MINISTÉRIO DA SAÚDE

GUIA BÁSICO de PRIVACIDADE de DADOS

DISTRIBUIÇÃO GRATUITA
VENDA PROIBIDA

Brasília DF 2025

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

GUIA BÁSICO de PRIVACIDADE de DADOS

Brasília DF 2025

1ª edição – 2025 – versão eletrônica

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

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

Ministro de Estado da Saúde:
Alexandre Rocha Santos Padilha

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

Organização:
Cidacs/Fundação Oswaldo Cruz:
Carlos Antonio de Souza Teles Santos
Maíra Lima de Souza
Maria Yury Travassos Ichihara
Maurício Lima Barreto

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

Revisão técnico-científica:
Antonio Ygor Modesto Oliveira – CGEVSA/Daevs/SVSA
Camila Pinto Damasceno – CGEVSA/Daevs/SVSA

Diagramação:
Sabrina Lopes – CGEVSA/Daevs/SVSA

Normalização:
Valéria Gameleira da Mota – Editora MS/CGDI

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

Ficha Catalográfica

Brasil. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis.
Guia Básico para Privacidade de Dados e Segurança da Informação [recurso eletrônico] / Ministério da Saúde, Secretaria de Vigilância em Saúde e Ambiente, Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis. – Brasília : Ministério da Saúde, 2025.
44 p. : il.

Modo de acesso: World Wide Web:
http://bvsms.saude.gov.br/bvs/publicacoes/guiabasico_privacidade_seguranca_informacao.pdf
ISBN 978-65-5993-900-8

1.Privacidade. 2.Segurança da Informação. 3. Lei de Proteção de Dados. I. Título.

CDU 004.85

Catalogação na fonte – Coordenação-Geral de Documentação e Informação – Editora MS – OS 2024/0249

Título para indexação:
Data Governance: Basic guide to data privacy

SUMÁRIO

APRESENTAÇÃO

O *Guia Básico para Privacidade de Dados* da Secretaria de Vigilância em Saúde e Ambiente (SVSA) tem como objetivo esclarecer pontos essenciais sobre o tema e fornecer orientações gerais para o acesso, o uso e o tratamento de dados sob gestão do Departamento de Análise Epidemiológica e Vigilância de Doenças Não Transmissíveis (Daent). Apresenta os principais conceitos e princípios aplicados ao dia a dia, bem como o tratamento de dados constantes nos sistemas de informação em saúde. Ao final, também é possível encontrar materiais complementares para implementação das boas práticas de privacidade de dados em sua coordenação ou departamento.

Este Guia buscou sintetizar as principais legislações sobre o assunto, de forma que seus fundamentos e suas principais formas de aplicação estejam acessíveis para consulta, e tem como objetivo disseminar conhecimento para que os agentes públicos possam manusear dados em sua rotina na área técnica dentro da SVSA de forma mais segura e padronizada.

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

SISTEMAS ATUALMENTE SOB GESTÃO DO DAENT/SVSA

- **Sinan on-line** – Sistema de Informação de Agravos de Notificação versão on-line (registro de casos de arboviroses).
- **Sinan Net** – Sistema de Informação de Agravos de Notificação versão NET.
- **Sinan Viva** – Sistema de Informação de Agravos de Notificação (registro de violência interpessoal e autoprovocada).
- **e-SUS Sinan** – Sistema de Informação de Agravos de Notificação versão WEB (registro de mpox e de doença de Chagas crônico).
- **Sinasc** – Sistema de Informações sobre Nascidos Vivos.
- **SIM** – Sistema de Informações sobre Mortalidade.
- **e-SUS Declarações** (em fase de implementação – novo SIM e Sinasc – versão WEB).
- **e-SUS Notifica** – Sistema de Notificação dos Casos de Síndrome Respiratória Leve (síndrome gripal).
- **Resp-Microcefalia** – Registro de Eventos de Saúde Pública (registro de casos de síndrome congênita ligada ao vírus Zika).
- **Vigitel** – Vigilância de Fatores de Risco e Proteção para Doenças Crônicas Não Transmissíveis por Inquérito Telefônico.

PESSOAS INTERESSADAS EM ACESSAR OS DADOS

- **Pessoa física** – titular, pesquisador, cidadão.
- **Pessoa jurídica** – órgão de governo, MPs, PGR (procuradoria), os órgãos de pesquisa, instituições de ensino superior, justiça (tribunais, polícia, CNJ), órgãos do Legislativo e conselhos.

1 | ESTRUTURA DO GUIA

O presente Guia está dividido em seis seções:

Nas seções 1 e 2, são apresentados os marcos regulatórios que regem o tratamento de dados pessoais e como podem ser aplicados no âmbito da SVSA.

Nas seções 3 e 4, são abordados os procedimentos para aplicação e acesso aos dados na SVSA.

Nas seções 5 e 6, encontram-se o glossário e uma sessão de perguntas frequentes.

E, ao final, temos as considerações finais e as referências.

2 | A LEI GERAL DE PROTEÇÃO DE DADOS E NORMAS CORRELATAS

2.1 O QUE É

A Lei n.º 13.709, também conhecida como Lei Geral de Proteção de Dados (LGPD), foi sancionada em 14 de agosto de 2018. Ela serve como um guia para empresas, instituições públicas e indivíduos sobre como coletar, armazenar e usar dados pessoais. A LGPD não apenas protege os cidadãos, garantindo seus direitos fundamentais de liberdade e de privacidade, como também estabelece regras claras para quem lida com essas informações. Isso significa que qualquer organização, seja ela grande ou pequena, que colete dados pessoais deve seguir as diretrizes estabelecidas pela Lei.

O não cumprimento dessa Lei pode resultar em sanções significativas, administrativas e cíveis, além de danos à reputação. Tais penalidades têm sua aplicação prevista para as pessoas físicas ou jurídicas que falharem em proteger a privacidade dos dados a elas cedidos.

Antes da promulgação da LGPD, a legislação brasileira sobre o tratamento de dados era fragmentada e dispersa em várias leis e regulamentos. Algumas das principais legislações que tratavam de aspectos relacionados ao tratamento de dados incluíam:

- **Constituição Federal de 1988:** embora não trate especificamente de dados pessoais, estabelece direitos fundamentais, como a privacidade e o sigilo de correspondência e comunicações.
- **Código de Defesa do Consumidor (Lei n.º 8.078, de 11 de setembro de 1990):** aborda a proteção de dados pessoais no contexto das relações de consumo, incluindo aspectos de publicidade e práticas comerciais.
- **Marco Civil da Internet (Lei n.º 12.965, de 23 de abril de 2014):** considerada a "Constituição da Internet" no Brasil, essa Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no País, incluindo disposições sobre privacidade, proteção de dados pessoais e registros de conexão e acesso a aplicações de internet.

- **Lei do Cadastro Positivo (Lei n.º 12.414, de 9 de junho de 2011):** regulamenta a formação e a consulta a bancos de dados com informações de adimplemento de pessoas naturais e jurídicas para formação de histórico de crédito.
- **Lei de Acesso à Informação (Lei n.º 12.527, de 18 de novembro de 2011):** focada na transparência e no acesso à informação pública, também inclui disposições sobre a proteção de dados pessoais e informações privadas sob custódia do Estado.
- **Códigos Penal e Civil:** ambos contêm disposições que podiam ser aplicadas ao tratamento inadequado de dados pessoais, como as relacionadas à invasão de privacidade, à difamação, à calúnia e ao uso indevido de informações pessoais.
- **Leis setoriais e para casos específicos:** diversas leis setoriais também tratam de proteção de dados em contextos específicos, como as leis relacionadas ao setor bancário, à saúde e às telecomunicações. Também existem leis para proteção específica, como a Lei Carolina Dieckmann (Lei n.º 12.737, de 30 de novembro de 2012 – tipificação criminal de delitos informáticos).

