# Segurança da informação

Resumo de políticas públicas

8 princípios orientadores da transformação digital do setor da saúde

Caixa de ferramentas de transformação digital

OPAS Organização Pan-Americana da Saúde
Organização Mundial da Saúde Américas

## ORGANIZAÇÃO, COORDENAÇÃO E DESENVOLVIMENTO

Departamento de Evidência e Inteligência para Ação em Saúde (EIH) da Organização Pan-Americana da Saúde (OPAS), em colaboração com o Centro de Implementação e Inovação em Políticas de Saúde (CIIPS), parte do Instituto de Efetividade Clínica e Sanitária (IECS), um Centro Colaborador da OPAS.


## AGRADECIMENTOS

A OPAS deseja agradecer ao Governo dos Estados Unidos da América pela contribuição financeira que tornou possível a elaboração desta importante obra, parte de uma caixa de ferramentas para apoiar o fortalecimento da implementação da iniciativa regional de telessaúde na luta contra as doenças não transmissíveis.

## RECONHECIMENTO

A OPAS reconhece e agradece o apoio da Agência Espanhola de Cooperação Internacional para o Desenvolvimento (AECID), da Agência dos Estados Unidos da América para o Desenvolvimento Internacional (USAID), do Governo do Canadá e Banco Interamericano de Desenvolvimento (BID), bem como da rede de especialistas que apoiam a iniciativa de sistemas de informação para a saúde da OPAS.

# Sumário

# Resumo

Um dos oito princípios orientadores da transformação digital do setor da saúde promovidos pela Organização Pan-Americana da Saúde (OPAS) é a **segurança da informação**. Este resumo de políticas públicas apresenta conceitos essenciais, linhas de ação recomendadas e indicadores para o monitoramento visando ao avanço da segurança da informação.

De acordo com a definição da OPAS, esse princípio visa a **estabelecer mecanismos de confiança e segurança da informação para o ambiente digital de saúde pública**. "Adotar instrumentos regulatórios sobre o tratamento e proteção de dados de saúde sensíveis, bem como diretrizes e padrões de segurança internacionais para sistemas de informação centrados no paciente. Esses sistemas devem ser implantados respeitando os direitos relativos à saúde para gerar uma 'cultura de gestão segura e confiável dos dados', ou seja, com equilíbrio entre a necessidade de acesso aos dados e a privacidade" *(1)*.

No contexto da saúde, as informações a serem protegidas não têm apenas caráter de bem, mas também envolvem dimensões éticas, legais e técnicas que devem ser resguardadas. Em termos da norma ISO, a segurança desses dados é definida como a preservação do sigilo, da integridade e da disponibilidade das informações. Dessa definição se depreendem os três elementos que, fundamentalmente, precisam ser considerados pelos mecanismos de segurança para que sejam funcionais nas organizações nas quais são implementados.

A segurança da informação, portanto, é estabelecida como uma base fundamental para o desenvolvimento bem-sucedido de qualquer organização, instituição ou sistema e envolve estratégias, planejamento e avanços implementados para proteger as informações contra riscos de ataque que tornariam possível o uso impróprio ou ilegal do bem em custódia.

Neste documento, faz-se uma revisão do estado atual da segurança da informação e se fornecem recomendações, linhas de ação e indicadores de monitoramento da segurança. É importante concentrar-se em um plano de ação que inclua, como princípios indissociáveis de sua eficácia, o desenvolvimento de um plano de segurança e proteção de dados enquadrado em políticas públicas e em conformidade com a legislação; a existência de uma estrutura de controle sobre o fluxo de informações em saúde, incluindo recomendações de segurança informática e riscos associados; o estabelecimento de mecanismos de monitoramento que permitam a detecção de incidentes; a geração de instâncias de arquivamento de consentimento informado; a centralização das certificações de segurança; e a promoção e elaboração de planos de formação continuada e desenvolvimento de pessoal.

Além disso, é preciso dispor de instrumentos normativos relacionados à proteção de dados sensíveis na área da saúde e de diretrizes internacionais sobre a segurança dos sistemas de informação para a saúde (SIS), a fim de promover o bom uso dos dados no que se refere ao equilíbrio entre acesso e privacidade.

