

Workshop LGPD

Inventário e classificação de Dados
Pessoais

Agenda

- O uso de dados e dados pessoais
- Onde os dados pessoais são abrigados e como classificá-los
- Como utilizar o LGPD Governance (PCP) para inventariar e classificar dados pessoais





Adilson Taub Junior

CIO/CTO
DPO certified

20+ years of experience, helping
companies solve problems with the
right tools

Contatos



/in/ataubjr/



adilsontj@rgm.com.br

Acadêmico



**Master of Business
Administration (MBA)**
Gestão Estratégica de Negócios

Formação Executiva
Compliance Empresarial (FGV)

Pós-graduação
Engenharia de Software

Graduação
Processamento de Dados

Certificações



Privacy & Security Management

Data Protection Officer (DPO)
Privacy and Data Protection Practitioner
Privacy and Data Protection Foundation
Information Security (ISO/IEC 27.001)



IT Governance and Service Management

IT Service Management (ISO/IEC 20.000)
ITIL V3 Fdn. Certified
COBIT 4.1 Fdn. Certified
ITIL V2 Fdn. Certified



Software Engineering

Professional Scrum Product Owner (PSPO I)
Professional Scrum Master (PSM I)
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF
IBM Certified Solution Designer (RUP)
Certified Expert in BPM

Mapa de habilidades



Comunicação e Oratória	
Gestão e Governança de TI	
Engenharia de Software (ALM)	
BPM	
Metodologias Ágeis	
Gestão de Projetos	
Compliance	
LGPD/GDPR	
Setor Público	