A LGPD unificou e fortaleceu o quadro legal para a proteção de dados pessoais no Brasil, consolidando e ampliando os direitos relacionados à privacidade e ao tratamento de dados pessoais. Um aspecto importante dessa Lei foi garantir o acesso aos dados identificados para pesquisa em conformidade com o que descreve o artigo 13.

VOCÊ SABIA?

A Emenda Constitucional n.º 115/2022 alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e as garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A LGPD tem como principais objetivos:

- **Proteger os direitos fundamentais de liberdade e de privacidade:** de forma geral, a LGPD visa proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.
- **Regular o tratamento de dados pessoais:** estabelecer normas claras e precisas para a coleta, o uso, o processamento, o armazenamento e a eliminação de dados pessoais por empresas e entidades governamentais.
- **Fortalecer a segurança dos dados:** promover medidas de segurança para proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- **Estabelecer regras claras para tratamento de dados:** oferecer um marco legal para que organizações compreendam suas responsabilidades e os procedimentos adequados para o tratamento de dados.
- **Promover a confiabilidade nas relações comerciais e institucionais:** aumentar a confiança do público em serviços que tratam dados pessoais, contribuindo para um ambiente de negócios mais seguro e confiável.
- **Fomentar a responsabilidade e a prestação de contas dos controladores:** incentivar uma cultura de proteção de dados nas organizações, em que os agentes que realizam tratamento de dados são responsabilizados e devem demonstrar a adoção de práticas eficazes de proteção de dados.
- **Assegurar a livre circulação de dados:** garantir que a proteção de dados pessoais não seja um obstáculo ao livre fluxo de informações, sendo importante para o desenvolvimento econômico e tecnológico.
- **Alinhar o Brasil aos padrões internacionais:** harmonizar a legislação brasileira com práticas globais de privacidade e proteção de dados, facilitando o comércio e a cooperação internacional.
- **Proteger os dados pessoais de abusos e uso indevido:** prevenir abusos no uso de dados pessoais e garantir que sejam utilizados de forma ética e responsável.
- **Promover o direito dos titulares de dados:** garantir que os indivíduos tenham direitos claros e meios efetivos para proteger seus dados, incluindo o direito de acesso, correção, exclusão e oposição ao tratamento de seus dados.

Esses objetivos refletem um equilíbrio entre a proteção dos direitos individuais e as necessidades das organizações de tratar dados pessoais para diversos fins legítimos, contribuindo para o desenvolvimento econômico e social.

2.2 HISTÓRICO

A LGPD foi inspirada em regulamentações internacionais, principalmente no Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Este último tem sido um marco na proteção de dados pessoais e serviu como um modelo para muitos outros países, incluindo o Brasil. A LGPD foi criada para modernizar e fortalecer as leis de proteção de dados no Brasil, adaptando-as para o século XXI. Antes da LGPD, o Brasil não tinha uma legislação específica que abordasse de forma abrangente a proteção de dados pessoais. A nova lei preenche essa lacuna e estabelece um padrão nacional para a coleta e o tratamento de dados, alinhando o Brasil às melhores práticas globais.

linha do tempo

2018

- A LGPD é sancionada, marcando um novo capítulo na legislação brasileira sobre proteção de dados, entrando em vigor parcialmente (arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B).

2020

- A LGPD entra totalmente em vigor, estabelecendo que todas as organizações devem se adaptar às novas regras.

2021

- A Autoridade Nacional de Proteção de Dados (ANPD) está autorizada a aplicar sanções, demostrando a exigência no cumprimento da lei, quando os artigos 52, 53 e 54 da LGPD, referentes às sanções administrativas, têm sua entrada em vigor em 1.º de agosto de 2021.

2022

- Novas atualizações e emendas, como a Lei n.º 14.289/2022, são adicionadas para fortalecer, no Brasil, ainda mais a proteção de dados sensíveis de saúde.

2023

- ANPD publica o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução ANPD n.º 04/2023), que regulamenta os artigos 52 e 53 da LGPD e define os critérios e os parâmetros para as sanções pecuniárias e não pecuniárias pela ANPD.
- ANPD publica um guia orientativo sobre tratamento de dados pessoais para o setor público.
- ANPD aprova o Mapa de Temas Prioritários para o biênio 2024-2025 e dispõe sobre a periodicidade do Ciclo de Monitoramento.

2024

- ANPD publica o *Guia Orientativo: tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas*.
- ANPD publica guia sobre legítimo interesse no tratamento de dados pessoais – *Guia Orientativo: hipóteses legais de tratamento de dados pessoais*.
- ANPD publica o *Guia de Atuação do Encarregado de Dados*.
- ANPD publica o *Glossário de Proteção de Dados Pessoais e Privacidade*.

2.3 REGULAMENTAÇÃO

A LGPD é regulamentada pela Autoridade Nacional de Proteção de Dados (ANPD), que é responsável por orientar e supervisionar as atividades de tratamento de dados, além de aplicar sanções em caso de não conformidade.

Outra instituição importante é a Controladoria-Geral da União (CGU), que atua em parceria com a ANPD para garantir a transparência e o cumprimento da lei. Esses órgãos trabalham em conjunto para criar um ambiente seguro e confiável para o tratamento de dados pessoais, protegendo tanto os cidadãos quanto as organizações.

Dentro da estrutura organizacional da ANPD, existe o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), um órgão consultivo cuja composição prevê 23 representantes titulares e suplentes, provenientes dos seguintes órgãos (Brasil, 2018):

I – 5 (cinco) do Poder Executivo federal;

II – 1 (um) do Senado Federal;

III – 1 (um) da Câmara dos Deputados;

IV – 1 (um) do Conselho Nacional de Justiça;

V – 1 (um) do Conselho Nacional do Ministério Público;

VI – 1 (um) do Comitê Gestor da Internet no Brasil;

VII – 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;

VIII – 3 (três) de instituições científicas, tecnológicas e de inovação;

IX – 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo;

X – 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais;

XI – 2 (dois) de entidades representativas do setor laboral.

O CNPD deve propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados e para a atuação da ANPD; elaborar estudos e relatórios; promover debates e audiências públicas para a proteção de dados pessoais e privacidade; além de disseminar o conhecimento sobre proteção de dados e privacidade para a sociedade.

É necessário, ainda, destacar a importância dos controles interno e externo na administração pública e privada, os quais são particularmente relevantes no contexto da LGPD, a fim de alcançar a conformidade legal.

O **controle interno** refere-se a mecanismos, políticas e procedimentos internos estabelecidos por uma organização para garantir a integridade financeira e operacional, a eficácia e a eficiência das operações, e a adesão às leis e aos regulamentos. Em relação à Privacidade de Dados, o controle interno implica:

- **Implementação da LGPD:** as organizações devem estabelecer controles internos robustos para garantir a conformidade com a LGPD, como políticas de privacidade, treinamentos de funcionários e processos de auditoria interna.
- **Gestão de Riscos:** inclui a identificação e o tratamento de riscos relacionados ao tratamento de dados pessoais.
- **Papel do Encarregado de Dados (DPO):** designação de um DPO para supervisionar o tratamento de dados e assegurar a conformidade com a LGPD.