**Palavras-chave:** segurança, ética, acessibilidade, sigilo, dados sensíveis, normas.

# Introdução

Segundo a declaração da Organização Pan-Americana da Saúde durante a Conferência de Alto Nível sobre Sistemas de Informação para a Saúde, realizada em fevereiro de 2021, é imprescindível proteger as informações sensíveis de saúde; em vista disso, é preciso colaborar e cocriar mecanismos para garantir a confidencialidade e a segurança das informações pessoais no ambiente digital de saúde pública, promovendo simultaneamente o acesso e a transparência nas informações e no conhecimento.

Pensar na segurança da informação significa levar em conta quais informações são disponibilizadas, por quais meios, para quem, onde ficam alojadas, como esses dados são processados, dentro de quais marcos regulatórios e normativos estão incluídos (ou quais é preciso criar) e como promover cenários e fluxos nos quais os direitos relacionados à saúde sejam respeitados. Por outro lado, deve-se assumir o desafio de garantir acesso fluido e transparente às informações, assegurando ao mesmo tempo o sigilo e privacidade das informações sensíveis, como as que estão associadas ao vínculo de pessoas ao sistema de saúde.

Os desafios enfrentados na busca por estratégias robustas e pelo equilíbrio entre a necessidade de acesso às informações em saúde e as particularidades de privacidade e segurança inerentes aos dados sensíveis nos convidam a considerar várias dimensões para abordar o princípio da segurança da informação.

Além da adoção de instrumentos normativos sobre o tratamento e a proteção de dados sensíveis de saúde, é importante conhecer e implementar diretrizes e normas internacionais de segurança para sistemas de informação centrados no paciente e concentrar-se em seus aspectos mais específicos em ambientes jurisdicionais, sem limitar-se exclusivamente a uma dimensão técnica, mas criando e fortalecendo um percurso rumo a uma cultura de gerenciamento seguro e confiável de dados.

As tecnologias digitais podem ajudar a melhorar o acesso aos grupos populacionais em maior situação de vulnerabilidade no âmbito da saúde, mas é preciso desenvolver capital humano e infraestrutura que permitam usar as tecnologias digitais de forma inclusiva, ética e segura. Nesse cenário, a segurança da informação é um princípio central.

A abordagem integral e a revisão da segurança da informação implicam o estabelecimento de mecanismos de confiança no ambiente digital de saúde pública, com consideração para as dimensões éticas, técnicas e legais.

Partindo do princípio que as informações são um bem essencial para as atividades e considerando a necessidade de proteção adequada, convém destacar em primeiro lugar que os dados de saúde são considerados informações sensíveis; o habeas data é uma ação que permite aos indivíduos saber quais dos seus dados pessoais são armazenados e utilizados por terceiros e optar pela possibilidade de atualizá-los, modificá-los ou excluí-los. Na Argentina, por exemplo, leva-se em consideração o marco legal nacional, destacando a menção do uso de informações na Constituição Nacional e a existência de um conjunto de leis que tratam especificamente da proteção dos dados pessoais, dos direitos do paciente com relação aos profissionais e instituições de saúde e do acesso à informação pública.

A Organização Mundial da Saúde (OMS), por sua vez, publicou orientações referentes a aspectos de saúde digital e cibersegurança, ao desenvolvimento de ecossistemas de saúde interoperáveis e à elaboração de requisitos jurídicos que garantam códigos éticos para salvaguardar a segurança dos pacientes e dos dados. Já a Agência da União Europeia para a Cibersegurança (ENISA) publicou avisos e recomendações de boas práticas em segurança da informação, especialmente no que diz respeito à evolução e às tendências das ameaças (2). A Rede Ibero-Americana de Proteção de Dados procura promover as políticas e os avanços normativos necessários para garantir a regulamentação avançada do direito à proteção de dados pessoais (3). Por último, as normas ISO estabelecem os controles e estratégias necessários para eliminar ou minimizar os riscos (4).

Com base em experiências bem-sucedidas e na detecção de padrões para avançar na implementação, destacam-se três dimensões e condições necessárias:

- Definição de uma política de segurança da informação para os diferentes atores ou organizações.

