educação na Saúde da Secretaria de Gestão do Trabalho e da Educação na Saúde – SGTES. Foi Diretora de Programas e Secretária Substituta da SGTES, Vice-Presidente do Conselho Brasileiro de Telemedicina e Telessaúde – CBTMS e Diretora de Relações Institucionais da Associação Brasileira de Telemedicina e Telessaúde – ABTMS. Atualmente é membro do Comitê Assessor da Rede Universitária de Telemedicina – RUTE e do Grupo de pesquisa Saúde, Tecnologia e Educação – SAITE (CNPq), além de líder do Grupo de Pesquisa Novas Tecnologias aplicadas à Saúde Digital (CNPq). É coordenadora adjunta do Núcleo de Apoio à Pesquisa em Políticas Públicas para a Metrópole – NAP Escola da Metrópole e coordenadora da Estação Multicêntrica de Estudos e Tendências de Recursos Humanos em Saúde FOUSP – ABENO. É uma das representantes do Brasil na Red de Lideres por la Primera Infância e incluída no Latin America Top 10.000 Scientists/2021. Atua desde de 2023 no Ministério da Saúde como Secretária de Informação e Saúde Digital. Bolsista Produtividade Desenvolvimento Tecnológico e Extensão Inovadora 2. Linhas de pesquisa: Educação Superior na Saúde, Educação Permanente na Saúde, Força de Trabalho em Saúde, Políticas Públicas de Educação e de Saúde, Primeira Infância, Telessaúde, Teleodontologia, Educação Mediada por Tecnologias, Políticas Públicas.





Ana Emilia Figueiredo de Oliveira

Professora titular da Universidade Federal do Maranhão – UFMA e líder do Grupo de Pesquisa Saúde, Inovação, Tecnologia e Educação – SAITE (CNPq/UFMA). Possui graduação em Odontologia pela Universidade Federal Fluminense – UFF, especialização em Gestão de Sistemas e Serviços de Saúde pela UFMA, mestrado e doutorado em Radiologia Odontológica pela Universidade Estadual de Campinas – UNICAMP e pós-doutorado, como professora visitante, pela University of North Carolina

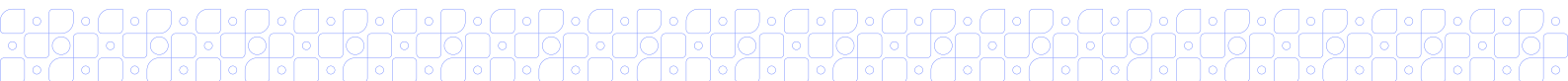
– UNC, em Chapel Hill, nos Estados Unidos da América. Atuou como coordenadora da Universidade Aberta do SUS – UNA-SUS/UFMA de novembro de 2009 a abril de 2024, diretora na Diretoria de Tecnologias na Educação – DTED/UFMA de novembro de 2019 a novembro de 2023 e presidente da Associação Brasileira de Telemedicina e Telessaúde – ABTMS entre 2015 e 2017. Foi homenageada pelo Ministério da Saúde, em 2024, na exposição “Dona Ivone Lara e Mulheres da Saúde” (tema Inovação e Tecnologias), pelo reconhecimento de sua contribuição para o desenvolvimento de tecnologias educacionais e pela promoção da saúde no Brasil.

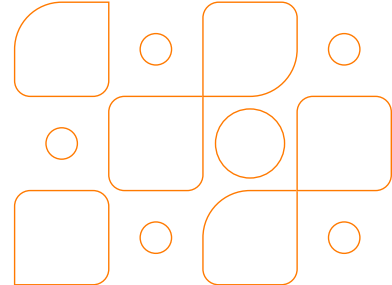


Deysianne Costa das Chagas

Graduada em Nutrição, mestre e doutora em Saúde Coletiva pela Universidade Federal do Maranhão – UFMA, além de especialista em Gestão de Políticas de Saúde Informadas por Evidência pelo Instituto de Ensino e Pesquisa do Hospital Sírio-Libanês de São Paulo e em Docência na Saúde pela Universidade Federal do Rio Grande do Sul – UFRGS. Professora assistente do Departamento de Ciências Fisiológicas da UFMA, professora permanente do Programa de Pós-Graduação em Rede da Rede Nordeste de

Formação em Saúde da Família – RENASF/UFMA, docente convidada do Programa de Pós-Graduação em Saúde Coletiva da UFMA e coordenadora-adjunta da Universidade Aberta do SUS – UNA-SUS/UFMA. Integra o grupo de pesquisa Saúde, Inovação, Tecnologia e Educação – SAITE e o Grupo de Pesquisa em Saúde Coletiva. Áreas de atuação: Saúde Digital, Tecnologia e Inovação em Educação na Saúde e Educação na Saúde.

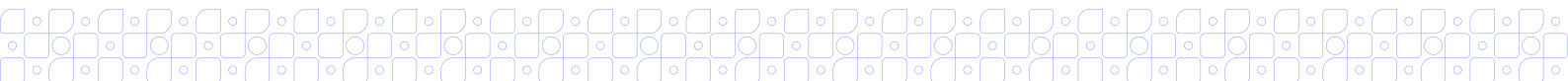


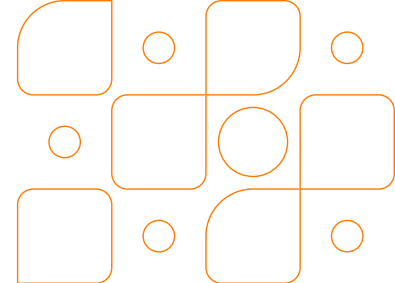


Elza Bernardes Ferreira

Possui graduação em Odontologia pela Universidade Federal do Maranhão – UFMA, doutorado em Ciências Médicas pela Universidade do Estado do Rio de Janeiro – UERJ e mestrado em Ciências da Saúde (UFMA), além das especializações em: Radiologia Odontológica pela Faculdade São Leopoldo Mandic – SLMANDIC; Saúde da Família pela Universidade Potiguar – UNP; Gestão de Sistemas e Saúde pela UFMA; Educação a Distância pelo Serviço Nacional de Aprendizagem Comercial

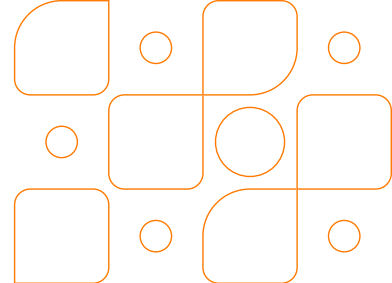
– Senac; Gestão do Trabalho e Educação na Saúde pela Universidade Federal do Rio Grande do Norte – UFRN; e Educação Digital pela Universidade do Estado da Bahia – UNEB. Atualmente, é docente efetiva da UFMA e coordenadora-geral da Universidade Aberta do SUS – UNA-SUS/UFMA. É membro da Associação Brasileira de Telemedicina e Telessaúde – ABTMS e compõe o Grupo de pesquisa Saúde, Tecnologia e Educação – SAITE (CNPq/UFMA). São áreas de sua atuação: Educação a Distância, Tecnologia e Inovação em Educação na Saúde, Imaginologia Odontológica, Atenção Primária em Saúde e Metodologias Inovativas em EaD.





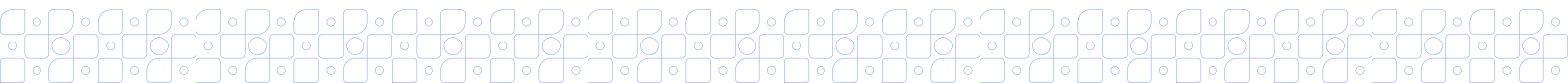
Lista de figuras

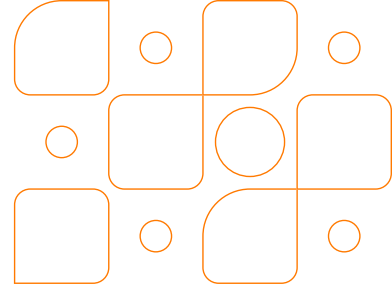
Figura 01. Tecnologias digitais em saúde	21
Figura 02. Integração de tecnologias de Saúde Digital no sistema de saúde com a contribuição de diferentes partes interessadas	22
Figura 03. Cibersegurança e proteção legal	26
Figura 04. Capa do Manual Instrutivo do Programa SUS Digital	27
Figura 05. Principais metas do Programa SUS Digital	28
Figura 06. Etapas do Programa SUS Digital	29
Figura 07. Acesso à internet no Brasil	35
Figura 08. Principais objetivos da política de privacidade	38
Figura 09. Diálogo usualmente aplicado na coleta de dados pessoais por estabelecimentos de saúde	47
Figura 10. Ciclo de vida dos dados pessoais	48
Figura 11. Principais ativos organizacionais relacionados ao ciclo de vida dos dados pessoais	51
Figura 12. Ciclo de vida dos dados pessoais	53
Figura 13. O caso do atendimento do Sr. José em uma Unidade Básica de Saúde – UBS	54
Figura 14. Aplicação prática das fases do ciclo de vida dos dados pessoais	51
Figura 15. Mapeamento e sinalização das medidas de segurança implementadas	56
Figura 16. Rede Nacional de Dados em Saúde	59
Figura 17. Teste diagnóstico durante pandemia de covid-19	60
Figura 18. Gov.br	61



Lista de quadros

Quadro 01. Normas relativas à informação em saúde	23
Quadro 02. Eixos de indicadores para elaboração do Plano de Ação	30
Quadro 03. Principais conceitos presentes na LGPD	43
Quadro 04. Relação entre o ciclo de vida e o tratamento de dados pessoais descrito na LGPD	49
Quadro 05. Conceitos dos principais ativos organizacionais relacionados ao ciclo de vida dos dados pessoais	52





Lista de abreviaturas e siglas

A

ABNT. Associação Brasileira de Normas Técnicas

ANPD. Autoridade Nacional de Proteção de Dados

C

CICIS. Comissão Intersetorial de Comunicação e Informação em Saúde

CIINFO. Comitê de Informação de Informática em Saúde

CNES. Cadastro Nacional de Estabelecimento de Saúde

CNS. Cartão Nacional de Saúde

CNS. Conselho Nacional de Saúde

CPF. Cadastro de Pessoa Física

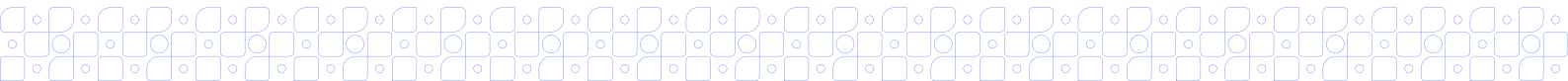
D

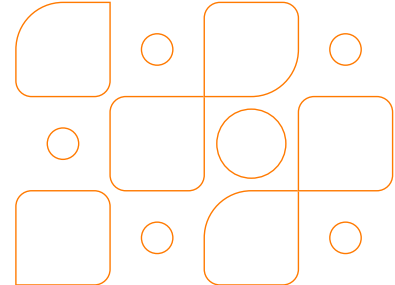
DataSUS. Departamento de Informática do Sistema Único de Saúde

Dataprev. Empresa de Processamento de Dados da Previdência Social

F

FNS. Fundo Nacional de Saúde





IA. Inteligência Artificial

ICP-Brasil. Infraestrutura de Chaves Públicas Brasileira

INMSD. Índice Nacional de Maturidade em Saúde Digital

IoT. Do inglês *Internet of Things*: Internet das Coisas

ISO/IEC. Do inglês *International Organization for Standardization / International Electrotechnical Commission*: Organização Internacional para Padronização / Comissão Eletrotécnica Internacional



LGPD. Lei Geral de Proteção de Dados Pessoais



MS. Ministério da Saúde

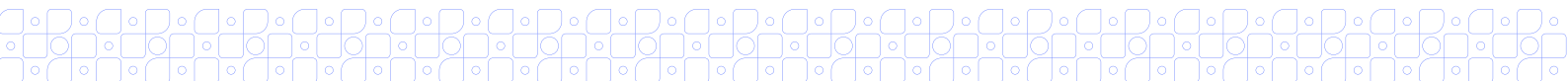


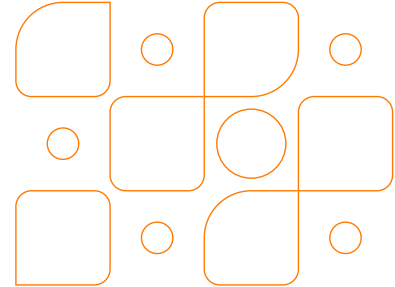
NBRs. Normas Brasileiras



OMS. Organização Mundial da Saúde

OPAS. Organização Pan-Americana da Saúde





PEC. Prontuário Eletrônico do Cidadão

PEP. Prontuário Eletrônico do Paciente

PNAD. Pesquisa Nacional por Amostra de Domicílios

PNIIS. Política Nacional de Informação e Informática em Saúde



RAS. Rede de Atenção à Saúde

RES. Registros Eletrônicos de Saúde

RGPD. Regulamento Geral de Proteção de Dados

RIPSA. Rede Integrada de Informações para a Saúde

RIPSA. Rede Interagencial de Informações para a Saúde

RNDS. Rede Nacional de Dados em Saúde



SIS. Sistemas de Informação em Saúde

SISP. Sistema de Administração dos Recursos de Tecnologia da Informação

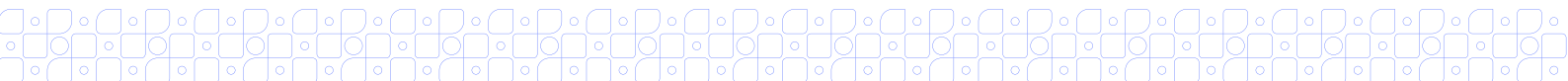
SNIS. Sistema Nacional de Informações em Saúde

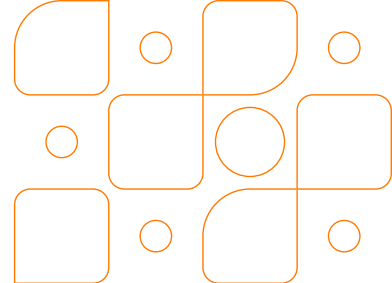
SUS. Sistema Único de Saúde



UBS. Unidades Básicas de Saúde

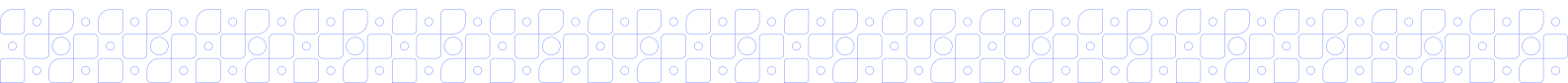
UFBA. Universidade Federal da Bahia

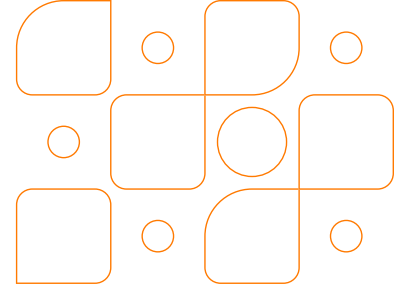




Sumário

Apresentação	19
1. Regulação da Saúde Digital no Brasil	20
1.1 Política Nacional de Informação e Informática à Saúde – PNIIS	25
1.2 Programa SUS Digital	27
2. Lei Geral de Proteção de Dados Pessoais (LGPD)	34
2.1 Conceitos importantes para LGPD	42
2.2 Proteção de Dados Pessoais	46
2.3 Ativos Organizacionais e a sua relação com o Ciclo de Vida dos Dados Pessoais	51
3. Rede Nacional de Dados em Saúde e Segurança da Informação	58
Considerações finais	63
Referências	64





Apresentação

Olá, prezado(a) estudante!

