Desafios e oportunidades decorrentes da LGPD para área de ES

Profa. Dra. Michelle S. Wangham

Mestrado em Computação Aplicada (UNIVALI)

Assessora de PD&I na RNP

wangham@univali.br

Agenda

- Contextualização
- Jornada da adequação à LGPD (boas práticas)
- *Privacy by Design*
- Desafios e oportunidades

Transformação digital

- Cultura centrada em dados
- Demanda urgente e complexa de PD
- Titular dos dados é o elemento central
- Tratamento de dados
  - Responsabilidades e deveres
  - Mais transparência, ética e segurança

The Data Environment Post-GDPR

	FROM	TO
AVAILABILITY	**SUPER ABUNDANCE** Personal data is "digital exhaust" that can be vacuumed up at will and used without restriction.	**SCARCITY** Personal data is like the car that produces the exhaust – and you're only borrowing it.
CULTURE	**DATA PREDATORS** "The guy with the most data wins." (Tim O'Reilly)	**DATA SHEPHERDS** Data must be managed "sensitively and ethically." (ICO Commissioner Elizabeth Denham)
STRATEGY	**BIG DATA** Personal data is a corporate asset, from which business value is extracted.	**BEG DATA** Personal data accessed via attractive value propositions that win consumers' permission.

Fonte

Privacy's not dead.
It's hiring.

Privacidade não morreu.
Elá está contratando

Fonte: Fabiani Borges

Entre em

slido.com

#eres2021

Resultados da pesquisa

LGPD NO MERCADO BRASILEIRO

- Publicado em 16/11/2021
- 366 participações
- diversas empresas em situações diferentes
- Maior nível de adequação: financeira e serviços de seguro.
- Menor nível: empresas de serviços
- Pequenas e médias: PD não se tornou uma prioridade.
- 60,8% investiu até R$100 mil
- 35% ~ 1 ano para adequação

Requisitos Atendidos	%
0 - 20%	24,4%
21 - 40%	15,9%
41 - 60%	26,8%
61 - 80%	23,2%
81 - 100%	9,8%

20% não iniciou ou planejou a adequação

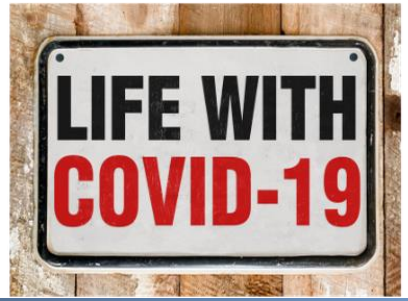

Proteção
de dados
ctrl

Jornada da Conformidade

Tecnologia

Pessoas

Processos

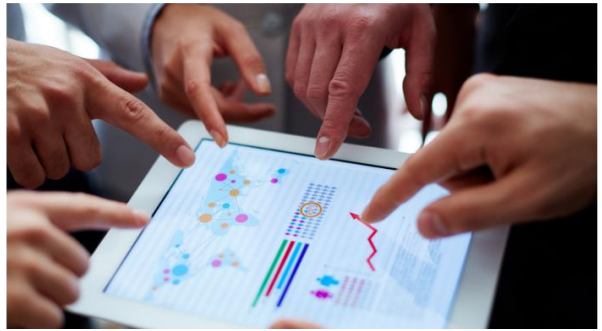


Jornada da Conformidade

Caminho recomendado: estabelecer **um programa de governança de dados**, em que a privacidade e segurança façam parte da **cultura** organizacional.


BEST
PRACTICE

Sensibilização e Comprometimento da Alta Gestão



Impactos/Retornos Positivos + Impactos/Retornos Negativos

Cisco Data Privacy Benchmark Study 2020

Return on Privacy Investment

Average Organization

$2.7M Privacy Benefits

$1.2M Privacy Spend

Privacy Benefits Compared to Investments
(% of Organizations)

- 47% Benefits at least 2 times investments
- 12% Benefits 1 to 2 times investments
- 33% Benefits roughly the same as investments
- 8% Benefits less than investments

Value of Privacy Maturity

Business Impact

Resultados da pesquisa

LGPD NO MERCADO BRASILEIRO

Quais os principais desafios enfrentados / a enfrentar pela sua Organização para se adequar à LGPD?

Ausência de definição e liderança de Proteção de Dados	40,2%
Falta de orçamento	38,1%
Falta de definição clara dos aspectos da lei	36,1%
Falta de conhecimento técnico	29,9%
Falta de referência técnica	27,8%
Outros	14,4%

Comitê Multidisciplinar

Atuar e cooperar com o desenvolvimento do Projeto/Programa

Ameaças internas e externas

Conscientizar e orientar

Atores na LGPD

(Auto) Diagnóstico de Conformidade

- **Levantamento das informações da instituição** (riscos envolvidos)
  - Estrutura organizacional e dos processos
  - Atos normativos internos
  - Controles existentes (segurança e políticas internas)
  - Matriz de riscos corporativos
  - Quais são os terceiros/parceiros
  - Quais são as políticas públicas ou projetos sociais que a instituição participa
  - Legislações que afetam diretamente a instituição

- **(Auto) Diagnóstico preliminar de conformidade (maturidade)**

(Auto) Diagnóstico de Conformidade

- **Gov.br**: um diagnóstico do atual estágio de adequação à LGPD.
  - apresenta um índice de maturidade, que possibilitará aos órgãos e entidades direcionar esforços e priorizar as ações necessárias para conformidade
  - https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd

(Auto) Diagnóstico de Conformidade

- https://diagnosticolgpd.abes.org.br/

(Auto) Diagnóstico de Conformidade

- https://diagnosticolgpd.com.br/ (OSTEC)

*“Duas das principais ferramentas de adequação à nova lei seguem essa lógica: **mapeamento de dados e relatórios de impacto** à proteção de dados.”*

Bruno Bioni

Mapeamento de Dados Pessoais

- Quais dados pessoais são tratados?
- Como foram/são coletados?
- Quais os tipos de tratamentos?
- Qual a finalidade do tratamento?
- Qual a base legal que legitima o tratamento?
- Há alguma classificação de informação?
- Onde eles estão armazenados?
- Quem é o responsável e o custodiante?
- Quem tem acesso aos dados?
- Qual a política de retenção desses dados?
- Com quem os dados são compartilhados? Há outras saídas? Nacional ou Internacional?
- Há algum mecanismo de anonimização ou criptografia do dado?