Por outro lado, o **controle externo** inclui as ações e os mecanismos de supervisão realizados por entidades externas, como agências reguladoras, auditores externos e outros órgãos de fiscalização. No que diz respeito à LGPD, envolve:

- **Fiscalização da ANPD:** a Autoridade Nacional de Proteção de Dados (ANPD) é responsável por monitorar e fiscalizar o cumprimento da LGPD.
- **Auditorias e Inspeções:** auditorias externas podem ser realizadas para verificar a conformidade com as normas de proteção de dados.
- **Relatórios para órgãos reguladores:** organizações podem ser obrigadas a fornecer relatórios sobre suas práticas de tratamento de dados para a ANPD e outros órgãos reguladores.

2.3.1 Privacidade de dados no Brasil: a Lei Geral de Proteção de Dados Pessoais (LGPD)

A LGPD é fundamental para assegurar os direitos fundamentais de liberdade e privacidade aos titulares dos dados, ao estabelecer as regras para a coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais, definindo os deveres e as responsabilidades dos encarregados, controladores e operadores de dados. Assim, obedece aos seguintes princípios:

- **Consentimento:** necessidade de consentimento explícito do titular para o tratamento de seus dados pessoais, exceto em casos específicos previstos em lei, a exemplo dos dados coletados e utilizados por órgãos da Administração Pública para percussão de suas competências legais e regulatórias.
- **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.

- **Segurança e prevenção:** implementação de medidas técnicas de segurança para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

A LGPD apresenta outros princípios que devem ser considerados durante todo o ciclo de tratamento dos dados. Eles são elencados da seguinte forma no texto do artigo 6.º da Lei:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- **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.
- **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.
- **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.
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
- **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.

A LGPD, com as práticas de controle interno e externo, desempenha um papel crucial na proteção da privacidade dos dados e na promoção de uma cultura de responsabilidade e transparência nas organizações brasileiras. Todas essas leis e normas trabalham em conjunto para criar um ambiente robusto e seguro para o tratamento de dados pessoais, tornando o Brasil um país alinhado às melhores práticas internacionais.

No entanto, vários desafios vêm sendo enfrentados para garantir a conformidade contínua com a LGPD e adaptar-se às mudanças regulatórias, equilibrando os interesses empresariais com o direito à privacidade e à proteção de dados.

2.4 O QUE SÃO DADOS SENSÍVEIS E COMO IDENTIFICÁ-LOS

O processo de tratamento de dados é chamado de ciclo de vida do tratamento e passa por cinco etapas: coleta, retenção, processamento, compartilhamento e eliminação.

- Coleta é a fase de recepção ou produção do dado.
- Retenção consiste no armazenamento ou no arquivamento dos dados, independentemente da forma utilizada (papel, mídia gravada, serviços em nuvem etc.).
- Processamento é qualquer operação que envolva a classificação, a reprodução, a modificação ou a utilização dos dados armazenados.
- Compartilhamento está relacionado às ações de uso compartilhado, distribuição, transmissão, comunicação ou transferência de dados pessoais.
- Eliminação diz respeito a excluir os dados pessoais armazenados.

DADO, INFORMAÇÃO, CONHECIMENTO

Dado → um fato bruto ou elemento que, por si só, não leva a uma compreensão de um contexto maior.

Informação → dados processados ou organizados que têm um significado ou propósito.

Conhecimento → informações processadas por indivíduos ou grupos, que servem para a tomada de decisões.

2.4.1 Quais são os tipos de dados?

Dados podem ser classificados em várias categorias, como público, aberto, restrito, sensível, pessoal, identificado, desidentificado, pseudo-anonimizado e anonimizado.

De acordo com o artigo 5.º da LGPD, dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". Já o dado pessoal sensível é o dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político. Ainda, são considerados dados sensíveis os dados sobre saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Os dados anonimizados são aqueles em que o titular não possa ser identificado.

2.4.2 Como um dado pode ser caracterizado como pessoal?

Como vimos anteriormente, um dado é considerado pessoal quando ele pode identificar um indivíduo. Dados pessoais são um subconjunto de dados sensíveis que estão relacionados a características muito íntimas, como origem racial, opiniões políticas, religião, saúde, entre outros.

Via de regra, os dados pessoais devem ser anonimizados para que possam ser utilizados em estudos e políticas públicas. Uma pergunta se mantém: como identificar dados pessoais e dados pessoais sensíveis?

Dados pessoais são informações relacionadas a pessoas naturais identificadas ou identificáveis. Assim, são dados como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço, vínculos empregatícios, CPF, CNPJ, NIS, PIS, Pasep e título de eleitor.

Dados pessoais sensíveis, por outro lado, são dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Desse modo, trata-se de características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, bem como características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas.

FIQUE DE OLHO

Como veremos mais à frente, na área de saúde é necessário ter especial atenção aos dados estigmatizantes. São aqueles dados que podem identificar a pessoa por uma condição específica ou acometimento, tais como origem, agravos específicos, prática cotidiana e condição socioeconômica.

2.5 SEGURANÇA DA INFORMAÇÃO

Segurança da informação pode ser definida como um conjunto de práticas e medidas destinadas a proteger informações e sistemas de informações contra acessos não autorizados, uso indevido, divulgação, destruição, modificação ou interrupção. O objetivo principal da segurança da informação é garantir que os dados e as informações de uma organização

ou de um indivíduo estejam seguros e protegidos contra diversas ameaças, sejam elas internas ou externas, acidentais ou maliciosas.

A segurança da informação inicialmente é fundamentada em três pilares principais, conhecidos como a tríade CIA (Confidencialidade, Integridade e Disponibilidade), explicados a seguir:

2.5.1 Confidencialidade

- **Definição:** a confidencialidade refere-se à proteção dos dados contra acessos não autorizados. Somente pessoas autorizadas devem ter acesso às informações confidenciais.
- **Relevância:** a confidencialidade é crucial para proteger a privacidade e os segredos comerciais de uma organização. Violações de confidencialidade podem resultar em perda de confiança, danos à reputação e prejuízos financeiros.
- **Exemplos de medidas:** criptografia de dados, controle de acesso rigoroso, autenticação multifatorial e políticas de uso adequado.

2.5.2 Integridade

- **Definição:** a integridade garante que os dados sejam precisos e completos e que não sejam alterados de maneira não autorizada. Isso significa que a informação deve ser mantida de maneira consistente e precisa ao longo de seu ciclo de vida.
- **Relevância:** a integridade é essencial para a tomada de decisões baseada em dados corretos. Qualquer alteração não autorizada pode comprometer a veracidade das informações e levar a decisões equivocadas.
- **Exemplos de medidas:** assinaturas digitais, *hash* de dados, controles de versão e políticas de auditoria.

2.5.3 Disponibilidade

- **Definição:** a disponibilidade assegura que os dados e os sistemas estejam acessíveis, quando necessário, para usuários autorizados. Isso significa que as informações devem estar disponíveis e funcionais no momento em que forem requisitadas.
- **Relevância:** a disponibilidade é fundamental para a continuidade dos negócios e operações. A falta de disponibilidade pode resultar em interrupções nos serviços, perda de produtividade e insatisfação do cliente.
- **Exemplos de medidas:** redundância de sistemas, becape de dados, planos de recuperação de desastres e manutenção regular dos sistemas.

Além da tríade CIA, alguns especialistas incluem outros dois pilares que complementam a segurança da informação: autenticidade e não repúdio ou irretratabilidade.