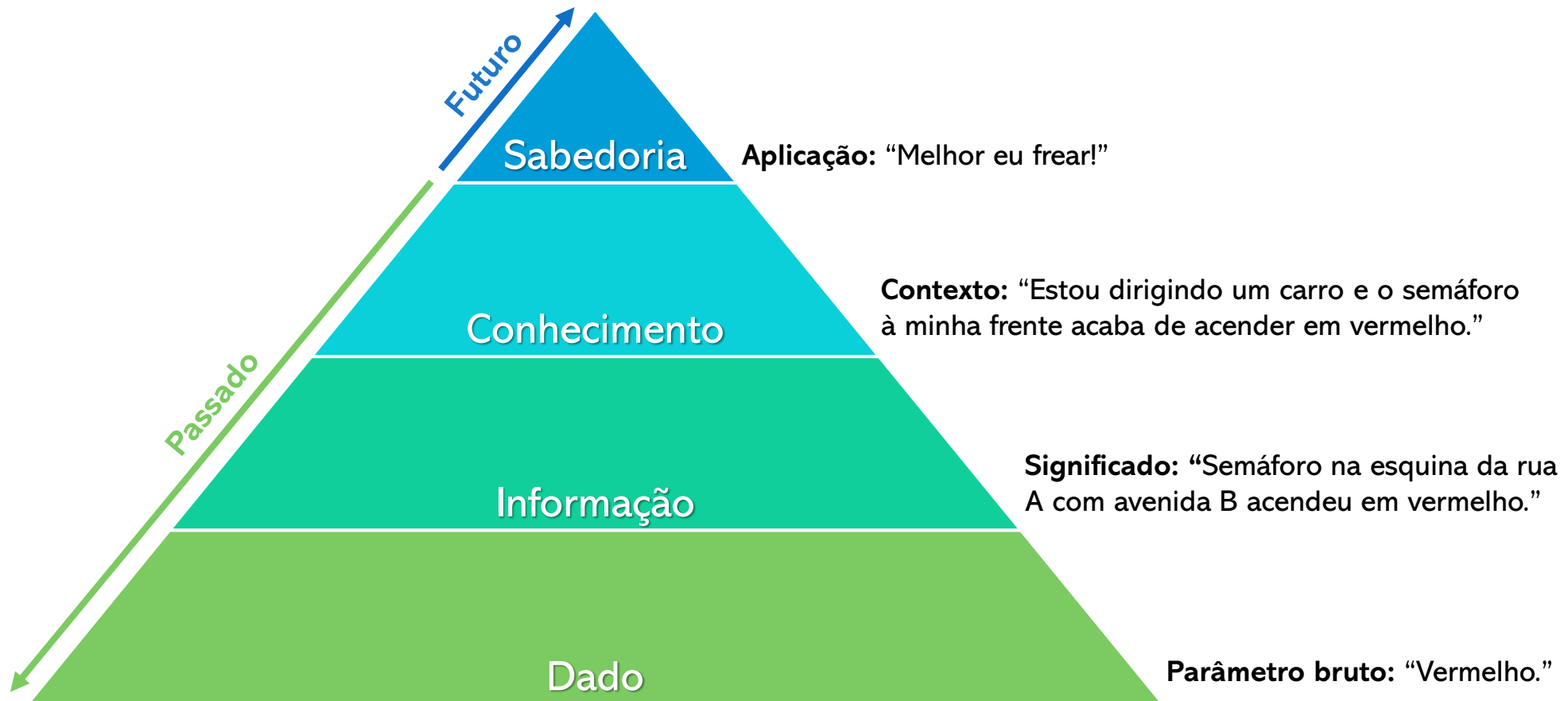
O uso de dados e dados pessoais

Volume de dados pessoais

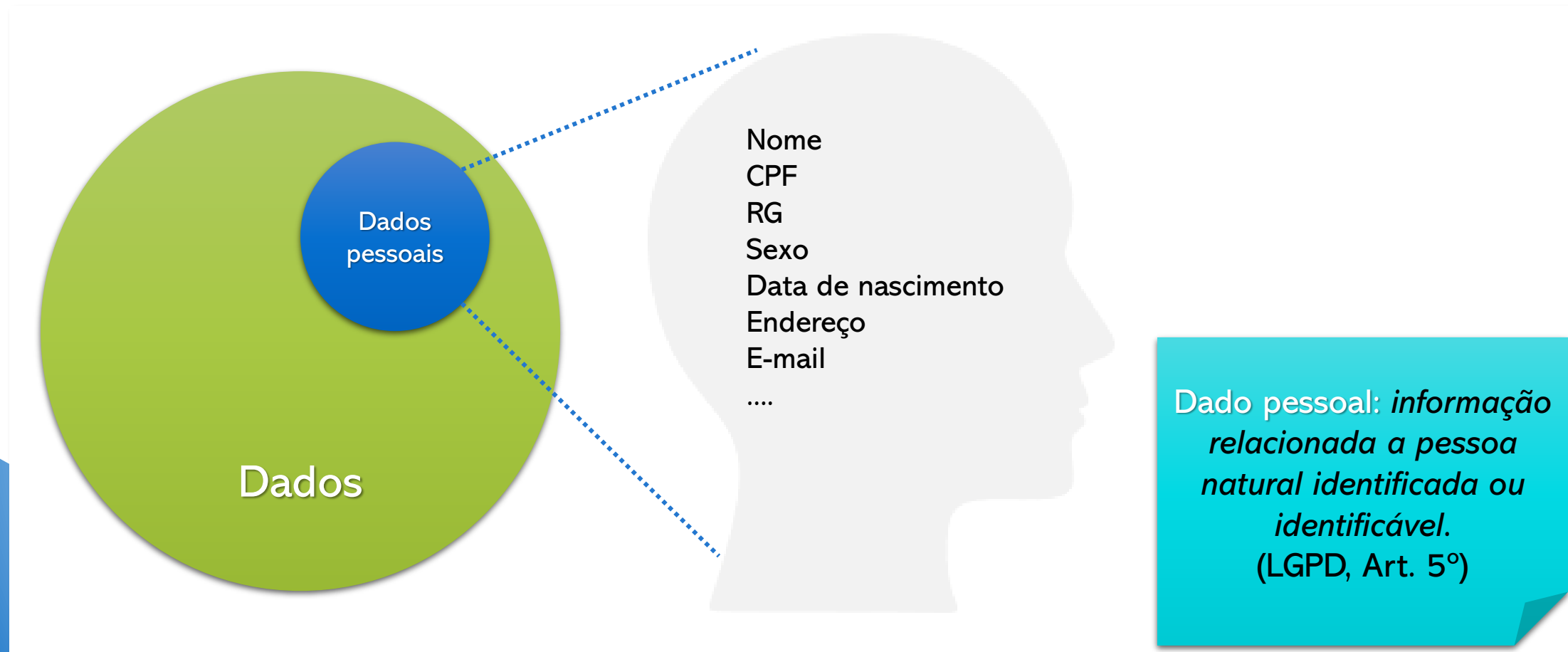


Fonte: Data Never Sleeps 9.0
(<https://www.domo.com/learn/infographic/data-never-sleeps-9>)