Template de Mapeamento

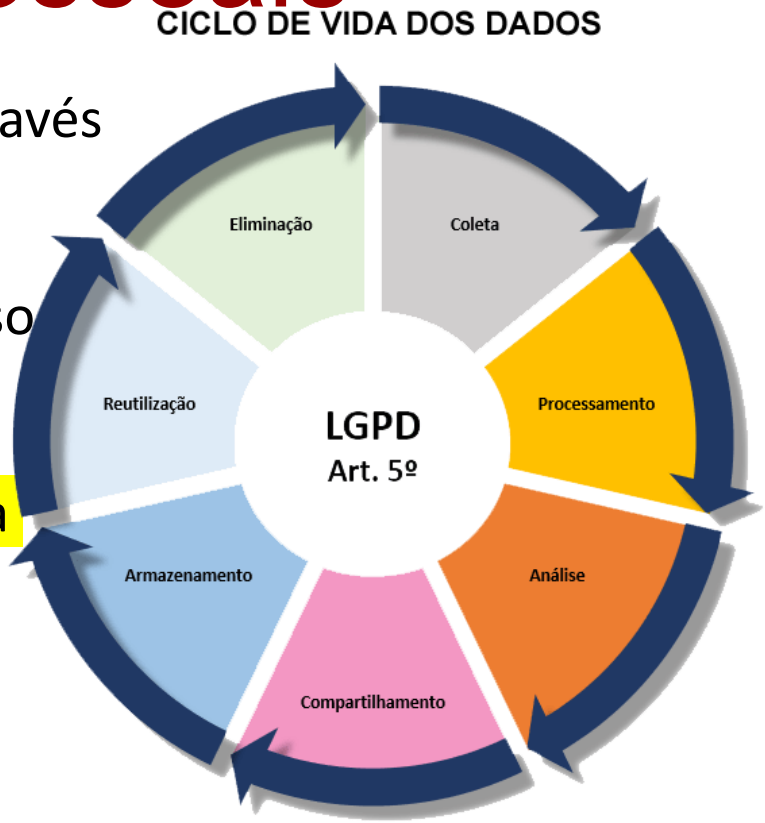
Responsável pelo preenchimento	Departamento	Ponto focal do departamento	Data	Versão

Atividade/Função de negócio/SW	Objetivo	Categoria do titular	Dado Pessoal	Sensível?

Como é feita a coleta?	Tempo de retenção	Transferência do dado	Base Legal	Justificativa/Leis complementares

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



Fonte:
https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd

Avaliação de Impacto (AIPD)

Atividade/função de negócio	Descrição do risco	Consequência	Probabilidade	Impacto	Severidade

Resposta ao risco	Conduta

		Impacto		
		Baixo	Médio	Alto
Probabilidade	Baixa	Baixa	Baixa	Média
	Média	Baixa	Média	Alta
	Alta	Média	Alta	Alta

“Mapear corretamente os dados tratados possibilita uma **melhor avaliação da segurança dos dados e a implementação correta de medidas de segurança** que mitiguem a ocorrência de eventuais incidentes”.

LGPD Acadêmico

Direitos dos Titulares de Dados

- *Confirmação, acesso aos dados, portabilidade, correção, eliminação, compartilhamento, revogação de consentimento, reclamação, etc…*

- Automatizar o processo de atendimento dos pedidos dos titulares
  - Portal de privacidade e outras ferramentas de apoio (registro, autenticação, controle de prazos, respostas)

Políticas e Procedimentos

- Avisos de privacidade (externos)
  - Política de uso de *cookies (gerenciamento)*
- Política de retenção e descarte de dados pessoais
- Política de classificação da informação e de ativos
- Plano de continuidade de negócios (PCN)
  - Política de *backup* e recuperação de DP
- Política de segurança (ex. trabalho em *home office*)
  - Gerenciamento de Dados em Dispositivos Móveis
- Processo para tratamento de incidentes de segurança
- Política de proteção de dados pessoais (interna)

Treinamento e Conscientização

- Programa de treinamento sobre proteção de dados e segurança da informação
  - E-mails e comunicados (intranet, redes sociais, sites) para colaboradores, fornecedores e titulares dos dados
  - Palestras, gamificação, dinâmica de grupos
  - Cursos (12 – 15horas) – formação específica sobre LGPD

Cadeia de fornecedores

- Estabelecer contratos e Conduzir avaliações de conformidades com terceiros/fornecedores (operadores)
  - Modelo de responsabilidade compartilhada
  - Solicitar aos fornecedores de software o envio do dicionário de dados
  - Avaliar os controles de segurança

A LGPD irá impactar o uso de *Cloud Computing* pelas empresas?

Forte auto-regulação!