2.5.4 Autenticidade

- **Definição:** a autenticidade garante que as informações sejam provenientes de fontes legítimas e que a identidade das partes envolvidas seja frequentemente verificada.
- **Relevância:** a autenticidade evita fraudes e garante que os dados não foram alterados ou manipulados por fontes não confiáveis.
- **Exemplos de medidas:** certificados digitais, sistemas de autenticação robusta e métodos de verificação de identidade.

2.5.5 Não repúdio ou irretratabilidade

- **Definição:** o não repúdio assegura que uma parte não possa negar a autoria de uma ação ou comunicação realizada.
- **Relevância:** o não repúdio é crucial para garantir a responsabilidade e a responsabilização das ações realizadas por usuários e sistemas.
- **Exemplos de medidas:** assinaturas digitais, registros de auditoria e *logs* de atividade.

2.5.6 Riscos de segurança da informação

É importante registrar que os maiores riscos de segurança da informação incluem:

- **Ataques cibernéticos:** abrangendo *malwares*, *phishing*, *ransomware* e ataques de negação de serviço (DDoS). Esses ataques visam explorar vulnerabilidades em sistemas e redes.
- **Vazamento de dados:** quando informações confidenciais são expostas, seja por falhas de segurança, erros humanos ou ataques maliciosos.
- **Falta de conscientização:** a negligência dos usuários em seguir práticas seguras, como senhas fortes e atualizações regulares, pode ser um grande risco.
- **Acesso não autorizado:** quando pessoas não autorizadas obtêm acesso a sistemas, bancos de dados ou informações sensíveis.
- **Falta de criptografia:** dados não criptografados estão vulneráveis a interceptações durante a transmissão.
- **Falhas de segurança em aplicativos:** aplicativos mal projetados ou com vulnerabilidades podem ser explorados por invasores.
- **Falta de becape e recuperação:** a perda de dados sem becapes adequados pode ser catastrófica.

2.5.7 Boas práticas e controles de segurança

Para garantir a eficácia da segurança da informação, além de entender seus pilares fundamentais, é crucial implementar boas práticas e controles específicos. Essas práticas e controles ajudam a proteger os dados e os sistemas de ameaças variadas. A seguir, estão algumas das principais práticas recomendadas:

2.5.8 Controle de acesso

- **Princípio do menor privilégio:** garanta que os usuários tenham apenas os privilégios mínimos necessários para realizar suas tarefas. Isso limita a exposição de dados e sistemas a acessos não autorizados.
- **Autenticação multifator (MFA):** adote métodos de autenticação que utilizem múltiplos fatores (como senha, *token*, biometria) para aumentar a segurança do acesso.
- **Gerenciamento de identidade e acesso:** utilize sistemas de gerenciamento de identidade de acesso para gerenciar e controlar o acesso dos usuários aos recursos de Tecnologias da Informação (TI) de forma centralizada.

2.5.9 Proteção de dados

- **Criptografia:** encripte dados em repouso e em trânsito para proteger informações sensíveis contra interceptações e acessos não autorizados.
- **Classificação de dados:** classifique os dados com base na sua sensibilidade e importância e aplique controles de segurança apropriados para cada classe de dados.
- **Descarte seguro:** garanta que os dados sejam destruídos de forma segura, quando não forem mais necessários, utilizando técnicas como destruição física ou sanitização de discos.

2.5.10 Segurança de rede

- ***Firewalls*:** implemente *firewalls* para controlar o tráfego de rede e impedir acessos não autorizados.
- **Sistemas de detecção e prevenção de intrusões (IDS/IPS):** utilize IDS/IPS para monitorar a rede em busca de atividades suspeitas e bloquear ataques em tempo real.
- **Segmentação de rede:** divida a rede em segmentos menores para limitar o impacto de possíveis violações e melhorar a segurança.

2.5.11 Segurança de aplicações

- **Desenvolvimento seguro:** adote práticas de desenvolvimento seguro, como revisão de código e testes de segurança, para identificar e corrigir vulnerabilidades no software.
- ***Patching* e atualizações:** mantenha sistemas e aplicações atualizados com os últimos *patches* de segurança para corrigir vulnerabilidades conhecidas.
- **Gerenciamento de vulnerabilidades:** realize varreduras regulares de vulnerabilidades e testes de penetração para identificar e corrigir falhas de segurança.

2.5.12 Gerenciamento de incidentes

- **Plano de resposta a incidentes:** desenvolva e mantenha um plano de resposta a incidentes para lidar rapidamente com incidentes de segurança e minimizar danos.
- **Equipes de resposta a incidentes:** forme equipes dedicadas à resposta a incidentes, treinadas para identificar, analisar e mitigar incidentes de segurança.
- **Registro e análise de *logs*:** monitore e analise *logs* de sistemas e eventos de segurança para detectar atividades suspeitas e responder prontamente.

2.5.13 Educação e conscientização

- **Treinamento contínuo:** ofereça treinamentos regulares para funcionários sobre práticas de segurança da informação e conscientização sobre ameaças como *phishing* e engenharia social.
- **Políticas de segurança:** desenvolva e comunique claramente as políticas de segurança da organização para todos os colaboradores, garantindo que entendam suas responsabilidades.
- **Simulações de ataques:** realize simulações de ataques, como exercícios de *phishing*, para testar a prontidão dos funcionários e melhorar a resposta a incidentes.

2.5.14 Becape e recuperação de desastres

- **Becape regular:** realize becapes regulares de dados críticos e armazene-os em locais seguros, preferencialmente fora do local principal de operação.
- **Teste de recuperação:** teste regularmente os procedimentos de recuperação de desastres para garantir que os becapes possam ser restaurados rapidamente em caso de incidente.
- **Planos de continuidade de negócios:** desenvolva e mantenha planos de continuidade de negócios para garantir a operação contínua em caso de interrupções graves.

2.5.15 Acesso aos dados

O acesso aos dados é uma área crítica que requer atenção especial. De acordo com as diretrizes da LGPD, o acesso deve ser feito de forma segura e restrita apenas a pessoas autorizadas. Isso inclui a implementação de autenticação de dois fatores, registros de *log* detalhados e monitoramento contínuo para detectar qualquer atividade suspeita. A ideia é minimizar os riscos de vazamentos de dados ou o uso indevido de informações.

IMPORTANTE

Na Lei Geral de Proteção de Dados (LGPD) do Brasil, diversos "personagens" ou entidades desempenham papéis fundamentais na proteção e no tratamento de dados pessoais. Esses personagens são definidos para estabelecer responsabilidades claras em relação ao tratamento de dados pessoais. Eles incluem:

1. **Titular dos dados → é a pessoa natural a quem se referem os dados pessoais. O titular tem diversos direitos garantidos pela LGPD, como o direito de acesso, correção, exclusão e informação sobre o uso de seus dados.**
2. **Controlador → pessoa natural ou jurídica, de direito público ou privado, que toma as decisões referentes ao tratamento de dados pessoais. O controlador é responsável por definir a finalidade e os meios de tratamento dos dados.**
3. **Operador → pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador age segundo as instruções do controlador.**
4. **Encarregado (*Data Protection Officer* – DPO) → pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).**
5. **Autoridade Nacional de Proteção de Dados (ANPD) → órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. A ANPD tem a responsabilidade de estabelecer normas e diretrizes para a Política Nacional de Proteção de Dados Pessoais.**

Esses "personagens" são essenciais para o funcionamento eficaz do regime de proteção de dados estabelecido pela LGPD, garantindo tanto a proteção dos direitos dos titulares dos dados quanto o tratamento adequado e legal desses dados por parte das organizações.