Você já parou para pensar em como os dados de saúde são protegidos e em quem garante essa segurança no ambiente digital? Como as normas e políticas públicas brasileiras vêm orientando o uso seguro e ético das tecnologias digitais em saúde?

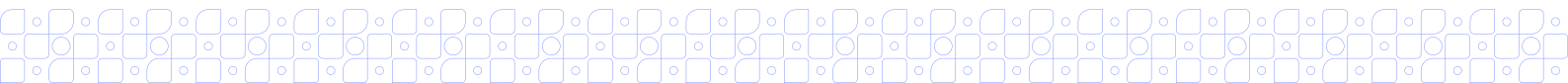
A rápida expansão tecnológica vivenciada nos últimos anos facilitou o acesso às informações, viabilizando o compartilhamento dos dados em nível mundial e transformando profundamente as rotinas laborais dos trabalhadores do setor da saúde. Essa transformação digital, entretanto, veio acompanhada de grandes desafios, que englobam não apenas a segurança e privacidade dos dados de saúde mas também a criação de ambientes digitais mais éticos.

Dessa forma, neste livro você encontrará uma introdução sobre a regulação da Saúde Digital no Brasil, seguida da discussão da Lei Geral de Proteção de Dados – LGPD, com foco na análise de princípios de segurança da informação e privacidade de dados. Além disso, serão abordados aspectos relacionados à preservação de dados pessoais e confidenciais, à segurança e à ética no compartilhamento dessas informações, bem como à Rede Nacional de Dados em Saúde – RNDS, enfatizando a proteção de dados pessoais.

Almejamos que você compreenda os principais conceitos e regulamentações sobre segurança da informação e proteção de dados pessoais no contexto da Saúde Digital. Assim, buscamos favorecer o desenvolvimento de uma visão crítica sobre a segurança da informação em suas diferentes vertentes, partindo da discussão de conceitos fundamentais, estudos de casos e experiências exitosas brasileiras. Com isso, esperamos estimular uma reflexão integrada entre teoria e prática, considerando o cenário atual, marcado por rápidas e constantes transformações digitais.

Vamos nos aprofundar nessa discussão?

Bons estudos!



1. Regulação da Saúde Digital no Brasil

Antes de avançarmos especificamente para a temática da segurança da informação, é fundamental compreendermos o contexto mais amplo da Saúde Digital no Brasil — já que ambas as áreas estão intrinsecamente conectadas.

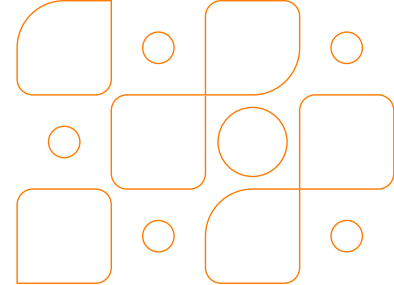


PARA REFLEXÃO

Você já refletiu sobre como as tecnologias digitais transformaram o cuidado em saúde e sobre as regras que garantem que esse processo seja realizado de maneira ética e segura?

No decorrer deste livro, convidamos você a entender os principais marcos regulatórios da Saúde Digital no Brasil e a compreender como eles asseguram a ética, a segurança e a inovação no cuidado em saúde.

A Saúde Digital tem se consolidado como um campo de conhecimento emergente (Fagherazzi *et al.*, 2020). Com a rápida integração de novas soluções tecnológicas,



como a Inteligência Artificial – IA, os dispositivos vestíveis e a telemedicina, ampliam-se os desafios contemporâneos relacionados ao processo de regulamentação, indispensável para garantir a segurança e a qualidade dos serviços prestados no setor da saúde em nível mundial.

O amplo espectro de utilização das tecnologias digitais envolve um complexo processo de estabelecimento de normas legais, éticas e técnicas. Essas normas funcionam como uma rede de proteção com o objetivo de garantir o uso seguro de dados e informações, estruturando um ecossistema informacional integrado, íntegro e seguro. Nessa conjuntura, torna-se urgente evidenciar o papel dos órgãos regulatórios (Yeung *et al.*, 2023).

Diante do cenário de ampliação do uso de tecnologias no setor da saúde, torna-se imprescindível garantir a segurança da informação, assegurando a confidencialidade, a integridade e a disponibilidade dos dados sensíveis dos pacientes. Na prática, o que se tem observado é que as iniciativas de estruturação regulatória ocorrem de forma assimétrica em escala internacional, com uma diversidade de legislações e abordagens diferentes.

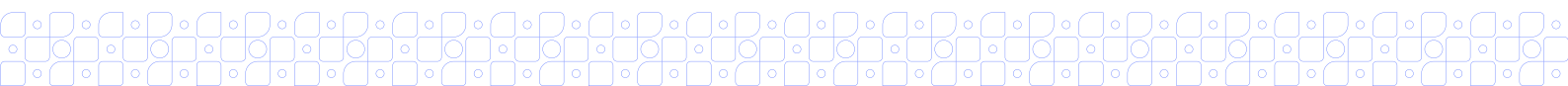
Figura 01. Tecnologias digitais em saúde

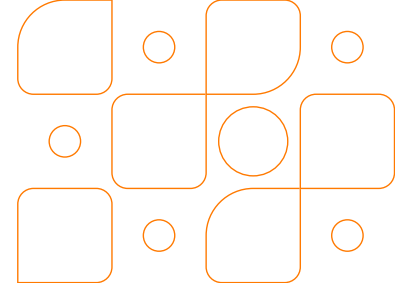


Fonte: Freepik, ©2010–2025.

Nessa perspectiva, Yeung *et al.* (2023) apontam que as orientações emitidas por órgãos internacionais, como a Organização Mundial da Saúde – OMS, podem ser consideradas estratégias-chave na tentativa de priorizar questões críticas, como a:

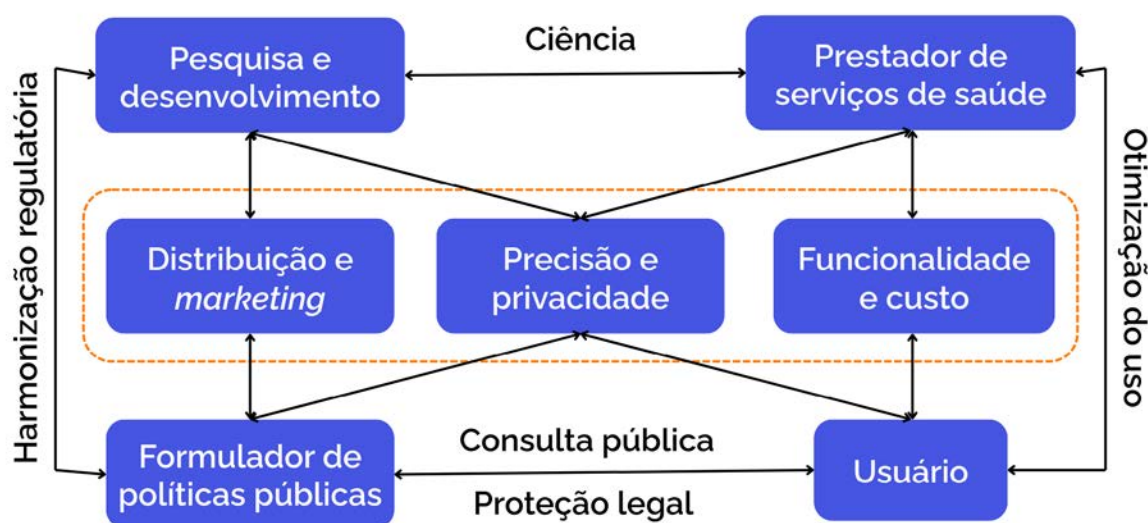
- Privacidade;
- Segurança dos dados;
- Ética;
- Segurança do paciente;
- Abordagem centrada no usuário;
- Validação clínica; e
- Harmonização regulatória.





Dessa forma, a regulação da Saúde Digital requer a colaboração entre diferentes partes interessadas, incluindo cooperações técnicas entre os governos e a participação da sociedade civil e de órgãos regulatórios, conforme esquematizado na figura a seguir:

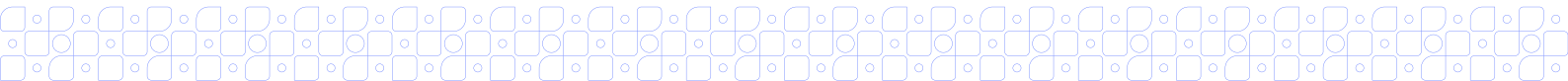
Figura 2 - Integração de tecnologias de Saúde Digital no sistema de saúde com a contribuição de diferentes partes interessadas



Fonte: UNA-SUS/UFMA, 2025. Adaptado de Yeung *et al.* (2023, p. 08).

No cenário brasileiro, a regulamentação da Saúde Digital pode ser compreendida a partir das iniciativas do Ministério da Saúde – MS na elaboração de um conjunto de documentos que formam o arcabouço legal, dando sustentação às ações desenvolvidas no âmbito da transformação digital no Sistema Único de Saúde – SUS.

Como vimos, a segurança dos dados assume papel estratégico. Isso acontece porque a regulação da Saúde Digital tem avançado no estabelecimento de diretrizes que definem requisitos básicos para a utilização ética, segura e responsável das informações, assegurando a confidencialidade dos dados sensíveis dos usuários do SUS.

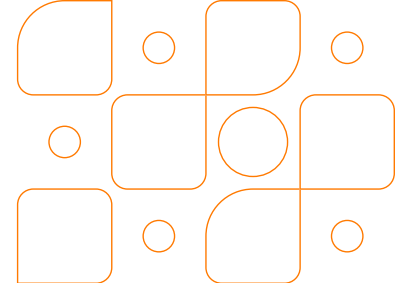


A adoção de uma abordagem integral e a revisão contínua das práticas de segurança da informação exigem o desenvolvimento de legislações que previnam falhas e evitem o vazamento de dados pessoais dos usuários.

Para tanto, é necessário esclarecer que todas as normativas desenvolvidas até hoje, que tratam sobre a regulamentação da Saúde Digital e que têm relação com segurança dos dados, tiveram suas bases legais construídas em documentos anteriores. Rachid *et al.* (2023) apontam que, o que chamamos de Saúde Digital se origina nos anos 1990, conforme apresentado no quadro abaixo:

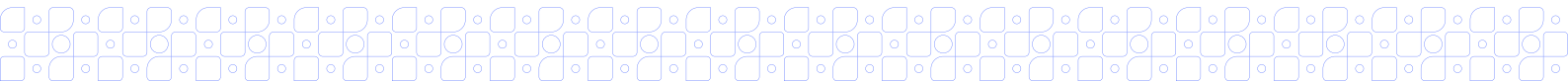
Quadro 01. Normas relativas à informação em saúde

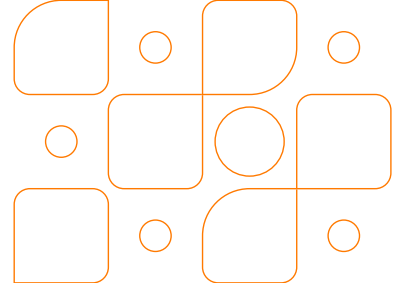
Ano	Ato formativo	Descrição
1990	Lei 8.080/1990 Lei Orgânica da Saúde	Art. 47 - estabelece que o Ministério da Saúde, em articulação com os níveis estaduais e municipais do SUS, organizará, no prazo de dois anos, um Sistema Nacional de Informações em Saúde – SNIS.
1991	Decreto 100/1991	Cria o Departamento de Informática do SUS – DataSUS como parte da Fundação Nacional de Saúde – FNS, a partir da incorporação de bens da Empresa de Processamento de Dados da Previdência Social – Dataprev.
1996	Portaria GM/MS 2.390/1996	Institui a Rede Integrada de Informações para a Saúde – RIPSA.
1998	Resolução CNS 227/1998	Cria a Comissão Intersetorial de Comunicação e Informação em Saúde – CICIS.
2002	Portaria GM/MS 1.919/2002	Cria a Rede Interagencial de Informações para a Saúde – RIPSA.
2004	Relatório da 12ª Conferência Nacional de Saúde	Contribui para a publicação da Política Nacional de Informação e Informática em Saúde – PNIIS após discussão e recomendações da 12ª Conferência Nacional de Saúde.



2005	Resolução CNS 349/2005	Reforma a CICIS.
2006	Portaria GM/MS 495/2006	Determina a reestruturação da RIPSA.
2009	Portaria GM/MS 2.466/2009	Cria o Comitê de Informação de Informática em Saúde – CIINFO/MS.
2011	Decreto 7.579/2011	Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISPA a fim de definir a política de gestão de recursos de tecnologia da informação do poder executivo federal.
	Portaria GM/MS 2.072/2011	Reformula o CIINFO/MS.
2015	Portaria GM/MS 589/2015	Institui a PNIIS.
2017	Portaria de Consolidação 1/2017	Consolida as normas sobre os direitos e deveres dos usuários da saúde, além da organização e do funcionamento do SUS.
2019	Decreto 9.795/2019	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Saúde, criando o Departamento de Saúde Digital.
2020	Decreto 10.332/2020	Institui a Estratégia de Governo Digital para o período de 2020 a 2022.
	Portaria GM/MS 1.434/2020	Institui o Programa Conecte SUS e altera a Portaria de Consolidação GM/MS 1/2017 para instituir a Rede Nacional de Dados em Saúde – RNDS.
2021	Portaria GM/MS 1.768/2021	Aprova a PNIIS.
2023	Portaria GM/MS 3.232	Altera a Portaria de Consolidação GM/MS 5/2017 para instituir o Programa SUS Digital.

Fonte: UNA-SUS/UFMA, 2025. Adaptado de Rachid *et al.* (2023).





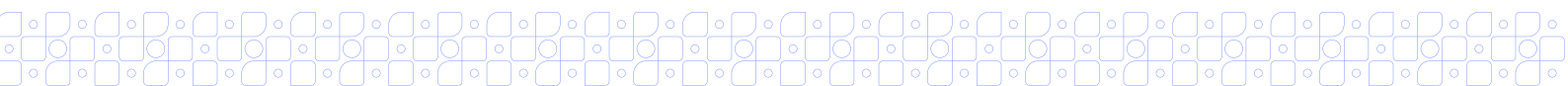
Entre todas as legislações mencionadas, merecem destaque aquelas que contribuíram para a consolidação de políticas estruturantes voltadas à consolidação da Saúde Digital no Brasil, como a PNIIS, o Programa SUS Digital e a RNDS. Todas essas iniciativas apresentam diretrizes ou princípios que dialogam com a proteção e segurança das informações em saúde.

A segurança da informação é, portanto, um eixo transversal que assegura a confidencialidade das informações sensíveis e assegura a integridade e a disponibilidade dos sistemas utilizados nos serviços de saúde. A seguir, vamos explorar, de forma mais aprofundada, como cada uma dessas políticas fortalece a segurança dos dados.

1.1 POLÍTICA NACIONAL DE INFORMAÇÃO E INFORMÁTICA À SAÚDE – PNIIS

A PNIIS foi inicialmente instituída pela Portaria GM/MS n.º 589, de 22 de maio de 2015 (Brasil, 2015), com o objetivo de promover a inovação e melhorar os processos de trabalho em saúde no SUS. Dada a intensificação da utilização das tecnologias digitais, o MS liderou os procedimentos de revisão dessa política, resultando na promulgação da Resolução n.º 659, de 26 de julho de 2021 (Brasil, 2021).