Gestão do conhecimento



Dados pessoais

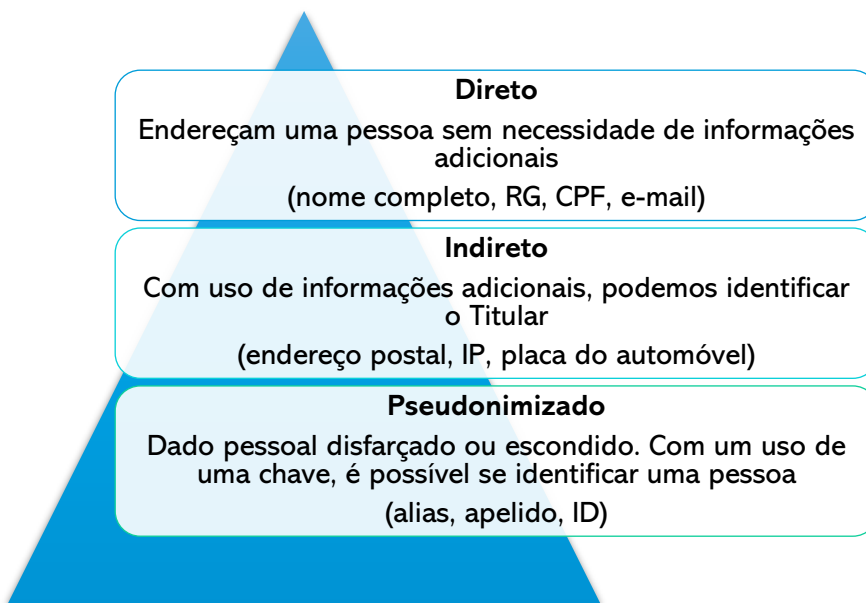


O que são dados pessoais

- **Art. 5º** Para os fins desta Lei, considera-se:

I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;

II - **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;



Dados anonimizados não fazem parte do escopo da LGPD, por não ser possível identificar o Titular (não há chave para reverter a anonimização)

Privacidade

“São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”

(Constituição Federal, Art. 5º, inciso X)

“é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

(Constituição Federal, Art. 5º, inciso LXXIX – EC 115/22)

Onde os dados pessoais são abrigados e como classificá-los

Objetivo da LGPD

- **Art. 1º** Esta Lei 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.

(Lei nº 13.709/18)

- Promulgada em 14 de agosto de 2018
- Em vigor desde 18 de setembro de 2020
- Sanções começaram a ser aplicadas em 01 de agosto de 2021

Escopo da LGPD



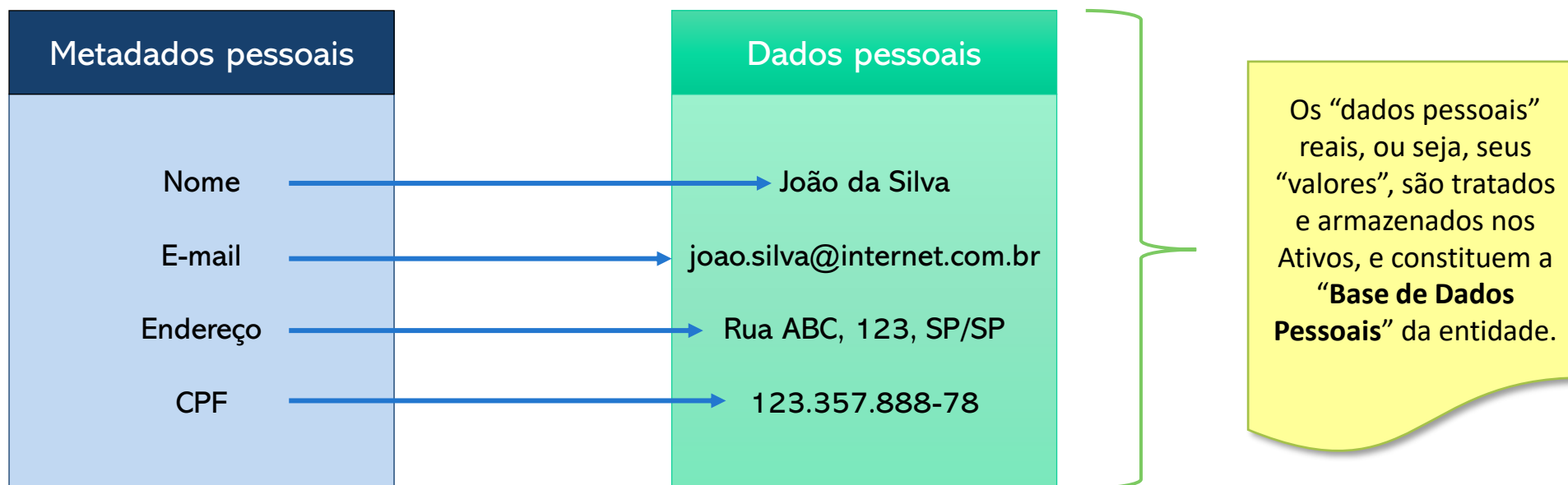
É necessário **justificar** todos os tratamentos de Dados Pessoais que você realiza e encontrar **bases legais** que sustentem as rotinas de coleta, processamento, armazenamento e distribuição desses dados

