



# Sumário

<b>Módulo 1</b>	<b>5</b>
Lição 1: Objetivos do módulo	6
Lição 2: Sociedade da Informação e dados pessoais	6
O contexto da <i>Data Driven Economy</i>	6
Como o cenário atual trabalha com os dados pessoais	7
O que são dados, informações e conhecimento?	7
Lição 3: Contextualização da GDPR e LGPD	8
Entendendo a importância da Legislação Europeia	8
A proteção de dados pessoais no Brasil	9
Lição 4: Introdução a Lei Geral de Proteção de Dados	9
As legislações setoriais no Brasil	9
Principais impactos da LGPD	9
Lição 5: Direito à Privacidade x Proteção de Dados Pessoais	11
O direito à privacidade e proteção	11
Lição 6: Incidência Material e Territorial	12
Incidência Material	12
Incidência Territorial	12
Casos de não aplicabilidade da LGPD	13
Lição 7: Conceitos fundamentais da LGPD	13
Os Tipos de Dados	13
Dados pessoais sensíveis e a discriminação	13
Personagens, figuras ou atores	14
Lição 8: Agentes de Tratamento de Dados Pessoais	14
Quem é considerado agente de tratamento?	14
O Controlador	15
O Operador	15
Lição 9: O Encarregado pelo Tratamento de Dados Pessoais	16
O Encarregado	16
Lição 10: Bases Legais para o Tratamento de Dados Pessoais	16
Lição 11: Princípios da LGPD	18
Lição 12: Autoridade Nacional de Proteção de Dados Pessoais (ANPD)	20
Responsabilidades gerais da ANPD	20
Competências gerais	20
Lição 13: Exercícios práticos sobre LGPD	21

Lição 14: 5 passos práticos para aplicar o que você aprendeu	21
<b>Módulo 2</b>	22
Lição 1: Objetivos do módulo	23
Lição 2: Ciclo de Vida dos Dados Pessoais	23
LGPD x LAI	23
Etapas do Ciclo de Vida dos Dados Pessoais	24
Lição 3: Direito dos Titulares dos Dados Pessoais	24
Quais os principais direitos dos titulares?	24
Atendimento à solicitação do Titular	25
Impossibilidade de Atendimento à Solicitação do Titular	26
Lição 5: Incidentes de Segurança da Informação com Dados Pessoais	26
Definição de Incidentes de Segurança para a GDPR	26
Em caso de Incidentes de Segurança com Dados Pessoais	26
Quem deve fazer a comunicação de incidentes?	27
Em que situação e o que deve ser comunicado ao titular dos dados?	27
O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)	28
Lição 5: Plano de Resposta e Remediação à Incidentes	28
Plano de Resposta à Incidentes e suas Etapas	29
Relatório Inicial de Incidentes	30
Incidentes de Segurança com Exposição de Dados Pessoais	30
Lição 6: Medidas de Segurança, Boas Práticas e Governança	30
Ações importantes para Boas Práticas e da Governança	31
<i>Privacy by Design</i>	31
<i>Privacy by Default</i>	32
Por que a conformidade é importante?	32
Adoção de boas práticas e de governança e a conformidade	32
Lição 7: Noções de Segurança da Informação (S.I) – ISSO 27.001	33
<i>Framework NIST</i>	33
<i>Framework ISO 27.001</i>	33
Lição 8: Responsabilização e Prestação de Contas	33
Lição 9: Principais Regulamentações no Cenário Mundial	33
Lição 10: Transferência Internacional de Dados Pessoais	34
Lição 11: 5 passos práticos para aplicar o que você aprendeu	35
Referências	36

Direitos desta edição reservados  
A Voitto Treinamento e Desenvolvimento  
[www.voitto.com.br](http://www.voitto.com.br)

*Supervisão editorial:* Thiago Coutinho de Oliveira

*Apresentação do curso:* Zilda Gonçalves

*Produção de conteúdo:* Diego Henrique Nobre Costa

Zilda Gonçalves é Advogada e Consultora em Privacidade e Proteção de Dados Pessoais, Direito Digital, Compliance, Negócios Digitais, Contratos, Inovação e Tecnologia e Professora. Fundadora e Coordenadora do Grupo de Estudos em Inteligência Artificial e Direito da CIAD/OAB MG, além de atuar na Comissão Especial de Privacidade e Proteção de Dados Pessoais da OAB.

### É PROIBIDA A REPRODUÇÃO

Nenhuma parte desta obra poderá ser reproduzida, copiada, transcrita ou mesmo transmitida por meios eletrônicos ou gravações sem a permissão, por escrito, do editor. Os infratores serão punidos pela Lei nº 9.610/98

# **Módulo 1**

## **Aspectos gerais da privacidade, proteção e informação**



## Lição 1: Objetivos do módulo

Trazer conhecimentos sobre a segurança de dados, conceitos de privacidade, proteção de dados pessoais e segurança da informação, abordando seus aspectos gerais.

### Responderemos perguntas do tipo:

- ✓ O que é a *LGPD*?
- ✓ Qual a diferença entre privacidade e segurança?
- ✓ Quais os princípios e direitos envolvidos?

## Lição 2: Sociedade da Informação e dados pessoais

### O contexto da *Data Driven Economy*



É o **cenário atual** onde **os dados são os ativos centrais** para **as empresas** e a **economia** gira em torno da **necessidade de tratá-los**. Podemos dizer que a sociedade e economia está baseada no **tratamento** de dados pessoais, uma vez que as atividades de negócio das empresas estão envolvidas nos **fluxos de informações**.

### Sociedade Da Informação

Estágio atual da sociedade, em que as informações são o **elemento principal** para o **desenvolvimento da economia**.

Como o **petróleo** também é um **ativo muito valioso** para a economia, os **dados** também são considerados **recursos fundamentais** na sociedade da informação.

“ Vistos como o **novo petróleo**, os dados são hoje **insumos essenciais** para praticamente todas as **atividades econômicas**. ”

**Ana Frazão,**  
Advogada e Professora de Direito Civil



## Como o cenário atual trabalha com os dados pessoais

Podemos observar no exemplo abaixo, uma sala de monitoramento em Madrid, onde eles tratam dados pessoais, por meio do uso da alta tecnologia e o autor diz o seguinte:

“(...). Esse é um excelente lugar para compreender por que os **algoritmos** se transformaram no segredo do sucesso de muitas grandes empresas: um segredo que lhes permite **canalizar um fluxo ingente de informação** para **tomar decisões fundamentais** para sua atividade.”



Sala de monitorização digital da Indra em San Fernando de Henares (Madri). **VICTOR SAINZ**.

“ Os algoritmos não têm só a capacidade de **explicar a realidade**, mas também de **antecipar comportamentos**. É uma vantagem para **evitar e minimizar riscos** e para **aproveitar oportunidades**. ”

*Jose Antonio Rubi*

## O que são dados, informações e conhecimento?

Os dados têm como característica serem **brutos, desorganizados, não analisados, ininterruptos e não relacionados**, além de serem **atos brutos**. Após serem processados **pela tecnologia da informação e adquirirem certo significado**, tornam-se **informação**.

Por exemplo, **atos e estatísticas reunidos por pesquisadores para sua análise** podem ser chamados **coletivamente** de “**atos**”. Os **atos**, em essência, **carecem de interpretação para que se tornem, finalmente, uma informação;**

**ATENÇÃO:** Sem serem interpretados ou tratados, **os atos tornam-se sem sentido**, a menos que recebam um propósito ou uma orientação para adquirir significado.

Já a **informação**, é a **estruturação ou organização dos dados**. Quando os dados são analisados, estruturados e recebem tratamento e contexto para torná-los úteis, obtemos **informações**.