Entre em

slido.com

#eres2021

Privacy by Design

The 7 Foundational Principles

Implementation and Mapping of Fair Information Practices

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

7 Princípios

- PbD envolve a **adoção de uma série de medidas técnicas e organizacionais, horizontais e verticais**, que precisam ser tomadas de maneira **permanente**, e que envolve **todos** os *stakeholders* da organização.
  - Suporte da alta gestão
  - Minimização de dados de DP (coleta)
  - Conhecer a fundo o ciclo de vida dos dados pessoais
  - Participação ativa do encarregado
  - Automatizar o PbD (trello, miro, git, Jira, etc) – usar as mesmas ferramentas das operações diárias
  - Minimizar e Mascarar a exposição de DP
  - Princípio do menor privilégio e controle de acesso

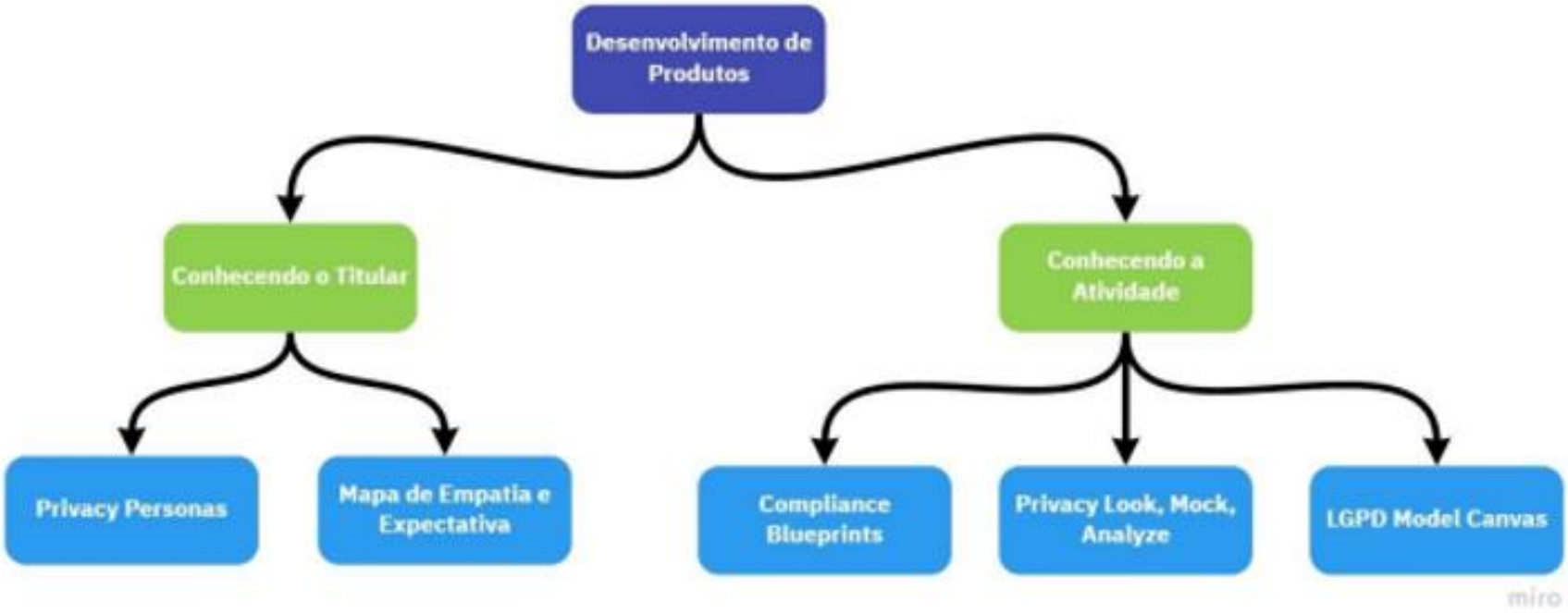
LGPD

- Art. 46. Os **agentes de tratamento 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.

- § 1º A autoridade nacional poderá dispor sobre **padrões técnicos mínimos** para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

- § 2º As medidas de que trata o caput deste artigo **deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução**.