- Garantia de coexistência das diferentes áreas em uma única rede.

- Definição de um marco normativo que regule a aplicação e o cumprimento das normas pelas partes intervenientes que estejam participando ou que desejem participar da rede.

O sucesso da execução das linhas de ação depende de uma clara definição de procedimentos e ao estabelecimento de objetivos com o aval e a participação ativa dos diversos atores envolvidos de forma coesa e articulada.

# Situação atual e identificação de lacunas

O primeiro aspecto a destacar é a **heterogeneidade dos marcos normativos existentes nos países da Região**. Observam-se diferentes estágios de desenvolvimento de normas *(5)*: Colômbia e Venezuela (Estado Plurinacional da) fazem menções a esse tópico em seus marcos constitucionais, e países como Argentina, Brasil, Chile, Peru, Paraguai e Uruguai têm também leis específicas sobre o tratamento dos dados pessoais.

A OPAS insta a identificar a necessidade de desenvolver normas que busquem um equilíbrio entre a acessibilidade e a privacidade para proteger o indivíduo sem atrasar ou bloquear o desenvolvimento de tecnologias de saúde digital *(1)*.

As diretrizes internacionais atuam como referências e orientações. Entretanto, é desejável gerar marcos próprios nas estratégias nacionais como um complemento às normas e diretrizes internacionais sobre proteção de dados. É possível detectar dificuldades específicas em alguns cenários nacionais devido à falta de mecanismos para garantir a segurança dos dados, à existência de heterogeneidades jurisdicionais relacionadas aos regulamentos e à ausência de acordos internacionais sobre padrões.

Em segundo lugar, é preciso desenvolver e estabelecer políticas públicas que incorporem um plano para a proteção e segurança dados de saúde, com foco em perfis de acesso em função de ações que o usuário precisa realizar.

Nesse aspecto, há dificuldades associadas **ao ambiente em constante evolução da segurança de dados e à falta de informação (em termos de números e da caracterização dos incidentes de cibersegurança na América Latina)**. Esse tipo de análise e monitoramento existe na União Europeia devido à ENISA *(2)*, que fornece informações atualizadas sobre a evolução e a tendência das ameaças e ajuda as partes interessadas a reconhecê-las e desenvolver estratégias de resposta. Além disso, oferece uma descrição geral das ameaças aos sistemas, dos agentes das ameaças e de tendências atuais e emergentes. Esse tipo de informação ainda não está disponível para a Região da América Latina.

Em terceiro lugar, há **poucos avanços em estratégias de capacitação sobre as diretrizes de segurança informática e os riscos associados para os atores envolvidos no fluxo de informações de saúde**. Essas estratégias fortaleceriam a formação de recursos humanos especializados que possam resolver incidentes de segurança e promoveriam o reconhecimento de leis gerais de proteção de dados *(5)* como instrumentos iniciais para estimular a discussão sobre responsabilidades pessoais e institucionais. Nesse sentido, um documento publicado pela Rede Ibero-Americana de Proteção de Dados procura fornecer um modelo de referência para a futura regulamentação na Região e uma revisão das normas vigentes relativas ao direito à proteção de dados em países que ainda não contam com marcos normativos ou que precisam atualizar a legislação existente *(3)*.

Além disso, **ainda não existem mecanismos de monitoramento que permitam detectar incidentes de segurança nos sistemas de informação em saúde**. Em vista disso, a estratégia nacional de cibersegurança precisa ser reforçada. Nessa área, a principal referência são as normas da Organização Internacional de Normalização *(4)*, que, embora estabeleçam controles e estratégias necessários para eliminar ou minimizar os riscos, não estão adaptadas a contextos locais.

Por último, **a população ainda não compreende seus direitos e responsabilidades com relação aos dados pessoais e à existência de instrumentos de consentimento informado para acesso, registro e proteção de informações confidenciais**. Por exemplo, na Argentina, a Lei 26.5296, aprovada em 2009, trata dos direitos do paciente na sua relação com profissionais e estabelecimentos de saúde e estabelece direitos essenciais na relação entre o paciente e os profissionais de saúde, as seguradoras e qualquer outro efetor.