Deverá se implementar medidas administrativas e técnicas de **segurança da informação**, para garantir a **Confidencialidade, Integridade e Disponibilidade** dos Dados Pessoais que você usa

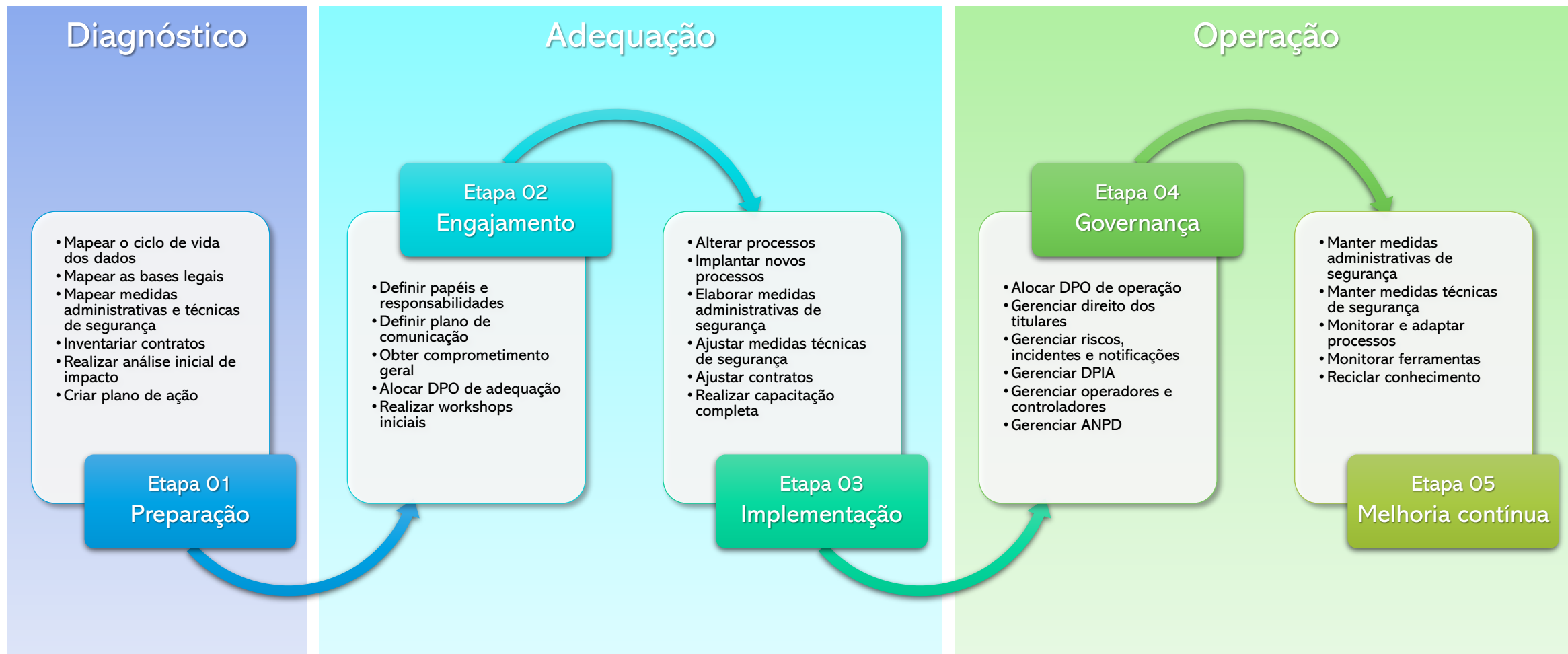
Por fim, é preciso implantar **novos procedimentos** operacionais obrigatórios segundo a LGPD e **modificar suas rotinas** atuais visando atender a todos os novos parâmetros legais em vigor, incluindo gerenciar os **Direitos dos Titulares**