Assim, quando um ou um conjunto de dados são **tratados**, de modo a transmitir uma **mensagem** dentro de um **contexto real**, temos as informações, as quais são providas de **propósito, significado e relevância**, podendo ser utilizadas pelo ser humano durante a **tomada de decisão, por meio da sua compreensão e análise**.

Por fim, o conhecimento é gerado através da habilidade em **analisar as informações encontradas**. Em outras palavras, o conhecimento acontece quando as informações são **integradas e processadas**, sendo que, através da análise do todo, podem ser encontradas determinadas **conclusões**, sendo capaz de produzir:



**ATENÇÃO:** A informação sem ser processada pelo indivíduo não resultará em nada, muito menos em conhecimento. **Portanto, se informação é dado trabalhado, então conhecimento é informação trabalhada.**

## Lição 3: Contextualização da GDPR e LGPD

### Entendendo a importância da Legislação Europeia

O **Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation - GDPR) - 2016/679**, é a legislação europeia que regula a **privacidade e proteção de dados pessoais**, sendo considerado um marco não apenas na UE, mas em diversos países que o utilizaram como **base para a elaboração de suas próprias legislações** e um desses países está inserido o Brasil.



## A proteção de dados pessoais no Brasil

**Lei nº 13.709, de agosto de 2018**, 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**.

## Lição 4: Introdução a Lei Geral de Proteção de Dados

### As legislações setoriais no Brasil

No Brasil o direito à privacidade e direito à proteção de dados pessoais teve início por meio de **legislações setoriais**:

**Código de Defesa do Consumidor**  
(Lei nº. 8.078/1990)



**Marco Civil da Internet**  
(Lei nº. 12.965/2014)



**Lei Geral de Proteção de Dados**  
(Lei nº 13.709/ 2018)



A **LGPD** versa **apenas e tão somente** sobre o **tratamento de dados pessoais** para **fins econômicos (aferição de lucro)** com aquela atividade.

“ A lei aprovada proporciona ao cidadão **garantias** em relação ao **uso de seus dados**, a partir de **princípios**, de **direitos do titular de dados** e de mecanismos de tutela idealizados tanto para **a proteção do cidadão** quanto para que o mercado e setor público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização. ”



**Laura Mendes e Danilo Doneda.**

*Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, p. 566, 2018.)*

### Principais impactos da LGPD

1. Proteção de liberdades e garantias **individuais dos titulares + Segurança jurídica** para **órgãos públicos e empresas privadas** que tratem dados pessoais para atingir sua **finalidade de negócio**;
2. Estabelece **as regras do jogo** para o tratamento dos dados pessoais no Brasil – **segurança jurídica** a todos os atores deste ecossistema (**titular dos dados pessoais e empresas públicas ou privadas**);

3. **Brasil passa a ser reconhecido mundialmente** por possuir uma legislação robusta e equivalente à norma da União Europeia: **facilitando e atraindo o investimento de empresas internacionais no nosso país**;
4. Disseminou **a cultura de Privacidade e Proteção de dados Pessoais** dentro das corporações e para **conscientização dos indivíduos (titulares de dados pessoais)**;
5. Elevou em termo de **reputação e oportunidades de atuação no mercado nacional e atração de negócios externos para o país**, além da **segurança para o fluxo de dados pessoais e investimentos**;
6. Possui **dupla função: econômica** (fomenta o desenvolvimento econômico) **e social** (garantia da proteção de direitos e liberdades fundamentais).

Oferecemos também **duas indicações valiosas**:



Um vídeo ministrado pelo fundador e professor da **Data Privacy Brasil**, **Bruno Bioni**, apresentando sobre **a importância da proteção de dados pessoais** dentro do mundo da informação e como as empresas e os governos relacionam a **proteção e privacidade do cidadão**.

[Clique aqui para acessar!](#)

E uma indicação do livro **“Data and Goliath”**, **Bruce Schneier** explica **como lidar com a tecnologia, selecionar a exposição e conquistar a privacidade** no ambiente da indústria da vigilância, em que cada vez mais toma-se o controle de nossos dados pessoais. [Leia o resumo pela PocketBook4You!](#)

## Lição 5: Direito à Privacidade x Proteção de Dados Pessoais

Ambos são direitos da personalidade, intrínsecos do ser humano, sendo considerados direitos fundamentais. Nesse caso, a privacidade está inserida no âmbito dos **direitos da personalidade**, além de ser considerado como **direito fundamental autônomo**.

Marco doutrinário para a tutela da privacidade foi o conceito ***"The right to be let alone"*** (Artigo intitulado ***"The Right to Privacy"***, de Warren e Brandeis, em 1890).

Assim, os autores mencionaram que os cidadãos precisam ter o **direito à privacidade garantido**, de modo que o Estado não pudesse intervir na sua vida privada. Por isso a relação de **"O direito de ficar só"** e **"o direito à vida privada"**.

Surge da **necessidade** de permitir espaço para o **desenvolvimento particular do indivíduo** e dos **seus pensamentos**, sem a imposição da autoridade pública sobre o seu agir e pensar íntimos.

### O direito à privacidade e proteção

Surge da **necessidade** de permitir espaço para o **desenvolvimento particular do indivíduo** e dos **seus pensamentos**, sem a imposição da autoridade pública sobre o seu agir e pensar íntimos.

#### O direito à privacidade

tem por objeto **a integridade moral do titular do direito, sua vida íntima**, envolvendo o **sigilo** sobre as informações pertencentes a esta **zona privada do indivíduo = Direito à inviolabilidade pessoal da intimidade**;

Direito positivado no ordenamento jurídico brasileiro como **direito fundamental (artigo 5º, X e XII, da CF/88)**.

O direito à **proteção de dados pessoais** surge **após** a origem do direito à privacidade, como um **resultado da sociedade da informação**.

A premissa regulatória da **proteção de dados pessoais**, é tutelar o cidadão para que tenha **o controle total sobre seus dados pessoais e sobre as atividades de tratamento** que podem impactar sua vida.

"(...) consistiria em uma **proteção dinâmica** e em uma **liberdade positiva**", ou seja, transcenderia o conceito básico de privacidade, abarcando as **possíveis implicações** que a manipulação dos dados poderiam causar à pessoa humana.

Sobre o tratamento de dados pessoais, é definido como toda operação realizada com dados pessoais, além de Todas as possibilidades de manuseio dos dados pessoais, independente do meio utilizado. Podemos encontrar informações mais detalhadas no **Artigo 5º, IX, da LGPD**.

## Lição 6: Incidência Material e Territorial

### Incidência Material



**Qualquer operação de tratamento de dados pessoais**, realizado por qualquer pessoa, **seja natural/física ou jurídica (de direito público ou privado)**, que realize o tratamento de dados de pessoas **para fins econômicos (aferição de lucros)**. Haverá incidência da LGPD, independente do meio em que as operações de tratamento de dados pessoais se realizarem (**seja por meio físico (analógico) ou digital**).

### Incidência Territorial



A **LGPD** se aplicará, **independente do país de sua sede ou do país onde estejam localizados os dados pessoais**, desde que:

1. A **operação de tratamento** seja realizada no território nacional;
2. A atividade de tratamento tenha por objetivo a **oferta ou o fornecimento de bens ou serviços** ou o **tratamento de dados de indivíduos** localizados no território nacional;
3. Os dados pessoais do tratamento foram **coletados no território nacional**.

**ATENÇÃO:** Consideram-se coletados no território nacional, os dados pessoais cujo titular nele se encontre no momento da coleta.