2.5.16 Sigilo

O sigilo é um dos pilares da LGPD e é crucial para manter a confiança do público. Ele deve ser mantido em todas as etapas do tratamento de dados pessoais, desde a coleta até o armazenamento e a eliminação. Isso é especialmente verdadeiro para dados sensíveis ou estigmatizantes, que podem incluir informações médicas, financeiras ou outras informações pessoais que poderiam ser prejudiciais se divulgadas.

2.5.17 Guarda dos dados

A guarda dos dados vai além do simples armazenamento. Ela envolve uma série de medidas de proteção para garantir que os dados estejam seguros. Isso inclui o uso de criptografia de ponta a ponta, *firewalls* robustos e outras tecnologias de segurança. Além disso, é importante realizar auditorias de segurança regulares e manter becapes seguros para prevenir perdas de dados.

2.5.18 Responsabilidades sobre dados pessoais

As responsabilidades sobre dados pessoais não se limitam apenas à organização que coleta os dados, mas se estendem a todos os indivíduos envolvidos no tratamento deles. Isso inclui funcionários, fornecedores e até mesmo terceiros que possam ter acesso aos dados. Cada um tem um papel a desempenhar e responsabilidades claras que devem ser documentadas e seguidas rigorosamente. Isso é crucial para garantir a integridade e a segurança das informações pessoais.

É importante ter em mente que, em caso de haver vazamento de dados, as pessoas envolvidas em toda a cadeia de custódia podem ser responsabilizadas em maior ou menor medida. Por isso, é importante colher termos de responsabilidade e sigilo de todos os colaboradores envolvidos no tratamento de dados pessoais.

2.5.19 *Traffic Light Protocol* (TLP)

Uma forma de implementar a segurança da informação em relação aos dados pessoais pode ser utilizando os sinais de trânsito de informação, conforme recomendado pelo Centro Integrado de Segurança Cibernética (Cisc) do Governo Digital[1].

De acordo com o Cisc, "O *Traffic Light Protocol* (TLP) é um padrão desenvolvido pelo *Forum of Incident Response and Security Teams* (FIRST) e tem como objetivo indicar limites de compartilhamento de informações entre pessoas, organizações ou comunidades[1]".

[1]Para mais informações sobre o TLP, sugerimos utilizar as informações disponíveis neste link: https://www.gov.br/cisc/pt-br/tlp#:~:text=O%20Traffic%20Light%20Protocol%20(TLP,entre%20pessoas%2C%20organiza%C3%A7%C3%B5es%20ou%20comunidades.

3 | PRIVACIDADE DE DADOS NA SVSA

A LGPD e as normativas correlatas têm um impacto direto e significativo na Secretaria de Vigilância em Saúde e Ambiente do Ministério da Saúde (SVSA/MS). Essa Secretaria lida com análise e monitoramento de **dados sensíveis** e **estigmatizantes** relacionados à saúde dos cidadãos, além da salvaguarda e preservação dos conjuntos de dados onde estes estão coletados.

O tratamento de dados pelas áreas técnicas deve seguir as diretrizes estabelecidas e as melhores práticas internacionais, de forma a assegurar a privacidade dos dados e a segurança das informações tratadas na SVSA. As pessoas envolvidas no tratamento de dados são o fundamento para que a integridade, a privacidade e a segurança de dados, bem como as informações, sejam garantidos.

SAIBA MAIS: você sabia que a LGPD também se aplica a dados processados fora do Brasil? Isso é especialmente relevante para empresas multinacionais e serviços on-line que coletam dados de cidadãos brasileiros. Mesmo que o processamento ocorra em outro país, se a atividade afetar indivíduos no Brasil, a LGPD será aplicável.

FIQUE DE OLHO

"O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (Brasil, 2018).

Para saber mais sobre o tema, consulte os links indicados ao final deste Guia.

3.1 LEI DE ACESSO À INFORMAÇÃO

3.1.1 O que é

A Lei de Acesso à Informação (LAI), oficialmente conhecida como Lei n.º 12.527, foi sancionada em 18 de novembro de 2011. Ela serve como um guia para o acesso a informações públicas e representa um marco significativo na transparência pública no Brasil. A LAI não apenas permite que os cidadãos tenham acesso a informações que são de interesse público, mas também estabelece regras claras para os órgãos governamentais sobre como disponibilizar essas informações.

3.1.2 Como se aplica à SVSA

A LAI tem um impacto direto na Secretaria de Vigilância em Saúde e Ambiente do Ministério da Saúde (SVSA/MS). A Vigilância em Saúde constitui um processo contínuo e sistemático de coleta, consolidação, qualificação/análise de dados e disseminação de informações acerca de eventos relacionados à saúde, visando ao planejamento e à implementação de medidas de saúde pública. Assim, a LAI permite que informações públicas, como relatórios de saúde e estatísticas, sejam facilmente acessíveis aos cidadãos. No entanto, é importante notar que algumas informações podem ser classificadas como sigilosas por lei, portanto não estão disponíveis para o público em geral.

3.1.3 Direitos e deveres

Os cidadãos têm o direito fundamental de acessar informações públicas e isso é garantido pela LAI. Por outro lado, os órgãos públicos, incluindo a SVSA/MS, têm o dever legal de fornecer essas informações de forma transparente e eficaz. No entanto, é crucial entender que algumas informações podem ser classificadas como sigilosas por razões de segurança nacional ou proteção de dados sensíveis, e essas são exceções ao acesso público.

3.1.4 Quando solicitar informações via LAI

Quando dados considerados públicos não estão disponíveis em acesso aberto, qualquer pessoa (natural ou jurídica) pode solicitar acesso a documentos públicos, dados e informações sobre política e programas de governo, entre outras informações.

3.1.5 Como solicitar dados via LAI

Antes da solicitação, é recomendável verificar se a informação está disponível e então proceder com a solicitação dos dados. No caso do governo federal, é necessário acessar o módulo LAI do portal Fala.BR[2].

[2]https://falabr.cgu.gov.br/web/home.

3.1.6 Quais as diferenças e as semelhanças entre LGPD e LAI

LGPD

Lei Geral de Proteção de Dados

1. Tratar dados pessoais
2. Avaliar alcance territorial da lei e transferência internacional de dados
3. Reportar-se à Autoridade Nacional de Proteção de Dados (ANPD)
4. Adequar-se com pelo menos uma das dez bases legais
5. Definir o tratamento de dados sensíveis
6. Manter o registro do processamento dos dados
7. Gerenciar o direito dos titulares
8. Nomear um encarregado/DPO de proteção de dados
9. Reportar as violações de dados
10. Gerenciar a previsão das sanções

LAI

Lei de Acesso à Informação

1. Acesso à informação
2. Alcance dos entes públicos, em regra
3. Assegurar a disponibilidade, autenticidade e integridade da informação
4. Desenvolver a cultura de transparência na Administração Pública
5. Aplicação dos princípios constitucionais
6. Qualquer um pode pedir acesso às informações públicas
7. Informações pessoais são restritas, as comuns e sensíveis
8. Os agentes públicos são responsabilizados por suas condutas
9. Não será dado acesso a informações classificadas como sigilosas
10. A autoridade poderá negar acesso às informações públicas

Fonte: https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd.

