
# LGPD:
# O QUE MUDA COM A LEI E COMO A RNP IRÁ APOIAR NA ADEQUAÇÃO DE INSTITUIÇÕES DE ENSINO E PESQUISA DO PAÍS

RNP
ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

# INTRODUÇÃO

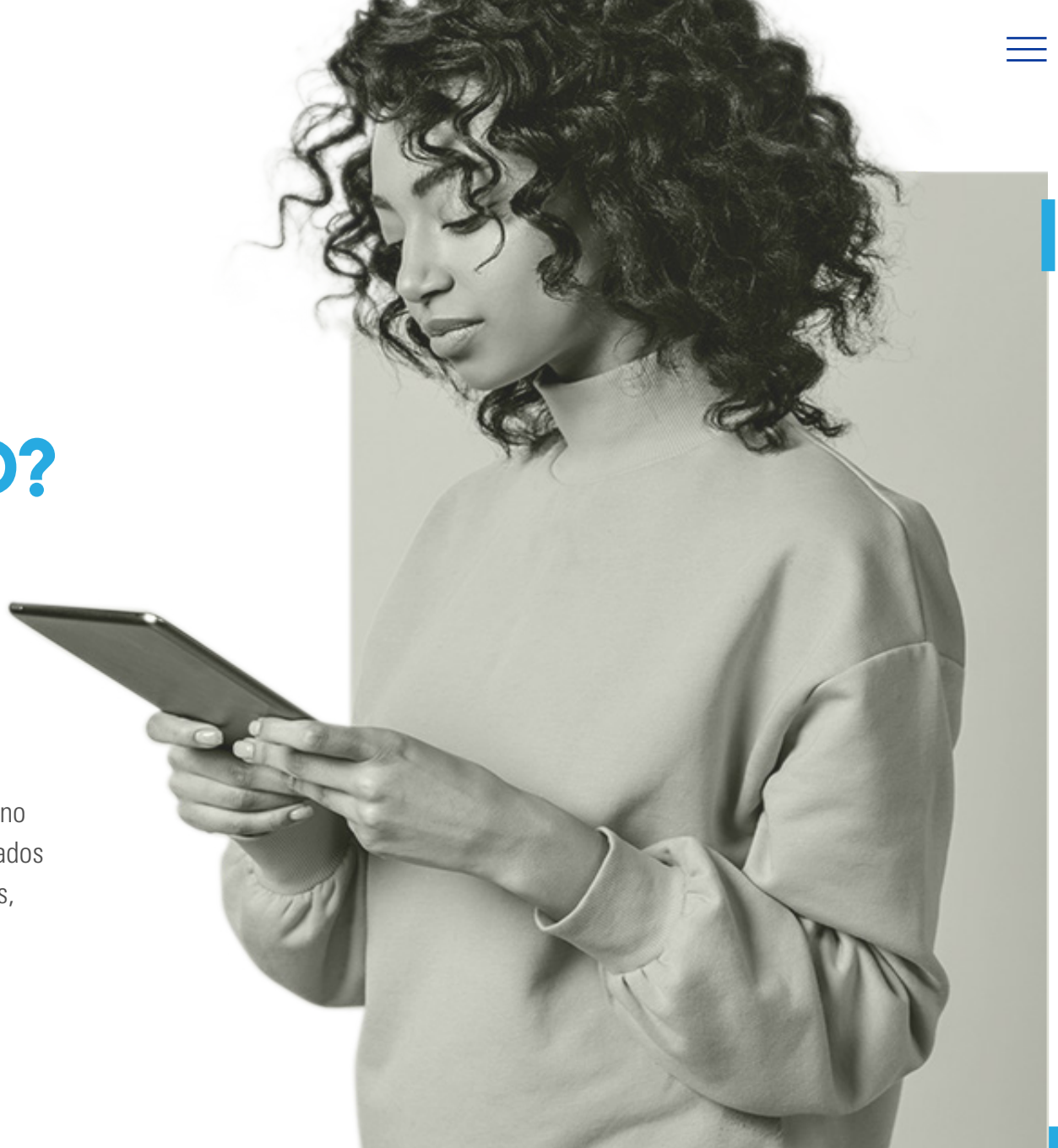
## VOCÊ JÁ PAROU PARA PENSAR SOBRE QUANTAS INFORMAÇÕES PESSOAIS SUAS PODEM ESTAR CADASTRADAS E EM QUANTOS LUGARES DIFERENTES?