## Casos de não aplicabilidade da LGPD

São considerados casos de **não aplicabilidade da LGPD** quando for para:

- Fins exclusivamente **particulares e não econômicos**;
- Fins exclusivamente **jornalísticos, artísticos e acadêmicos**;
- Realizado para fins exclusivos de **segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (esse tratamento será regido por legislação específica)**;
- Tratamento de dados pessoais provenientes de **fora do território nacional**, que não sejam objeto de tratamento por **agentes brasileiros** e nem sejam objetos de **transferência internacional**.

## Lição 7: Conceitos fundamentais da LGPD

Todos os conceitos podem ser verificados no **Artigo 5º da LGPD**, que pode ser considerado um **manual de interpretação de LGPD**, definindo conceitos que nortearão a sua aplicação e entendimento. Sendo assim, é importante reconhecê-los.

### Os Tipos de Dados

A LGPD se aplicada em dados pessoais com finalidades econômicas, assim ela traz diversas categorias de classificação desses dados.

#### Dados Pessoais

Toda informação relacionada a uma pessoa natural identificada ou identificável. Como por exemplo:

- **Nome, RG;**
- **Foto da pessoa;**
- **GPS, histórico de pagamentos.**

#### Dado Pessoal Sensível

Dados vinculados a um indivíduo capaz de identificar ou promover sua discriminação se não for tratado. Como por exemplo:

- **Origem racial ou étnica;**
- **Referente à saúde ou à vida sexual;**

### Dados pessoais sensíveis e a discriminação

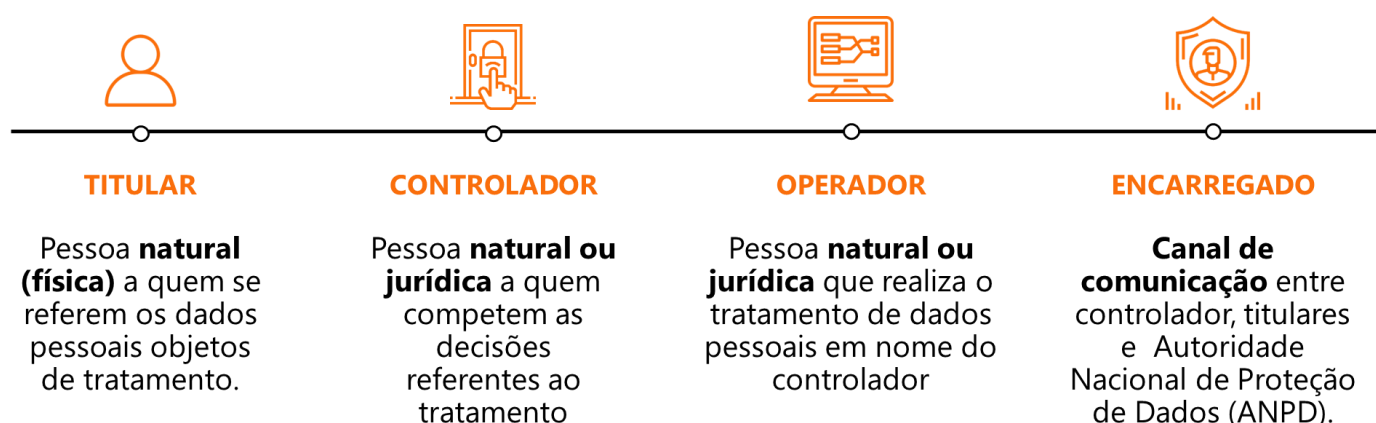
É necessário tomar cuidado com os dados pessoais sensíveis, uma vez que eles podem ter **graves consequências** caso receba o **tratamento inadequado**, verifique algumas delas a seguir:



- ✓ São dados críticos que poderão **implicar riscos e vulnerabilidades graves** aos **direitos e liberdades fundamentais**.
- ✓ As bases legais para tratamento são diferenciadas e limitadas (**Art.11, LGPD**).
- ✓ Consentimento além de **livre, informado e inequívoco** – também deve ser **específico e destacado**.
- ✓ Não há possibilidade para tratamento com base no **Legítimo Interesse e Proteção ao Crédito** (**vedado pela Lei de Cadastro Positivo**).

## Personagens, figuras ou atores

Sujeitos no processo de **tratamento de dados pessoais** envolvidos na LGPD:



## Lição 8: Agentes de Tratamento de Dados Pessoais

Quem é considerado agente de tratamento?

Ressalta-se que os agentes de tratamento devem ser **definidos a partir de seu caráter institucional**. São considerados **agentes de tratamento**:



Não são considerados controladores (autônomos ou conjuntos) ou operadores, **os indivíduos subordinados**, tais como os **funcionários**, os **servidores públicos** ou as **equipes de trabalho** de uma organização, já que atuam sob o poder diretivo do agente de tratamento.



No contexto de uma pessoa jurídica, **a organização é o agente de tratamento para os fins da LGPD**, já que é esta que **estabelece as regras para o tratamento de dados pessoais**, a serem executadas por seus representantes ou prepostos.



**Pessoas naturais** também podem ser consideradas **controladoras** ou **operadoras de dados pessoais**.

O **agente de tratamento** é definido para **cada operação de tratamento de dados pessoais**, portanto, a mesma organização poderá ser **controladora e operadora**, de acordo com sua atuação em diferentes operações de tratamento.

## O Controlador

Agente responsável por tomar **as principais decisões referentes ao tratamento de dados pessoais**. Será considerado **controlador dos dados pessoais** quando atuarem de acordo com **os próprios interesses**, com **poder de decisão** sobre as finalidades e os elementos essenciais de tratamento. Entre as decisões do Controlador, incluem-se **as instruções fornecidas a operadores contratados** para a realização de um **determinado tratamento de dados pessoais**.

A **LGPD** atribui **obrigações específicas** ao **Controlador**, como:

- Elaborar **Relatório de Impacto à Proteção de Dados Pessoais (art. 38)**;
- Comprovar que **o consentimento** obtido do titular atende às **exigências legais (art. 8º, 2º)**;
- Comunicar à **ANPD** a ocorrência de **incidentes de segurança (art. 48)**.

**Responsabilidades em relação à reparação por danos decorrentes de atos ilícitos** é distinta de acordo com a qualificação do agente de tratamento.

Os direitos dos titulares (**art. 18**) são, em regra, **exercidos em face do controlador**, a quem compete, entre outras providências, fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento

## O Operador

Agente responsável por realizar **o tratamento de dados em nome do controlador**. Atuam de acordo com **os interesses do controlador**, sendo-lhes **facultada** apenas a definição de elementos não essenciais à finalidade do tratamento. Deve ser uma **entidade distinta** do controlador. Atuará como **operador** ao tratar dados conforme **a finalidade do tratamento** definida pelo **controlador**.

A **LGPD** atribui **obrigações específicas** ao **Operador**, como:

- Deve seguir **estritamente** as instruções do controlador
- Firmar contratos que estabeleçam o **regime de atividades e responsabilidades** com o controlador;
- Deve dar ciência ao controlador em caso de contrato com **sub operador**.

Embora não exista um conceito de **sub operador** na LGPD, a **ANPD** o definiu como, aquele **contratado pelo operador para auxiliá-lo** a realizar o tratamento de dados pessoais em nome do controlador. A relação direta do **sub operador** é com **o operador e não com o controlador**.

## Lição 9: O Encarregado pelo Tratamento de Dados Pessoais

### O Encarregado

Conhecido como **Data Protection Officer (DPO)**, responsável em garantir a **conformidade** de uma organização pública ou privada à LGPD. De acordo com o **§ 3º do art. 41**, normativas futuras da ANPD poderão trazer hipóteses de dispensa da necessidade de indicação do **encarregado**, conforme a **natureza e o porte da entidade ou o volume de operações de tratamento de dados**.