Quadro comparativo entre a LGPD e a LAI

		LAI Lei de Acesso à Informação	LGPD Lei Geral de Proteção de Dados
1	Tratamento da informação	Art. 4º, III, IV, V; art. 25, 26, 31, 34, 35, 36, 37.	Capítulo II – art. 7º ao 16, art. 23 ao 32, art. 37 ao 45.
2	Disponibilidade, autenticidade e integridade	Art. 4º, VI, VII, VIII; art. 6º, 8º & 3º, V, 13, 23, 35, III.	Art. 17, 18, 19, 20, 26.
3	Segurança	Art. 3º, 7º, 11, 23, 24, 26, 36, 37.	Art. 6º, 11, 12, 13, 26, 34, 38, 40, 44, 46, 47, 48, 49, 50, 55-J.
4	Entes públicos	Art. 1º e 2º	Art. 23 ao 32, Capítulo IV.

Fonte: https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd.

3.2 LEI N.º 14.289/2022 – LEI DO SIGILO SOROLÓGICO

3.2.1 O que é

A Lei n.º 14.289, de 3 de janeiro de 2022, estabelece a obrigatoriedade de preservar o sigilo sobre a condição de pessoas que vivem com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV), bem como de pessoas com hanseníase e tuberculose. Essa Lei também altera a Lei n.º 6.259, de 30 de outubro de 1975. Ela proíbe a divulgação de informações que permitam identificar a condição de tais pessoas em diversos âmbitos, incluindo serviços de saúde, estabelecimentos de ensino, locais de trabalho, Administração Pública, segurança pública, processos judiciais e mídia escrita e audiovisual.

3.2.2 Como se aplica à SVSA

A Lei n.º 14.289/2022 tem um impacto direto na Secretaria de Vigilância em Saúde e Ambiente do Ministério da Saúde. Ela estabelece diretrizes adicionais para o tratamento de dados sensíveis e estigmatizantes em saúde, como informações sobre doenças crônicas ou condições que possam ser discriminatórias. Isso significa que a SVSA/MS deve seguir protocolos rigorosos para garantir que esses dados sejam tratados com o máximo cuidado e confidencialidade, incluindo a anonimização ou a exclusão

desses dados quando não forem estritamente necessários ao tratamento em questão. Isso inclui informações sobre doenças e agravos como HIV/aids, hepatite, tuberculose e hanseníase.

3.2.3 Direitos e deveres

Tal como acontece com outras leis de proteção de dados, a Lei n.º 14.289/2022 estabelece direitos e deveres para os cidadãos e para as instituições públicas. Ela reforça a necessidade de transparência, responsabilidade e cuidado no tratamento de dados pessoais, especialmente aqueles que são sensíveis ou estigmatizantes. Isso inclui a obrigação de obter consentimento explícito para o uso desses dados e a responsabilidade de mantê-los seguros.

PARA SABER MAIS

Acesse o texto da Lei.

4 APLICANDO A LGPD E OUTRAS LEGISLAÇÕES NA SVSA

4.1 NÚCLEO DE GOVERNANÇA DE DADOS E OUTRAS INSTÂNCIAS

O Núcleo de Governança de Dados (NGD) é responsável por garantir a conformidade com a LGPD e outras leis relacionadas à proteção de dados dentro da SVSA. Possui infraestrutura específica para acesso e tratamento de dados identificados dos sistemas sob sua gestão.

4.2 SALA DE ACESSO RESTRITO

A Sala de Acesso Restrito (SAR) é utilizada para controlar o acesso a dados pessoais e sensíveis; nesse ambiente, restrito e seguro, são armazenadas as bases de dados nacionais sob gestão do Daent. É onde são realizadas as rotinas de tratamento e a manipulação de dados, visando garantir a segurança dos dados nela contidos.

4.3 QUEM SÃO OS GUARDIÕES

Os guardiões são os responsáveis por realizar o tratamento de rotina das bases, além de conceder autorização para que pessoas interessadas possam acessar os dados dos sistemas de informação do MS. Também se encarregam, em cada área técnica, por garantir a segurança e a integridade dos dados. Eles são treinados e habilitados para gerenciar o acesso e a utilização dos dados.

4.4 ENCARREGADOS DE DADOS

O encarregado de dados é responsável por supervisionar o cumprimento da LGPD e de outras leis de proteção de dados dentro da organização. Ele atua como um ponto de contato entre o Ministério da Saúde e os titulares dos dados, sendo responsável por garantir que os dados sejam tratados de forma ética e segura.

5 | COMO ACESSAR DADOS NA SVSA

5.1 QUEM PODE ACESSAR OS DADOS?

Em princípio, qualquer cidadão pode solicitar o acesso a seus dados pessoais. Isso porque o titular do dado tem o direito de solicitá-lo, assim como de fazer correções, anonimizações, bloqueios e eliminações. O acesso aos dados pessoais por outros interessados (pessoas naturais ou jurídicas), a exemplo da lista de pessoas de interesse referidas anteriormente, deve seguir os princípios elencados na LGPD e as regulamentações definidas pela SVSA. É necessário que a pessoa solicitante encaminhe o pedido para a instância correta dentro da instituição, ou seja, a área responsável pela vigilância do agravo/doença e/ou gestora do sistema de informação que contém as informações de interesse, e siga os protocolos internos definidos por estas instâncias.

5.2 NORMAS E DOCUMENTOS

Os tratamentos de dados realizados pelo Ministério da Saúde se dão de acordo com o art. 7°, incisos II, III, IV, VI e IX, e o art. 11, inciso II, alíneas "a", "b" e "c", bem como os artigos 23 e 26, todos da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.° 13.709/2018, e limitam-se ao cumprimento de obrigações legais e regulatórias, execução de políticas públicas, execução de contrato e realização de estudos de pesquisa. Ressalta-se que o tratamento de dados pessoais de crianças e de adolescentes realizado pela SVSA é feito no melhor interesse daqueles, nos termos da legislação pertinente.

Uma vez identificada a possibilidade de solicitar dados, informações e documentos, há alguns caminhos que o solicitante precisa seguir para acessá-los. Primeiro, é preciso verificar se o pedido segue os princípios da LGPD (art. 6º), especialmente os princípios da finalidade, da adequação, da necessidade, da não discriminação, da responsabilização e da prestação de contas. É importante ter em mente que nem sempre será necessário acesso aos dados identificados ou às bases completas por meio da Sala de Acesso Restrito (SAR). A infraestrutura de dados do governo federal fornece várias possibilidades para que pessoas naturais ou jurídicas possam acessar dados, a saber:

5.3 PROTOCOLO – ACESSO POR MEIO DA LAI OU LGPD

O Serviço de Informação ao Cidadão (SIC) pode ser acessado pelo link **https://www.gov.br/saude/pt-br/acesso-a-informacao/sic** ou pelo Fala.BR, pelo link **https://falabr.cgu.gov.br/web/home**. Por meio desse serviço, é possível fazer a solicitação de pedido de informação de dados e documentos públicos, conforme explicado nas partes 1 e 2 deste Guia.

5.4 TRANSPARÊNCIA ATIVA – PORTAL OPENDATASUS (DADOS ABERTOS)

O Ministério da Saúde disponibiliza bases desidentificadas por meio do portal OpenDataSUS ou pelo portal de Dados Abertos. São diversos conjuntos de dados que podem ser baixados por qualquer pessoa com acesso à internet.

Antes de realizar o encaminhamento de pedidos para acesso ou tratamento de dados pela SVSA, é importante verificar se os dados que você precisa estão disponíveis nos links:

https://dados.gov.br/dados/organizacoes/visualizar/ministerio-da-saude;
https://opendatasus.saude.gov.br/.