Ferramentas e Metodologias para desenvolvimento de produtos

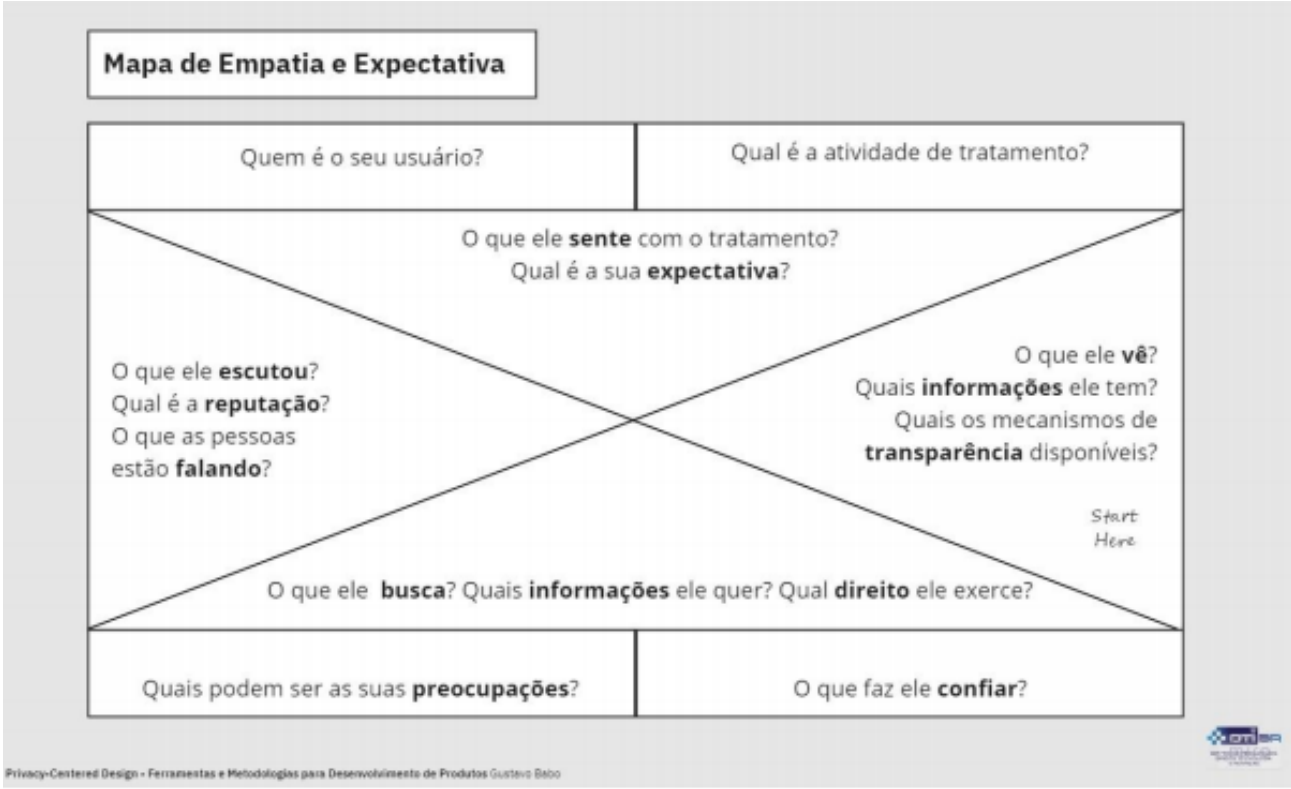


FONTE: Centro DTI BR

Ferramentas e Metodologias

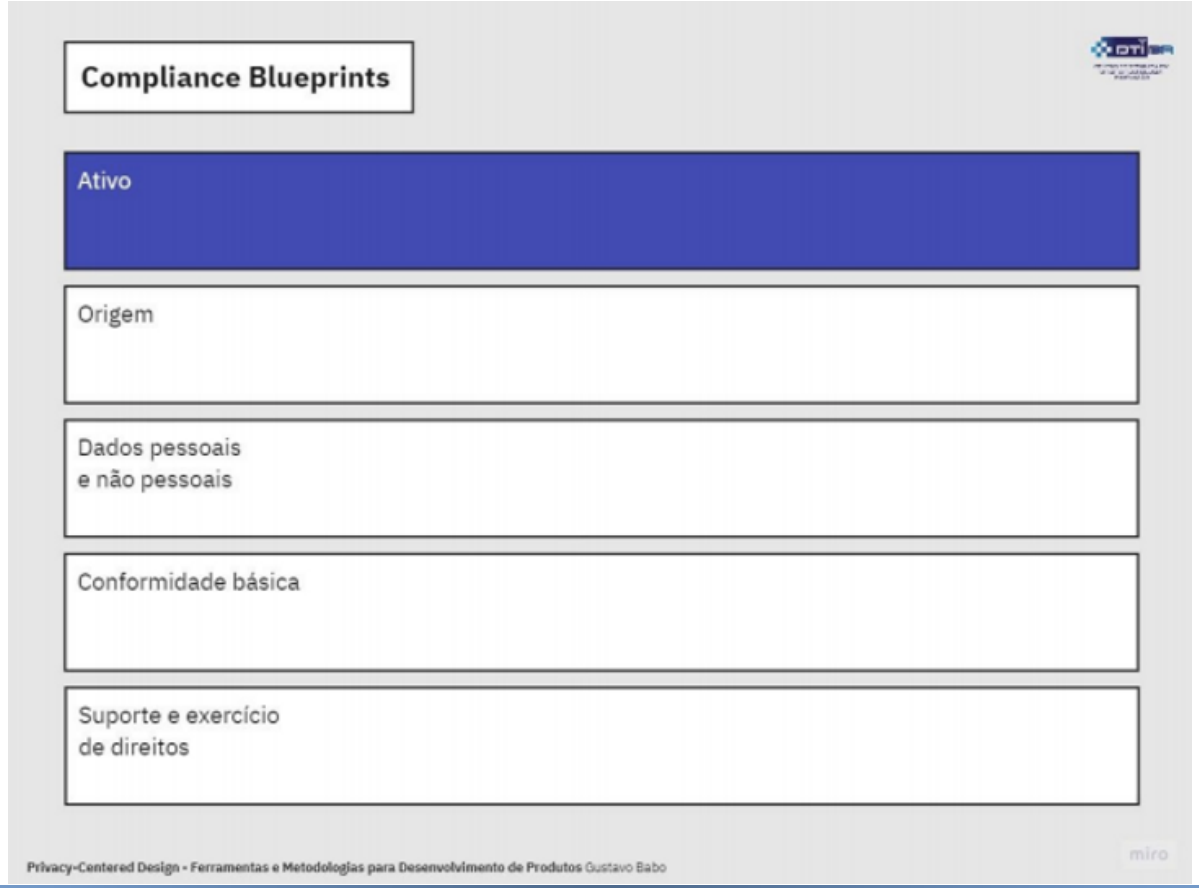
FONTE:
Centro DTI BR

Ferramentas e Metodologias



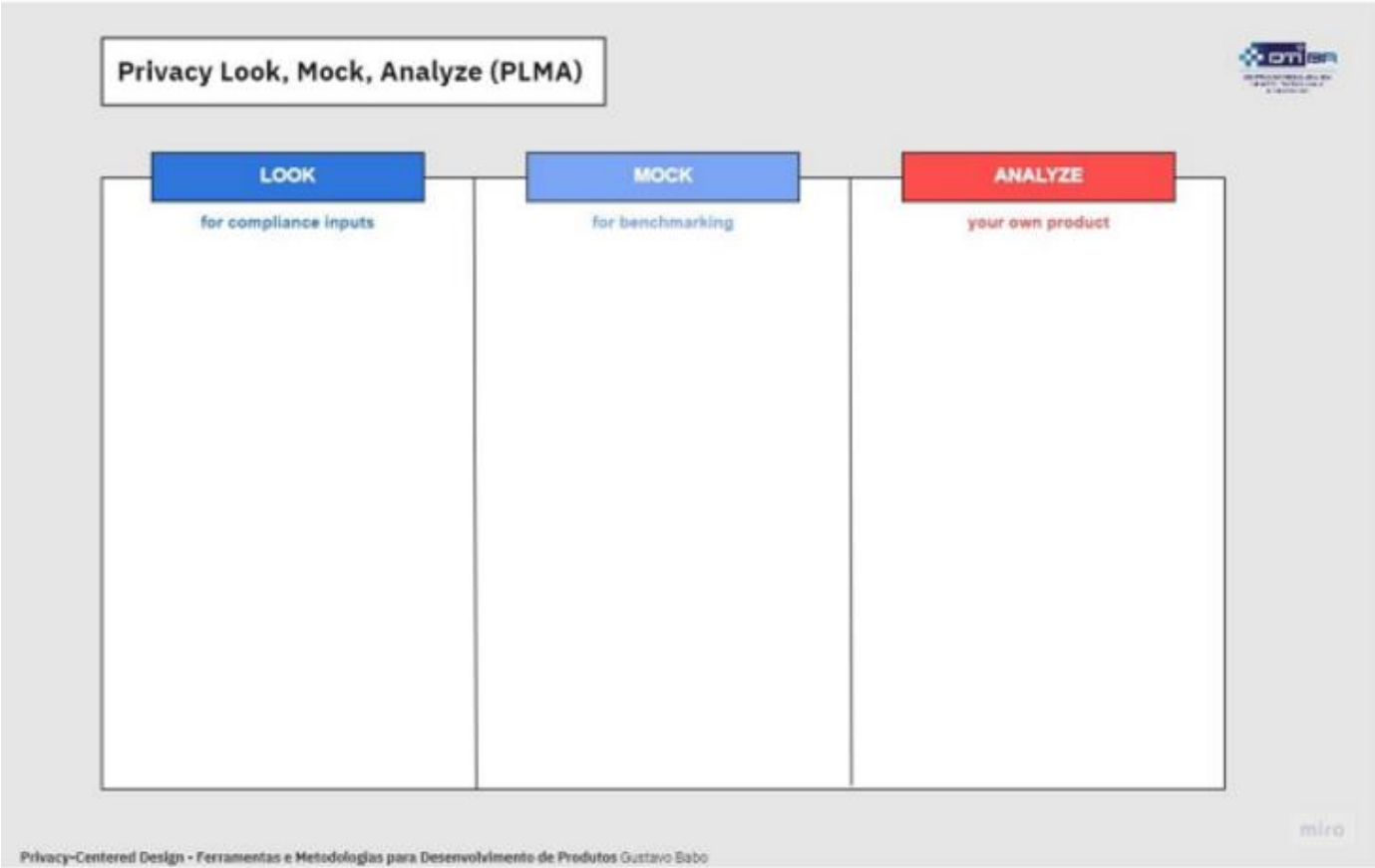
FONTE:
Centro DTI BR

Ferramentas e Metodologias



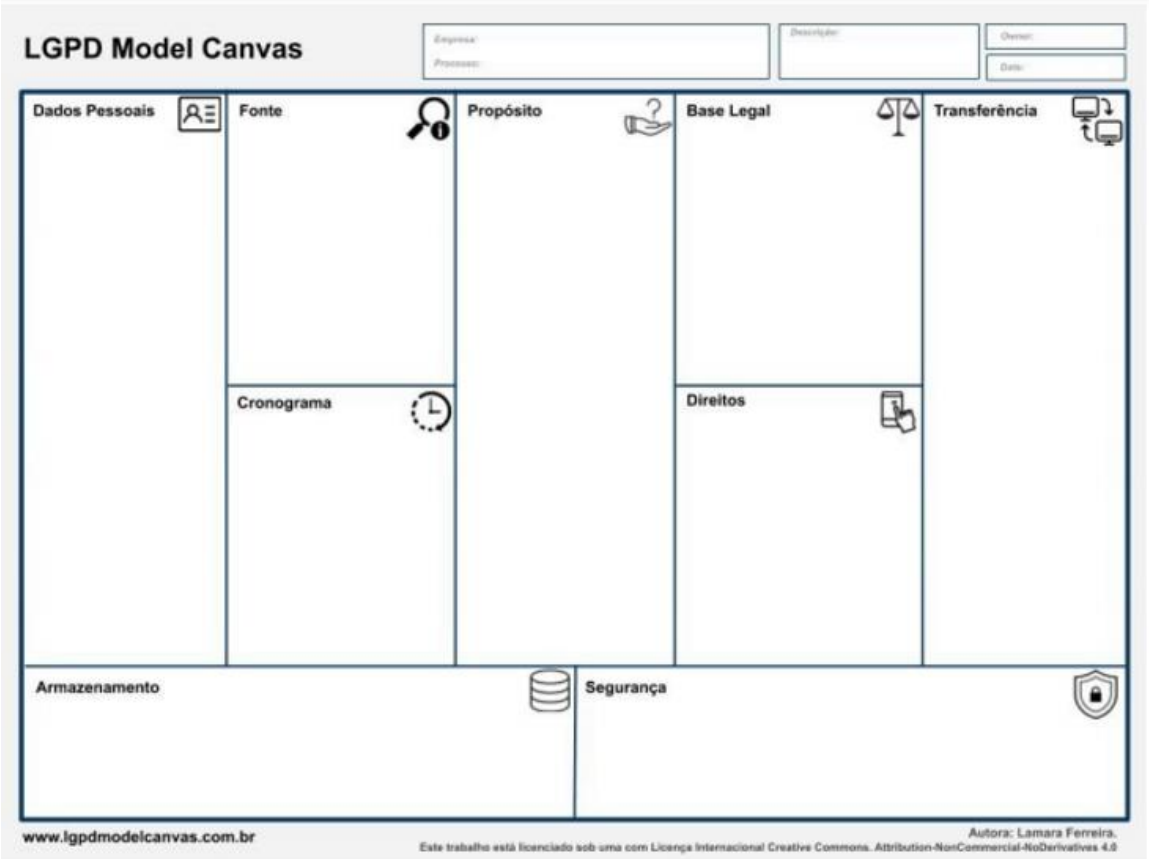
FONTE:
Centro DTI BR

