# Diretrizes e Boas Práticas para Adequação à LGPD

**Profa. Dra. Michelle S. Wangham**

Laboratório de Sistemas Embarcados e Distribuídos
Programa de Mestrado em Computação Aplicada
UNIVALI – Santa Catarina

**wangham@univali.br**

# Agenda

Contextualização e Motivação

Etapas para Adequação

Mapeamento e Fluxo de Dados

Segurança em Camadas

Boas práticas

Join at

slido.com

#LGPD-LINEA

# Contextualização


# Conformidade com a LGPD


- Trata-se de um grande projeto de governança de dados e pode ser encarado de duas formas:
  - **Caminho rápido**: realizar um *assessment*, identificar os riscos e procurar medidas corretivas até a data;
  - **Caminho recomendado**: estabelecer **um programa de governança de dados**, em que a privacidade e segurança façam parte da **cultura** organizacional.

# Jornada da Conformidade

Tecnologia

Pessoas

Processos

# Jornada da Conformidade



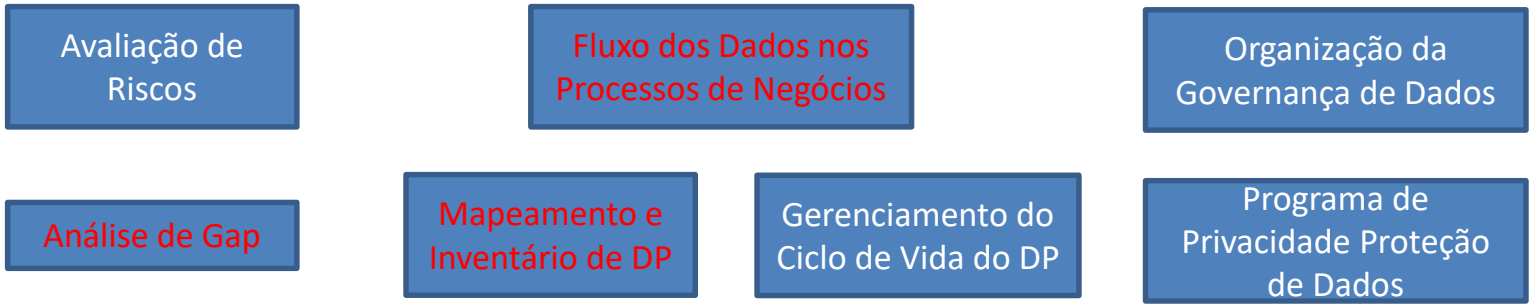

# Etapas para Adequação

- *Framework* SGPD


FONTE: Kyriazoglou, J. (2016); Data Protection and Privacy Management System. Data Protection and Privacy Guide -Vol. 1

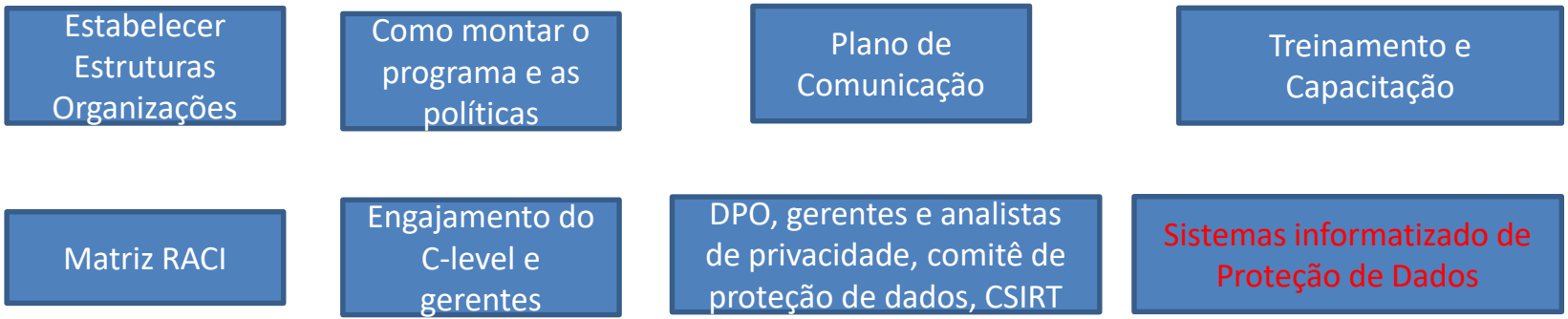
# 1. Preparação

- Analisar os requisitos e necessidades de proteção de dados e privacidade
- Coletar leis, regulamentos e normas relevantes
- Estabelecer um Plano de Ação