Dados e metadados pessoais

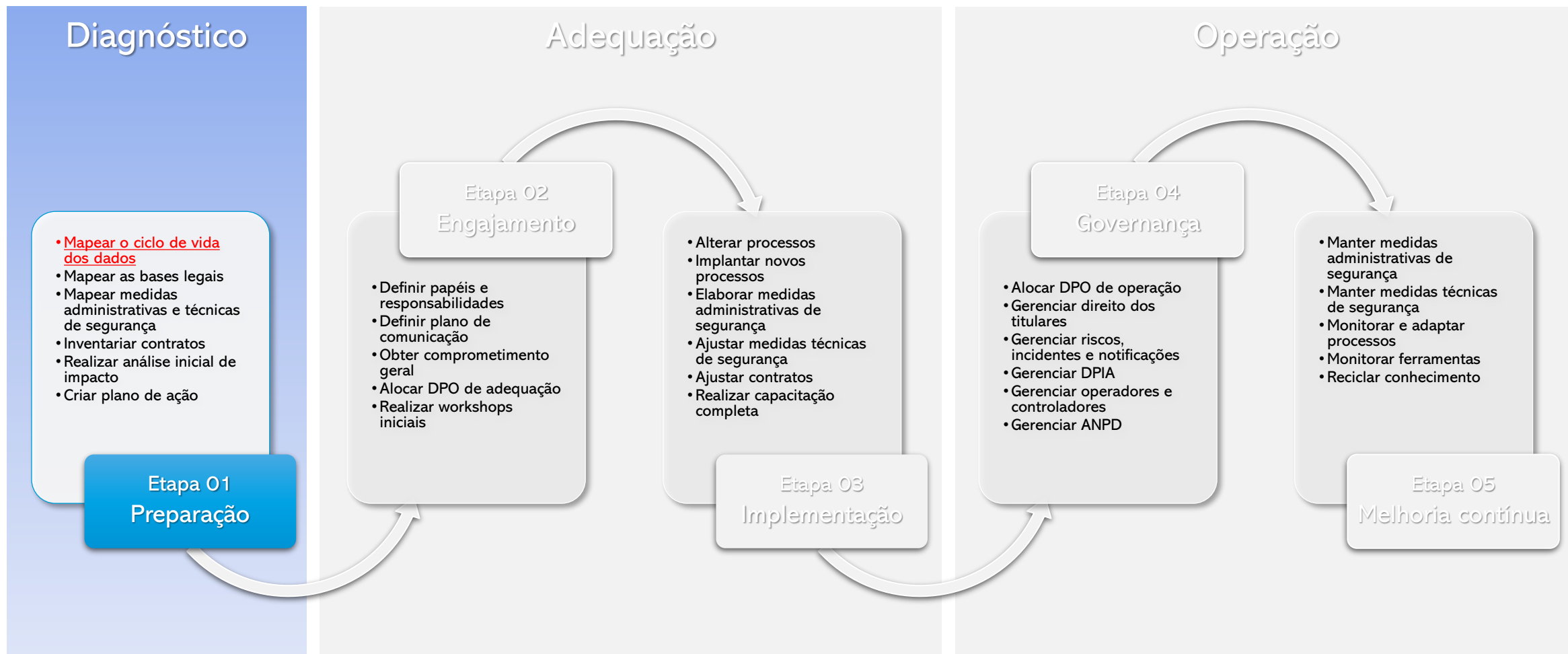
- Em um projeto de adequação à LGPD, inicialmente, o foco são os **metadados pessoais** e não o **valor** desses dados.



Como implementar um SGPD



Como implementar um SGPD



Diagnóstico

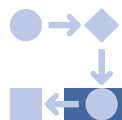
1. Preparação

- **Principal objetivo da etapa:**
 - Elaborar o *Plano de Ação* com atividades claras e objetivas que deverão ser executadas posteriormente para garantir a adequação do controlador à LGPD.
- **Perguntas que devemos responder nessa etapa:**
 - Quais Dados Pessoais utilizamos e como eles trafegam por nossas rotinas?
 - Por que utilizamos esses Dados Pessoais e como justificamos isso?
 - Utilizamos apenas os Dados Pessoais minimamente necessários para cumprir nossos objetivos?
 - Quais são os compromissos que nossa empresa assume em relação à privacidade e segurança de dados?
 - Quais os níveis de Confidencialidade, Integridade e Disponibilidade dos nossos Ativos de Informação?
 - Como está nosso website corporativos em relação à LGPD?
 - Temos um DPO?
 - Sob quais riscos de privacidade estamos atuando hoje? Como tratá-los?
 - O que temos que fazer para cobrirmos as lacunas em relação à LGPD?

Etapa de Preparação

Passo 1.1 Encontrar os Dados Pessoais

Mapear os processos de negócio



- Usar modelagem BPMN
- Identificar atores
- Determinar objetivo e responsável de cada processo

Inventariar seus Ativos



- Classificar o tipo (físico ou eletrônico)
- Detalhar quem mantém o Ativo
- Associar aos processos de negócio
- *Envolvimento do time de TI*

Inventariar seus Artefatos e Dados



- Artefatos são documentos (físicos ou eletrônicos) que circulam pelos Ativos (devem ser associados)
- Dados pessoais estão dentro de Artefatos e podem ser reutilizados em vários artefatos

Classificar seus Dados Pessoais



- A LGPD classifica os dados pessoais em “normais” ou “sensíveis”
- O Decreto Federal 10.046 estende essa classificação e pode ser utilizado em conjunto