Ferramentas e Metodologias



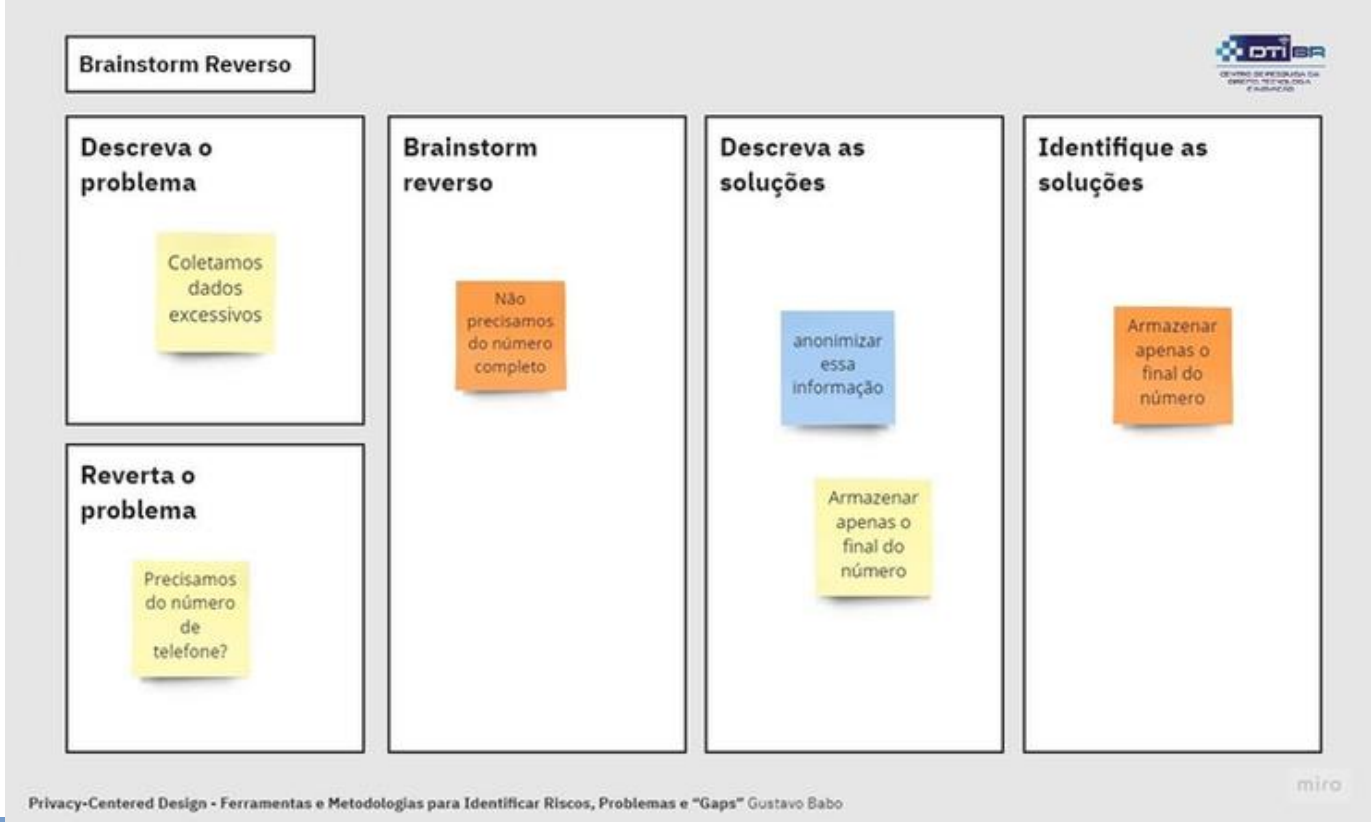
FONTE:
Centro DTI BR

Ferramentas e Metodologias



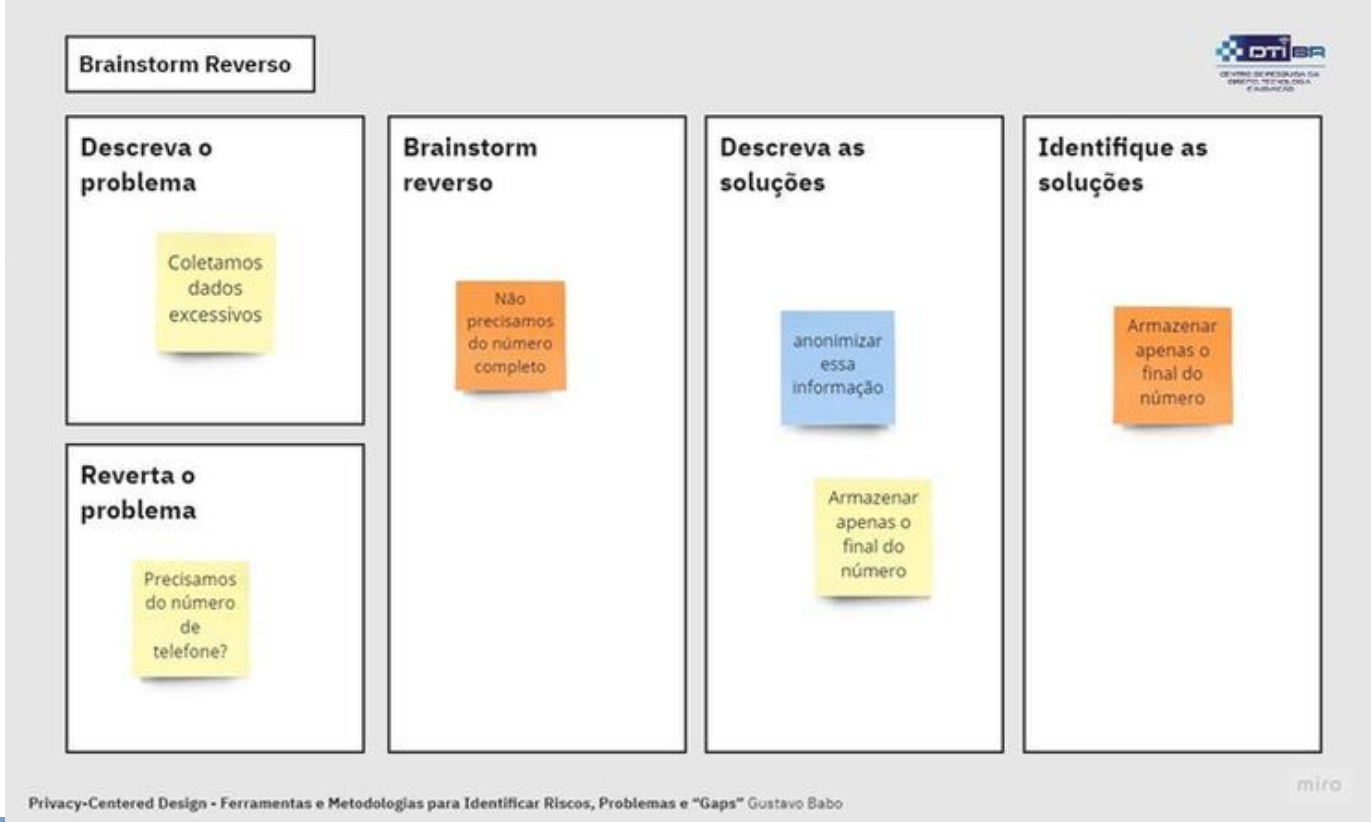
Criado por:
Lamara Ferreira
FONTE:
Centro DTI BR