Como essas informações são coletadas, tratadas e armazenadas? Com quem elas são compartilhadas? Como a proteção dessas informações é realizada para garantir a sua privacidade? Ao passar um dado pessoal seu, você teve ciência da real necessidade de disponibilizá-la e o que seria feito com aquele dado? Aliás, antes disso, no que consiste um dado pessoal? São nessas e em outras questões que a Lei Geral de Proteção de Dados Pessoais (LGPD) – nº 13.709/2018 – têm impacto direto, ao regulamentar o tratamento de dados pessoais, a fim de proteger os seus direitos fundamentais de liberdade e de privacidade.

Sancionada em agosto de 2018, a lei é munida de uma série de medidas que incluem princípios e controles jurídicos de governança e segurança da informação que instituições públicas e privadas precisam implementar para a adequação. Neste material desenvolvido pela Rede Nacional de Ensino e Pesquisa (RNP), você conhecerá mais sobre a LGPD, ao entender os benefícios para os titulares dos dados, os impactos para as instituições que realizam o seu tratamento e o método de adequação adotado pela RNP. Aproveite a leitura!

# AFINAL, O QUE É E PARA QUE SERVE A LGPD?

Todos os dias, milhões de empresas e instituições, públicas e privadas, captam e tratam dados pessoais de seus clientes, usuários e empregados. Em alguns casos, essas informações são indispensáveis para o desempenho do ofício daquele negócio. É o que acontece com as instituições de ensino e pesquisa. Essas organizações lidam com dados pessoais de alunos, professores, funcionários, terceiros e fornecedores, que são coletados, armazenados e fluem para outras entidades, como órgãos governamentais, parceiros ou instituições financeiras, por exemplo.



Por outro lado, o dado pessoal é um ativo precioso que precisa ser preservado para garantir sua privacidade. E essa afirmação não é apenas um palpite, é a conclusão de uma discussão propulsora de transformações ao redor do mundo, inclusive, no Brasil. Um exemplo acontece na Europa: desde 2018, o *General Data Protection Regulation* (GDPR ou Regulamento Geral de Proteção de Dados, em português) regulamenta a proteção dos dados pessoais, incluindo os processos de coleta, armazenamento e compartilhamento de informações.
A medida prevê a garantia de privacidade e proteção de dados pessoais.

Por aqui, a Lei Geral de Proteção de Dados Pessoais (LGPD), assim como a determinação europeia que inspirou sua criação, consiste em um conjunto de normas gerais que aborda princípios, tratamento dos dados pessoais, direitos dos titulares e sanções que podem ser aplicadas caso não haja cumprimento por empresas públicas ou privadas.
A Lei nº 13.709/2018 regulamenta o tratamento dessas informações do cidadão brasileiro, dentro e fora das fronteiras do país, nos meios digitais ou físicos (como papel).