A LGPD atribui **obrigações específicas** ao **DPO**, como:

- Receber comunicações **dos titulares e da autoridade nacional**, adotando providências;
- Orientar funcionários e os contratados da entidade sobre **as práticas a serem tomadas de proteção**;
- Executar as demais atribuições determinadas pelo **controlador** ou **pelas normas complementares**.

A ANPD poderá **estabelecer normas complementares** sobre a definição e atribuições do **Encarregado** pelo Tratamento dos Dados Pessoais (DPO). A identidade e as informações de contato do encarregado deverão ser **divulgadas publicamente**, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (**§ 1º do art. 41 da LGPD**).

## Lição 10: Bases Legais para o Tratamento de Dados Pessoais

O tratamento de dados pessoais deve-se **amparar em uma base legal**. São verdadeiras condições **de legitimidade para o tratamento de dados pessoais**. Não há hierarquia entre as bases legais. Possível cumular, se cabível no **contexto do tratamento**.

**Rol taxativo** – não existe nenhuma outra hipótese para tratamento, além das **expressamente previstas na LGPD**;

**Art. 7º - bases legais para tratamento de dados pessoais**

**Art. 11 – bases legais para tratamento de dados pessoais sensíveis.**

Veja os seguintes tipos de bases e hipótese legais:

### Consentimento

Permite o tratamento de dados pessoais para **fins específicos** mediante a autorização dos titulares dos dados, determinando que **as empresas** devem ser **transparentes** e informando quais dados serão utilizados de **forma clara**.

### Tutela da Saúde

Utilizadas apenas por **profissionais** e **procedimentos** da **área da saúde** e de **vigilância sanitária** para tratar dados pessoais que sejam necessários para a realização de suas **atividades**.

### Cumprimento de Obrigação Legal ou Regulatória

O tratamento de dados pessoais é justificado pela **obrigação** de cumprir **outras leis**. No caso, ao acionar uma empresa na justiça, ela tem o direito de **armazenar dados** para a **defesa em julgamento**.

### Execução de Políticas Públicas

Aplicada à **administração pública** e não a empresa, ela garante o tratamento e o uso compartilhados de dados pessoais se for **necessário** a aplicação em prática de **políticas públicas previstas em leis**, além de regulamentos ou respaldas em **contratos** e **convênios**.

### Proteção ao Crédito

Garante aos órgãos proteção ao crédito, de modo que possam continuar incluindo dados de consumidores em **cadastros positivos**, além de **comunicar** aos órgãos competentes que existe essa dívida, para que o mercado possa continuar consultando os órgãos de proteção ao crédito para **avaliar o perfil do pagador**.

### Exercício Regular de Direitos

Uso de dados pessoais para o **exercício regular de direitos** é garantido pela LGPD, a fim de que possa exercer direitos em processos judiciais, administrativos e arbitrais para o tratamento.

### Legítimo Interesse

Os dados pessoais podem ser tratados quando **necessário** para atender aos interesses legítimos do **controlador ou de terceiros**, desde que **não** se sobreponha a **direitos e liberdades** fundamentais do titular dos dados.

### Proteção da Vida ou Incolumidade Física

É possível justificar o uso de dados pessoais quando for **indispensável** para a proteção da **vida e da segurança física** do titular, sem precisar de seu consentimento.

### Execução de Contrato ou Procedimento Preliminares

Prevê que os dados pessoais podem ser utilizados para executar ou preparar um contrato do qual o titular seja parte, **a pedido do titular**.

### Estudos por Órgãos de Pesquisa

Sempre que possível deve ser feita a **anonimização dos dados**, adotando procedimentos que impossibilitem a associação direta ou indireta entre um dado e um indivíduo. Além disso, os dados devem ser tratados exclusivamente dentro do **órgão de pesquisa** e **estritamente para a finalidade do estudo**.

### Prevenção à Fraude e Segurança

No tratamento desses dados, inclusive **biométricos** ou **faciais**, **podemos** mencionar alguns exemplos, tais como, para acesso a locais restritos; para efetivação ou confirmação de transações bancárias; para combate a fraudes em processos de identificação; a estes não se limitando, desde que se esteja diante do uso de **sistemas eletrônicos**.

## Lição 11: Princípios da LGPD

Visando o reconhecimento de boas condutas, destacamos os **10 princípios que norteiam a LGPD** e devem ser **respeitados**:

### Finalidade

Os dados pessoais devem ser tratados para **cumprir propósitos legítimos**, autorizados por lei, específicos, explícitos e informados ao titular.

### Adequação

Os dados pessoais devem ser tratados de forma **compatível com as finalidades informadas ao titular**, garantindo o titular a ciência do que é feito com os dados.



### Necessidade

Os dados pessoais devem ser **pertinentes, proporcionais e não excessivos**, isto é, limitados ao mínimo necessário em relação aos fins para os quais são tratados.

### Qualidade

Os dados pessoais devem ser **precisos, claros, relevantes e atualizados**, e todas as medidas razoáveis devem ser tomadas para essa garantia, de acordo com a **finalidade de seu tratamento**.

### Segurança

Os agentes de tratamento devem aplicar **medidas técnicas e administrativas** para garantir a segurança adequada dos dados pessoais contra quaisquer tipos de **tratamentos não autorizados**.

### Não Discriminação

É expressamente proibido qualquer tipo de tratamento de dados pessoais que **implique discriminação ilícita ou abusiva**. Também denominados de **dados pessoais sensíveis**.

### Livre Acesso

Os agentes de tratamento devem garantir aos titulares meios eficazes para que possam realizar **consulta facilitada e gratuita** sobre os dados.

### Transparência

Os titulares devem ter **fácil acesso a informações claras e precisas** sobre o tratamento de seus dados pessoais e saber quais são os agentes envolvidos, **sem o compartilhamento indevido**.

### Prevenção

Além das medidas de detecção e resposta a incidentes, também é necessário **adotar medidas técnicas e administrativas** para **prevenir que eventuais incidentes ocorram**, garantindo a segurança.

### Responsabilidade

Os agentes de tratamento devem demonstrar o **cumprimento da legislação de proteção de dados pessoais** e o quão eficazes são.

## Lição 12: Autoridade Nacional de Proteção de Dados Pessoais (ANPD)



É o **órgão da administração pública federal** responsável por **zelar, implementar e fiscalizar** o cumprimento da **LGPD no Brasil**. O papel da ANPD é amplo e vai além de apenas fiscalizar e aplicar sanções em caso de violação à LGPD. Além deste caráter **fiscalizatório e sancionatório**, a ANPD também exerce papel de **natureza normativa e deliberativa**. E ela é composta por:



### Responsabilidades gerais da ANPD

**Fiscalizar e fazer cumprir** a aplicação da LGPD com o objetivo de proteger os **direitos e liberdades fundamentais** das **pessoas naturais** em relação ao tratamento e promover a conscientização pública e a compreensão dos riscos, regras, salvaguardas e direitos em relação ao tratamento de dados pessoais.

### Competências gerais

<b>Fiscaliza aplicação da LGPD</b>  Aspecto <b>preventivo</b> e <b>remediador</b> , fiscalizando operações de dados.	<b>Aconselhar e promover</b>  O <b>conhecimento</b> das normas e das políticas para a <b>população</b> .
<b>Administrar incidentes</b>  Ser <b>informada</b> devidamente pelos <b>controladores</b> sobre qualquer incidente.	<b>Estabelecer Padrões</b>  Definição das <b>cláusulas contratuais, normas e diretrizes</b> .