Ferramentas e Metodologias para Dinâmicas e Insights



FONTE:
Centro DTI BR

Ferramentas e Metodologias para Dinâmicas e Insights



FONTE:
Centro DTI BR

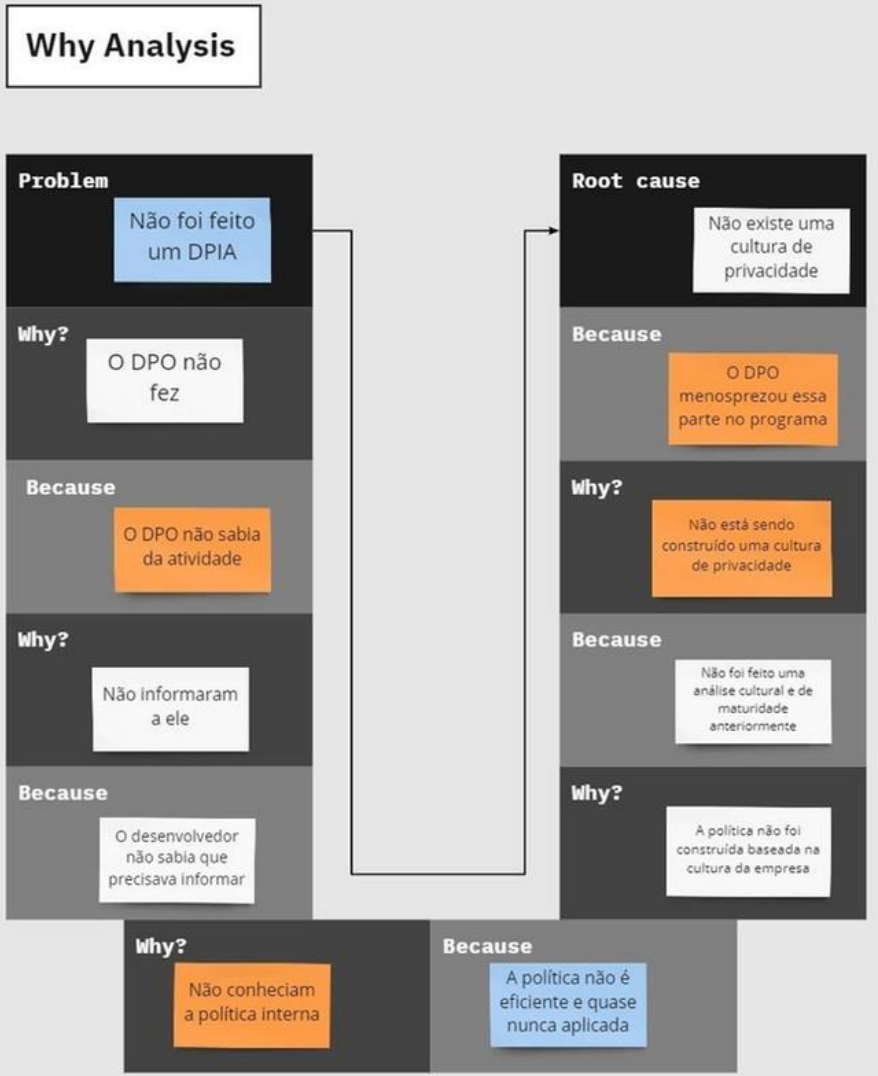
Ferramentas e Metodologias para Dinâmicas e Insights