Entre eles, menciona-se o sigilo, na medida em que o paciente tem o direito de que toda pessoa que participe da elaboração ou manipulação da documentação clínica, ou tenha acesso a seu conteúdo, mantenha a devida confidencialidade, salvo expressa disposição em contrário emitida por autoridade judicial competente ou com autorização do próprio paciente. Outros exemplos incluem a Lei Orgânica 459 de 2021 do Equador sobre proteção de dados pessoais *(6)* e a lei de proteção de dados pessoais da Colômbia, Lei 1581 de 2012 *(7)*.

Entretanto, **ainda é um desafio assumir o papel do paciente como titular dos dados e incentivar sua participação ativa no princípio da segurança**. Os usuários continuam não adotando o direito de exigir a proteção de suas informações, aplicações corretas de proteção dos dados e continuidade e robustez do monitoramento preventivo de anomalias.

# Linhas de ação

A OPAS propõe a segurança da informação como um dos oito princípios orientadores da transformação digital do setor da saúde (1,8,9), promovendo as seguintes linhas de ação:

**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).

Levando em conta a complexidade envolvida na conquista da segurança da informação, as linhas de ação recomendadas abrangem aspectos técnicos, legais, de planejamento e de gestão, tanto por parte das organizações quanto dos governos. Considerar a segurança desde o início, convidando a romper a lógica na qual ela aparece ligada somente a riscos e falhas ou em um estágio posterior de planejamento e implementação, fará com que as linhas de ação sejam mais organizadas, expansíveis e eficientes, tanto em nível institucional (no planejamento de fluxos), quanto em nível governamental (na criação do cenário mais sólido possível).

A seguir estão listadas algumas recomendações que complementam as linhas de ação estabelecidas pela OPAS no documento *8 princípios orientadores da transformação digital do setor da saúde*, que são úteis para os diferentes atores envolvidos na segurança da informação, desde instituições até agências do governo:

## 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

- Avaliar e definir um marco normativo que estabeleça as normas de aplicação para os participantes da rede. Esse marco deve estabelecer claramente as diretrizes mínimas de conformidade, bem como indicar claramente as sanções ou penalidades às quais os diferentes atores ou organismos estão expostos no que diz respeito ao acesso aos dados nos eixos da privacidade, sigilo e segurança da informação.

## 2. DESENVOLVER UMA ESTRUTURA DE CONTROLE SOBRE O FLUXO DE INFORMAÇÕES EM SAÚDE, COM ELEMENTOS DE DIRETRIZES DE SEGURANÇA INFORMÁTICA E RISCOS ASSOCIADOS

- Gerar mecanismos de auditoria que permitam fazer controle periódico dos diferentes organismos participantes da rede para garantir o cumprimento das normas de aplicação para os participantes da rede.

## 3. ARTICULAR MECANISMOS DE MONITORAMENTO QUE PERMITAM A DETECÇÃO DE INCIDENTES, ASSIM COMO A VERIFICAÇÃO DO CORRETO CUMPRIMENTO DOS PADRÕES E CONDIÇÕES DE ACESSO E TRATAMENTO DE INFORMAÇÕES

- Definir um plano de contingência e o funcionamento de uma unidade para coordenar emergências na rede de teleinformática, gerir eventuais incidentes de segurança e alertar os participantes da rede de forma a poder neutralizar tais ameaças de maneira preventiva ou corretiva. Essa unidade deve atuar como um repositório de informações sobre tais incidentes e divulgar as ferramentas e técnicas de defesa que devem ser aplicadas no âmbito da rede.

## 4. ESTABELECER FERRAMENTAS E INSTRUMENTOS DE CONSENTIMENTO INFORMADO PARA ARMAZENAMENTO E PROTEÇÃO DAS INFORMAÇÕES SENSÍVEIS

- Considerar as características das plataformas e da interface de acesso e a disponibilização de informações e enquadrá-las em um fluxo que exija compromisso formal e assinatura de termos de consentimento livre e esclarecido e acordos de confidencialidade que os usuários devem cumprir antes de acessar as informações consolidadas.

- Também se recomenda o monitoramento e acompanhamento desses acessos, com a respectiva validação.