## Lição 13: Exercícios práticos sobre LGPD

O site do **Data SUS**, responsável pelos dados do sistema de saúde, foi alvo de **ataques cibernéticos** e **perda do banco de dados** de vacinação pública.



A **LGPD na saúde** é bastante específica, uma vez que:

- Tratam **dados sensíveis** que afetam a **vida íntima de indivíduos**;
- Dados utilizados por **diversas instituições** que **compartilham as informações**.

Para se aprofundar ainda mais sobre o contexto da LGPD acesse nova *live* sobre como se **adequar** à nova lei de proteção de dados, [clikando aqui](#).

## Lição 14: 5 passos práticos para aplicar o que você aprendeu

1. **Invista** na **segurança de dados** da organização;
2. **Veja** a LGPD como um benefício para a organização, não como ameaça;
3. **Foque** nas pessoas para tratar de segurança de dados;
4. **Utilize** os **princípios da LGPD** como fortaleza;
5. **Se informe** sempre sobre as alterações em regulamentações.

## **Módulo 2**

# **Tratamento de Dados Pessoais e Organização da Privacidade**

## Lição 1: Objetivos do módulo

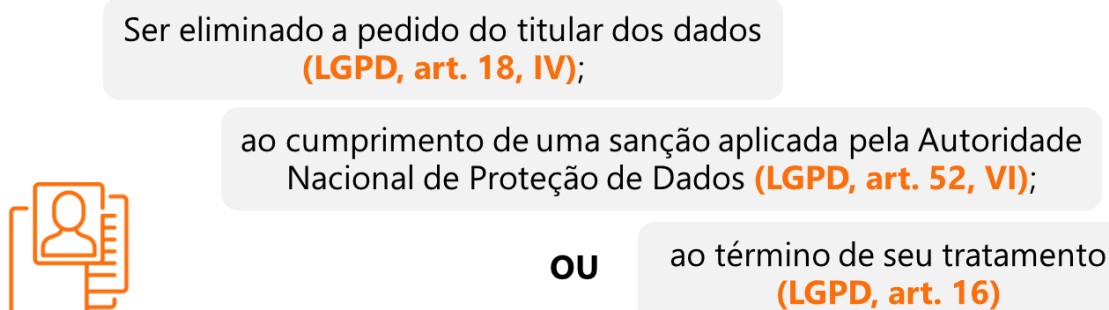
Neste módulo, trataremos do Ciclo de Vida dos Dados Pessoais, passando por cada uma das suas fases, enquanto está sendo objeto de tratamento pelas instituições (sejam públicas ou privadas), à luz da LGPD.

### Responderemos perguntas do tipo:

- ✓ Como garantir a transparência do tratamento de dados?
- ✓ Quais os procedimentos para mitigar incidentes com dados?
- ✓ Qual a responsabilidade da ANPD para garantir a segurança?

## Lição 2: Ciclo de Vida dos Dados Pessoais

O **dado pessoal** é coletado para atender a uma **finalidade específica** e pode, por exemplo:



Assim, um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante **um período de tempo**, de acordo com certos critérios de eliminação.

### LGPD x LAI

A **luz da LGPD**, considera como tratamento todas as operações realizadas com dados pessoais.

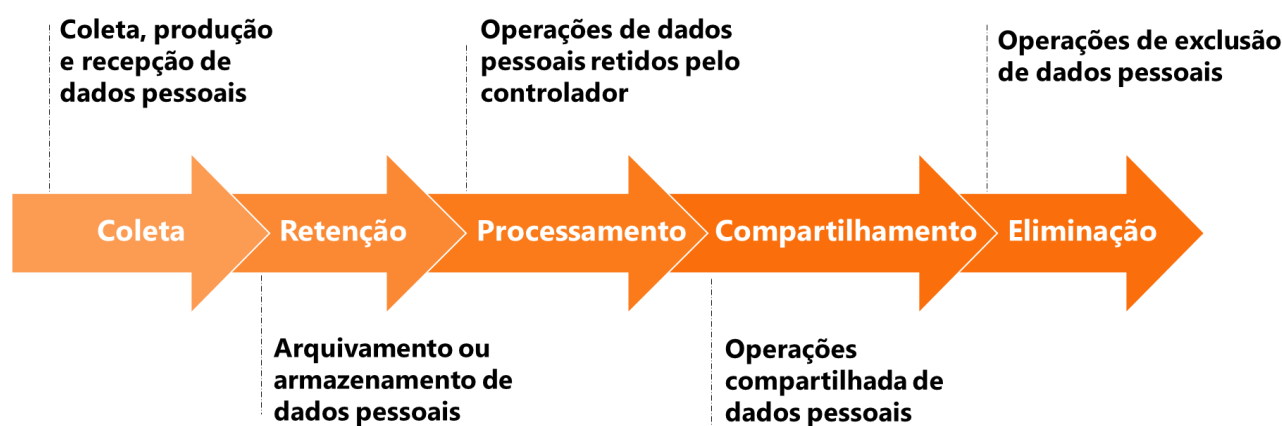
A **Lei de Acesso à Informação - LAI (Lei ne 12.527, de 18 de novembro de 2018)** e o seu regulamento **(Decreto ne 7.724, de 16 de maio de 2012)** igualmente apresentam **regras específicas** para o acesso a documentos de interesse público e que, não raro, contêm também dados pessoais.



A **LGPD** e a **LAI** também devem, portanto, ser interpretadas **sistematicamente!**



## Etapas do Ciclo de Vida dos Dados Pessoais



## Lição 3: Direito dos Titulares dos Dados Pessoais

O Titular dos Dados Pessoais é toda **pessoa natural** a quem se referem os dados pessoais que são objeto de tratamento (**Art. 5º, V, LGPD**).

### QUESTÃO POLÊMICA:

A LGPD **não é aplicável a pessoas falecidas**, já que em seu texto, dispõe que sua aplicabilidade se dará ao tratamento de dados pessoais de **pessoas naturais**?

No **art. 6º Código Civil de 2002 (CC/02)**, há a seguinte disposição: A existência da **pessoa natural** termina com a morte. Contudo, em matéria de Privacidade e Proteção de Dados Pessoais, há polêmicas sobre **o nível de proteção aos dados pessoais de pessoas já falecidas**.

Nos termos do **art. 17 da Lei Geral de Proteção de Dados Pessoais (LGPD)**, toda pessoa natural tem **assegurada a titularidade de seus dados pessoais** e garantidos os direitos fundamentais de **liberdade, de intimidade e de privacidade**.

### Quais os principais direitos dos titulares?

Segundo o Artigo 18 da LGPD, podemos destacar os seguintes pontos:

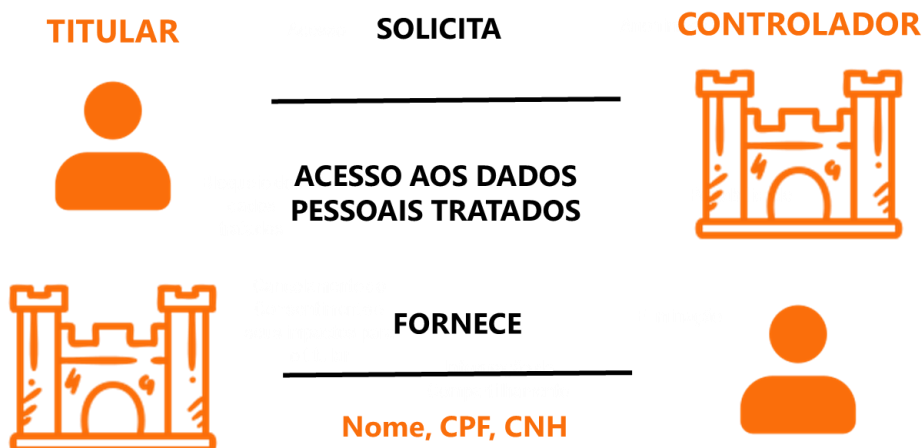
- Confirmação da **existência de tratamento** e o **acesso aos dados**;
- **Correção** de dados incompletos, inexatos ou desatualizados;
- **Anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- **Portabilidade dos dados** a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a **regulamentação da autoridade nacional**, observados os segredos comercial e industrial;

- **Eliminação** dos dados pessoais tratados com o **consentimento do(a) titular**, exceto nas hipóteses previstas no **art. 16 da lei**;
- **Informação das entidades públicas e privadas** com as quais o controlador realizou uso **compartilhado** de dados;
- Informação sobre a possibilidade de não fornecer **consentimento** e sobre **consequências** da negativa;
- **Revogação do consentimento**, nos termos do **§ 5.º do art. 8.º da lei**.