# 2. Organização

- Desenhar e implantar o programa de proteção de dados e privacidade
- Designar um encarregado/DPO
- Envolver e obter o compromisso de todas as partes interessadas relevantes



# 3. Desenvolvimento e Implantação

- Projetar um sistema de classificação de dados;
- Desenvolver e implementar políticas, procedimentos e controles para cumprir leis de privacidade e requisitos da organização.

Aprovação do processamento de DP (consulta prévia)

Sistema transferência internacional de DP

Treinamento corporativo para proteção de DP

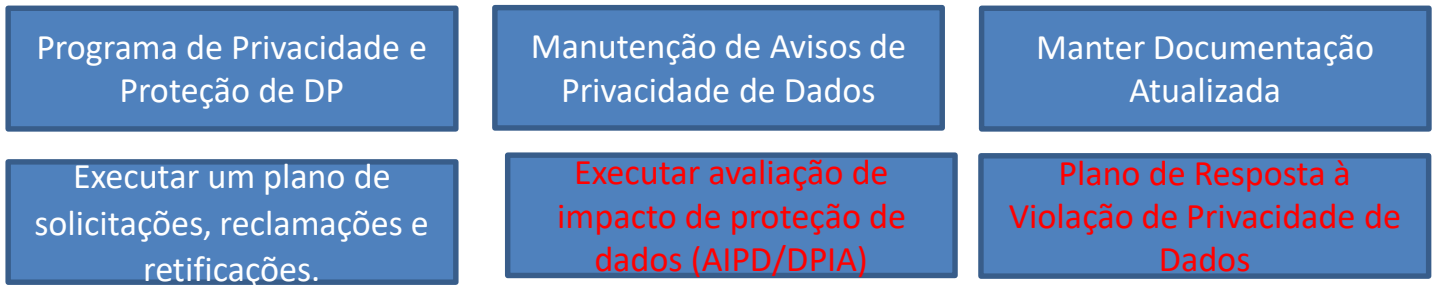
Registrar os Bancos de Dados (DP)