# O QUE É UM DADO PESSOAL?

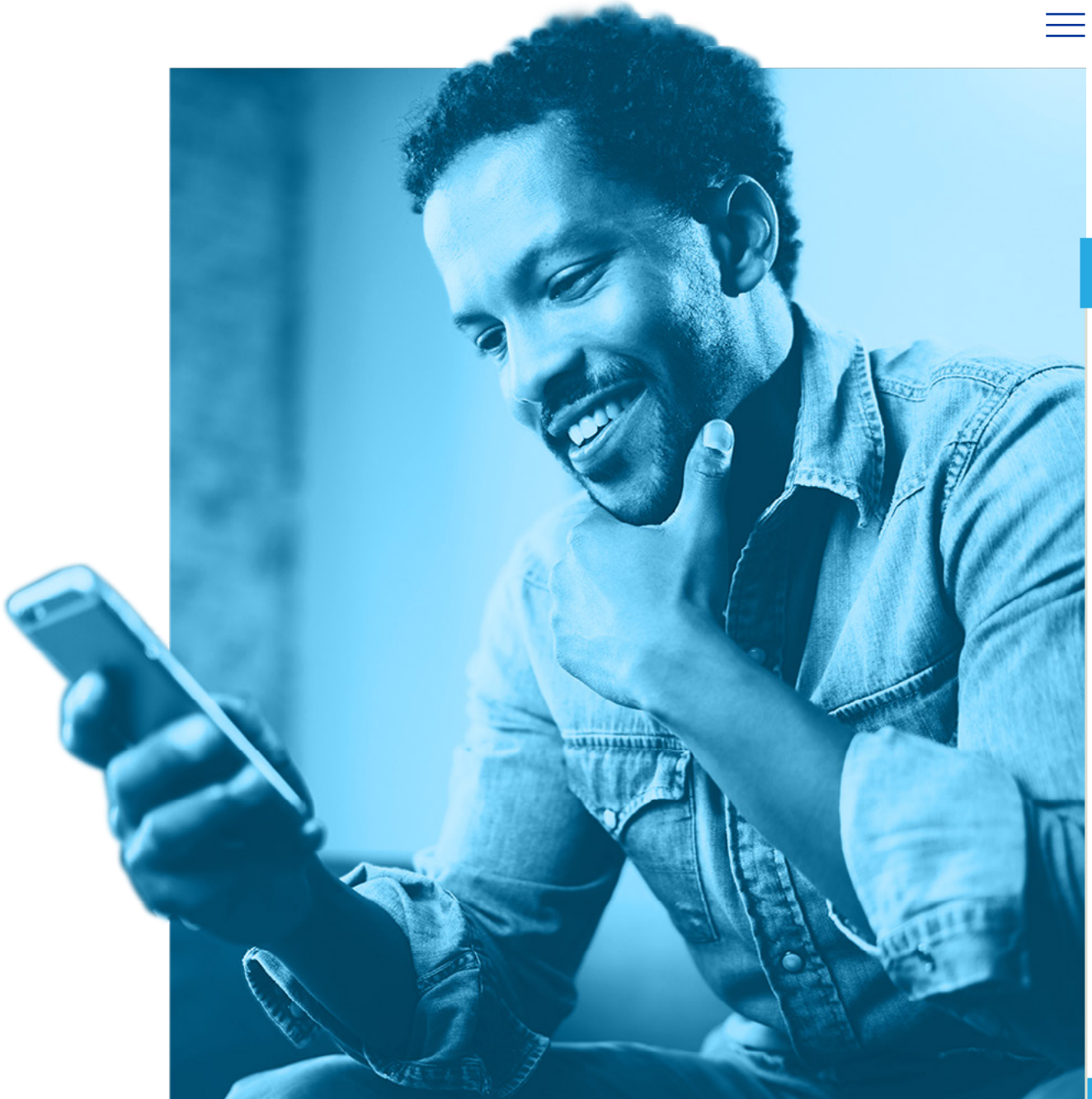
Antes de falar sobre a proteção dele, é preciso entender o que, de fato, é um dado pessoal. O conceito é abrangente, mas simples:

**SE UMA INFORMAÇÃO IDENTIFICA OU PERMITE IDENTIFICAR UMA PESSOA, ELA É CONSIDERADA UM DADO PESSOAL.**

**VEJA ALGUNS EXEMPLOS:**

- **NOME E SOBRENOME**
- **GÊNERO**
- **DATA DE NASCIMENTO**
- **DOCUMENTOS PESSOAIS** (CPF, RG, CNH, CARTEIRA DE TRABALHO, PASSAPORTE E TÍTULO DE ELEITOR)
- **MATRÍCULA DE UM ALUNO OU FUNCIONÁRIO**
- **DEPARTAMENTO ONDE TRABALHA**
- **ENDEREÇO RESIDENCIAL**
- **LOCALIZAÇÃO VIA GPS**
- **NÚMERO DO TELEFONE**
- **ENDEREÇO DE E-MAIL**

Aqueles que são potencialmente passíveis de discriminação se expostos ou vazados, como origem racial ou étnica, convicção religiosa ou filosófica, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, bem como informações genéticas, biométricas ou sobre a saúde ou a vida sexual de alguém. Sempre que é necessário realizar um tratamento de dados sensíveis, a criticidade na análise, garantias de segurança e tratamento deve ser maior, pois os controles adequados devem ser implementados para proteger esse tipo de informação contra vazamentos.



# OS FUNDAMENTOS E PRINCÍPIOS DA LGPD

Alguns fundamentos e princípios previstos na LGPD estruturam e regem como deve ser a proteção de dados pessoais.