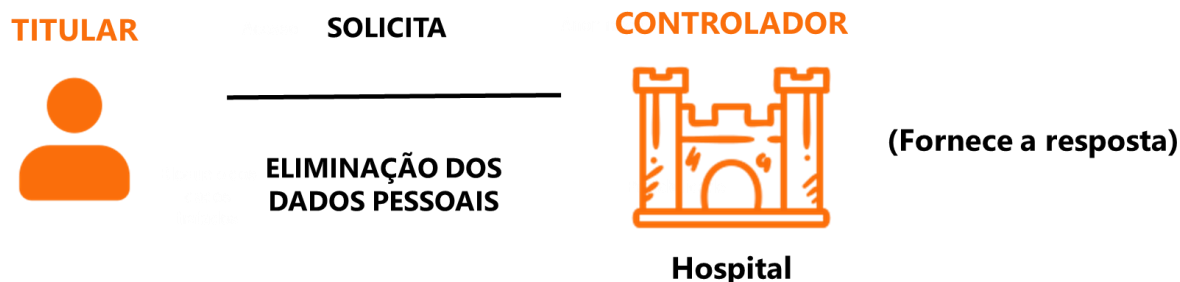


O **titular dos dados** tem direito a solicitar a **revisão de decisões tomadas** unicamente com base em **tratamento automatizado de dados pessoais** que afetem seus interesses, incluídas as decisões destinadas a definir o seu **perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade** (**Art.20 da LGPD**).

Atendimento à solicitação do Titular



## Impossibilidade de Atendimento à Solicitação do Titular



**Impossibilidade** de eliminação por necessidade de armazenamento dos dados pessoais, em cumprimento de uma **obrigação legal ou regulatória imposta** ao controlador, nos termos do **Art. 7º, inciso II, da LGPD**.

## Lição 5: Incidentes de Segurança da Informação com Dados Pessoais

### Incidente de Segurança

Qualquer evento adverso confirmado, relacionado à **violação na segurança de dados pessoais**, tais como **acesso não autorizado, acidental ou ilícito** que resulte na **destruição, perda, alteração, vazamento** ou ainda, qualquer forma de **tratamento de dados inadequada ou ilícita**, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

**O Art. 46 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD)** determina que os **agentes de tratamento de dados pessoais** devem adotar medidas de segurança, técnicas e administrativas aptas a **proteger os dados pessoais de acessos não autorizados** e de **situações acidentais ou ilícitas** de **destruição, perda, alteração, comunicação** ou qualquer forma de tratamento inadequado ou ilícito.

### Definição de Incidentes de Segurança para a GDPR

Violação da segurança que provoque de modo acidental ou ilícito, **a destruição, a perda, alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (Art. 4º do GDPR)**.

### Em caso de Incidentes de Segurança com Dados Pessoais

Diante de algum incidente de segurança da informação, o que pode ser feito? Verifique alguns procedimentos a seguir:

- Avaliar internamente o incidente. Vide **formulário de avaliação constante** do sítio eletrônico da ANPD;
- Comunicar ao **encarregado (Art. 5º, VIII da LGPD)**;
- **Comunicar ao controlador**, se você for o operador, nos termos da LGPD;
- **Comunicar à ANPD e ao titular de dados**, em caso de risco ou dano relevante aos titulares (**Art. 48 da LGPD**);
- Elaborar **documentação com a avaliação interna do incidente**, medidas tomadas e análise de risco, para fins de cumprimento do princípio de **responsabilização e prestação de contas (Art. 6º, X da LGPD)**.

Quem deve fazer a comunicação de incidentes?



É obrigação do **controlador** comunicar à **Autoridade Nacional de Proteção de Dados (ANPD)** e ao **titular** a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

As informações **devem ser claras e concisas**. Além do que prescreve o **§ 1º do artigo 48 da LGPD**, recomenda-se que a comunicação contenha as seguintes informações:

- |  |  |
|--|--|
| <b>1</b> <b>Entidade</b> ou <b>Pessoa</b> responsável pelo tratamento.   | Em casos de <b>comunicação parcial</b> :                             |
| <b>2</b> <b>Encarregado</b> de dados ou outra <b>pessoa de contato</b> . | <b>4</b> Indicar que se trata de uma <b>comunicação preliminar</b> ; |
| <b>3</b> Indicação se a notificação é <b>completa ou parcial</b> .       | <b>5</b> ou de uma <b>comunicação complementar</b> .                 |

Os **agentes de tratamento** devem registrar **qualquer incidente** que ocorram com dados pessoais e sob sua **responsabilidade** ser capaz de registrar:

- |  |   |
|--|---|
| <b>1</b> <b>Data e hora</b> de detecção, do incidente e duração;             | <b>4</b> <b>Resumo</b> do incidente de segurança com dados pessoais;                        |
| <b>2</b> <b>Circunstâncias</b> em que ocorreu a violação de segurança;       | <b>5</b> <b>Prováveis consequências</b> de riscos para direitos e liberdades dos titulares; |
| <b>3</b> <b>Descrição dos dados pessoais</b> e informações <b>afetadas</b> ; | <b>6</b> <b>Medidas tomadas</b> para resolver as consequências do incidente                 |

Em que situação e o que deve ser comunicado ao titular dos dados?

- 1 Sempre que o incidente de segurança possa **acarretar um risco ou dano relevante aos titulares afetados**.
- 2 Critérios mais objetivos serão objeto de **futura regulamentação** e **não poderão ser aqui exigidos sob pena de se inovar na LGPD**.
- 3 Risco ou dano relevante para os **titulares envolvendo dados sensíveis** ou de indivíduos em **situação de vulnerabilidade**.
- 4 O **volume de dados envolvido**, o quantitativo de **indivíduos afetados**, a **boa-fé** e as **intenções dos terceiros**.

## O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)



É **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** (**Art. 5º, inciso XVII, da LGPD**).

## Lição 5: Plano de Resposta e Remediação à Incidentes

### Plano de Resposta à Incidentes com Dados Pessoais

Processo que descreve como uma **organização** deverá lidar com **um incidente de violação de dados**. O objetivo é **minimizar os danos** que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

#### Art.46 da LGPD

Os **agentes de tratamento** devem adotar medidas aptas a **proteger os dados pessoais** de acessos não autorizados e de situações **acidentais** ou **ilícitas**.