A nova regulamentação propõe a definição de princípios e diretrizes norteadoras dos Sistemas de Informação em Saúde – SIS para setores públicos e privados, mantendo a promoção da inovação e incorporando a Saúde Digital. Algumas das diretrizes, como disposto no art. 4º dessa resolução (Brasil, 2021), são:



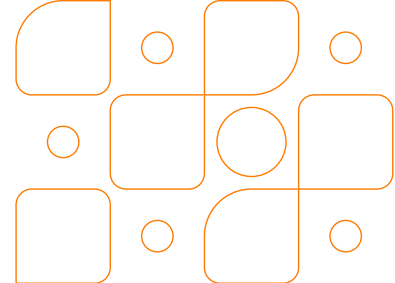


Figura 03 - Cibersegurança e proteção legal



I - coordenação nacional das ações de Saúde Digital pelo Ministério da Saúde e pelas secretarias de saúde estaduais, municipais e do Distrito Federal em seus respectivos territórios, conforme diretrizes do Plano Nacional de Saúde e da Estratégia de Governo Digital do Brasil;

II - acompanhamento periódico das ações de Saúde Digital pelo Conselho Nacional de Saúde – CNS e conselhos de saúde estaduais, municipais e distrital; [...];

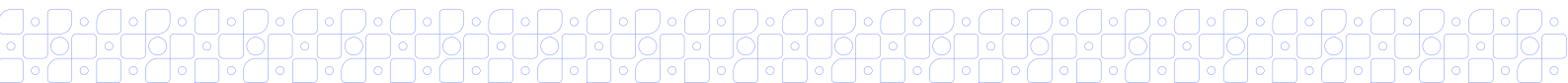
VII - fortalecimento da área de Saúde Digital nas três esferas de gestão, com apoio à organização, ao desenvolvimento e à integração da atenção, proteção, promoção, prevenção e recuperação à saúde e participação da sociedade; [...].

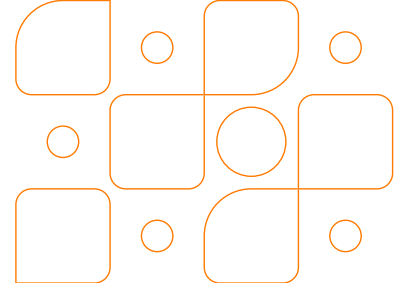
Fonte: Freepik, ©2010–2025.

Um dos pilares fundamentais da PNIIS é a segurança da informação, diretamente relacionada ao fortalecimento da transparência e ao acesso seguro e qualificado às informações em saúde pela população. O art. 2º do capítulo I da resolução determina que um dos seus princípios é a confidencialidade, a privacidade, a proteção de dados e a segurança da informação de saúde pessoal como direito de todo indivíduo (Brasil, 2021).

Em suas diretrizes, a PNIIS também dispõe sobre a implementação de mecanismos de segurança, incentivando o uso de assinaturas eletrônicas e tecnologias biométricas. As medidas de proteção devem controlar o acesso aos sistemas, aos dados e às informações em saúde, de modo a assegurar sua disponibilidade, autenticidade e integridade.

A resolução destaca, ainda, que cabe ao MS “gerir e normatizar o uso dos padrões nacionais de interoperabilidade, segurança e conteúdo semântico” (Brasil, 2021, cap. III, art. 15, inc. V). Em síntese, a PNIIS representa um marco estratégico para a modernização da segurança da informação, contribuindo para a construção de ambientes digitais mais éticos e seguros e consolidando-se como uma referência na adoção de uma maior transparência.





PARA SABER MAIS

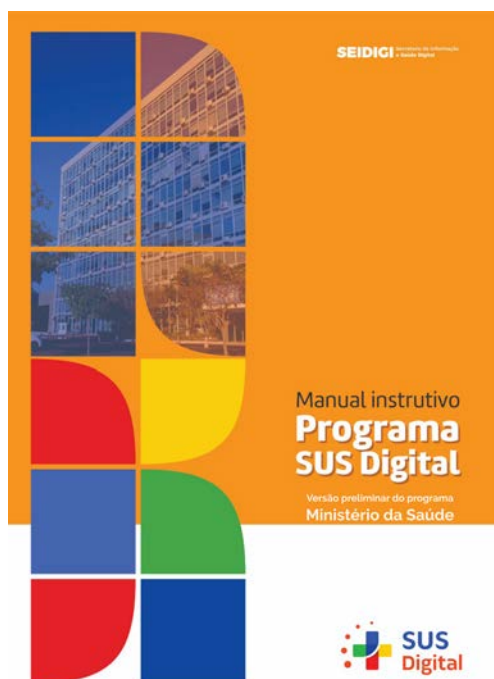
Para entender um pouco mais sobre a PNIIS, acesse:

- [Resolução n.º 659, de 26 de julho de 2021.](#)

1.2 PROGRAMA SUS DIGITAL

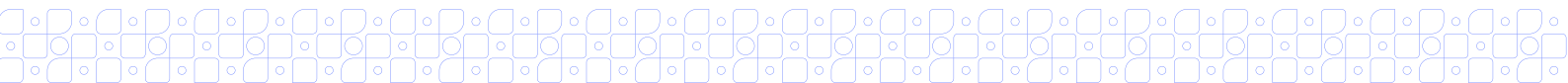
Até aqui, vimos que o conceito multifacetado de Saúde Digital já aborda a ligação entre saúde e tecnologia. Neste programa, ressaltamos ainda a importância da informação, uma vez que, para o MS, a transformação digital deve ser aplicada ao campo da saúde como um todo.

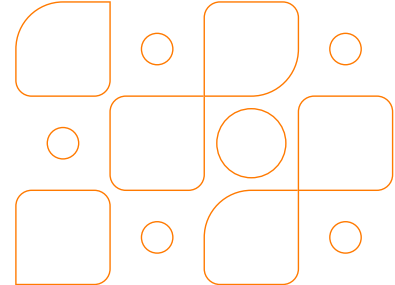
Figura 04 - Capa do Manual Instrutivo do Programa SUS Digital



O Programa SUS Digital foi lançado pela Portaria GM/MS n.º 3.232, de 1º de março de 2024, visando promover a transformação digital no âmbito do SUS. Para isso, a iniciativa propõe uma abordagem multidisciplinar, que considera a intersecção entre as áreas da saúde, a informação e a tecnologia. Dessa forma, o programa fomenta o acesso da população aos serviços de saúde e garante o cuidado integral e eficiente em todo território brasileiro (Brasil, 2024).

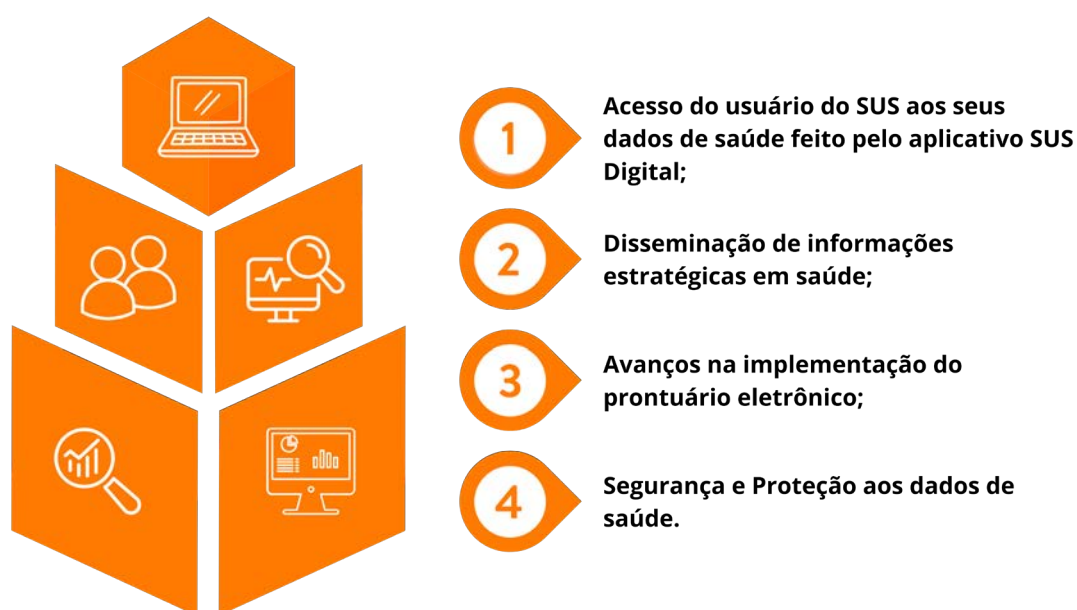
Fonte: Brasil (2024a).





Isso quer dizer que, ao incluir a vigilância em saúde, a atenção integral, a formação e a educação permanente, além de todas as esferas de gestão, a transformação digital se mostra um pilar fundamental para os processos de planejamento, monitoramento, avaliação, pesquisa, desenvolvimento e inovação em saúde, de acordo com as principais metas definidas no Programa SUS Digital (Brasil, 2024). Acompanhe-as na figura a seguir:

Figura 05. Principais metas do Programa SUS Digital



Fonte: UNA-SUS/UFMA, 2025. Adaptado de Brasil (c2025b).

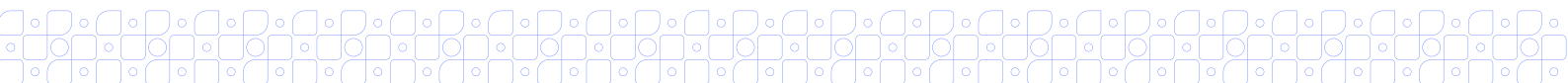
O programa ainda considera que a Saúde Digital abrange, entre outros, o uso de (Brasil, 2024):

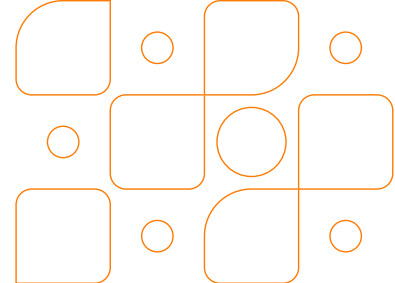
Ciências de dados;

Registros eletrônicos de saúde - RES;

Telessaúde;

Robótica;





Aplicativos móveis de saúde;

Sistemas de informação interoperáveis;

Inteligência artificial - IA;

Dispositivos vestíveis;

Medicina personalizada;

Internet das Coisas - IoT aplicados à saúde.

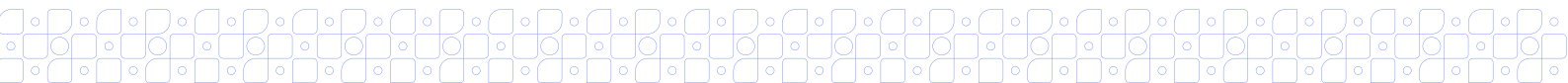
Para operacionalização dessa iniciativa, foram propostas três etapas:

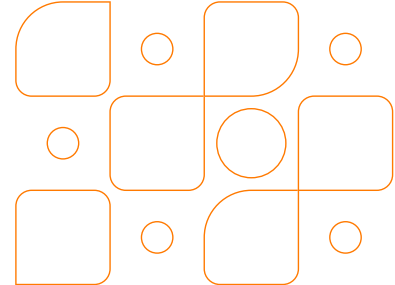
Figura 06. Etapas do Programa SUS Digital



Fonte: UNA-SUS/UFMA, 2025.

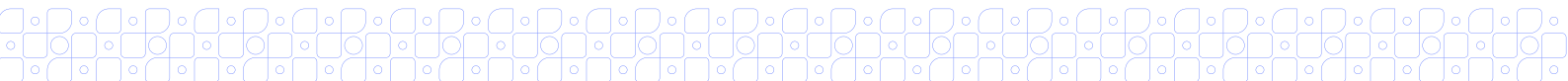
Destacamos ainda que a elaboração do Plano de Ação, além de descrever objetivos claros, metas quantificáveis com valores estabelecidos e cronogramas de execução, considerou outros aspectos, incluindo a inserção de indicadores em pelo menos um dos eixos apresentados no quadro a seguir:

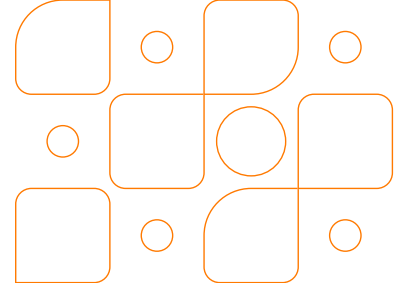




Quadro 02. Eixos de indicadores para elaboração do Plano de Ação

Eixo 1	Cultura de Saúde Digital, formação e educação permanente em saúde I - Formação e educação permanente em Saúde Digital; II - Fortalecimento do ecossistema de Saúde Digital, por meio da promoção de inovação aberta, da estruturação de rede colaborativa para o compartilhamento de experiências, conhecimentos, cultura e práticas entre os atores e da cocriação com cidadãos e sociedade civil organizada; III - Fortalecimento do uso de estudos e evidências para incorporação de tecnologias digitais em saúde; IV - Fomento à cultura da proteção de dados pessoais e sensíveis de saúde; e V - Qualificação dos registros em saúde.
Eixo 2	Soluções tecnológicas e serviços de Saúde Digital no âmbito do SUS I - Apoio à informatização do SUS e adoção de Prontuários Eletrônicos que atendam aos padrões de interoperabilidade da RNDS; II - Suporte à melhoria da infraestrutura para os sistemas digitais e de conectividade; III - Fortalecimento dos mecanismos de segurança de acesso aos sistemas, dados e informações de saúde; IV - Indução da estruturação e do funcionamento de soluções tecnológicas e serviços de Saúde Digital no âmbito dos estabelecimentos e serviços de saúde; V - Fortalecimento da Saúde Digital para atendimento à saúde das populações negligenciadas, vulneráveis e isoladas geograficamente e dos povos originários; e VI - Ampliação da oferta de telemedicina e Telessaúde no âmbito do SUS, em território nacional.





Eixo 3

Interoperabilidade, análise e disseminação de dados e informações de saúde

I - Promoção da interoperabilidade de dados de saúde com a RNDS;

II - Gestão e governança no compartilhamento de dados de saúde;

III - Elaboração de estudos técnicos, diretrizes e protocolos, análise e disseminação de dados para subsidiar estratégias de Saúde Digital e inovação em saúde;

IV - Padronização dos modelos de informação nacionais, bem como dos vocabulários e das terminologias em saúde;

V - Promoção da disseminação de dados e informações em saúde, mantendo a confidencialidade, a privacidade, a proteção de dados e a segurança da informação de saúde pessoal; e

VI - Preservação da autenticidade, da integridade, da rastreabilidade e da qualidade da informação em saúde.

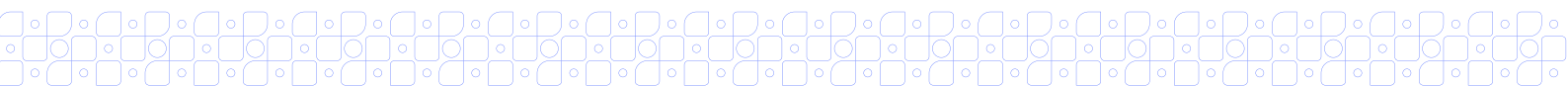
Fonte: UNA-SUS/UFMA, 2025. Adaptado de Brasil (2024a, p. 6–7).