## OS FUNDAMENTOS LISTADOS NA LEGISLAÇÃO SÃO:

- O respeito à privacidade
- A autodeterminação informativa, que significa o direito de controlar o acesso e a utilização de informações pessoais
- A liberdade de expressão, de informação, de comunicação e de opinião
- A inviolabilidade da intimidade, da honra e da imagem
- O desenvolvimento econômico e tecnológico e a inovação
- A livre iniciativa, a livre concorrência e a defesa do consumidor
- E os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais

# A LEI AINDA PREVÊ QUE O TRATAMENTO DE DADOS PESSOAIS DEVE CONSIDERAR DEZ PRINCÍPIOS ESSENCIAIS:

## 1 FINALIDADE

Quando um cidadão autoriza o uso dos seus dados, a organização que os detém deve ter propósitos legítimos, específicos, explícitos e informados ao titular. Além disso, essas informações não podem ser tratadas com outros fins posteriormente.

## 2 ADEQUAÇÃO

Os dados pessoais tratados precisam ser compatíveis com as finalidades informadas pela instituição ao titular que a concedeu. Por exemplo, não há justificativas claras para que uma instituição de tecnologia solicite dados sobre a origem racial ou convicção religiosa de alguém.

## 3 NECESSIDADE

As instituições devem utilizar apenas informações essenciais, pertinentes e proporcionais para a realização de suas finalidades. Nada de excessos!

## 4 LIVRE ACESSO

As pessoas às quais as informações tratadas pertencem têm o direito de consultar, de maneira fácil e gratuita, sobre os dados que a instituição detém a seu respeito: quais dados são esses? O que essa organização faz com as informações coletadas? De que maneira elas são tratadas? Por quanto tempo?

## 5 QUALIDADE DOS DADOS

As instituições precisam garantir aos donos dos dados tratados que essas informações são exatas, claras, relevantes e atualizadas, de acordo com a necessidade e a finalidade do tratamento desses dados.

## 6 TRANSPARÊNCIA

As empresas precisam garantir aos titulares informações claras, precisas e de fácil acesso sobre o tratamento de seus dados. Também informar ao titular se compartilharem as informações pessoais tratadas, inclusive com operadores essenciais para alguma função.

## 7 SEGURANÇA

As instituições devem utilizar medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados, como invasões por hackers, bem como situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais.

## 8 PREVENÇÃO

As organizações devem adotar medidas de controle antecipadas para prevenir a ocorrência de vazamentos ou danos aos dados pessoais em tratamento.

## 9 NÃO DISCRIMINAÇÃO

Os dados pessoais não podem ser usados para fins discriminatórios, ilícitos ou abusivos.

## 10 RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

As instituições precisam demonstrar que estão adotando medidas eficazes, comprovar que estão cumprindo as normas de proteção de dados pessoais e apresentar a eficácia dessas medidas.

# O QUE MUDA COM A LEI?

**A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS É CONSIDERADA A MUDANÇA MAIS IMPORTANTE EM RELAÇÃO À PRIVACIDADE DO TITULAR DE DADOS PESSOAIS NO BRASIL, POR REGULAMENTAR A PROTEÇÃO DE DADOS E A PRIVACIDADE NO PAÍS.**

## A LEGISLAÇÃO ATINGE, DE FORMA NÃO OPCIONAL, TODOS OS DADOS TRATADOS POR ÓRGÃOS PÚBLICOS E INSTITUIÇÕES PRIVADAS:

- Cujos titulares estejam no território brasileiro
- Que a coleta desses dados tenha acontecido no país
- Ou que tenham sido coletados devido a alguma oferta de produtos ou serviços no Brasil

**TAMBÉM DEVEM SE ADEQUAR À LGPD PESSOAS FÍSICAS QUE TRATAM DADOS COM FINS ECONÔMICOS, COMO PROFISSIONAIS LIBERAIS, POR EXEMPLO.**

Com o conjunto de práticas e normas, há benefícios para os titulares dos dados, que passam a ter mais controle sobre o uso de suas informações e impactos para as instituições públicas e privadas, que precisam se adequar sobre como tratam a privacidade e a segurança das informações de seus clientes.

# OS BENEFÍCIOS PARA OS TITULARES

## PARA ENTENDER O QUE MUDA COM A LGPD, É PRECISO COMPREENDER:

Um dado pessoal pertence, exclusivamente, à pessoa a quem ele diz respeito. E um benefício que afeta diretamente o titular desses dados é a transparência. O cidadão tem direito de saber, de maneira clara, quais dados seus são coletados, para quais necessidades, se aquelas informações estão protegidas e se são compartilhadas com outras instituições ou empresas. Ele também pode fazer questionamentos, pedir alterações ou solicitar a revogação do consentimento de seus dados a qualquer momento.