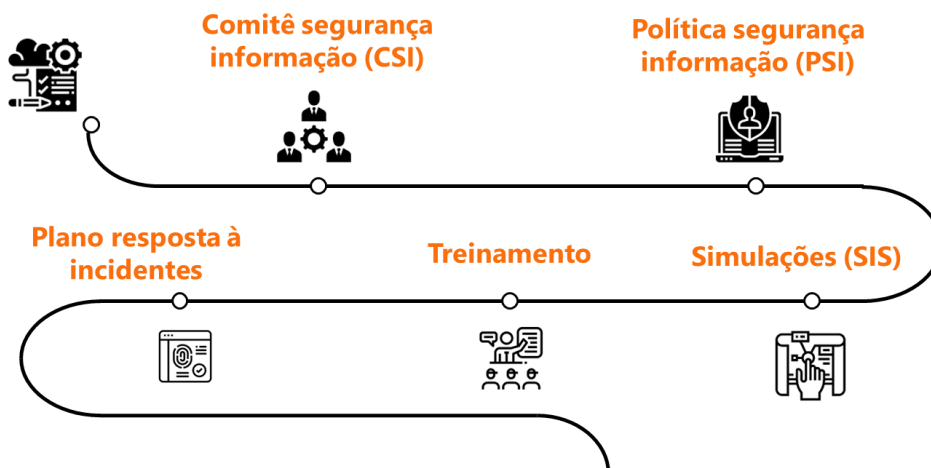
#### Art.48 da LGPD

O **controlador** deverá comunicar à **autoridade nacional** e **ao titular** a ocorrência de incidente de segurança.



## Plano de Resposta à Incidentes e suas Etapas

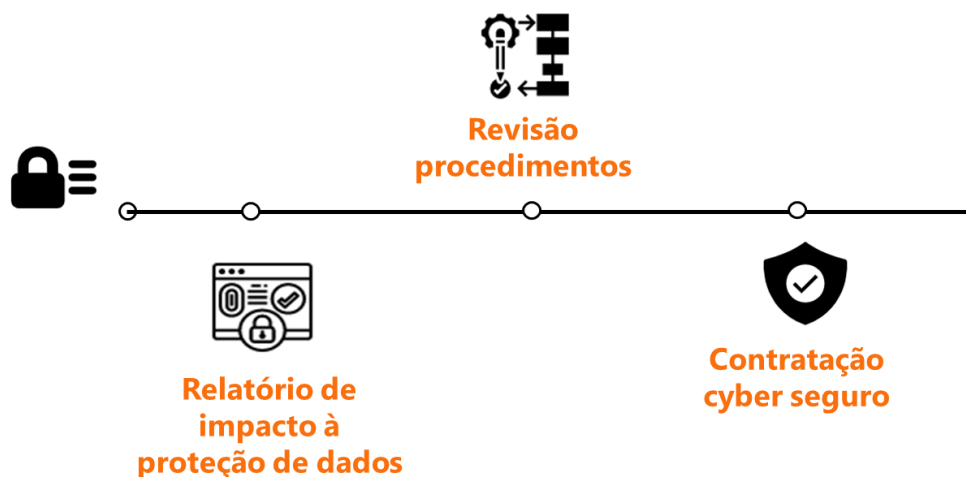
A primeira **etapa de Preparação** é composta pelos seguintes elementos:



A segunda **etapa de Execução** é composta pelos seguintes elementos:



A terceira **etapa de Recuperação** é composta pelos seguintes elementos:



## Relatório Inicial de Incidentes



## Incidentes de Segurança com Exposição de Dados Pessoais

### Riscos

Relação existente de uma ameaça que se concretize com o **grau de vulnerabilidade** do sistema receptor a seus efeitos.

### Riscos de Segurança

Evento que possui **chance de ocorrência futura** que não é **nula** e que apresenta **impacto negativo significativo**.

### Dano Relevante

Prejuízo sofrido pelo **patrimônio econômico** ou **moral de alguém**.

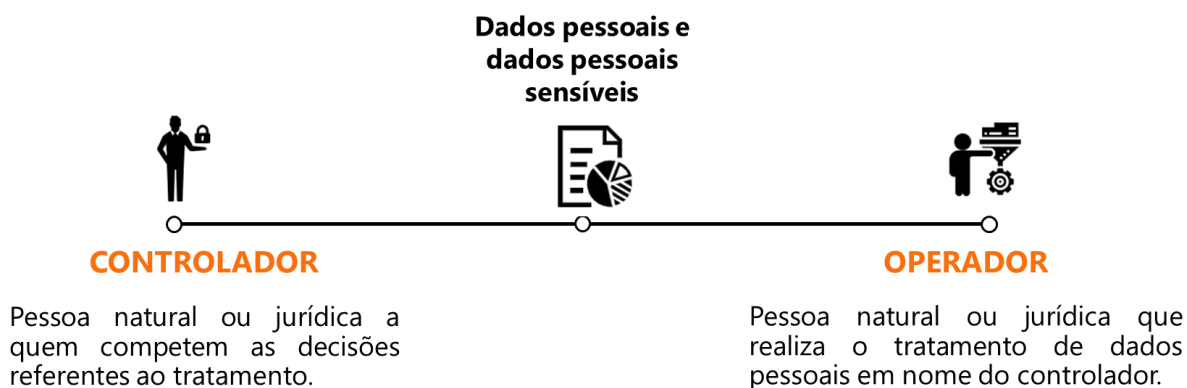


**Risco de Segurança = Chance de ocorrência + Impacto negativo estimado + Incerteza relacionada com as medidas**

## Lição 6: Medidas de Segurança, Boas Práticas e Governança

**Boas práticas e governança** são critérios definidos pela LGPD (art. 50). **Controladores e operadores** poderão formular regras de boas práticas e de governança para **estabelecer as condições da organização, funcionamento, procedimentos** (reclamações, pedidos), **normas de segurança, padrões técnicos, obrigações de cada um destes atores, ações educativas, as formas de fiscalização e mitigação de riscos**, dentre outros.

E quem são os agentes envolvidos nesse processo?



## Ações importantes para Boas Práticas e da Governança

Para a criação de um **Programa de Governança em Privacidade (PGP)** eficiente deve-se:

1. **Conhecer previamente** a empresa e o modelo de negócio adotado;
2. **Mapear os dados** que são coletados e usados pela empresa;
3. **Identificar os riscos e criar mecanismos** com o intuito de **proteger os dados** contra ameaças;
4. **Treinar todos os colaboradores e demonstrar** a importância de seguir as normas e os procedimentos criados **em conformidade com a LGPD**.
5. **A gestão e a atualização contínua do programa** também são pontos importantes que devem ser considerados.



## Privacy by Design

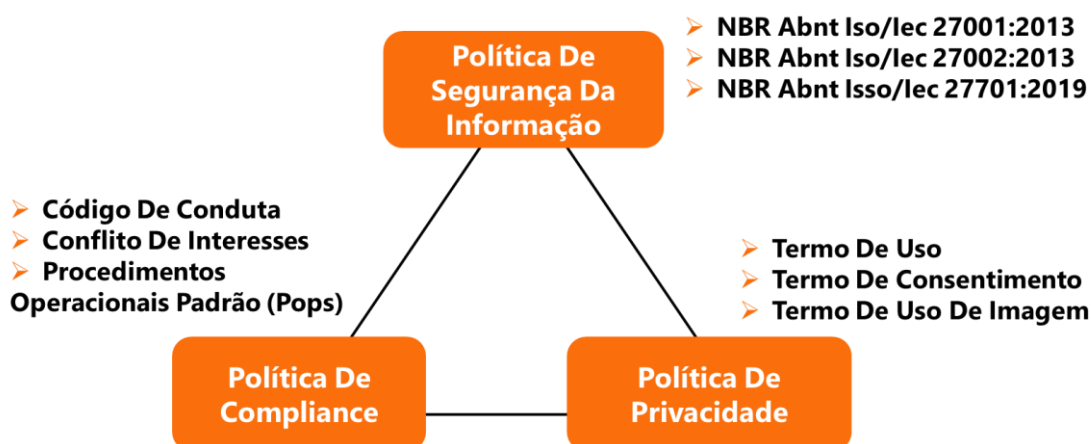
Utilização das **medidas técnicas, físicas e organizacionais** adequadas para garantir que toda e qualquer ação para os tratamentos de dados pessoais é desenvolvido **considerando todos os requerimentos aplicáveis** à proteção de dados pessoais, **desde o início do projeto ou da operação**.