## 5. CENTRALIZAR CERTIFICAÇÕES DE SEGURANÇA

- Criar serviços que permitam gerir de forma centralizada os aspectos inerentes à certificação de dados sensíveis de saúde por meio da utilização de tecnologias de certificação de cadeias de blocos (*blockchain*).

- Gerar mecanismos que permitam atualizar o marco normativo diante do surgimento de novas tecnologias ou pontos cegos que não tenham sido considerados, assegurando o cumprimento dos padrões de segurança.

## 6. ELABORAR E IMPLEMENTAR PLANOS DE COMUNICAÇÃO E CAPACITAÇÃO SOBRE DIREITOS E RESPONSABILIDADES EM RELAÇÃO AOS DADOS PESSOAIS

- Desenvolver documentos e espaços de formação, divulgação e conscientização para transmitir assertivamente o conhecimento sobre o marco legal vigente. É primordial que os atores envolvidos conheçam seus direitos e obrigações. A robustez técnica ou dos fluxos é inútil sem o respaldo de definições formais referentes a direitos, obrigações, regras do jogo e boas práticas a serem cumpridas pelas pessoas e instituições envolvidas no ciclo de vida das informações.

- No nível governamental, explicitar os direitos de cada pessoa com relação às suas informações e as obrigações por parte das instituições de fazer um tratamento correto. Essa dimensão deve estar presente na agenda.

## 7. ATUALIZAR NORMAS E FERRAMENTAS EXISTENTES RELACIONADAS À PROTEÇÃO DE DADOS

- Devido ao surgimento de novas tecnologias e cenários complexos, é preciso lembrar que a situação não é estática. É preciso ter a capacidade de gerar ciclos de melhoria contínua e atualização, tanto na dimensão técnica como normativa e ética, que incorporem ao longo do tempo todos os elementos novos que se sobrepõem ao princípio da segurança. Não basta definir uma série de medidas ou fazer um planejamento estático, é preciso também abordar situações que não estejam cobertas e ajustar e monitorar continuamente os processos.

- No caso dos governos, rever a vigência ou caducidade das normas que afetam esses fluxos, a fim de modificar ou promover a criação ou adesão a novos marcos normativos.

## 8. FORTALECER A ARTICULAÇÃO INTRA E INTERINSTITUCIONAL

- A articulação é outro aspecto fundamental. Do ponto de vista interno, em nível institucional, a segurança da informação é um elemento coeso e integrado aos demais princípios orientadores da transformação digital da saúde. Se houver várias áreas envolvidas dentro de uma organização, deve-se propiciar a coesão com relação à forma de lidar com o carregamento, o armazenamento, as solicitações e os fluxos para disponibilização. Do ponto de vista externo, é necessário conhecer o cenário jurisdicional, nacional e

internacional no qual a segurança da informação está enquadrada para o correto cumprimento e consideração das premissas e obrigações que precisam ser cumpridas.

- A criação de espaços e mesas de trabalho com outras instituições e áreas do governo permite fortalecer e reforçar os acordos. Recomendam-se iniciativas governamentais para convocar órgãos públicos para lidar com as informações a fim de aprofundar a dimensão da segurança; os órgãos no setor da saúde são um caso especial devido às características de seus dados.

## 9. DEFINIR REGRAS CLARAS PARA O FLUXO DE INFORMAÇÕES: CARREGAMENTO E DISPONIBILIZAÇÃO

- Em termos do carregamento e das características dos dados, um importante chamado à ação diz respeito à obtenção de uma referência exclusiva para a identidade do usuário e à criação de credenciais e perfis de habilitação para uso e acesso aos sistemas, capacitando ativamente os atores envolvidos em diretrizes de segurança informática, riscos associados e qualidade dos dados inseridos.

- Cada informação ou "informação bruta" resultante desse carregamento deve ser minuciosamente analisada em termos de suas características (nível de agregação, nominalização, conteúdo de informação sensível) e, com base nisso, deve-se definir quem pode acessá-la e em que formato, usando qual meio ou plataforma. É provável que esses dados precisem ser previamente processados, com anonimização e eliminação de possíveis identificadores indiretos.