# OS IMPACTOS PARA AS INSTITUIÇÕES

Não há para onde fugir. Governo e empresas têm que adotar políticas e planos de proteção de dados para se adequar à lei e garantir maior segurança aos dados pessoais dos clientes e usuários.

**PARA ISSO, PRECISAM INICIAR UM PLANO DE ADEQUAÇÃO, COM ATIVIDADES COMO:**

Identificar e revisar como é o fluxo destas informações dentro da instituição, conferir se existem vulnerabilidades de segurança e estruturar um plano de ações necessárias para adequação, envolvendo medidas como a criação de políticas, adequações contratuais, aplicação de controles em processos e sistemas de informação e capacitação de seus colaboradores.

Quem não cumprir os requisitos de proteção de dados pessoais está sujeito a advertências, multas, podendo chegar até na suspensão das atividades.

# PODEM HAVER EFEITOS DA LGPD NO CAIXA DAS INSTITUIÇÕES:

**POR MEIO DE MULTAS QUE PODEM CHEGAR A 2% DO FATURAMENTO, COM LIMITE DE R$ 50 MILHÕES POR INFRAÇÃO.**

Em casos mais críticos, em última instância, as empresas que tiverem recorrência na inconformidade com a LGPD podem sofrer proibições do exercício das atividades. Além do "peso no bolso" e das determinações rigorosas, a publicização do não cumprimento das normas pode abalar a reputação das instituições.

Por outro lado, as organizações em acordo com a lei contribuem com o direito à privacidade do usuário e uma mudança de cultura de maior responsabilidade no tratamento dos dados pessoais. Além de credibilidade dos clientes, essas instituições conquistam vantagem reputacional no mercado, considerando que a lei contribui para um cenário com maior igualdade de condições entre as empresas do segmento.

# COMO SE ADEQUAR À LGPD?

## É IMPORTANTE RESSALTAR:

Não existe uma fórmula com um passo a passo aplicável a todas as organizações quando o assunto é o caminho para estar em conformidade com a LGPD. Cada instituição, a depender do volume, da natureza, da maturidade e dos sistemas de armazenamento de dados pessoais, precisa adotar controles adequados para garantir a segurança dos dados e a privacidade do usuário.

No entanto, a RNP adotou internamente e compartilha um método que pode guiar instituições parceiras a dar o pontapé inicial rumo à adequação.

# CONFIRA:

**TUDO COMEÇA COM UM DIAGNÓSTICO SOBRE O TRATAMENTO DE DADOS PESSOAIS EM UMA INSTITUIÇÃO.**
**SEM ESSA ETAPA, NÃO HÁ COMO SEGUIR EM FRENTE. AQUI, É PRECISO REUNIR ALGUMAS INFORMAÇÕES QUE GUIARÃO UM PLANO DE AÇÕES POSTERIOR.**

**1**

Primeiro, é necessário fazer um mapeamento dos dados pessoais tratados pela instituição, respondendo a algumas questões: que dados são esses? De que tipo eles são? De quem são (estudantes, clientes, funcionários e/ou familiares)? Onde eles estão armazenados? Como eles são protegidos?
De onde eles vêm? Para onde vão? Qual o fluxo dessas informações? Além de armazenadas, elas são compartilhadas com terceiros?
O mapeamento provavelmente resultará em necessidades de ajustes em processos de governança, contratuais e tecnológicos, desdobrando na necessidade de adequação de políticas de privacidade, contratos de prestação de serviços e sistemas como revisão dos campos coletados e controles de segurança implementados. Lá vai uma dica: se a instituição não possuir todos os processos internos mapeados, talvez seja melhor seguir por departamentos.

**2**

Hierarquize essas informações: quais dados são mais importantes e merecem prioridade na atenção? Por exemplo, os dados armazenados na seção acadêmica de uma instituição provavelmente são mais críticos em relação aos repositórios que guardam informações do login usado para acessar um site da organização, como nome completo, e-mail e senha.

**3**

Identifique os pontos de possíveis vazamentos: proteger os dados pessoais envolve controles físicos, processuais e tecnológicos. Uma vez que se conhece o fluxo dos dados pessoais, é necessário identificar em quais pontos podem sofrer vazamentos.
É importante identificar falhas de segurança que podem ser ocasionadas a partir de pessoas, incidentes físicos ou incidentes cibernéticos. Lembre-se: algumas informações estão presentes em mais de um banco de dados. Então, é preciso mapear os sistemas a partir dos dados tratados ou identificar que tipo de informações há em cada repositório.