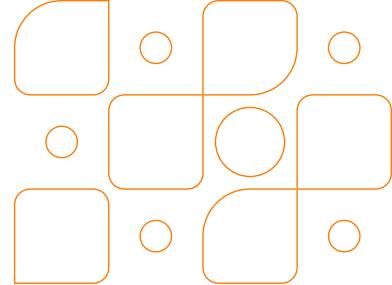
Como podemos observar, o Programa SUS Digital amplia ainda mais a necessidade de fortalecimento da segurança da informação, principalmente no âmbito do setor público. Isso ocorre em virtude da crescente ampliação da digitalização dos serviços de saúde e do uso de tecnologias, como a inteligência artificial, os Prontuários Eletrônicos, a telemedicina e os sistemas interoperáveis.



FIQUE ATENTO

A segurança da informação está diretamente relacionada ao processo de transformação digital e deve abranger a criação de ecossistemas digitais que visem à proteção da confidencialidade, da integridade e da disponibilidade das informações, principalmente dos dados sensíveis.





Nesse aspecto, a segurança da informação está presente na elaboração de indicadores que irão compor o Plano de Ação, além de ser um dos sete domínios contemplados no INMSD (Brasil, 2024b), como podemos verificar logo abaixo:

1 - Gestão e Governança em Saúde Digital;

2 - Formação e Desenvolvimento Profissional;

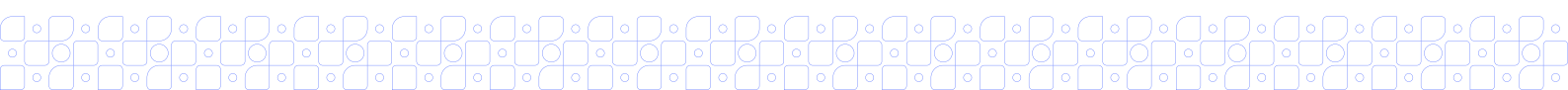
3 - Sistemas e Plataformas de Interoperabilidade;

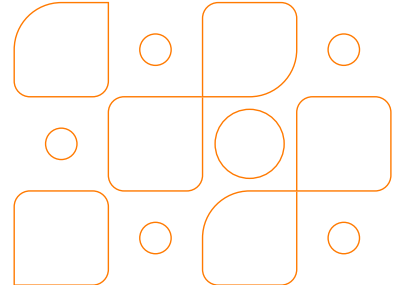
4 - Telessaúde e Serviços Digitais;

5 - Infraestrutura;

6 - Avaliação, Monitoramento e Disseminação de Informações Estratégicas;

7 - Infraestrutura e Segurança.





PARA REFLEXÃO

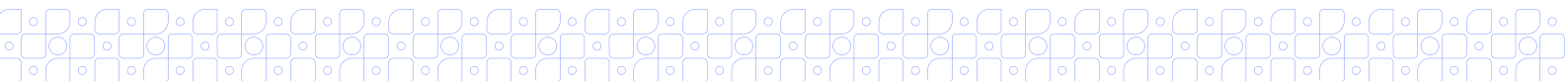
Agora é hora de refletir! Todos os 5.570 municípios, os 26 estados e o Distrito Federal aderiram ao Programa SUS Digital. Acesse o painel informativo do Ministério da Saúde:

- [Programa SUS Digital – Monitoramento da Adesão e do Diagnóstico Situacional.](#)

Após navegar pelo site, considerando a abrangência do programa, avalie:

Quais são os principais desafios para a implementação do Programa SUS Digital no seu município, especialmente no que se refere à proteção de dados e à segurança da informação?

E quais fragilidades relacionadas à segurança da informação foram identificadas no diagnóstico situacional da sua macrorregião?



2. Lei Geral de Proteção de Dados Pessoais – LGPD

Você já parou para pensar no quanto as transformações tecnológicas vivenciadas nas últimas décadas impactaram a nossa sociedade? No cerne dessas mudanças, está o rápido avanço tecnológico dos meios de comunicação. Ele é o responsável por provocar reestruturações no fluxo de compartilhamento de dados e informações, tornando-o contínuo e multidirecional a nível mundial.

Diante dessas inovações na circulação de dados e informações, se mostra importante estabelecer limites entre a vinculação dos indivíduos e as entidades públicas ou privadas. Isso se deve ao fato de que essa relação é mediada pela conectividade de softwares que operam a partir da coleta, do processamento e da divulgação de uma quantidade expressiva de dados (Anthonysamy; Rashid; Chitchyan, 2017).

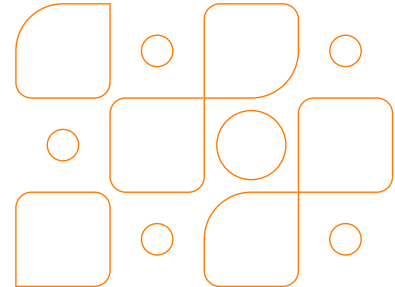


Figura 07. Acesso à internet no Brasil

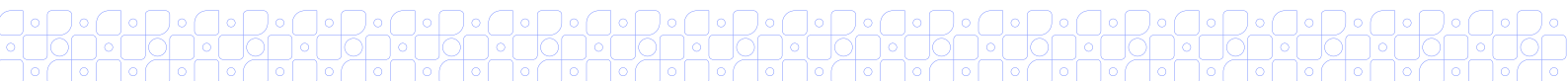


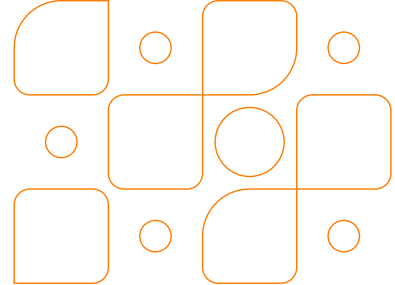
No Brasil, os dados da Pesquisa Nacional por Amostra de Domicílios – PNAD apontaram que, em 2023, havia cerca 72,5 milhões de domicílios com acesso à internet (92,5%) (Nery, 2024). Em um cenário cada vez mais conectado, os desafios relacionados à segurança da informação se ampliam, uma vez que ambientes digitais são espaços desterritorializados e podem produzir efeitos deletérios aos indivíduos, às organizações e aos governos.

Fonte: Freepik, ©2010–2025.

Dessa forma, tornou-se fundamental regulamentar legislações que promovam o intercâmbio de dados e informações de forma segura, diminuindo a exposição de indivíduos, organizações e governos a eventos adversos — como vazamento de informações sigilosas, fraudes diversas e invasão de privacidade. Nesse sentido, foi sancionada, em 2018, a Lei n.º 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD, que dispõe sobre a manipulação de dados pessoais (Brasil, 2018).

A LGPD descreve direitos, princípios e obrigações que resguardam a proteção de direitos fundamentais, como a liberdade e a privacidade, tendo sua fundamentação teórica alicerçada no Regulamento Geral de Proteção de Dados – RGPD. Desenvolvido pela União Europeia, o RGPD reúne um conjunto de elementos que protege a privacidade e assegura os direitos dos cidadãos (Santos Neto; Ishikawa; Maciel, 2021).





Consoante o texto do RGPD, a LGPD representa um marco brasileiro na proteção de dados (Oliveira; Novais, 2024). A lei estabelece uma série de princípios e diretrizes voltados ao uso à disseminação de novas tecnologias que fazem parte da contemporaneidade. Nesse sentido, os autores Santos Neto, Ishikawa e Maciel afirmam que:

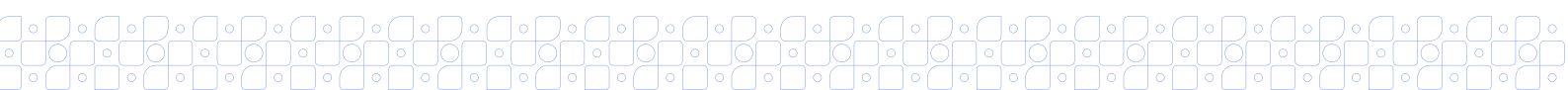


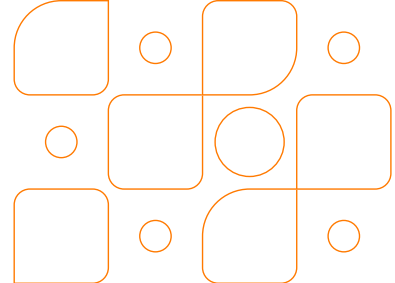
Na sociedade contemporânea, que se organiza na complexidade de um sem-número de informações, a dificuldade em se discriminar os fatos de inverdades, somada à manipulação e construção de notícias inverídicas — fake news —, a confiança vem despontando como um legitimador do cotejo de fatos e dados sobre seu objeto, com apurados e sistemáticos filtros" (Santos Neto; Ishikawa; Maciel, 2021, p. 176).

No âmbito jurídico, não há dúvidas de que a LGPD cria um conjunto de "novos conceitos", dispostos em seus 65 artigos, além de dispor de princípios, sanções e requisitos para o tratamento de dados pessoais. Garantir a conformidade legal visa evitar sanções administrativas e direciona todos os que manuseiam dados e informações a reconsiderarem reformulações de protocolos e diretrizes de uso interno à luz da LGPD (Fernandes; Nuzzi, 2022).

Com relação aos aspectos éticos, essa norma difundiu, a partir dos seus princípios, a importância de garantir a privacidade, a segurança de dados e o respeito à dignidade humana, especialmente diante da crescente quantidade de dados e informações de saúde compartilhadas por várias entidades governamentais, instituições de pesquisa e entidades privadas.

Assim, o artigo 6º da LGPD estabelece os princípios fundamentais que refletem diretamente a responsabilidade social e ética a ser adotada no tratamento de dados pessoais, conforme descrito a seguir (Brasil, 2018):





Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

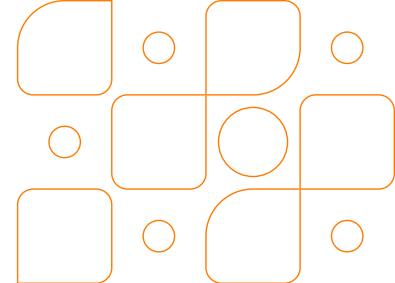
V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;



X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Assim, a LGPD reforça a importância da adoção de medidas de segurança para proteger os dados pessoais, principalmente na área da saúde, na qual os vazamentos de informações pessoais ligadas ao estado de saúde dos usuários e/ou pacientes podem resultar em discriminação, estigmatização e constrangimentos, configurando uma violação direta da privacidade e da confidencialidade.

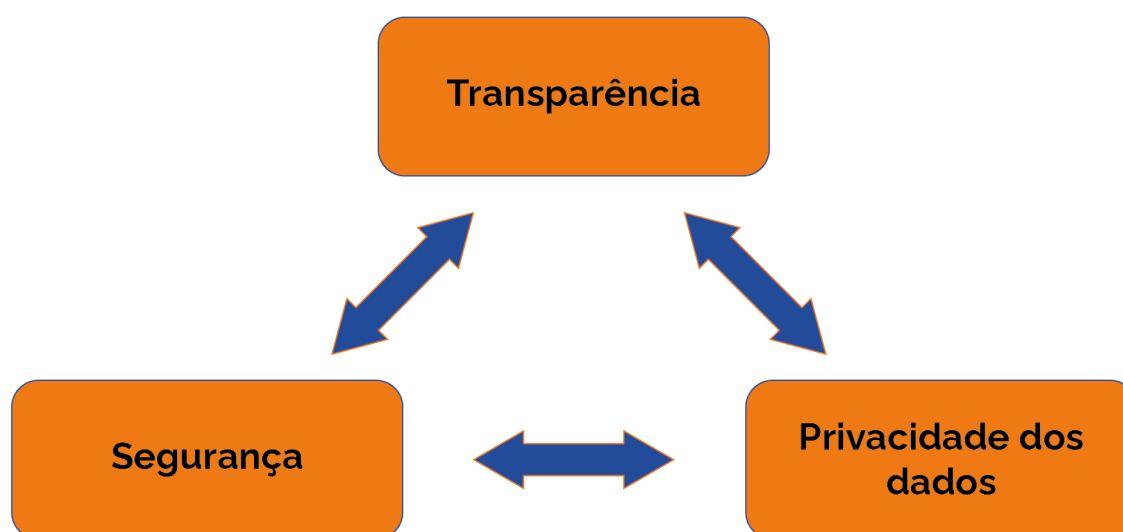


VOCÊ SABIA?

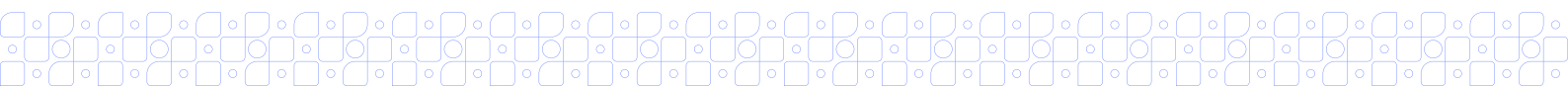
Uma política de privacidade descreve formalmente todas as diretrizes que envolvem o acesso, o armazenamento, a coleta, a avaliação, o controle, a distribuição, a eliminação, a extração e o processamento de dados durante a utilização de um sistema ou aplicativo. Sob essa ótica, seu principal objetivo é assegurar a transparência, a segurança e a privacidade das informações dos usuários.

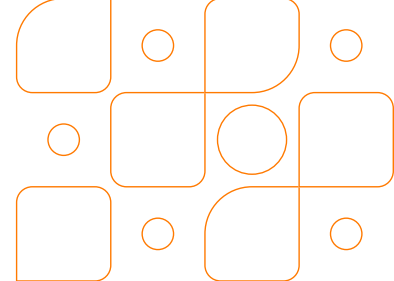
A figura a seguir demonstra a relação multidirecional entre os principais objetivos da política de privacidade:

Figura 08. Principais objetivos da política de privacidade



Fonte: UNA-SUS/UFMA, 2025.





A LGPD exige aos órgãos e às instituições a elaboração, a divulgação e a atualização constante de suas políticas de privacidade.



PARA SABER MAIS

O Meu SUS Digital disponibiliza aos seus usuários uma política de privacidade. Fique alerta, pois, ao utilizar o aplicativo, você concorda formalmente com os termos apresentados pela organização sobre o uso dos seus dados pessoais. Para conhecer a política de privacidade completa do aplicativo Meu SUS Digital e entender como os seus dados são protegidos de acessos não autorizados, vazamentos ou uso indevido, acesse o portal oficial:

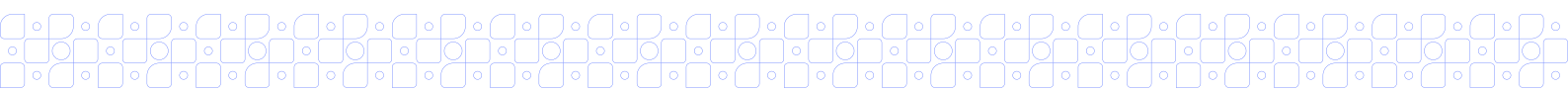
- [Política de privacidade – Meu SUS Digital](#)

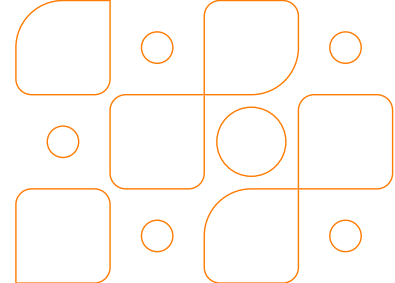
Além disso, depois desta introdução sobre a LGPD, você pode assistir ao vídeo elaborado pela Universidade Federal da Bahia – UFBA, que trata da importância dessa lei na garantia de direitos constitucionais. Para isso, acesse:

- [LGPD - Vídeo 1: Apresentação](#)

Embora, à primeira vista, a LGPD represente um marco importante para a proteção de dados, sua implementação nos serviços de saúde é um processo desafiador. Os obstáculos começam na ausência de medidas de segurança e de adaptação tecnológica e organizacional, especialmente em estabelecimentos de menor porte e em instituições públicas (Borges *et al.*, 2023).