# Indicadores de monitoramento

Com o objetivo de avançar no desenvolvimento e na implementação da segurança da informação em saúde, são propostos os indicadores a seguir. É importante esclarecer que esta lista não é exaustiva; cada país ou região pode incorporar outros indicadores, definir o nível de desagregação necessário e determinar a frequência de medição.

## INDICADORES TRANSVERSAIS AOS OITO PRINCÍPIOS ORIENTADORES DA TRANSFORMAÇÃO DIGITAL EM SAÚDE

- Existência de uma estratégia nacional de saúde digital estabelecida por meio de um instrumento normativo.
- Existência de uma estrutura institucional no governo para liderar a estratégia de transformação digital em saúde.
- Existência de um orçamento destinado a uma agenda digital que preveja os recursos humanos e tecnológicos necessários.

## INDICADORES ESPECÍFICOS DE SEGURANÇA DA INFORMAÇÃO

A identificação de indicadores de monitoramento da segurança da informação é fundamental para fazer um acompanhamento descomplicado e eficaz e comprovar que as condições que asseguram o armazenamento, acesso e tratamento adequados dos dados sejam devidamente cumpridas ou ajustadas.

Os procedimentos de monitoramento da proteção de dados pessoais requerem elementos organizados e coordenados que permitam alertar sobre potenciais riscos e lidar com incidentes de segurança que possam ameaçar as informações dos usuários. Recomenda-se que isso seja planejado e desenvolvido paralelamente à estratégia de implementação de sistemas de informação em saúde, em vez de ser uma mera adaptação às características existentes de cada sistema. Esse deve ser um dos elementos principais do planejamento para estimular a estruturação e organização e promover a solidez e robustez da estratégia de segurança da informação.

A seguir, apresentam-se recomendações e sugestões relacionadas aos eixos centrais de monitoramento, luta por privacidade, sigilo, segurança e cumprimento das normas.

**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.**

- Existência de um marco normativo que estabeleça diretrizes para o cumprimento da privacidade, do sigilo e da segurança da informação, bem como sanções ou penalidades.
- Existência de um mecanismo de monitoramento do marco normativo com uma frequência determinada que permita identificar erros e omissões, apontar a necessidade de modificações e regular aspectos não contemplados.

**2. Desenvolver uma estrutura de controle sobre o fluxo de informações em saúde, com elementos de diretrizes de segurança informática e riscos associados.**

- Existência de uma agência governamental responsável por assegurar a cibersegurança no setor da saúde e coordenar emergências na rede de teleinformática.
- Existência de fluxos definidos para monitorar e responder a incidentes.

**3. Articular mecanismos de monitoramento para detecção de incidentes e verificação do correto cumprimento dos padrões e condições de acesso e tratamento de informações.**

- Estratégia de monitoramento definida para monitorar a atividade dos usuários da rede.
- Existência de um repositório de informações sobre incidentes.

**4. Estabelecer ferramentas e instrumentos de consentimento informado para armazenamento e proteção de informações sensíveis.**

- Número de termos de sigilo assinados entre as partes.
- Número de termos de consentimento livre e esclarecido assinados.

**5. Centralizar certificações de segurança.**

- Número de serviços criados que permitem gerir de forma centralizada a certificação de dados de saúde confidenciais por meio da utilização de tecnologias de certificação de cadeias de blocos (*blockchain*).

**6. Elaborar e implementar planos de comunicação e capacitação sobre direitos e responsabilidades relacionados a dados pessoais.**

- Número de documentos divulgados sobre direitos e responsabilidades quanto a dados pessoais.
- Existência de espaços de formação em direitos e responsabilidades quanto a dados pessoais.
- Campanhas de divulgação e conscientização para transmitir assertivamente conhecimento sobre o marco legal vigente.

**7. Atualizar normas e ferramentas existentes relacionadas à proteção de dados.**

- Estratégia de atualização das normas definidas.

**8. Fortalecer a articulação intra e interinstitucional.**

- Existência de espaços e mesas de trabalho entre diferentes instituições e áreas de governo, com a inclusão de usuários.