**4**

Depois, é hora de realizar uma avaliação de riscos, considerando possíveis vulnerabilidades, ameaças e agentes de ameaças relacionados aos dados pessoais e a todos os pontos de vazamento identificados, como por exemplo, um vazamento de dados por hackers que exploram vulnerabilidades de uma aplicação que dá acesso ao banco de dados. Essa medida é a estrutura para garantir segurança da informação e gerenciamento de riscos.

**5**

Por fim, todas as informações relevantes identificadas e avaliadas devem ser condensadas em um documento padrão chamado Relatório de Impacto à Proteção de Dados Pessoais (RIPD), também conhecido como D*ata Protection Impact Assessment* (DPIA). Esse relatório deve conter a descrição dos processos de tratamento de dados e possíveis riscos às liberdades civis e aos direitos fundamentais. A Autoridade Nacional de Proteção de Dados (ANPD) pode analisar o documento  a fim de verificar a conformidade da instituição com a lei.

**COM ESSES DADOS LEVANTADOS, UMA ESTRATÉGIA DE ADEQUAÇÃO PODE SER DEFINIDA. ENTÃO, A PRÓXIMA ETAPA É A IMPLEMENTAÇÃO DE UM PLANO DE AÇÃO QUE PREVÊ A CONFORMIDADE DA INSTITUIÇÃO COM A LEI, INCLUINDO UM CONJUNTO DE AÇÕES ENVOLVENDO PROCESSOS, POLÍTICAS, CONTROLES DE SEGURANÇA, ADEQUAÇÕES JURÍDICAS E ADEQUAÇÕES DE SISTEMAS DE INFORMAÇÃO.**

## ETAPA2 - ESTRATÉGIA DE ADEQUAÇÃO

**1**

A privacidade dos titulares de dados precisa ser protegida das ameaças existentes. As ferramentas para isso são tecnologias e processos, utilizar recursos como a anonimização, pseudonimização, criptografia, minimização de dados e segurança por padrão. Essas medidas visam reduzir os riscos de exposição de dados pessoais e fazem parte de um programa de governança em privacidade, que prevê também a atuação de um Encarregado de Proteção de Dados da instituição. Trata-se de uma pessoa, física ou jurídica, responsável pela proteção de dados pessoais na instituição. As instituições têm obrigação de ter esse tipo de profissional e oferecer condições adequadas para que ele possa gerir o tratamento de dados pessoais e, assim, responder a demandas e solicitações de usuários.

**2**

As instituições precisam estar preparadas para fazer a gestão dos dados dos titulares, que têm o direito à transparência sobre os dados que lhes dizem respeito, como o tipo de dado coletado, para que fim e com quem ele é compartilhado, e desenvolver um plano de contingenciamento em caso de vazamentos de dados. Se os titulares quiserem, eles têm o direito ao esquecimento, podendo solicitar que as instituições apaguem as informações armazenadas, mesmo que eles tenham concedido um dia.

**3** Para estar em conformidade com a LGPD e prezar pela segurança da informação, é necessário criar contratos, processos, políticas e normas já de acordo com as novas diretrizes, além de revisar e adequar os documentos, sistemas e bancos de dados já existentes.

**4** Ainda sobre a proteção de dados, algumas práticas devem estar bem estruturadas, como a implementação de controles processuais e tecnológicos de segurança; monitoramento e adequação dos sistemas, prevendo a correção de vulnerabilidades e minimização de dados; plano de gestão de vulnerabilidades; e resposta a incidentes.

**5** Mantenha suas equipes atualizadas. Como vimos, a LGPD tem implicações que envolvem todas as áreas de uma instituição. A qualificação das equipes para entendimento, alinhamento e operacionalização das ações derivadas torna-se fundamental.