*Privacy by Design*

Controles de Segurança da Informação e proteção de DP

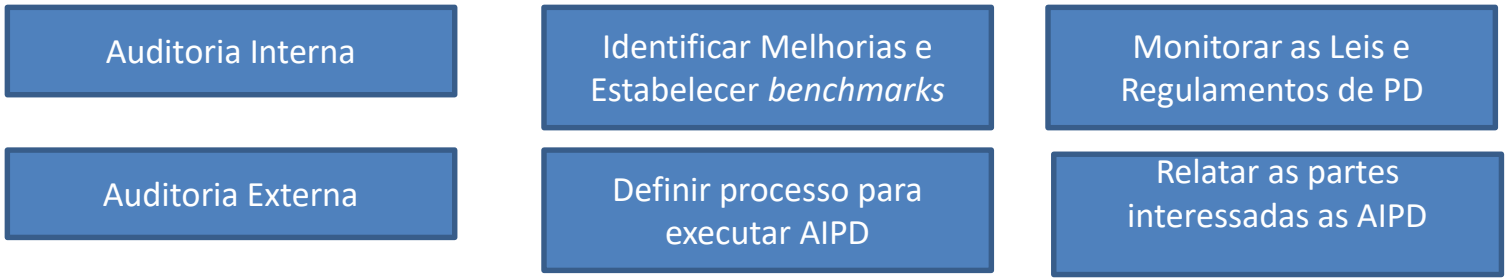
# 4. Governança

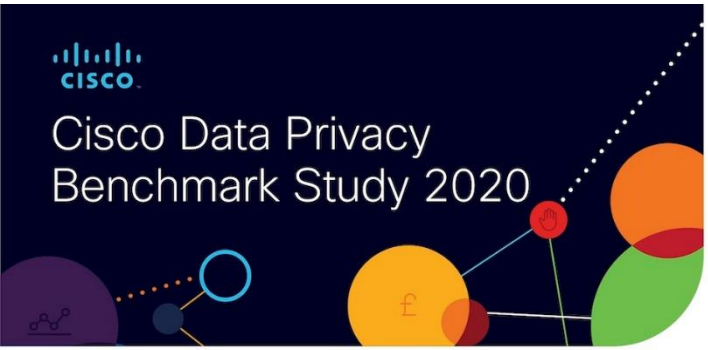
- Desenhar e configurar estruturas de governança
- Envolver e obter o comprometimento de todas as partes interessadas relevantes
- Relatar todas as questões de privacidade (processo contínuo).



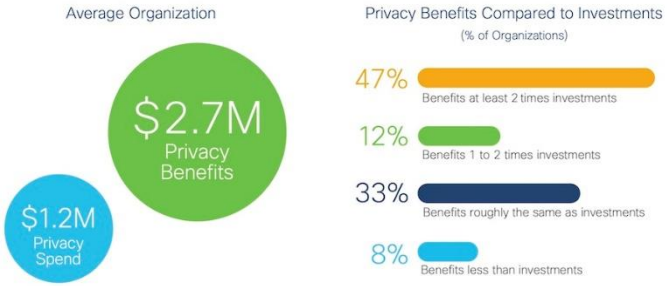
# 5. Avaliação e Melhoria Contínua

- Monitorar a operação e a resolução de todas as questões relacionadas à privacidade;
- Avaliar regularmente a conformidade com processos e políticas internas;
- Melhorar a proteção de dados e as medidas de privacidade.






## Return on Privacy Investment




## Value of Privacy Maturity


## Business Impact




Business Impact

# Por onde começar?

# Mapeamento de Dados Pessoais

- Quais dados pessoais são tratados?
- Quais os tipos de dados?
- Qual a finalidade do tratamento?
- Qual a base legal que legitima o tratamento?
- Como são coletados?
- Onde eles estão armazenados?
- Quem é o responsável e o custodiante?
- Quem tem acesso aos dados?
- Com quem os dados são compartilhados?
- Qual a política de retenção desses dados?