Outra opção de acesso aos dados é o programa TABNET, disponível em:
https://datasus.saude.gov.br/informacoes-de-saude-tabnet/.

5.5 GOV.BR – INTEROPERABILIDADE DE ID

Também vale a pena citar, mencionando iniciativas governamentais, que o portal gov.br, mantido pela Secretaria de Governo Digital, possui mais de 5 mil serviços disponíveis aos cidadãos. Com a disponibilidade das contas prata e ouro e por meio de aplicativo próprio, é possível acessar dados como o cartão de vacinação.

Para acessar os serviços com o ID único do governo, é necessário realizar cadastro no site **acesso.gov.br/** e identificar qual órgão fornece os serviços ou as informações de que se necessita. A partir daí, pode-se solicitar acesso aos dados e às informações via aplicativo específico ou por meio de solicitação por protocolo.

6 | PERGUNTAS FREQUENTES

6.1 PERGUNTAS E RESPOSTAS FREQUENTES SOBRE A LGPD

6.1.1 O que é a LGPD?

A LGPD, ou Lei Geral de Proteção de Dados Pessoais, é a legislação brasileira que estabelece diretrizes para coleta, processamento e armazenamento de dados pessoais, além de garantir direitos aos indivíduos a quem os dados se referem.

6.1.2 Quais direitos a LGPD garante aos titulares dos dados?

A LGPD garante uma série de direitos, incluindo o direito de acesso, correção, exclusão, portabilidade dos dados, informação sobre compartilhamento de dados e revogação do consentimento.

6.1.3 Quem precisa cumprir a LGPD?

Todas as empresas e organizações que tratam dados pessoais de indivíduos no Brasil ou que coletam dados de cidadãos localizados no Brasil devem seguir as diretrizes da LGPD, independentemente do país em que a empresa está sediada.

6.1.4 Qual é a diferença entre dado pessoal e dado sensível?

Dado pessoal é qualquer informação que possa identificar uma pessoa. Dado sensível é um subconjunto de dados pessoais que inclui informações sobre origem racial, convicções religiosas, opinião política, saúde, vida sexual.

6.2 PERGUNTAS E RESPOSTAS FREQUENTES SOBRE A LAI

6.2.1 O que é a Lei de Acesso à Informação?

A Lei de Acesso à Informação (Lei n.º 12.527/2011) é a legislação brasileira que regula o direito constitucional de acesso dos cidadãos às informações públicas. A LAI estabelece procedimentos para que o poder público promova a transparência e permita que as pessoas solicitem e recebam informações públicas de maneira eficaz.

6.2.2 Quem pode solicitar informações com base na LAI?

Qualquer cidadão, brasileiro ou estrangeiro, sem a necessidade de justificar a solicitação, tem o direito de solicitar informações aos órgãos e às entidades do poder público no âmbito federal, estadual e municipal.

6.2.3 Quais informações podem ser acessadas pela LAI?

Com a LAI, é possível acessar qualquer informação pública que não esteja classificada como sigilosa, incluindo dados sobre a Administração Pública, gastos governamentais, processos administrativos, políticas públicas e outros dados de interesse da sociedade.

6.2.4 Como posso solicitar informações por meio da LAI?

As informações podem ser solicitadas pessoalmente, nos Serviços de Informações ao Cidadão dos órgãos públicos, ou eletronicamente, por meio do site **https://www.gov.br/acessoainformacao/pt-br/assuntos/pedidos**.

7 | CONSIDERAÇÕES E RECOMENDAÇÕES

O presente Guia foi elaborado com o objetivo de trazer mais segurança para o tratamento de dados dentro da SVSA. Destaca-se que o material aqui contido não descarta futuras atualizações, orientações e regulamentações sobre o tema da privacidade de dados e segurança de informação. Recomenda-se o acompanhamento constante de decisões proferidas pelas autoridades competentes.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Documentos e publicações**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 14 fev. 2025.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Vazamento de dados.** Brasília, DF: NIC.br, 2024. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 14 fev. 2025.

BRASIL. Decreto n.º 8.771, de 11 de maio de 2016. Regulamenta a Lei n.º 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela Administração Pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Diário Oficial da União**: seção 1, Brasília, DF, 12 maio 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 14 fev. 2025.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Marco Civil da Internet – estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União:** seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/L12965.htm. Acesso em: 14 fev. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União:** seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 fev. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD) – Texto compilado. Brasília, DF: Presidência da República, 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 14 fev. 2025.

BRASIL. Lei n.º 14.460, de 25 de outubro de 2022. Altera a Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais –, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza

especial e transforma cargos em comissão. **Diário Oficial da União:** seção 1, Brasília, DF, 26 out. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em: 14 fev. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Instrução Normativa SGD n.º 117, de 19 de novembro de 2020. Dispõe sobre a indicação do encarregado pelo tratamento dos dados pessoais no âmbito dos órgãos e das entidades da Administração Pública Federal direta, autárquica e fundacional. **Diário Oficial da União:** seção 1, Brasília, DF, 20 nov. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596. Acesso em: 14 fev. 2025.

Referência atualizada

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Boas Práticas para Implementação na Administração Pública Federal: Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF: MGI, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 6 out. 2025.

BRASIL. Ministério da Saúde. **Dados abertos do Ministério da Saúde**. Brasília, DF: MS, 2024. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/dados-abertos. Acesso em: 14 fev. 2025.

BRASIL. Ministério da Saúde. **Decisões sobre a LGPD no Ministério da Saúde.** Brasília, DF: MS, 2024. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/decisoes. Acesso em: 14 fev. 2025.

BRASIL. Ministério da Saúde. **Lei Geral de Proteção de Dados (LGPD) no Ministério da Saúde**. Brasília, DF: MS, 2024. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd. Acesso em: 14 fev. 2025.

BRASIL. Ministério da Saúde. **Serviço de Informação ao Cidadão (SIC).** Brasília, DF: MS, 2024. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/sic. Acesso em: 14 fev. 2025.

ESPÍNDOLA ARGENTI, H. **How does the legal bases for processing personal data differ between GDPR and LGPD**? 2022. Dissertação (Mestrado em Direito da Informação e Comunicação) – Universidade de Oslo, Oslo, 2022. Disponível em: https://www.duo.uio.no/handle/10852/101162?locale-attribute=en. Acesso em: 14 fev. 2025.

GODINHO, A. M. *et al.* **Tutela jurídica do corpo eletrônico: novos desafios ao direito digital.** Brasília, DF: Editora Foco, 2022.

LANDERDAHL, R. *et al*. **Tratamento de dados pessoais pelo Poder Público***:* guia orientativo. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 11 fev. 2025.

VARGAS, G. *et al.* **Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas***:* guia orientativo. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 14 fev. 2025.

Referência anterior

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de privacidade e proteção de dados na administração pública.** Brasília, DF: MGI, 2024. Disponível em: https://www.gov.br/governodigital/ptbr/privacidade_e_seguranca/guias/guia_lgpd.pdf. Acesso em: 14 fev. 2025.

GLOSSÁRIO

GLOSSÁRIO SIMPLIFICADO PARA A LGPD

Acesso: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer ou eliminar dados.

Agentes de tratamento: o Controlador e o Operador.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Armazenamento: ação ou resultado de manter ou conservar em repositório um dado.