Nesse contexto, é imprescindível a contratação de profissionais especializados, a reformulação dos processos de trabalho e a promoção de mudanças nos aspectos éticos, culturais e estruturais das organizações de saúde. Cabe enfatizar, ainda, a necessidade de capacitações contínuas em letramento digital para a prevenção da desinformação (Mendonça; Sousa, 2025).





Esses desafios também foram identificados pela Organização Pan-Americana da Saúde – OPAS. A organização enfatiza a existência de avanços ainda tímidos nas estratégias de capacitação voltadas às diretrizes de segurança da informação e à mitigação dos riscos relacionados ao fluxo de dados em saúde (OPAS, c2023).



FIQUE ATENTO

A OPAS reforça as dificuldades impostas pela construção de diversos marcos regulatórios na América Latina e a inexistência de mecanismos eficazes de monitoramento, capazes de detectar falhas de segurança nos SIS. Diante desse contexto, fica evidente que a estratégia de capacitação sobre segurança da informação ainda é incipiente, carecendo de investimentos estruturados e ações contínuas sobre a importância da segurança da informação no ambiente digital (OPAS, c2023).

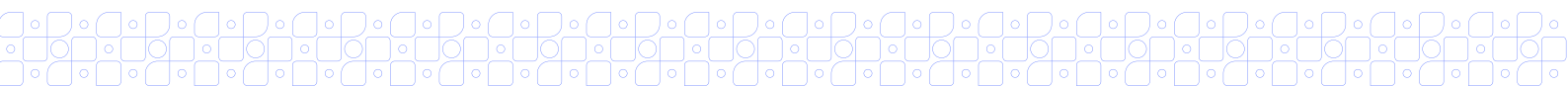
A Opas delibera que a segurança da informação é um pilar fundamental para a transformação digital em saúde, enfatizando a necessidade de incorporar esse tema de forma estratégica por meio das seguintes linhas de ação (OPAS, c2023, p. 06):

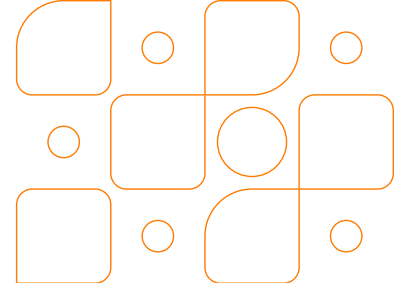
1

Contar com instrumentos normativos que regulem o tratamento e o acesso aos dados de saúde nos eixos da privacidade, sigilo e segurança da informação;

2

Estabelecer políticas públicas que incorporem um plano para a proteção e segurança dados de saúde, definindo perfis de acesso a partir das ações que o usuário deve realizar;





3

Treinar ativamente todos os atores envolvidos no fluxo de informações de saúde sobre as diretrizes de segurança informática e os riscos associados;

4

Articular mecanismos de monitoramento que permitam a detecção de incidentes de segurança nos sistemas de informação em saúde;

5

Contar com instrumentos de consentimento informado para o acesso, registro e proteção de informações confidenciais;

6

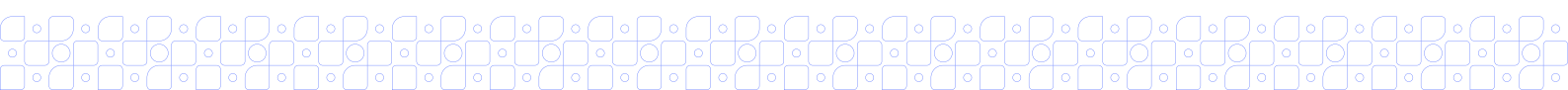
Habilitar serviços centralizados de certificação de segurança para dados de saúde confidenciais por meio de tecnologias de certificação de cadeias de blocos (blockchain), entre outros;

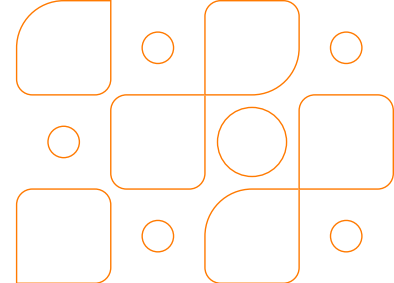
7

Adotar planos de comunicação para conscientizar a população sobre seus direitos e responsabilidades em relação aos seus dados pessoais;

8

Atualizar os regulamentos atuais de proteção de dados, muitos dos quais foram criados antes da era digital, para que incluam novos tópicos (como cibersegurança).





PARA REFLEXÃO

A LGPD é fundamental no ambiente de trabalho, pois sua aplicação se reflete nas práticas organizacionais e na cultura da proteção de dados, garantindo mais segurança, ética e transparência no tratamento de informações pessoais. Agora, convidamos você a aprofundar seus conhecimentos sobre essa lei a partir da sua realidade. Para isso, reflita:

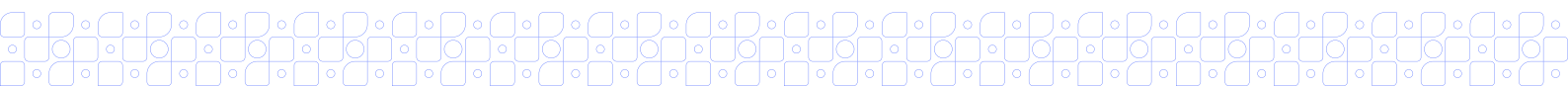
1. Os profissionais de saúde integrantes da sua equipe conhecem seus direitos e deveres relacionados à LGPD?
2. Existe algum documento que oriente a mudança da cultura organizacional voltada à proteção de dados?
3. As equipes de saúde já receberam algum treinamento sobre a LGPD?

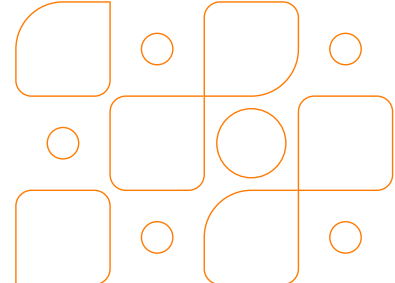
2.1 CONCEITOS IMPORTANTES DA LGPD

Vamos conhecer agora alguns conceitos que a LGPD apresenta em seu texto constitucional, que são fundamentais para compreendermos a importância das mudanças nas estruturas regulatórias de todos os órgãos e instituições que trabalham diretamente com dados e informações.

Essa lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou jurídica, seja de direito público ou privado, independentemente do meio, onde a organização está sediada ou de onde os dados se encontram — desde que a operação seja realizada no território nacional.

Dessa forma, a LGPD considera alguns conceitos apresentados no quadro a seguir:

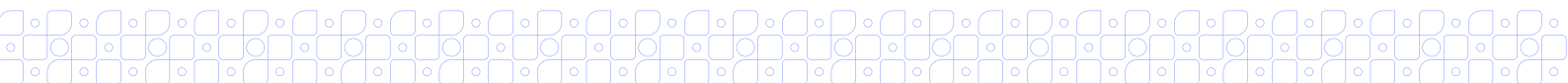


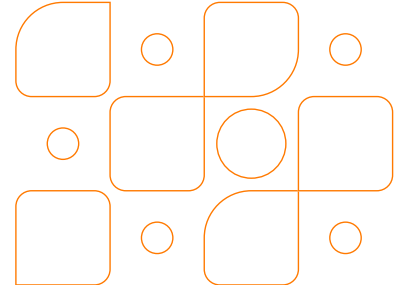


Quadro 03. Principais conceitos presentes na LGPD

Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável;
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...].

Fonte: UNA-SUS/UFMA, 2025. Elaborado a partir de dados extraídos de Brasil (2018).





Especialmente na área da saúde, todas essas definições se aplicam aos hospitais, às clínicas, aos laboratórios de análises clínicas, às operadoras de planos de saúde e aos vários sistemas de informações, como o Prontuário Eletrônico do Cidadão – PEC.

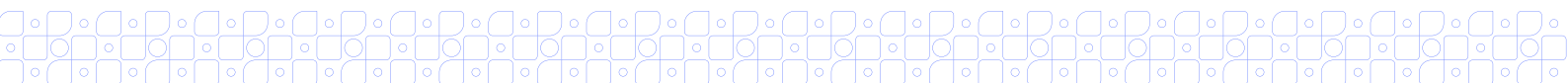
No cotidiano das instituições de saúde, diversas situações evidenciam a relevância dos conceitos relacionados à proteção de dados, tais como:

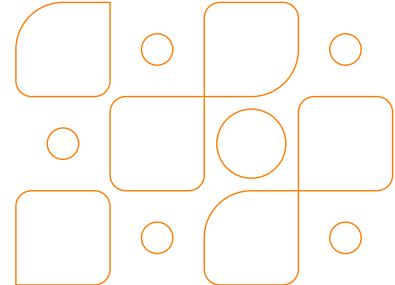
Registro inicial

Dados pessoais, como nome completo, endereço e telefone, são frequentemente requeridos pelos estabelecimentos de saúde. Nesse contexto, os usuários são reconhecidos como **titulares** dos dados, uma vez que suas informações serão coletadas, tratadas e armazenadas por unidades de saúde, sistemas de informação, operadoras de planos de saúde ou profissionais da área da saúde.

Informações específicas

A partir do registro inicial, outras informações mais específicas passam a ser coletadas, como diagnósticos médicos, uso de medicamentos, resultados de exames, prontuários e laudos. Além disso, os **dados anonimizados** são amplamente utilizados na área da saúde para realização de pesquisas acadêmicas. Eles podem ser classificados como variáveis demográficas — que envolvem idade, sexo, raça, estado civil e nível de escolaridade — e variáveis clínicas — que se referem à incidência e à prevalência de doenças.





Controle dos dados

O **controlador** é a pessoa, física ou jurídica, do setor público ou privado, responsável por tomar as decisões sobre o tratamento dos dados pessoais. Dessa forma, o controlador determina quais dados serão coletados, qual será a finalidade da coleta e por quanto tempo as informações serão armazenadas. Na área da saúde, as secretarias, as clínicas e as operadoras de planos de saúde podem atuar como controladoras.

Operacionalização dos dados

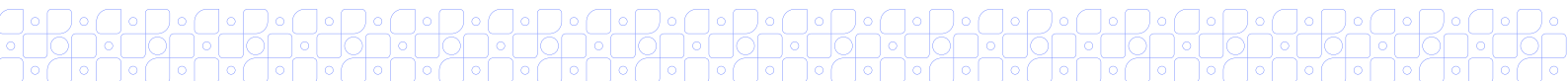
O **operador** é o responsável por realizar o tratamento de dados pessoais em nome do controlador, podendo ser uma pessoa natural ou jurídica, de direito público ou privado. Ou seja, empresas terceirizadas, como laboratórios, clínicas e consultorias especializadas (na área de tecnologia) podem exercer função de operadoras.

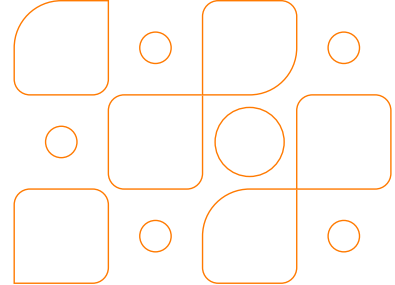
Existem situações em que o controlador também exerce a função de operador, pois, além de tomar as decisões sobre o tratamento de dados pessoais, ele também executa diretamente esse tratamento. Um exemplo disso é o aplicativo Meu SUS Digital, no qual o Ministério da Saúde atua simultaneamente como controlador e operador dos dados.



FIQUE ATENTO

Diariamente, compartilhamos nossos dados com empresas e instituições do setor de saúde. Por isso, é indispensável que todo usuário adote uma postura ativa na proteção dessas informações, prevenindo acessos indevidos e possíveis vazamentos de credenciais.





Assim, é importante reforçar práticas recomendadas em relação à segurança da informação. Confira algumas orientações importantes:

As senhas devem ser mantidas em total sigilo, evitando qualquer forma de exposição ou compartilhamento;

Quando os aplicativos oferecerem a opção de verificação em duas etapas, ative esse recurso para aumentar a segurança, visto que ele funciona como uma camada extra de proteção;

Evite reutilizar senhas;

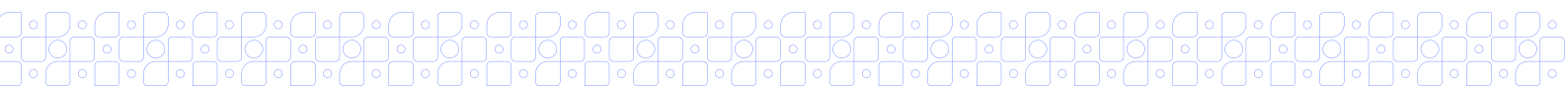
Use uma combinação de letras maiúsculas e minúsculas, números e símbolos durante a criação de senhas — evite senhas óbvias, como repetições do tipo “12345678” e números pessoais relacionados a telefones ou datas de aniversário;

Guarde suas senhas com segurança, não as salve no navegador ou em locais de fácil acesso; e

Troque suas senhas periodicamente, bem como em casos de vazamento ou uso de dispositivos infectados por vírus.