Etapa de Preparação

Passo 1.2 Justificar os Tratamentos de Dados Pessoais



Elencar cada tratamento de dado

- Um processo pode ter “n” tratamentos em execução
- Identificar os detalhes sobre o ciclo de vida dos dados para cada tratamento
- Identificar parâmetros adicionais (como o uso de operadores, dados de crianças, compartilhamento e rotinas automatizadas)



Classificar as hipóteses

- Utilizar os incisos definidos no Art. 7º para dados normais
- Utilizar os incisos definidos no Art. 11º para dados sensíveis
- *Envolvimento do time jurídico*



Associar fundamentos legais

- Algumas hipóteses de tratamento podem exigir a indicação de fundamentos legais adicionais para justificar cada tratamento de dados
- *Envolvimento do time jurídico*

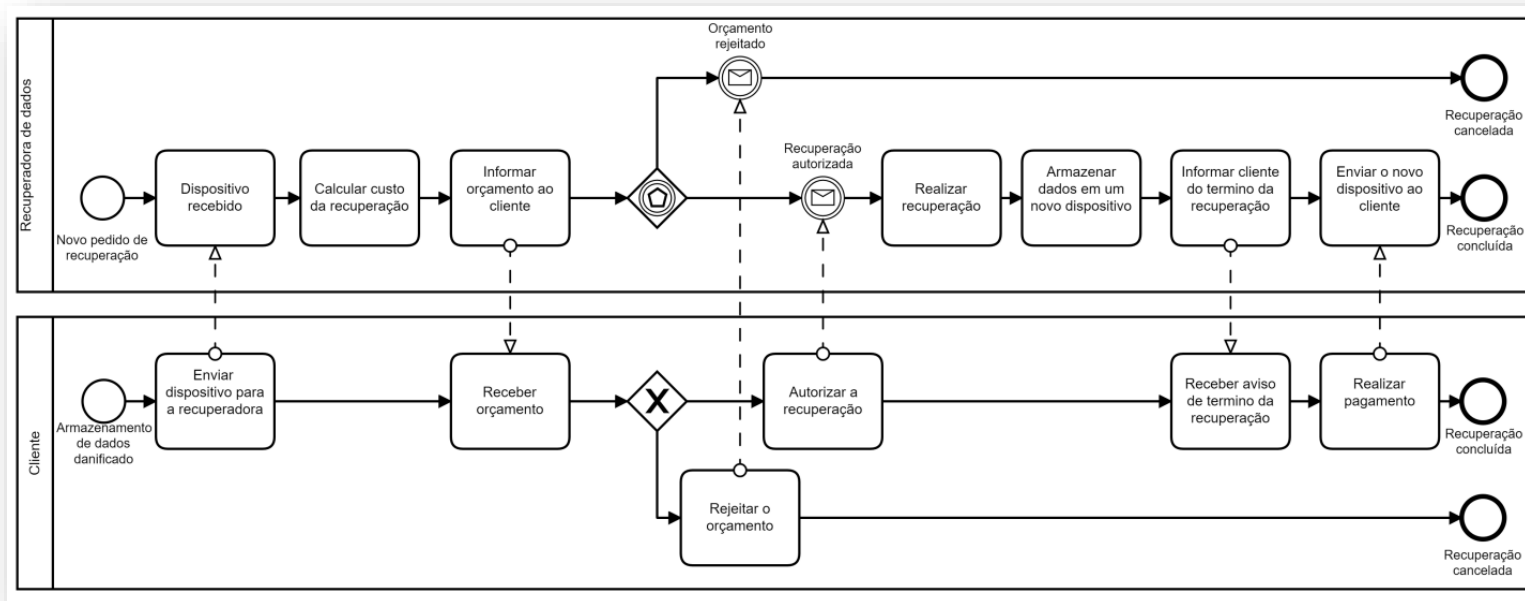


Analisar o princípio da Necessidade

- Para cada tratamento inventariado, é necessário indicar quais artefatos são utilizados e, dentro desses artefatos, quais dados pessoais são **REALMENTE** necessários para cumprir a finalidade do tratamento de dados
- *Envolvimento do time jurídico*

Modelagem de processos de negócio

- Atualmente a notação mais completa para mapeamento de processos de negócio é a **Business Process Model and Notation (BPMN) 2.0**.