## Privacy by Default

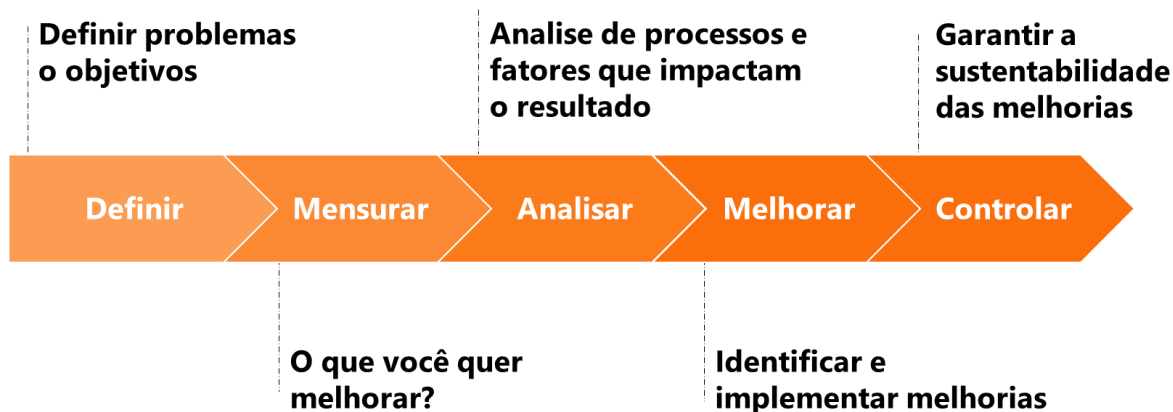
Assegurar que os dados pessoais tratados são os **estritamente necessários ao desenvolvimento da atividade empresarial** e sejam processados e arquivados – ou realizem quaisquer dos outros **procedimentos vinculados ao tratamento**.

## Por que a conformidade é importante?

No juízo de gravidade do incidente, será **avaliada eventual comprovação** de que foram adotadas medidas técnicas adequadas que tornem **os dados pessoais afetados ininteligíveis**, no âmbito e nos **limites técnicos de seus serviços**, para terceiros não autorizados a acessá-los. Mas do que se trata o **Tripé de Boas Práticas para LGPD?**



## Adoção de boas práticas e de governança e a conformidade



## Lição 7: Noções de Segurança da Informação (S.I) – ISSO 27.001

### Framework NIST

A Estrutura de Segurança Cibernética NIST, é uma orientação sobre como os **stakeholders** das organizações podem **gerenciar e reduzir o risco** de ataques cibernéticos.

### Framework ISO 27.001

Criado para prover um **modelo** para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um **Sistema de Gestão de Segurança da Informação (SGSI)**.

## Lição 8: Responsabilização e Prestação de Contas



É a 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.

## Lição 9: Principais Regulamentações no Cenário Mundial

Argentina	Japão	México
<b><i>Lei de Proteção de Dados da Argentina (Lei nº 25.326)</i></b> <ul style="list-style-type: none"><li>➤ Coleta de dados realizada mediante o consentimento do usuário;</li><li>➤ Titular dos dados tem o direito de acessar, corrigir, deletar e solicitar a exclusão de seus dados.</li></ul>	<b><i>Emenda APPI de 2017</i></b> <ul style="list-style-type: none"><li>➤ Preceitos básicos para a proteção de dados pessoais;</li><li>➤ Incluído na “lista branca” de países conforme a lei;</li></ul>	<b><i>Ley Federal de Protección de Datos Personales en Posesión de los Particulares</i></b> <ul style="list-style-type: none"><li>➤ Foco nas relações entre usuários e entidades privadas;</li><li>➤ Concede direitos aos processamentos de dados pessoais.</li></ul>

## Lição 10: Transferência Internacional de Dados Pessoais

A Transferência Internacional de Dados Pessoais, para a Lei Geral de Proteção de Dados (LGPD) estabelece que **a transferência internacional de dados** é a “[...] transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro” **(artigo 5º, inciso XV)**.

**Exemplos de atividades:**



**Compartilhamento de base de dados entre empresas do mesmo grupo econômico.**



**Armazenamento de dados em *data centers* localizados no exterior.**



**Contratação de provedor de computação em serviço de nuvem.**

A LGPD aborda **três aspectos estruturantes** da regulação da transferência internacional de dados no **Brasil**:

- 1. Hipóteses** permitidas para a ocorrência **(artigo 33)**;
- 2. Verificação** do nível de proteção do país estrangeiro **(artigo 33, inciso I e artigo 34)**;
- 3. Realização**, pela Autoridade Nacional de Proteção de Dados (ANPD), da definição do conteúdo de **cláusulas-padrão contratual (artigo 35)**

Um dos casos permitidos ocorre quando **o controlador** oferece e comprove garantias de **cumprimento dos princípios**, dos **direitos do titular** e do **regime de proteção de dados** previstos na Lei Geral de Proteção de Dados Pessoais, na forma de:

- ✓ **Cláusulas contratuais específicas** para determinada transferência;
- ✓ **Cláusulas-padrão contratuais**, conhecidas internacionalmente como **SCCs (Standard Contractual Clauses)**;
- ✓ **Normas corporativas globais** ou **regras corporativas vinculantes**, globalmente conhecidas como BCRs **(Binding Corporate Rules)**;
- ✓ Selos, certificados e códigos de conduta **regularmente emitidos**.

As **transferências de dados pessoais** para **fora da UE** estão sujeitas a **mecanismos legais rigorosos**, buscando garantir que o país de destino ofereça **nível de proteção adequado**.  
Estão entre esses mecanismos:



**Cláusulas-Padrão  
Contratuais (SCCs)**



**Regras Corporativas  
Vinculantes (BCRs)**

## Lição 11: 5 passos práticos para aplicar o que você aprendeu

1. **Entenda** quais são as **finalidades** para um bom tratamento de dados pessoais;
2. **Identifique** qual a importância dos registros de tratamento de dados para as **organizações**;
3. **Compreenda** os **tipos de incidentes** com dados atrelados aos **princípios** de proteção de dados pessoais de titulares;
4. **Busque** reconhecer as **funções** dos profissionais responsáveis pelo **controle e tratamento dos dados pessoais** de usuários e quais medidas para mitigar acidentes;
5. **Adequação** a LGPD em garantir a conformidade com **todos os setores da organização**.



## Referências

Get Privacy. 10 bases legais da LGPD que justificam o tratamento de dados: consentimento, legítimo interesse e mais. Disponível em: <https://getprivacy.com.br/entenda-as-bases-legais-da-lgpd/>

Dinamize. Conheça as bases legais da LGPD e entenda como elas se aplicam no marketing. Disponível em: <https://www.dinamize.com.br/blog/bases-legais-da-lgpd/>

Fleming, Cristina. LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis. Conjur. 2021. Disponível em: <https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis>

Brasil. Lei Nº 13.709, De 14 De Agosto De 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)

González, Mariana. Conheça o cenário das leis de proteção de dados ao redor do mundo. Id blog. 2020. Disponível em: <https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/>