2.2 PROTEÇÃO DE DADOS PESSOAIS

A coleta e o processamento de dados, especialmente os pessoais, são realizados para atender a uma finalidade específica, como podemos observar no exemplo a seguir:



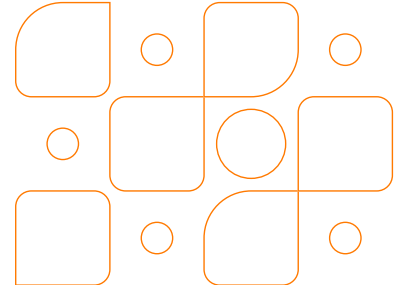
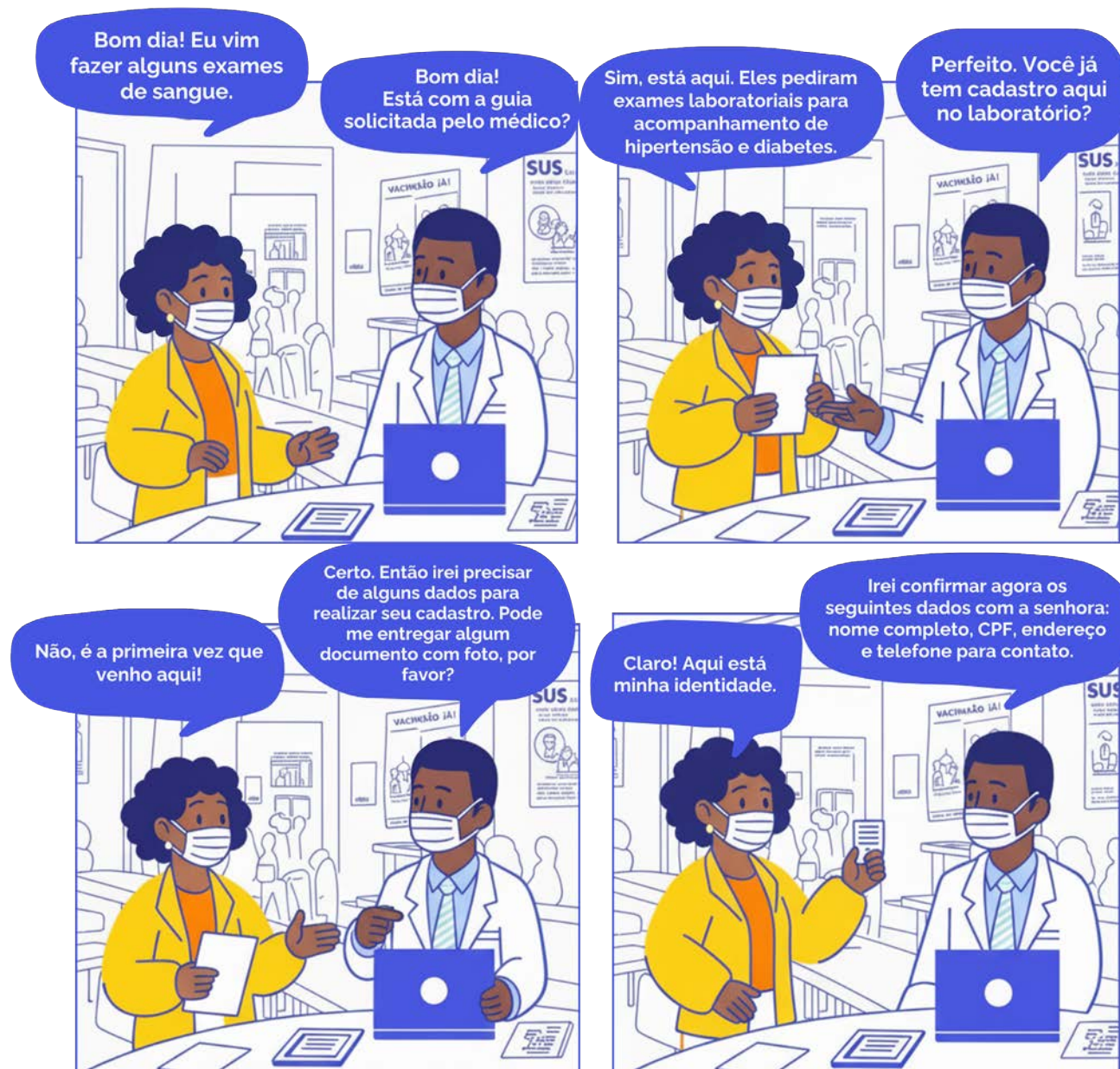
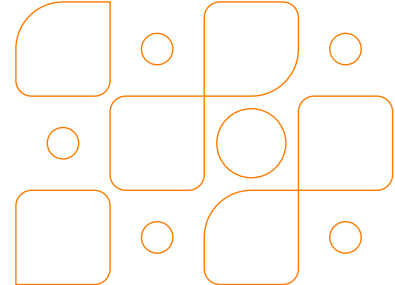


Figura 09. Diálogo usualmente aplicado na coleta de dados pessoais por estabelecimentos de saúde



Fonte: Imagem gerada com auxílio do Gemini 2.5 Flash Image. Google, 2025.

A partir desse diálogo entre uma cliente e um funcionário de um laboratório de análises clínicas, conseguimos observar que houve a coleta de dados considerados pessoais. O laboratório de análises clínicas precisa, então, identificar quais tipos de dados estão sob seu gerenciamento — isso também se aplica a outros órgãos e instituições da área da saúde.



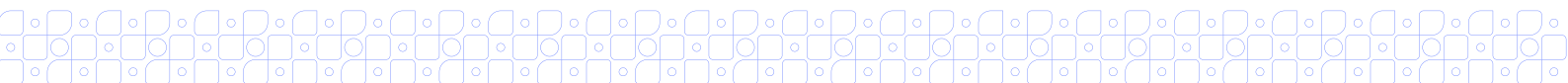
Dessa forma, é fundamental que os profissionais e as instituições compreendam o ciclo de vida dos dados pessoais. Esse ciclo corresponde a uma espécie de parametrização organizada em fases, que contempla a coleta, a retenção, o processamento, o compartilhamento e a eliminação de dados (Brasil, 2020), como indica a figura abaixo:

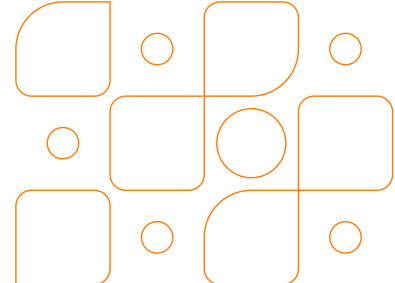
Figura 10. Ciclo de vida dos dados pessoais



Fonte: UNA-SUS/UFMA, 2025. Elaborado a partir de dados extraídos de Brasil (2020).

A gestão segura e eficiente das informações coletadas e utilizadas pelos serviços de saúde, tem correspondência direta com as operações realizadas no ciclo de vida dos dados. Do artigo 5º da LGPD, é importante destacarmos a definição de tratamento de dados:





Art. 5º Para os fins desta Lei, considera-se:

[...]

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração [...]” (Brasil, 2018).

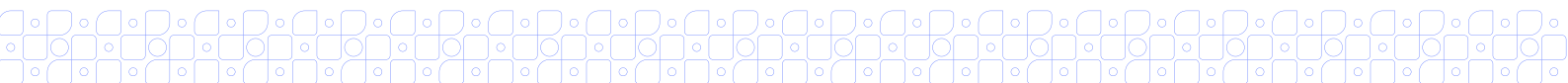
Conforme podemos perceber, existe uma correlação entre as etapas do ciclo de vida e o conceito de tratamento de dados pessoais definido pela LGPD, como demonstra o quadro a seguir:

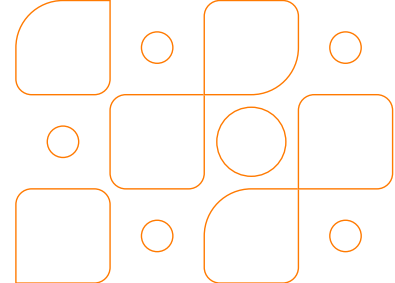
Quadro 04. Relação entre o ciclo de vida e o tratamento de dados pessoais descrito na LGPD

Fases do ciclo de tratamento	Operações de tratamento – LGPD, Art. 5º, X
01 - Coleta	Coleta, produção, recepção;
02 - Retenção	Arquivamento e armazenamento;
03 - Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação;
04 - Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão;
05 - Eliminação	Eliminação.

Fonte: UNA-SUS/UFMA, 2025. Adaptado de Brasil (2020, p. 45).

Dessa forma, podemos observar que, para gerenciar os dados pessoais, as instituições e os órgãos da área da saúde precisam conhecer profundamente os seus processos de trabalho. Só assim conseguem identificar quais tipos de informações pessoais precisam ser tratadas e avaliar a necessidade de criar políticas de governança de dados.





Nos casos de violações diretas da privacidade e confidencialidade dos dados pessoais, a Autoridade Nacional de Proteção de Dados – ANPD deve ser informada. Uma vez constatadas irregularidades, podem ser aplicadas as seguintes sanções administrativas (Brasil, 2018, art. 52):

I - Advertência, com indicação de prazo para adoção de medidas corretivas;

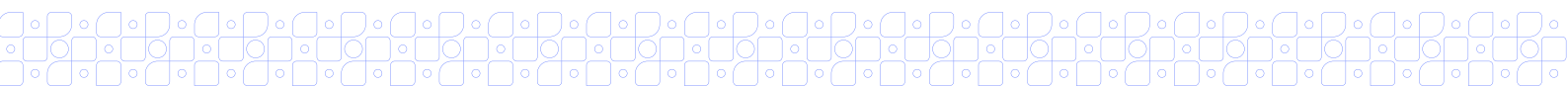
II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

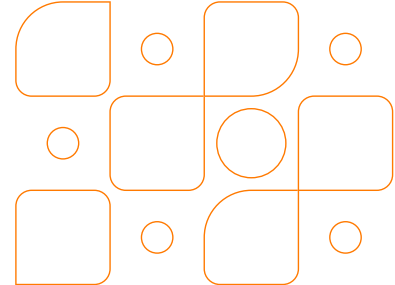
III - Multa diária, observado o limite total a que se refere o inciso II;

IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - Eliminação dos dados pessoais a que se refere a infração; [...].





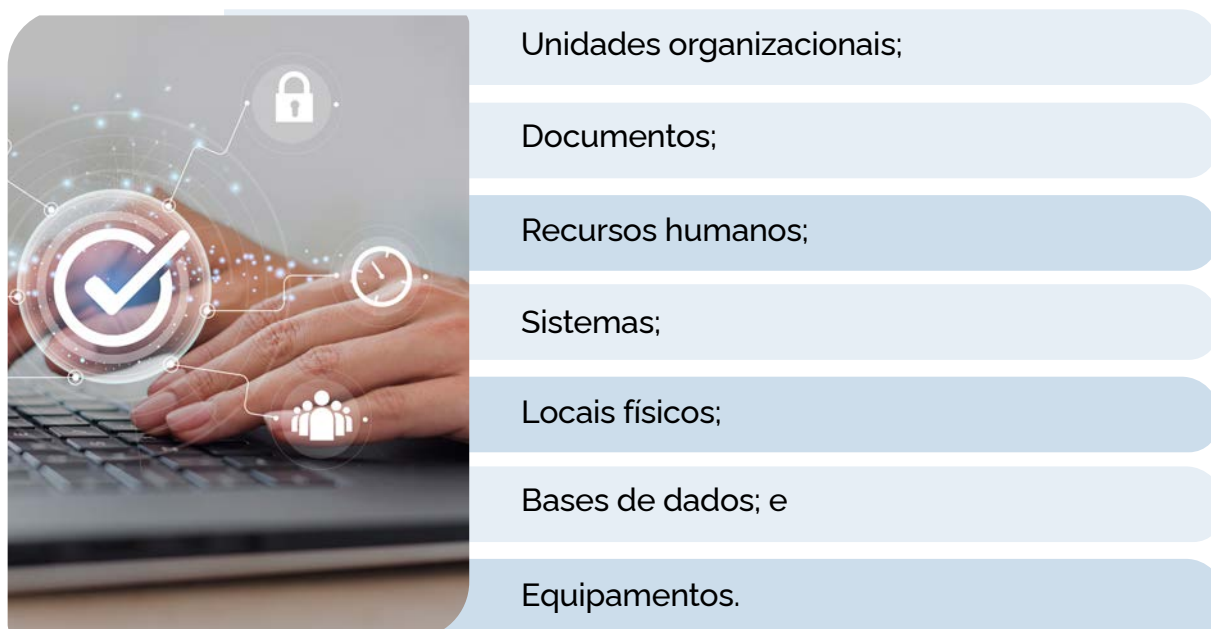
2.3 ATIVOS ORGANIZACIONAIS E SUA RELAÇÃO COM O CICLO DE VIDA DOS DADOS PESSOAIS

No tópico anterior, foi apresentada uma situação ocorrida em um laboratório de análises clínicas para ilustrar a importância da LGPD em estabelecimentos e órgãos da área da saúde, considerando a coleta e o tratamento de diversos dados sensíveis.

Os dados registrados pelo atendente, nesse contexto, provavelmente eram armazenados em um sistema interno do laboratório, como cotidianamente acontece na vida real. Esse exemplo evidencia a necessidade de mapear e identificar todos os ativos organizacionais que estão relacionados como ciclo de vida do tratamento de dados pessoais.

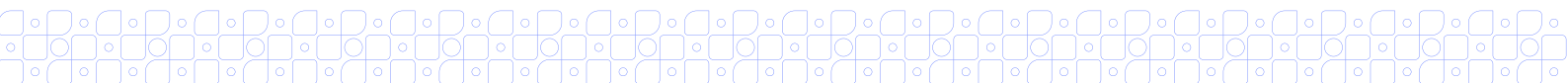
O Guia de Boas Práticas da LGPD indica que os principais ativos são (Brasil, 2020):

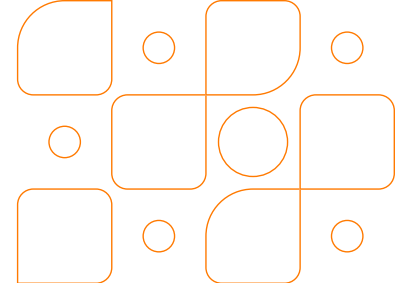
Figura 11. Principais ativos organizacionais relacionados ao ciclo de vida dos dados pessoais



Fonte: Freepik, ©2010–2025.

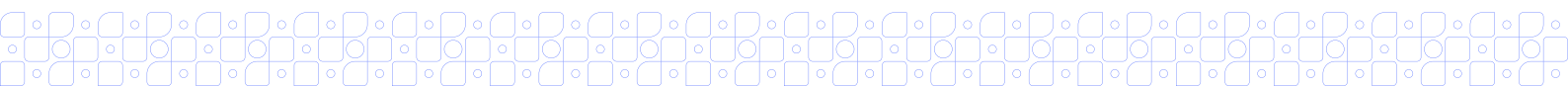
No quadro a seguir, você pode conferir a definição de cada um desses princípios:

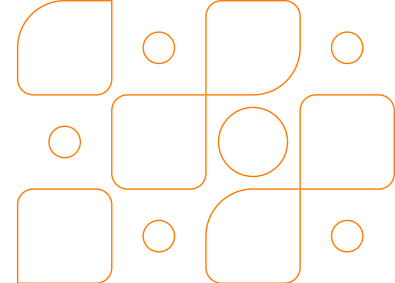




Quadro 05. Conceitos dos principais ativos organizacionais relacionados ao ciclo de vida dos dados pessoais

Unidades organizacionais	Órgãos e entidades da Administração Pública;
Documentos	Unidade de registro de informações, qualquer que seja o suporte e formato;
Recursos humanos	Qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
Sistemas	Qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais;
Locais físicos	Determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa etc.;
Bases de dados	É uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico;





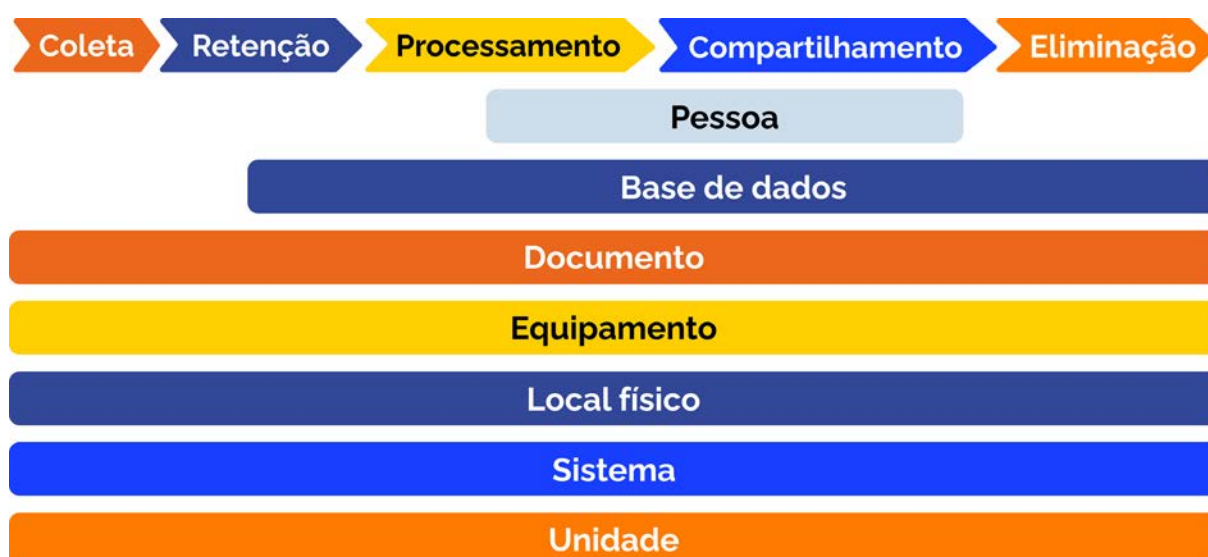
Equipamentos	Objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.
---------------------	--

Fonte: UNA-SUS/UFMA, 2025. Elaborado a partir de dados extraídos de Brasil (2005; 2020).