# Mapeamento de Dados Pessoais

## GDPR Data Map

Designed by: Anthony Budd | Designed for: Ideea | Date: 22/1/17 | Version: 1.2

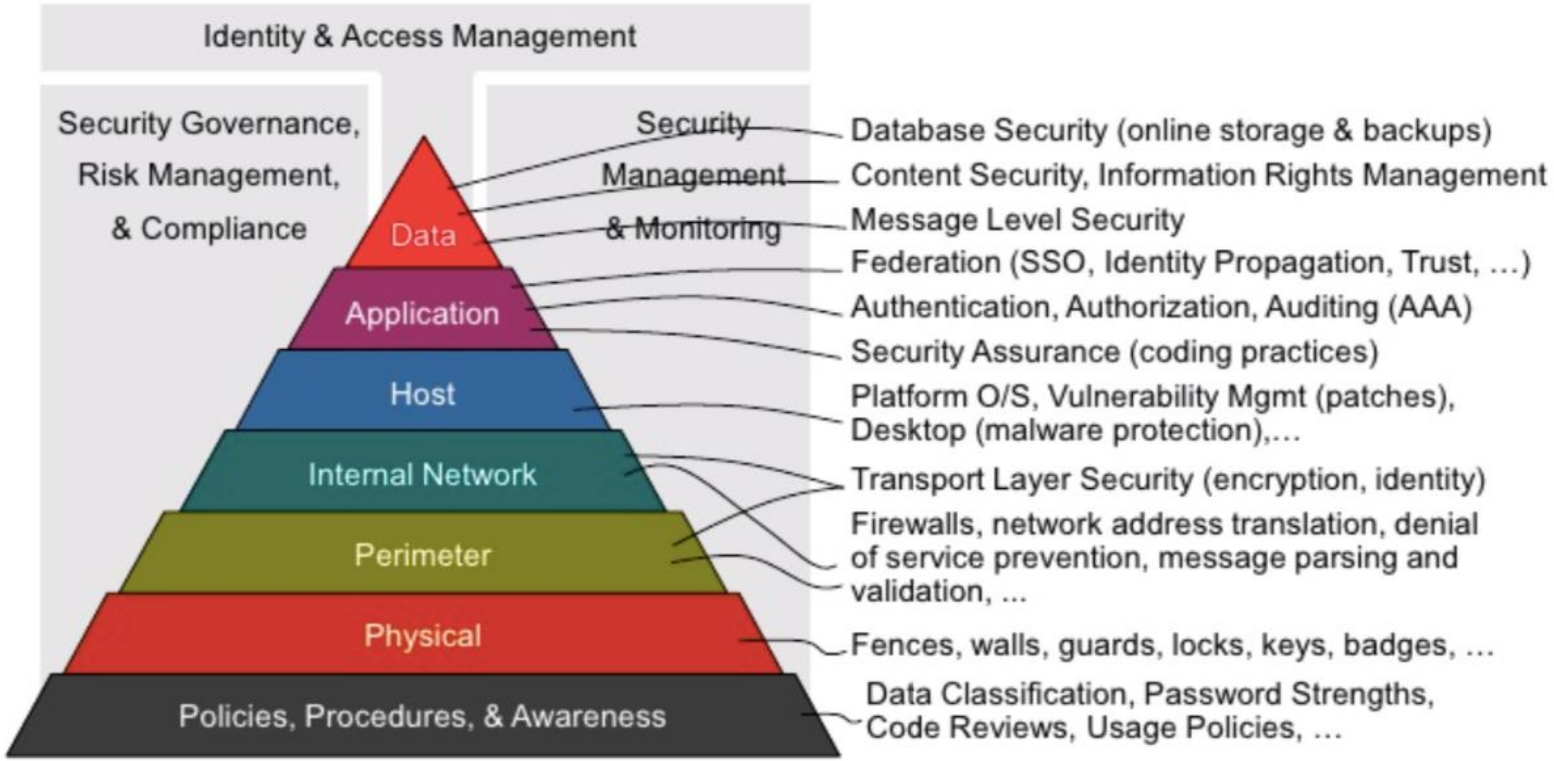
| Source<br>How was this data collected?<br>· Contact Form<br>· External Organisation | Personal Data<br>What data are you collecting?<br>· Email Address<br>· IP Address<br>· Ethnic Origin<br>· Phone Number | Reason<br>Why are you collecting this data?<br>· Marketing<br>· CRM<br>· Processing/ Analytics | Handling<br>Explain how you will store the data, how it will be processed and who has access to it. | Disposal<br>When is this data disposed?<br>· Upon Request<br>· After 6 Months | Consent Obtained | Subject is a over 13 | Mission critical data | Sensitive personal data |
|---|---|---|---|---|---|---|---|---|
| Contact Form | Full Name<br>Email Addres<br>IP Address<br>Phone Number | We need this data because this is how we take new business enquiries | WordPress Database Site Admins | Cron - removed after 30days | ✓ | ✓ | ✓ | ✗ |

*by Anthony Budd, innovation consultant at [Ideea]*

# Fluxo de Dados Pessoais

- Maior entendimento de como os dados se movem através e fora da organização.
- Documenta o ciclo de vida do dado, desde a coleta, uso, até o armazenamento/descarte.
- Relaciona as etapas com processos, sistemas, áreas da organização.
- Deve apresentar também o compartilhamento com terceiros.