FONTE:
Centro DTI BR

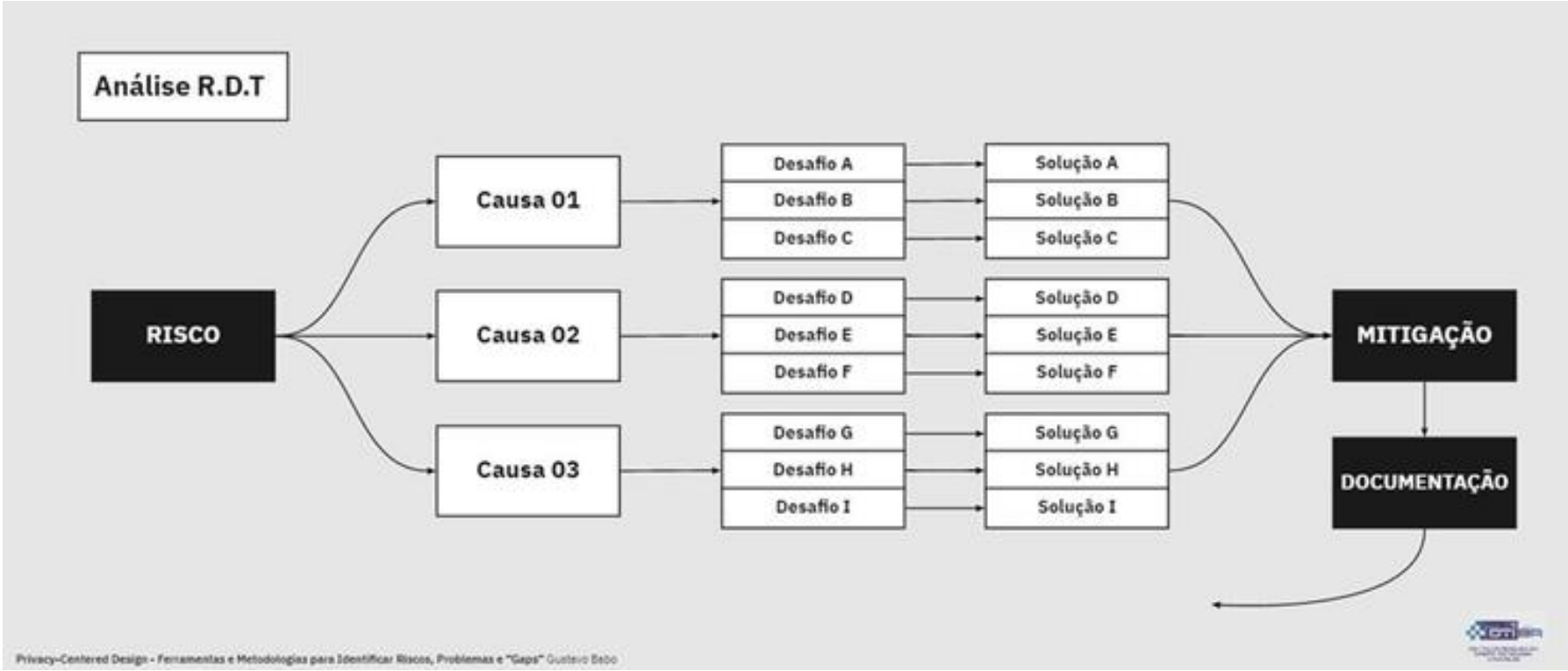
FONTE:
Centro DTI BR

Ferramentas e Metodologias para Dinâmicas e Insights

FONTE:
Centro DTI BR



Ferramentas e Metodologias para Dinâmicas e Insights



FONTE:
Centro DTI BR

Desafios e Oportunidades decorrentes da LGPD

Importante: construir soluções seguras e robustas

- Sem segurança não há proteção de dados – Engenharia de Segurança
- PbD: foco na prevenção desde a concepção
- Pouca formação sobre o tema nos cursos e nas empresas
- Solarwinds, eSUS, Equifax, Starbucks: comprometimento de credenciais (Github)
- (CERT.br) Mais de **80% dos incidentes** seriam evitados se
  - todas as correções (patches) fossem aplicadas
  - todos os serviços tivessem 2FA / MFA
  - houvesse mais atenção a erros e configurações

Reconhecimento facial

- Finalidade: é que determina se tais capturas são lícitas ou não. Metrô de SP – fins publicitário. Segurança pública. **Identificação X Autenticação**
- **Falhas** nos softwares e demais tecnologias utilizadas
- Consentimento como base legal – traz dificuldades para gestão
- Diretrizes do conselho europeu - proibição de reconhecimento facial de emoções e de reconhecimento facial que tenha como único propósito determinar a cor de pele, religião/crença, sexo, raça, origem étnica, idade, condições de saúde ou status social de uma pessoa.
- **Carta aberta** pedindo a proibição global de tecnologias de reconhecimento biométrico que permitem vigilância em massa e discriminatória
  - *Access Now, Anistia Internacional, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF) e o Instituto Brasileiro de Defesa do Consumidor (IDEC)*

Como a Inteligência Artificial impacta a proteção de dados pessoais no cenário atual?

- **Inteligência artificial**
  - **40% das tecnologias de compliance** em proteção de dados dependerão de IA para serem devidamente implementadas.
  - Desafio das regulamentações de uso de dados.
  - **Proposta de Regulamento de IA da União Europeia** (abril 2021): regular a IA a partir de uma abordagem baseada no risco (reconhecimento fácil)
  - Parecer conjunto das Autoridades de Proteção de Dados da União Europeia (EDPB e EDPS) sobre o regulamento
    - identificação biométrica remota de indivíduos em espaços acessíveis ao público, as autoridades apelam a uma proibição geral de qualquer utilização de IA para o reconhecimento automatizado de características humanas (RF) em espaços acessíveis ao público, **em qualquer contexto**.

Blockchain é incompatível com a LGPD?

- *É possível usar blockchain sem prejuízo à segurança de dados* (juíza Renata Baião)
  - imutabilidade não é obstáculo direto ao atendimento às exigências dos regramentos
- IDD – identidade descentralizada
  - informações referentes à identidade na blockchain - dados podem ser anonimizados (criptografia assimétrica) – centrada no titular
  - titular dos dados não quiser mais utilizá-los – inutilizar a chave privada

Obrigada. Perguntas?

Profa. Dra. Michelle S. Wangham

Mestrado em Computação Aplicada (UNIVALI)

Assessora de PD&I na RNP

wangham@univali.br

Materiais

- https://www.udemy.com/course/lgpd-executivo-conhecimentos-aceleradores-de-conformidade/
- https://www.lgpdacademicooficial.com.br/
- https://miro.com/miroverse/user-journey/
- https://dataprivacy.com.br/publicacoes/
- https://www.dataprivacybr.org/
- https://blog.idwall.co/privacy-by-design-implementar-processos-tecnologia/
- https://www.dtibr.com/post/privacy-centered-design-ferramentas-e-metodologias-para-desenvolvimento-de-produtos
- https://mooc.campusvirtual.fiocruz.br/rea/ciencia-aberta/serie2/curso2/introducao.html
- https://privacidade.rnp.br