Ainda nessa perspectiva, após o mapeamento de todos os processos envolvidos no tratamento de dados pessoais, será necessário identificar quais ativos organizacionais participam de cada etapa. Essa identificação permite melhorar as práticas de segurança da informação, que devem ser aplicadas a todos os setores dos órgãos e das instituições.

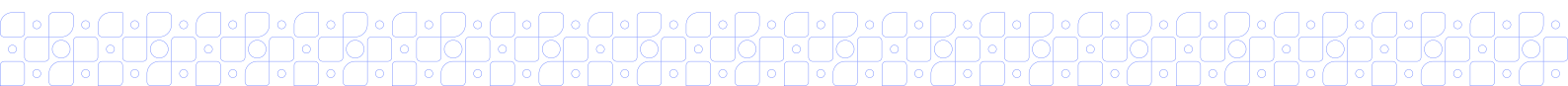
Conforme demonstrado na figura abaixo, é possível entender como esses ativos se distribuem ao longo das fases do ciclo de vida dos dados pessoais:

Figura 12. Ciclo de vida dos dados pessoais



Fonte: UNA-SUS/UFMA, 2025. Adaptado de Brasil (2020, p. 48).

Para reconhecer a aplicação prática das fases do ciclo de vida dos dados pessoais e a forma que devem ser tratados os dados pessoais em Saúde Digital conforme a LGPD, vamos analisar a história do atendimento do Sr. José em uma Unidade Básica de Saúde – UBS:



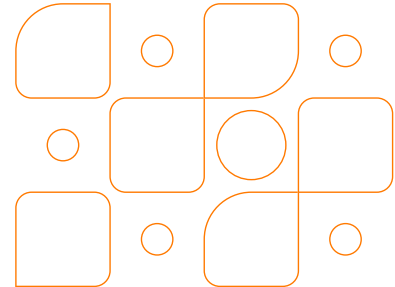


Figura 13. O caso do atendimento do Sr. José em uma Unidade Básica de Saúde – UBS



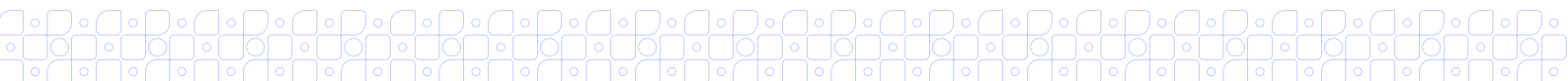
Fonte: Imagem gerada com auxílio do Gemini 2.5 Flash Image. Google, 2025.

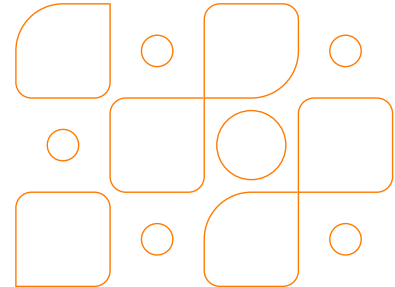
José, de 67 anos, chegou à UBS do bairro Maria Bonita na cidade de Esperança. Com o chapéu nas mãos e um envelope de exames no bolso, ele foi recebido pela recepcionista, que solicitou seu nome e cartão do SUS para registro das informações no sistema.

Figura 14. Aplicação prática das fases do ciclo de vida dos dados pessoais

Fase de coleta

Na fase de **coleta**, podem ser utilizados vários ativos, como sistemas, documentos físicos, equipamentos e local físico. O caso apresentado demonstra que a entrada dos dados se deu via registro no sistema, mas também pode ocorrer a partir da entrega de documentos físicos. Além disso, foram utilizados o computador e o espaço físico da UBS, configurando diferentes ativos organizacionais.





Fase de retenção

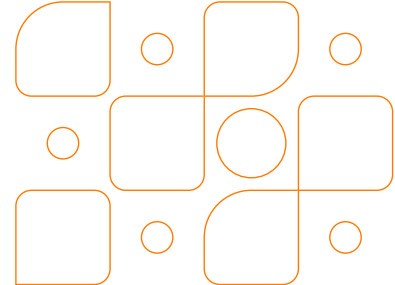
Na fase da **retenção**, são avaliados todos os ativos envolvidos na função de armazenamento de dados. Como vimos anteriormente, a entrada de dados pode ser feita por meio de sistemas ou documentos físicos, e, nesse sentido, o armazenamento pode ser feito em bases de dados, arquivos de documentos físicos, equipamentos e/ou sistemas. As unidades ocasionais e os locais físicos também são ativos importantes e devem ser considerados. Quando o armazenamento for feito em nuvem, os serviços contratados e/ou conveniados para tal precisam estar em conformidade com a LGPD.

Fase de processamento

A etapa de **processamento** pode ser desenvolvida nos sistemas internos ou contratados pelos órgãos e/ou instituições. Cabe ressaltar que o processamento também se aplica aos documentos físicos; portanto, convém observar a localização das unidades organizacionais e dos equipamentos utilizados, bem como verificar os recursos humanos disponíveis para a execução da etapa.

Fase de compartilhamento

Na fase de **compartilhamento**, é preciso analisar os ativos utilizados na distribuição e divulgação de dados pessoais. No caso de instituições ou órgãos que lidam com um grande volume de dados, o compartilhamento pode ser realizado internamente (entre setores) ou externamente (para outras entidades). Nesses termos, se faz necessário mapear os sistemas utilizados, os destinatários, as unidades organizacionais e os equipamentos utilizados para transmitir, exibir ou divulgar dados pessoais.



Fase de eliminação

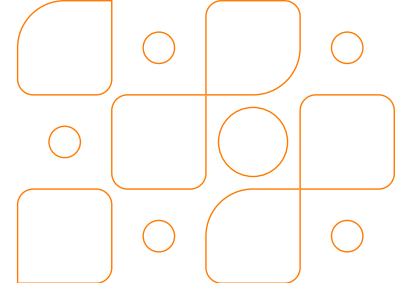
A última fase é a de **eliminação**, que exige a identificação dos ativos envolvidos no armazenamento dos dados pessoais. Dessa forma, torna-se viável a verificação das solicitações de exclusão de dados pessoais feitas pelos titulares e/ou a verificação, por parte de órgãos e instituições, de demandas relacionadas ao descarte de dados pessoais. Nesta etapa, ainda são examinados em quais ativos os dados estão armazenados, como bases de dados, sistemas, equipamentos e/ou documentos físicos. Ademais, considerando a complexidade da fase de eliminação, deve-se levar em conta os locais físicos, as unidades organizacionais e a utilização de serviços de armazenamento de nuvens.

Após a identificação de todos os ativos que participam do ciclo de vida, as organizações e instituições devem iniciar as discussões para avaliar quais medidas de segurança são necessárias para garantir a proteção dos dados pessoais. À medida que as estratégias de segurança forem implementadas, devem ser mapeadas e sinalizadas, conforme a figura abaixo:

Figura 15. Mapeamento e sinalização das medidas de segurança implementadas



Fonte: UNA-SUS/UFMA, 2025. Adaptado de Brasil (2020, p. 49).



Nesse sentido, recomenda-se a elaboração de políticas internas de segurança de dados pessoais fundamentadas no uso de frameworks, bem como nas Normas Brasileiras – NBRs da Associação Brasileira de Normas Técnicas – ABNT e nas normas internacionais da International Organization for Standardization – ISO e da International Electrotechnical Commission – IEC listadas a seguir:

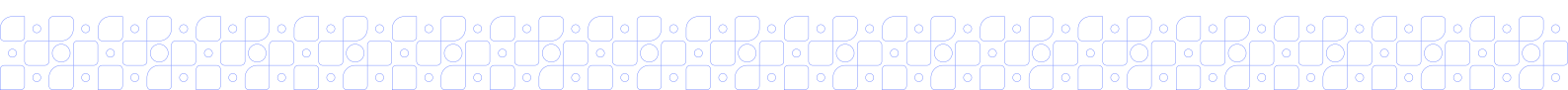
ABNT NBR ISO/IEC 27001 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos;

ABNT NBR ISO/IEC 27002 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação;

ABNT NBR ISO/IEC 27701 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;

ISO/IEC 29151 – *Information technology — Security techniques — Code of practice for personally identifiable information*;

ISO/IEC 29134 – *Information technology — Security techniques — Guidelines for privacy impact assessment*.



3. Rede Nacional de Dados em Saúde e segurança da informação

A Rede Nacional de Dados em Saúde – RNDS é uma plataforma criada pelo MS para promover a integração dos dados em todo território nacional. A sua principal finalidade é facilitar a interoperabilidade de vários sistemas de saúde de forma segura e sistematizada (Brasil, c2025a).

Na figura a seguir, podemos entender melhor sobre essa rede:

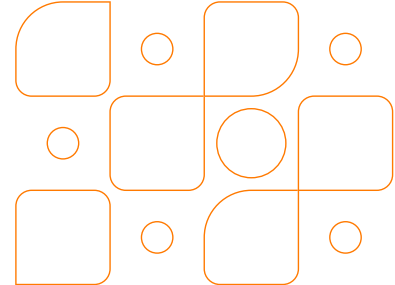


Figura 16. Rede Nacional de Dados em Saúde



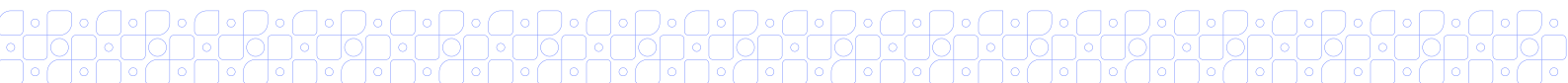
A RNDS é a rede que conecta os atores e dados em saúde de todo o país, estabelecendo o conceito de **plataforma nacional de inovação, informação e serviços digitais de saúde**.

Não é um sistema de informação, e sim uma plataforma capaz de conectar qualquer sistema de informação.

Fonte: UNA-SUS/UFMA, 2025. Adaptado de Cosems (2023).

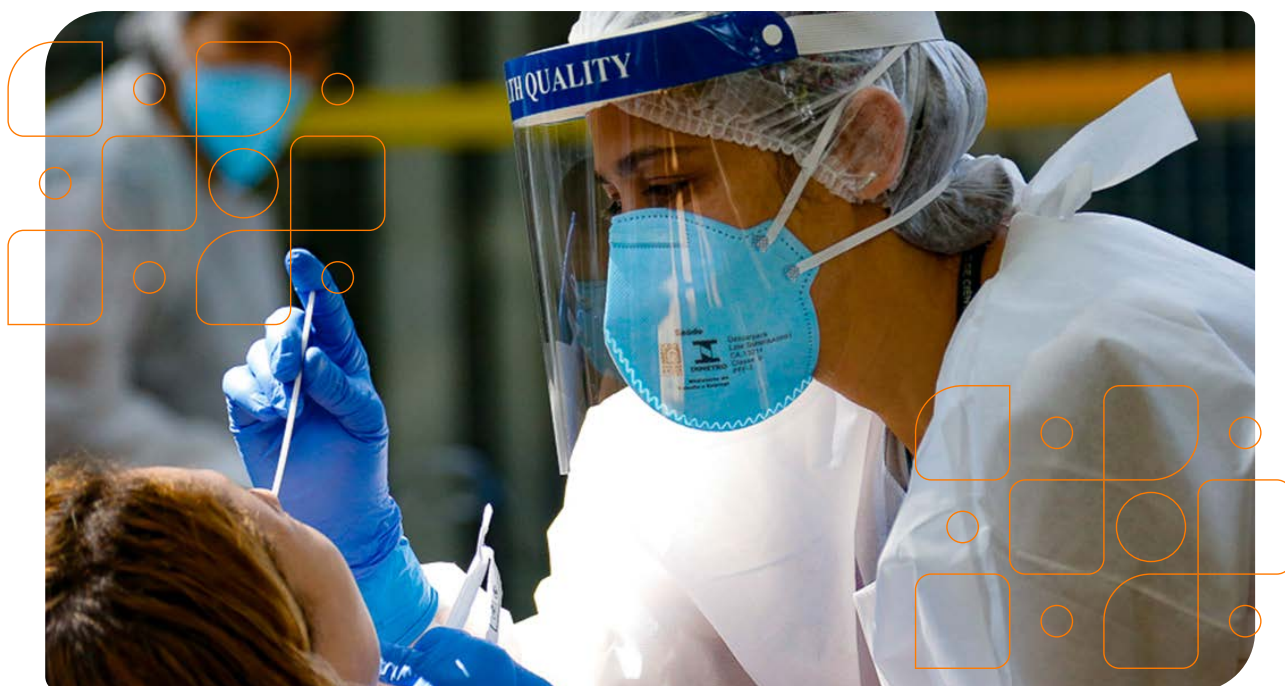
A ideia inicial da RNDS foi proporcionar uma gestão mais eficiente da informação, em virtude de o setor da saúde gerar uma quantidade volumosa de dados. Nesse sentido, é necessário investimentos constantes no aperfeiçoamento do intercâmbio de informações interpostas entre os pontos da Rede de Atenção à Saúde – RAS para aprimorar os atendimentos oferecidos à população.

Dessa forma, a RNDS é alimentada por diversas bases de dados, geradores e consumidores de informações, como os Sistemas de Informação em Saúde – SIS, laboratórios de análises clínicas e estabelecimentos de saúde. A partir disso, a rede centraliza e organiza as informações em nuvem, permitindo que os cidadãos (por meio do aplicativo Meu SUS Digital), gestores e profissionais da saúde utilizem esses dados para (Zara *et al.*, 2021):



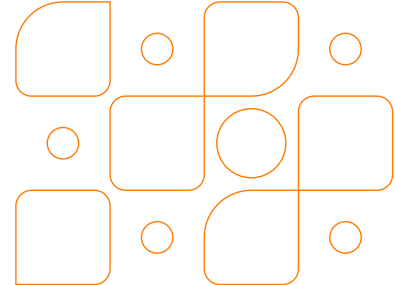
- Evitar duplicidade de solicitação de exames e consultas;
- Analisar perfis epidemiológicos;
- Realizar vigilância em saúde;
- Avaliar e monitorar políticas públicas; e
- Produzir pesquisas.

Figura 17. Teste diagnóstico durante pandemia de covid-19.



Fonte: Cecília Bastos. Universidade de São Paulo, 2021. USP Imagens.

A pandemia de covid-19 funcionou como um catalisador diante da demanda de expansão do compartilhamento de informações com mais rapidez e precisão. Devido ao agravamento dessa emergência global de saúde pública, o projeto piloto da RNDS, que estava previsto para o final do ano de 2019 no estado de Alagoas, passou a disponibilizar resultados de exames de identificação do vírus e registros de vacinação (Conasems, 2023).