**9. Definir regras claras para o fluxo de informações: carregamento e disponibilização.**

- Existência de uma referência exclusiva para a identidade dos usuários e criação de credenciais e perfis de habilitação para uso e acesso aos sistemas.
- Número de capacitações para os atores envolvidos sobre diretrizes de segurança informática, riscos associados e qualidade dos dados inseridos.

# Recomendações gerais

Sem subestimar a importância da dimensão técnica, é essencial que, durante a elaboração de políticas de segurança da informação, os tomadores de decisão considerem os seguintes aspectos:

- O papel do paciente como titular dos dados e sua participação ativa no princípio da segurança da informação.

- A necessidade de uma abordagem integral, transversal e multidisciplinar de acordo com funções específicas dentro das organizações.

- Enfatizar a divulgação e a conscientização para que os diferentes atores da rede conheçam marco legal vigente.

- Assegurar a integridade dos dados e sua disponibilização para os diferentes atores da rede.

- Desenvolver marcos regulatórios apropriados. Embora haja acordos e consenso sobre as referências normativas, vale ressaltar a conveniência de gerar marcos nacionais ou jurisdicionais próprios que levem em conta as particularidades dos fluxos e sistemas envolvidos.

- A natureza sensível dos dados resultantes das interações das pessoas com o ambiente de saúde requer o desenvolvimento de ferramentas, plataformas e estratégias com um desenho específico que preveja a correta identificação das pessoas que intervêm e participam.

Recomenda-se que sejam desenvolvidas estratégias abrangentes para facilitar e incentivar o uso dos dados no maior número possível de ações positivas sem comprometer a segurança e os direitos de seu titular.

# Bibliografia e recursos


1. Organização Pan-Americana da Saúde. 8 princípios orientadores da transformação digital do setor da saúde: um apelo à ação pan-americana. Washington, D.C.: OPAS; 2021. Disponível em: https://iris.paho.org/handle/10665.2/54669.

2. Agência da União Europeia para a Cibersegurança. Sobre a ENISA. Heraklion: ENISA; 2021. Disponível em: https://www.enisa.europa.eu/about-enisa/about/pt.

3. Rede Ibero-Americana de Proteção de Dados. Recomendaciones de La Red Iberoamericana de Protección de Datos (RIPD) para el tratamiento de datos personales sobre la salud en tiempos de pandemia. Disponível em: https://www.redipd.org/sites/default/files/2021-09/recomendaciones-ripd-tratamiento-datos-personales-salud-en-pandemia.pdf.

4. Organização Internacional de Normalização. Genebra: ISO; 2020. Disponível em: https://www.iso.org/home.html Plazzotta F, Sommer JA. Informática en salud orientada a la comunidad. In: Luna D, de Quirós FGB (eds.). Buenos Aires: Hospital Italiano de Buenos Aires; 2018.

5. Presidência da Nação da Argentina. Ley 26.529. Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/norma.htm.

6. Governo do Equador. Ley Orgánica 459. Protección de Datos Personales. Quito: Governo do Equador; 2021.

7. Governo da Colômbia. Ley 1.581. Protección de Datos Personales de Colombia. Bogotá: Governo da Colômbia; 2012. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

8. Organização Pan-Americana da Saúde. Roteiro para a transformação digital do setor da saúde na Região das Américas [Resolução CD59/6]. 59º Conselho Diretor da OPAS, 73ª sessão do Comitê Regional da OMS para as Américas; 20 a 24 de setembro de 2021. Washington, D.C.: OPAS; 2021. Disponível em: https://www.paho.org/pt/documentos/cd596-roteiro-para-transformacao-digital-do-setor-da-saude-na-regiao-das-americas.

9. Organização Pan-Americana da Saúde. Plano de ação para o fortalecimento dos sistemas de informação para a saúde 2019-2023 [Resolução CD57/9]. 57º Conselho Diretor da OPAS, 71ª sessão do Comitê Regional da OMS para as Américas; 30 de setembro a 4 de outubro de 2019. Washington, D.C.: OPAS; 2019. Disponível em: https://iris.paho.org/handle/10665.2/51617.


OPAS/EIH/IS/23-0016

OPAS Organização Pan-Americana da Saúde

Organização Mundial da Saúde
Escritório Regional para as Américas