# PARA ACABAR COM AS DÚVIDAS: COMO MITIGAR RISCOS?

Um guia sobre direitos e obrigações para a proteção de dados pessoais

## OBRIGAÇÕES DE SUA ORGANIZAÇÃO COM RELAÇÃO AOS DADOS PESSOAIS:

- Demonstrar conformidade
- Implementar *Privacy by Design*
- Deixar claras as responsabilidades entre controladores e terceiros
- Ter acordos claros entre controladores e operadores
- Formalizar as instruções para os operadores
- Manter registros claros de todos os processamentos
- Garantir boas práticas de segurança da informação
- Notificar os titulares de dados em caso de vazamentos
- Ter um Encarregado de Proteção de Dados estabelecido

TITULAR DOS DADOS

SUA ORGANIZAÇÃO

## DIREITOS DO TITULAR DOS DADOS:

- A confirmação da existência dos dados sendo tratados por aquela empresa ou instituição
- Acesso aos dados que estão sendo tratados
- Correção de dados incompletos, inexatos ou desatualizados
- A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade
- A portabilidade dos dados a outro fornecedor de serviço ou produto
- Eliminação de dados tratados com o consentimento
- Informação acerca de dados compartilhados com terceiros
- Informação acerca das consequências do não consentimento
- A revogação do consentimento

Esses direitos devem ser exercidos preferencialmente de forma eletrônica, telefone ou carta, sem custo para os titulares.

## OBRIGAÇÕES DE SUA ORGANIZAÇÃO COM A ANPD:

- Demonstração de conformidade
- Notificar os vazamentos de dados
- Realizar a avaliação de impacto de proteção de dados
- Consultar a autoridade antes do processamento
- Ter um plano de contingenciamento de vazamentos
- Definir um encarregado de proteção de dados pessoais

SUA ORGANIZAÇÃO

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

## COMPETÊNCIAS DA ANPD PARA A SUA ORGANIZAÇÃO:

- Monitorar e exigir a conformidade com a LGPD
- Requisitar informações necessárias para a realização de suas atividades
- Impor limitações, advertências, multas ou paralisação dos processamentos

Infográfico baseado em conteúdo da International Association of Privacy Professionals (IAPP)

# PRECISA DE AJUDA PARA SE ADEQUAR?

## AINDA VEM UM BAITA DESAFIO PELA FRENTE!

Mas pode contar com a gente nessa empreitada. A RNP, pioneira em um ecossistema de inovação, tecnologia da informação, educação e ciência, pode ajudar você e a instituição da qual você faz parte a estar em conformidade com a proteção e garantia dos direitos fundamentais de liberdade e de privacidade.

## PARA APOIAR NOSSAS INSTITUIÇÕES PARCEIRAS A ESTAREM EM CONFORMIDADE COM A NOVA LEI, COM MAIOR ASSERTIVIDADE E SEGURANÇA, OFERECEMOS:

- Apoio metodológico, com orientações, insumos e eventos para a comunidade
- Serviços de consultorias, que atuam na estruturação de um plano de adequação à LGPD
- Capacitações, para você e sua equipe entenderem, na prática, como a legislação transformará a rotina das instituições

## APOIO METODOLÓGICO

A RNP integra a comunidade de ensino e pesquisa na construção e disseminação de um método LGPD.

Promovemos encontros, trocamos experiências e compartilhamos artefatos que apoiam as instituições nessa jornada.

## CONSULTORIAS

Utilize o serviço de consultoria para contar com uma solução customizada conforme as necessidades da instituição em que você atua e, assim, atingir os objetivos de conformidade com a LGPD.

Oferecemos serviços para instituições em ciclos de evolução e adequação de aplicações e plataformas baseados no conceito *Privacy by Design*.

## CAPACITAÇÕES

A Escola Superior de Redes (ESR), unidade de serviço da RNP, possui cursos específicos sobre LGPD com certificação profissional. Desde seus fundamentos até a formação completa em *Public Data Protection Officer* (PDPO).

# CONSULTE-NOS, CAPACITE SUAS EQUIPES E ACELERE O PROCESSO DE ADEQUAÇÃO DE SUA INSTITUIÇÃO!

Contratação facilitada para órgãos públicos: de acordo com a Lei nº 8.666/93, Art 24 – inciso XXIV, órgãos públicos são isentos de licitação para contratação da RNP e ESR.

## FALE CONOSCO!

**RNP**

**0800 722 0216**

**ATENDIMENTO@RNP.BR**

**WWW.RNP.BR**

**ESR**

**ATENDIMENTO@ESR.RNP.BR**

**WWW.ESR.RNP.BR**

## ESSE MATERIAL AJUDOU VOCÊ?

Compartilhe esse *e-book* e nos acompanhe em nossas redes sociais.

**Acesse nossa página com conteúdos completos sobre LGPD e fique por dentro dos próximos eventos, nossos cursos, serviços disponíveis e quem são os especialistas que podem ajudar você nessa jornada de adequação.**