Ativos de informação

- A transferência e o processamento de informações ocorrem em **Ativos de Informação**, os quais não precisam necessariamente serem automatizados ou eletrônicos.
- É através de um **Ativo de Informação** que se realiza o tratamento de dados pessoais, ou seja, é onde ocorre o **Ciclo de Vida de um Dado Pessoal**.
- Exemplos de Ativos de Informação:
 - Servidor de Arquivos
 - Sistema de Planejamento Orçamentário
 - CRM
 - ERP
 - Ouvidoria
 - Estação de Trabalho
 - WhatsApp
 - Arquivo morto
 - Sistema de catraca
 - Lista de convidados



Artefatos

- Os Dados Pessoais são processados pelos **Ativos de Informação** dentro de documentos (físicos ou eletrônicos) identificados como **Artefatos**.
- Um determinado Artefato, geralmente, pode abrigar um ou mais **Dado Pessoal**.
- Exemplos de Artefatos:
 - Curriculum Vitae
 - Pedido de Compra
 - Ata de reunião
 - Crachá de colaborador
 - Vídeo de vigilância
 - Formulário de matrícula
 - Prontuário médico

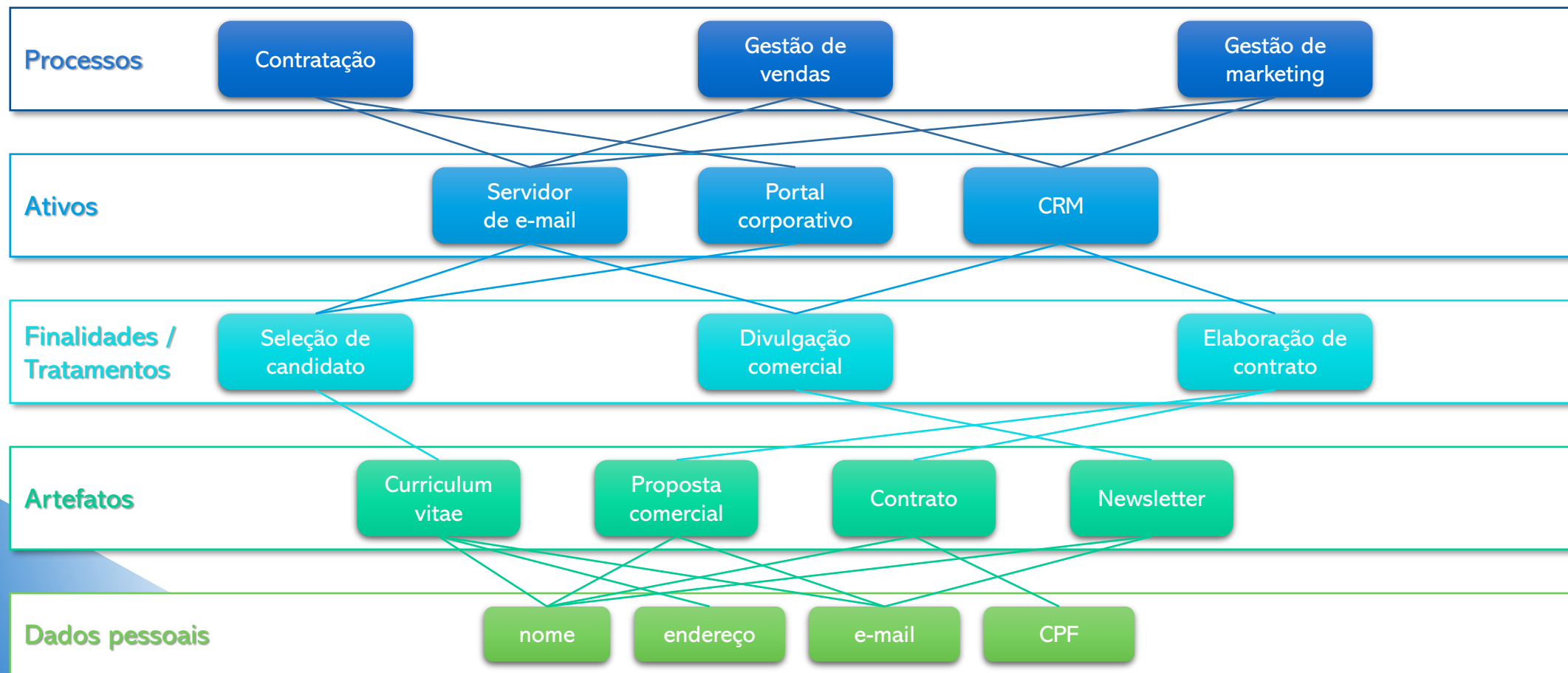
Dados pessoais

- Dentro de um determinado **Artefato** estão dispostos os **Dados Pessoais**, que identificam, direta ou indiretamente uma Pessoa Física (Titular de Dados).
- Um **Dado Pessoal** deve ser classificado, buscando entender seu tipo e, muitas vezes, quais controles devem ser implementados sobre esse Dado Pessoal para garantir sua segurança.
 - A LGPD classifica **Dados Pessoais** em apenas 2 (dois) tipos – Dado Pessoal e Dado Pessoal Sensível
 - O Art. 2º do Decreto Federal 10.046/19 expande a classificação de **Dados Pessoais**:
 - Dados biográfico (normal e sensível)
 - Dados cadastrais
 - Dados biométricos (sensível)
 - Dados genéticos (sensível)