Nessa perspectiva, uma rede de serviços complexa como a RNDS, enquanto plataforma de integração nacional de dados, necessita de padrões de segurança que preservem a confidencialidade. Em conformidade com a LGPD, a arquitetura tecnológica da RNDS possui blockchain, serviços de elegibilidade e consentimento informado (Oliveira *et al.*, 2021; Zara *et al.*, 2021).

Figura 18. Gov.br



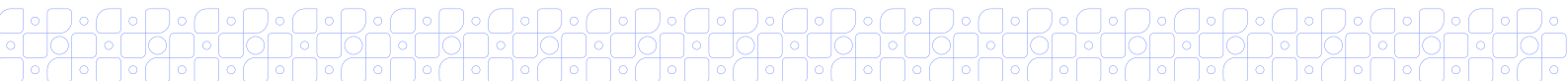
Fonte: Brasil (c2025b).

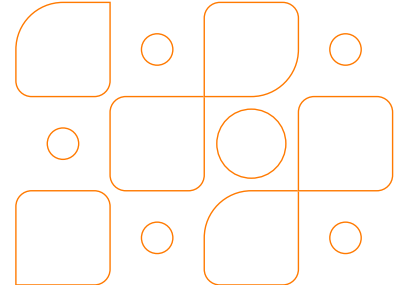
Na prática, o acesso às informações pessoais por parte dos usuários só pode ser realizado pelo próprio titular dos dados pessoais, por meio de autenticação do Gov.br.

Para os profissionais da saúde, são aplicadas as regras de vinculação ao Prontuário Eletrônico do Paciente – PEP, usando a autenticação de certificado digital da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Dessa forma, todos os dados são coletados, processados, armazenados e rastreados de acordo com estabelecimentos de saúde, Cadastros de Pessoa Física – CPFs e categorias profissionais habilitadas (Oliveira *et al.*, 2021; Zara *et al.*, 2021).

Apesar do grande volume de informações previamente enviados à RNDS, a rede é capaz de hospedar os dados no DataSUS ou em outros sistemas de informações. Com a utilização de tecnologias de rastreabilidade, como a blockchain, é possível identificar a origem de todos os dados, assegurando a observância aos padrões de segurança estabelecidos.

Além disso, os dados de saúde são considerados sensíveis pela LGPD. Embora a legislação preveja uma cessão de dados pessoais para fins de execução de políticas públicas, realização de estudos por órgãos de pesquisa licenciados e tutela de saúde, Oliveira *et al.* (2021) descrevem que a RNDS adotou cinco premissas negociais importantes:





1

Os dados de saúde dos indivíduos são compartilhados com os profissionais de saúde vinculados à rede de atendimento a fim de promover a continuidade do cuidado;

2

O profissional de saúde somente pode acessar os dados de um indivíduo durante um contato assistencial;

3

O contato assistencial pressupõe a verificação de três condições: CPF ou Cartão Nacional de Saúde – CNS da pessoa atendida, CPF do profissional de saúde e Cadastro Nacional de Estabelecimento de Saúde – CNES ao qual esse profissional está vinculado;

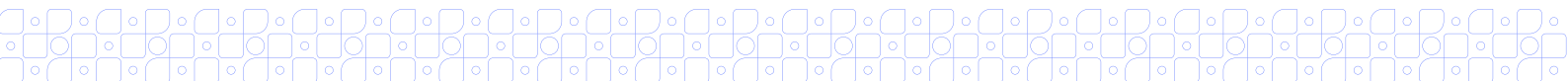
4

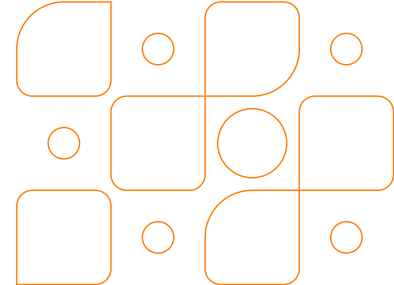
O indivíduo poderá ativamente exercer o direito de se retirar do processo de compartilhamento de dados pessoais de saúde da RNDS e gerir o acesso para profissionais de saúde a partir do seu consentimento explícito;

5

O indivíduo, titular de dados pessoais sensíveis de saúde, tem direito de ser informado sobre a finalidade e o tratamento de seus dados, devendo, portanto, ser notificado sempre que algum profissional acessar suas informações.

Assim, a LGPD é aplicada à RNDS com o objetivo de promover a segurança da informação. Apesar dos consideráveis avanços, ainda existem desafios relacionados à formulação de regulamentações específicas para o compartilhamento de dados pessoais.





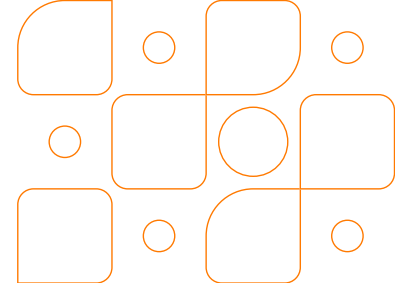
Considerações finais

Chegamos ao final do livro “Segurança da informação em Saúde Digital”!

Nele, vimos que o Programa SUS Digital foi um marco decisivo na consolidação da transformação digital no sistema público de saúde do Brasil. O fortalecimento da infraestrutura tecnológica permitiu grandes avanços relacionados à interoperabilidade entre os SIS. Diante desse cenário cada vez mais conectado e carregado de dados e informações, as discussões acerca da segurança da informação ocupam um eixo estratégico na preservação da privacidade.

Nesse sentido, a LGPD representou um marco significativo na proteção de dados pessoais no Brasil, a partir de 2018. Baseada no Regulamento Geral de Proteção de Dados – RGPD, desenvolvido pela União Europeia, sua institucionalização envolve a compreensão de princípios e diretrizes que estabelecem regras obrigatórias para todos os agentes públicos e privados responsáveis pelo tratamento de dados e informações no país.

Embora a LGPD proteja o tratamento de dados pessoais, a sua implementação ainda enfrenta desafios no âmbito dos órgãos e das instituições de saúde. Isso se deve à necessidade expressa de mudanças na cultura organizacional, que exige a criação de políticas internas de segurança da informação e, em muitos casos, modificações estruturais. Além desses aspectos, garantir o direito à proteção da informação é essencial para preservar os aspectos éticos e fortalecer a cidadania digital, alicerçada no uso responsável de informações pessoais.



Referências

ANTHONY SAMY, P.; RASHID, A.; CHITCHYAN, R. Privacy Requirements: Present & Future. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 39., 2017. **Anais [...]**. Buenos Aires: Software Engineering in Society Track, 2017. Disponível em: <https://doi.org/10.1109/ICSE-SEIS.2017.3>. Acesso em: 12 nov. 2025.

BORGES, R. C. *et al.* Segurança da informação: realidades na atenção primária em uma metrópole brasileira. **Journal of Health Informatics**, v. 15, n.º esp., 2023. Disponível em: <https://doi.org/10.59681/2175-4411.v15.iEspecial.2023.1111>. Acesso em: 12 nov. 2025.

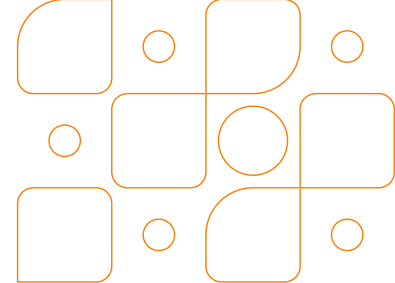
BRASIL. Comitê Central de Governança de Dados. **Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD)**. 2. ed. [Brasília, DF]: Gov.br, 2020. E-book (69 p.). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 12 nov. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Arquivo Nacional. **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.

BRASIL. Ministério da Saúde. **Manual Instrutivo do Programa SUS Digital**. Brasília, DF: Ministério da Saúde, 2024a. E-book (38 p.). Disponível em: <https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/guias-e-manuais/2024/manual-instrutivo-do-programa-sus-digital/view>. Acesso em: 12 nov. 2025.

BRASIL. Ministério da Saúde. **Portaria GM/MS n.º 3.727, de 21 de maio de 2024**. Altera a Portaria de Consolidação GM/MS nº 5, de 28 de setembro de 2017, para dispor sobre o Índice Nacional de Maturidade em Saúde Digital (INMSD), no âmbito do Programa SUS Digital. Brasília, DF: Ministério da Saúde, 2024b. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2024/prt3727_22_05_2024.html. Acesso em: 14 nov. 2025.



BRASIL. Ministério da Saúde. **Portaria n.º 589, de 20 de maio de 2015**. Institui a Política Nacional de Informação e Informática em Saúde (PNIIS). Brasília, DF: Ministério da Saúde, 2015. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2015/prt0589_20_05_2015.html. Acesso em: 12 nov. 2025.

BRASIL. Ministério da Saúde. Rede Nacional de Dados em Saúde. **Gov.br**, c2025a. Disponível em: <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds>. Acesso em: 29 de ago. 2025.

BRASIL. Ministério da Saúde. SUS Digital. **Gov.br**, c2025b. [Composição da SEIDIGI]. Disponível em: <https://www.gov.br/saude/pt-br/composicao/seidigi/sus-digital>. Acesso em: 14 nov. 2025.

BRASIL. Portaria GM/MS n.º 1.768, de 30 de julho de 2021. Altera o Anexo XLII da Portaria de Consolidação GM/MS n.º 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). **Diário Oficial da União**: seção 1, Brasília, DF, n. 144, p. 45, 2 ago. 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gm/ms-n-1.768-de-30-de-julho-de-2021-335472332>. Acesso em: 12 nov. 2025.

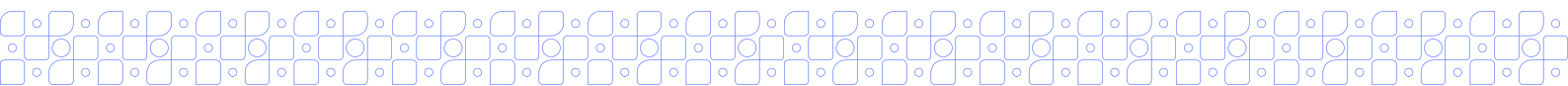
COSEMS (Espírito Santo). Municípios capixabas conectam unidades básicas de saúde à RNDs. **CONASEMS**, Brasília, DF, 17 jan. 2023. Notícias. Disponível em: https://portal.conasems.org.br/rede-cosems/noticias/810_municipios-capixabas-conectam-unidades-basicas-de-saude-a-rnds. Acesso em: 12 nov. 2025.

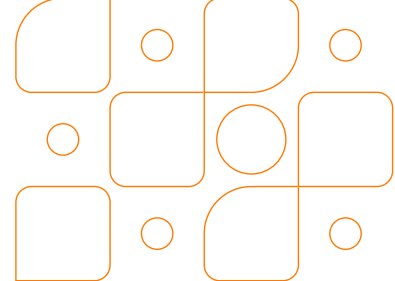
FAGHERAZZI, G. *et al.* Digital health strategies to fight COVID-19 worldwide: challenges, recommendations, and a Call for Papers. **Journal of Medical Internet Research**, v. 22, n.º 6, p. 1–9, 2020. Disponível em: <https://doi.org/10.2196/19284>. Acesso em: 12 nov. 2025.

FERNANDES, M. E.; NUZZI, A. P. E. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. **Research, Society and Development**, v. 11, n.º 12, 2022. Disponível em: <https://doi.org/10.33448/rsd-v11i12.34247>. Acesso em: 12 nov. 2025.

MENDONÇA, A. V. M.; SOUSA, M. F. Desafios contemporâneos para a Saúde Digital: letramento, educação midiática e prevenção à desinformação. **Revista Panamericana de Salud Pública**, v. 49, e14, abr. 2025. Disponível em: <https://doi.org/10.26633/RPSP.2025.14>. Acesso em: 12 nov. 2025.

NERY, C. Internet foi acessada em 72,5 milhões de domicílios do país em 2023. **Agência IBGE Notícias**, 16 ago. 2024. PNAD Contínua. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41024>. Acesso em: 12 nov. 2025.





OLIVEIRA, L. J.; NOVAIS, T. G. Lei geral de proteção de dados pessoais: responsabilidade civil no vazamento de informações. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n.º 5, p. 1614–1631, maio 2024. Disponível em: <https://doi.org/10.51891/rease.v10i5.13668>. Acesso em: 12 nov. 2025.

OLIVEIRA, T. L. de *et al.* LGPD e Saúde Pública: A Rede Nacional de Dados em Saúde e a Proteção de Dados Pessoais. In: DALLARI, A.; MONACO, G. **LGPD na Saúde**. São Paulo: Editora Revista dos Tribunais, 2021.

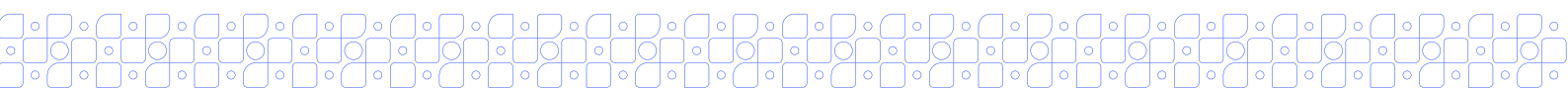
ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE. Departamento de Evidência e Inteligência para Ação em Saúde. **Segurança da informação**. Washington, D. C.: OPAS, c2023. 16 p. Disponível em: <https://iris.paho.org/handle/10665.2/59549>. Acesso em: 12 nov. 2025.

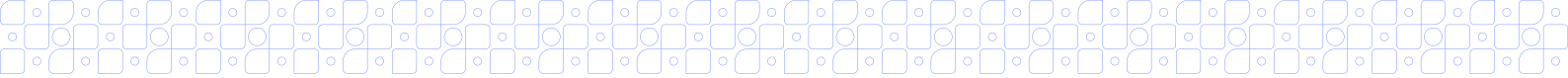
RACHID, R. *et al.* Saúde digital e a plataformização do Estado brasileiro. **Ciência & Saúde Coletiva**, v. 28, n.º 7, p. 2143–2153, jul. 2023. Disponível em: <https://doi.org/10.1590/1413-81232023287.14302022>. Acesso em: 28 de ago. 2025.

SANTOS NETO, A. B.; ISHIKAWA, L.; MACIEL, M. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, v. 16, n.º 40, p. 163–177, set./dez. 2021. Disponível em: <https://doi.org/10.20912/rdc.v16i40.604>. Acesso em: 12 nov. 2025.

YEUNG, A. W. K. *et al.* The promise of digital healthcare technologies. **Frontiers in Public Health**, v. 11, e1196596, 2023. Disponível em: <https://doi.org/10.3389/fpubh.2023.1196596>. Acesso em: 12 nov. 2025.

ZARA, A. L. S. A. *et al.* (org.). **Rede nacional de dados em saúde: o que precisamos saber?** Goiânia: Cegraf UFG, 2021. E-book (55 p.). Disponível em: <http://repositorio.bc.ufg.br/handle/ri/19740>. Acesso em: 12 nov. 2025.





Segurança da Informação em Saúde Digital

Realizado o Depósito legal na Biblioteca Nacional conforme a Lei n.º 10.994, de 14 de dezembro de 2004.

TÍTULO	Segurança da Informação em Saúde Digital
ORGANIZADORAS	Paola Trindade Garcia Ana Estela Haddad Ana Emilia Figueiredo de Oliveira Deysianne Costa das Chagas Elza Bernardes Ferreira
SUPORTE	Digital
PROJETO GRÁFICO E CAPA	Jackeline Mendes Pereira
PÁGINAS	68
TIPOGRAFIA	Rawline CORPO E TÍTULOS