# Segurança em Camadas




Fonte: Oracle

# CIS Controls™

V7.1

## Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

## Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

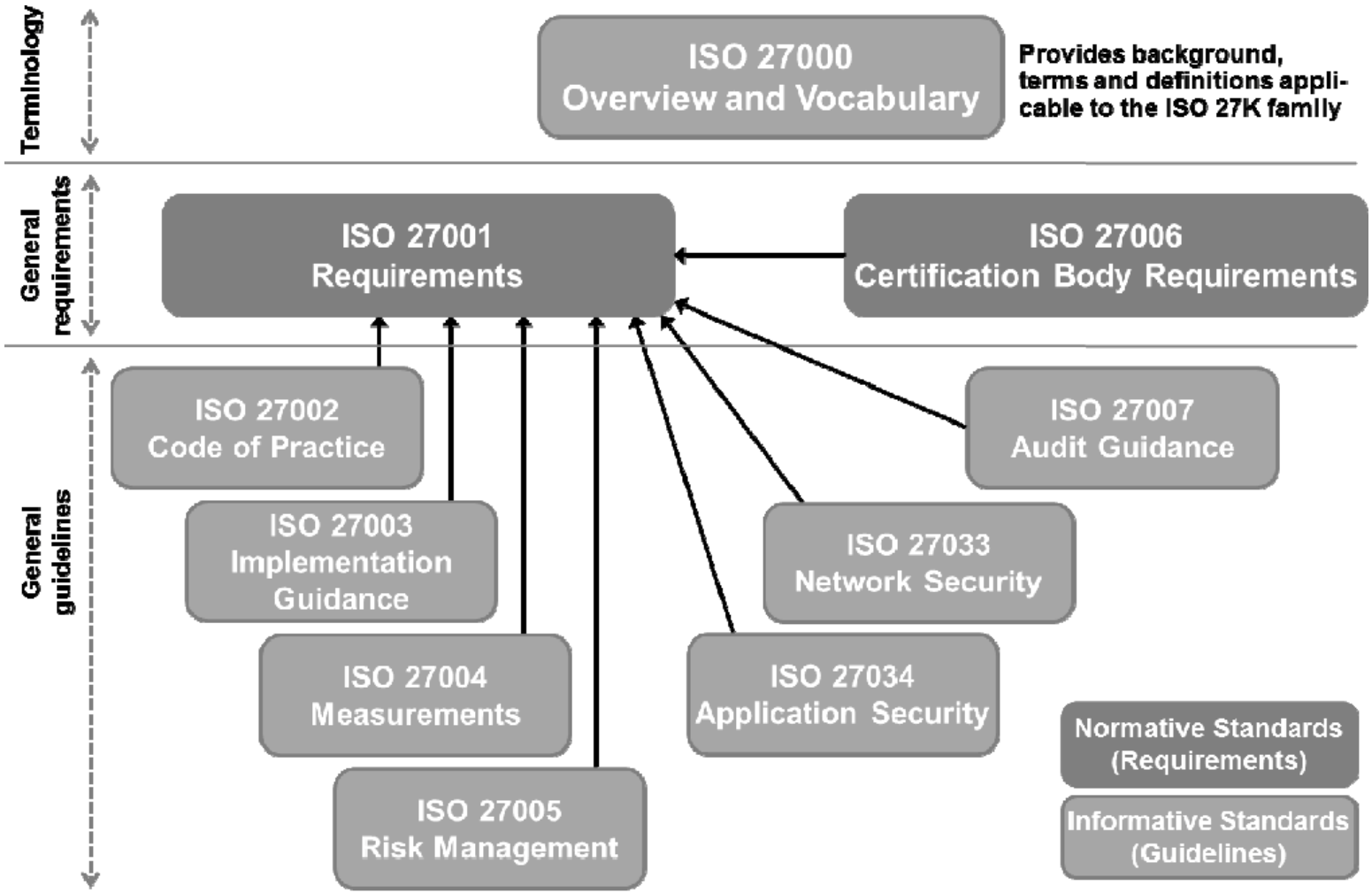



Figure 5. Interrelations within the ISO 27 K family of standards [9]

# ISO 27701 SGPD/PIMS

- Criada em 2019 como uma extensão da 27001 e da 27002
- **Objetivo**: adicionar requisitos e diretrizes para o estabelecimento, implementação, manutenção e melhoraria continua de um SGPD
- Construir uma visão de privacidade baseada nesta ISO é um caminho interessante para conformidade com a LGPD, independente da certificação.