Classificação de dados pessoais

- O framework utilizado no projeto atende tanto a LGPD como o Decreto Federal 10.046/19, estabelecendo os seguintes grupos de classificação de dados pessoais:
 - **Biográfico:** Descrevem fatos particulares da vida do Titular como seu nome, sexo, data de nascimento, endereço físico ou eletrônico, profissão;
 - **Cadastral:** Apontam informações que relacionam o Titular a algum cadastro como matrícula, CPF, RG, título de eleitor;
 - **Biográfico sensível:** São dados biográficos ou cadastrais sensíveis como raça, cor, opção sexual, associação a sindicatos ou partidos políticos, gênero;
 - **Biométrico sensível:** São dados que identificam, biometricamente, uma pessoa física como sua voz, foto, íris e impressão digital. Vale ressaltar que as boas práticas definem que fotos, voz e imagem devem ser considerados sensíveis apenas se forem processados em rotinas automatizadas, caso contrário, devem ser considerados dados pessoais biográficos não-sensíveis;
 - **Genético sensível:** Informações relativas às características hereditárias dos indivíduos, obtidas pela análise de ácidos nucleicos ou por outras análises científicas, como por exemplo a sequência de DNA de uma pessoa, perfil genético e associação parental genética, informações sobre testes genéticos e predisposições a doenças, amostras biológicas como saliva e cabelo;
 - **Dado sensível de saúde:** Dados de saúde que não sejam genéticos como tipo sanguíneo, resultados de exames laboratoriais não genéticos, dados de PCD, doenças que um Titular de dados tem ou já teve, pressão arterial etc.

Hierarquia da informação pessoal



Exemplo de inventário de dados pessoais (1/2)

- **Processo de Negócio:** Admissão de Colaborador
- **Objetivo do processo:** Realizar a contratação de um novo colaborador para o quadro da entidade, disponibilizando mais força de trabalho a um determinado time de trabalho
- **Ativos de Informação envolvidos:** e-mail, ERP, WhatsApp
- **Artefatos envolvidos:** Curriculum, e-mail de agendamento de entrevista, contrato de prestação de serviços, crachá, carteirinha de plano de saúde
- **Dados pessoais envolvidos:** Nome, data de nascimento, endereço de e-mail, endereço residencial, telefone, dados bancários, tipo sanguíneo, histórico médico

Exemplo de inventário de dados pessoais (2/2)

Finalidade #01

Seleção de candidato

- **Ativo utilizado:** e-mail
- **Artefato utilizado:** Curriculum
- **Dados pessoais tratados:** Nome, data de nascimento, telefone, e-mail, endereço residencial
- **Hipótese de tratamento:** Legítimo interesse do Controlador (Art. 7º, inciso IX)
- **Tempo de armazenamento:** 12 meses
- **Compartilha dados com terceiros:** Não
- **Usa operador:** Não
- **Trata dados de crianças ou adolescentes:** Não

Finalidade #02

Contratação

- **Ativo utilizado:** Folha de Pagamento, eSocial, ERP
- **Artefato utilizado:** Contrato de Trabalho
- **Dados pessoais tratados:** Nome, data de nascimento, telefone, e-mail, endereço residencial, dados bancários, CPF, PIS
- **Hipótese de tratamento:** Execução de Contratos (Art. 7º, inciso V)
- **Tempo de armazenamento:** 5 anos após demissão
- **Compartilha dados com terceiros:** SIM: Receita Federal, via eSocial
- **Usa operador:** SIM: Terceirizado da Contabilidade
- **Trata dados de crianças ou adolescentes:** Não

Finalidade #03

Convite para festas

- **Ativo utilizado:** e-mail, Whatsapp
- **Artefato utilizado:** Convite
- **Dados pessoais tratados:** Nome, telefone, e-mail
- **Hipótese de tratamento:** Consentimento do Titular (Art. 7º, inciso I)
- **Tempo de armazenamento:** N/A
- **Compartilha dados com terceiros:** Não
- **Usa operador:** Não
- **Processo de consentimento:** XPTO
- **Trata dados de crianças ou adolescentes:** Não

Demonstração prática

Obrigado!

Adilson Taub Jr.

<https://www.linkedin.com/in/ataubjr/>

RGM Tecnologia

www.rgm.com.br

SCAN ME