Arquivamento: ato ou efeito de manter registrado um dado, embora já tenha perdido a validade ou esteja esgotada a sua vigência;

- **avaliação:** ato ou efeito de calcular valor sobre um ou mais dados;
- **classificação:** maneira de ordenar os dados conforme algum critério estabelecido;
- **coleta:** recolhimento de dados com finalidade específica;
- **comunicação:** transmitir informações pertinentes a políticas de ação sobre os dados;
- **controle:** ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- **difusão:** ato ou efeito de divulgação, propagação, multiplicação dos dados;
- **distribuição:** ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- **eliminação:** ato ou efeito de excluir ou destruir dado do repositório;

- **extração:** ato de copiar ou retirar dados do repositório em que se encontrava;
- **modificação:** ato ou efeito de alteração do dado;
- **processamento:** ato ou efeito de processar dados;
- **produção:** criação de bens e de serviços a partir do tratamento de dados;
- **recepção:** ato de receber os dados ao final da transmissão;
- **reprodução:** cópia de dado preexistente obtido por meio de qualquer processo;
- **transferência:** mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- **transmissão:** movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
- **utilização:** ato ou efeito do aproveitamento dos dados.

Autoridade Nacional de Proteção de Dados (ANPD): autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, responsável por zelar, implementar e fiscalizar o cumprimento da Lei n.º 13.709, de 14 de agosto de 2018, em todo o território nacional.

Avaliação de impacto à proteção de dados pessoais: documentação que o controlador pode ter que preparar com uma descrição dos processos de tratamento de dados, avaliando os riscos para a privacidade e as medidas para mitigar esses riscos.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado anonimizado: dado relativo ao titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dados pessoais: informação relacionada à pessoa natural identificada ou identificável.

Dados pessoais sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político; dado referente à saúde ou à vida sexual; dado genético ou biométrico.

Dados pseudonimizados: dados que não podem ser atribuídos a um titular específico sem o uso de informações adicionais mantidas separadamente.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da Administração Pública Federal em seu âmbito de atuação.

Incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental.

Interesse público: condição que pode justificar a divulgação de informações, desde que observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

Legítimo interesse: hipótese legal que autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses do controlador ou de terceiros, desde que compatíveis com o ordenamento jurídico, lastreados em situações concretas e vinculados a finalidades legítimas, específicas e explícitas, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, respeitados os direitos e a legítima expectativa do titular.

Lei Geral de Proteção de Dados (LGPD): lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Medidas de segurança: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Medidas de segurança, técnicas e administrativas: medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Órgão de pesquisa: órgão ou entidade da Administração Pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua, em sua missão institucional ou em seu objetivo social ou estatutário, a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Princípio da adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Princípio da finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Princípio da não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Princípio da 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.

Princípio da 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.

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Suboperador: contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

Titular dos dados: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento: toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Violação de dados pessoais: incidente de segurança que acarreta destruição, perda, alteração, comunicação ou acesso não autorizados a dados pessoais.

GLOSSÁRIO SIMPLIFICADO PARA A LEI DE ACESSO À INFORMAÇÃO

Acesso negado: situação em que um pedido de informação é recusado com base em exceções previstas na LAI ou em outras leis aplicáveis.

Classificação de informação: grau de sigilo de informação definido em razão de sua imprescindibilidade à segurança da sociedade ou do Estado como ultrassecreta, secreta ou reservada.

Controladoria-Geral da União: órgão responsável por garantir a correta aplicação da LAI no âmbito do Poder Executivo Federal.

Consulta pública: processo em que o poder público solicita a colaboração da sociedade para a discussão de determinados temas ou projetos, garantindo ampla participação e utilização das informações disponibilizadas.

Dados abertos: dados que são disponibilizados por órgãos e entidades públicas, de forma livre e desimpedida, para uso e reutilização pela sociedade, normalmente em formatos que permitem tratamento automatizado.

Desclassificação: ato administrativo que retira o grau de sigilo de uma informação.

Desclassificação de informação: processo pelo qual uma informação anteriormente classificada como sigilosa tem o seu grau de sigilo removido, tornando-se acessível ao público.

Informação pública: dado ou documento produzido ou custodiado por órgãos ou entidades públicas, acessível a qualquer cidadão, contudo nem todos passíveis de disponibilização.

Informação sigilosa: informação que, em razão de seu conteúdo e sua relevância, tem o acesso restrito por um determinado período.

Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, com acesso restrito por um determinado período para a proteção da privacidade.

Informação classificada: informação que foi submetida a um processo de classificação devido à sua sensibilidade e que necessita de proteção para evitar divulgação que possa prejudicar a segurança do Estado ou de indivíduos.

Lei de Acesso à Informação: legislação que regula o acesso a informações públicas no Brasil.

Órgão ou entidade pública: instituições que integram a estrutura do Estado, inclusive o Poder Executivo, Legislativo e Judiciário, em todos os níveis de governo, responsáveis por custodiar e proporcionar acesso às informações públicas, conforme estipulado pela LAI.

Ouvidoria: canal disponibilizado por órgãos e entidades para que os cidadãos possam registrar reclamações, elogios, solicitações e denúncias, inclusive em relação ao acesso à informação.

Prazo de sigilo: tempo durante o qual a informação permanecerá classificada antes que possa ser reavaliada para desclassificação ou acesso público.

Pedido de informação: solicitação de acesso a informações públicas feita por qualquer cidadão.

Proteção da informação: conjunto de medidas de segurança que visam resguardar as informações de acessos, usos, divulgações, alterações, críticas ou distorções não autorizadas.

Restrição de acesso: hipóteses legais que justificam a não disponibilização de certas informações ao público geral, como informações pessoais ou sigilosas.

Recursos: instrumentos que o cidadão pode utilizar para contestar uma negativa de acesso ou a não resposta a um pedido de informação dentro dos prazos previstos.

Recursos da LAI: mecanismos de apelação disponíveis aos cidadãos para contestar decisões sobre pedidos de acesso a informações. Inclui recursos a instâncias superiores dentro do próprio órgão e à CGU.

Relatório estatístico: apresentação de dados sobre a quantidade de pedidos de informação recebidos, atendidos e negados, bem como sobre as principais categorias de informações solicitadas.

Reclassificação: ato pelo qual uma informação que havia sido desclassificada ou teve o grau de sigilo reduzido torna-se novamente classificada devido a uma reavaliação da necessidade de proteção.

Sistema Eletrônico do Serviço de Informações ao Cidadão (e-SIC): plataforma on-line por meio da qual se podem enviar pedidos de acesso à informação aos órgãos e às entidades do poder público, acompanhar prazos e receber respostas.

Sobrestamento: condição temporária na qual um pedido de informação fica retido devido à necessidade de análise mais detalhada ou aguardando o término do prazo de sigilo.

Transparência: princípio que orienta a atuação do poder público, promovendo a abertura de informações e processos à sociedade, sendo um dos fundamentos da LAI para fortalecer a democracia e incentivar a participação social.

Transparência ativa: obrigatoriedade dos órgãos e das entidades públicas de divulgar uma série de informações de interesse público, independentemente de solicitações.

Transparência passiva: direito do cidadão de requerer informações públicas aos órgãos e às entidades sem necessidade de justificativas.

Utilização de informações públicas: referente ao direito de usar as informações acessadas para qualquer fim lícito, respeitando-se, no entanto, os atributos relativos a direitos autorais e a informações pessoais ou sigilosas.

Lembre-se de que este é apenas um glossário básico. Para uma compreensão integral, consulte as legislações completas e as resoluções das autoridades citadas neste Guia.

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

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

Ouv SUS 136 Ouvidoria-Geral do SUS

SUS

MINISTÉRIO DA SAÚDE

Governo Federal