# ISO 27701 SGPD/PIMS

- Para empresas que desejarem certificar, é necessário solicitar a ISO 27001 (SGSI/ISMS) e junto a extensão para 27701 (SGPD/PIMS);
- Trata-se de um processo de adequação que normalmente dura de 06 meses à 01 ano, para depois uma certificadora avaliar e conduzir o processo;
- A certificação tem validade de 03 anos.

Join at

slido.com

#LGPD-LINEA


BEST
PRACTICE

# Boas Práticas

- ✓ Crie o Comitê Multidisciplinar de Governança de Dados (TI, Processos, Seg, Jurídico)
- ✓ Conheça a LGPD e a GDPR
- ✓ Faça um Diagnóstico (Análise de *Gap*)


https://diagnosticolgpd.com.br/

# Boas Práticas

- Engajamento da Alta Direção – DPO
- Capacite o time para implantar a LGPD
- Obtenha todos os processo de negócios da empresa
- Faça o mapeamento de dados e dos fluxos de dados
  - Crie um processo para atualização constante
- Análise de riscos de segurança
- Defina um Plano de Ação (com prazos)
- Use Ferramentas (ver lista) – reforce a segurança

# Ferramentas

- *Data Loss Prevention (DLP)*
- *Endpoint protection*
- *Mobile Device Management (MDM)*
- *Encryption software*
- *Identity and Access Management (IAM)*
- *Cloud Data Protection (CDP)*
- *Consent Management Applications*
- *Compliance software*
- *Customer Data Management (CDM)*
- *Data backup and recovery solutions*
- *Enterprise Content Management (ECM)*
- *Big data encryption*
- *Application- level encryption*

Fonte:

# Boas práticas

- Produza e revise os documentos obrigatórios (ver lista)
- Defina como irá responder aos titulares dos dados (automatize)
- Treinamento e conscientização constantes

**Cultura da privacidade e a ética digital**

# Documentos

| Atividade | Descrição | Execução |
|---|---|---|
| Política de Proteção de Dados Pessoais | Artigo 46 | Obrigatório |
| Avisos de Privacidade | Artigo 9 | Obrigatório |
| Aviso de Privacidade para Funcionários | Artigo 9 | Obrigatório |
| Política de Retenção de Dados | Artigos 5, 18,19. Seção II e III | Obrigatório |
| Cronograma de Retenção de Dados | Artigos 40 e Seção II | Obrigatório |
| Formulário de consentimento do titular | Artigos 7 e 8. Seção I e II | Obrigatório |
| Formulário de consentimento dos pais | Artigo 14. Seção III | Obrigatório |

Fonte: ostec Segurança digital de resultados

# Documentos

| Atividade | Descrição | Execução |
|---|---|---|
| Nomeação e descrição de cargo do DPO, se for exigido um | Artigo 41 | Obrigatório |
| Registro (inventário) de todas as atividades de processamento | Artigo 37 | Obrigatório |
| Registro dos resultados da AIPD | Artigo 38 | Obrigatório em algumas circunstâncias |
| Cláusulas contratuais padrão para a transferência de dados pessoais para controladores, se houver transferência fora do território estabelecido | Artigos 33, 35 e 64 | Obrigatório em algumas circunstâncias |
| Contrato de processamento de dados do fornecedor | Artigos 7 e 39 | Boa prática |
| Procedimento de resposta e notificação de violação de dados | Artigo 50 | Boa prática |
| Registro de violação de dados | Artigo 31, 33 e 42. Seção IV | Boa prática |
| Formulário de Notificação de Violação de Dados para a Autoridade Supervisora | Artigo 33 e 50 | Boa prática |

# Perguntas?

**Profa. Dra. Michelle S. Wangham**

**wangham@univali.br**