RGM
TECNOLOGIA

Workshop LGPD

O que é a LGPD e como ela se aplica à gestão Pública

Apresentação

- **Objetivos do workshop**
  - Apresentar os principais aspectos da Lei Geral de Proteção de Dados, destacando sua aplicação à Gestão Pública;
  - Demonstrar a lógica e os principais temas associados à implementação de um Sistema de Gestão de Proteção de Dados (SGPD);

RGM TECNOLOGIA

Agenda

- **Trilha 01 – O que é a LGPD e como ela se aplica à Gestão Pública**
  - Privacidade e dados
  - Gestão do conhecimento
  - As principais características da LGPD
  - Os papéis previstos na LGPD
  - A LGPD aplicada à gestão pública
- **Trilha 02 – Implementando um SGPD**
  - Escopo de adequação à LGPD
  - O que é um SGPD
  - Gestão do tratamento de dados pessoais
    - Processos de negócio
    - Ativos de informação, artefatos e dados pessoais
    - Finalidades e hipóteses de tratamento de dados pessoais
    - Segurança da informação (e a ISO/IEC 27.001)
    - Medidas administrativas de segurança
    - Medidas técnicas de segurança
  - Gestão de riscos
  - Relatório de análise de impacto de proteção de dados (DPIA)
  - Gestão de incidentes e notificações
  - Gestão de direitos dos titulares de dados
  - Gestão de consentimentos

RGM TECNOLOGIA

Adilson Taub Junior

CIO/CTO
DPO certified

19+ 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

Pós-graduação
Engenharia de Software

Graduação
Processamento de Dados

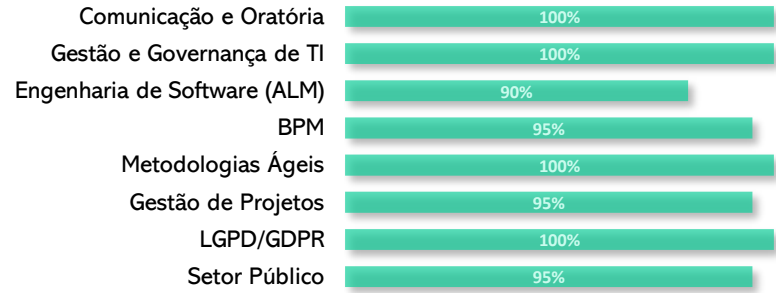
Certificações

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



Trilha 01

O que é a LGPD?

E como ela é aplicada à Gestão Pública

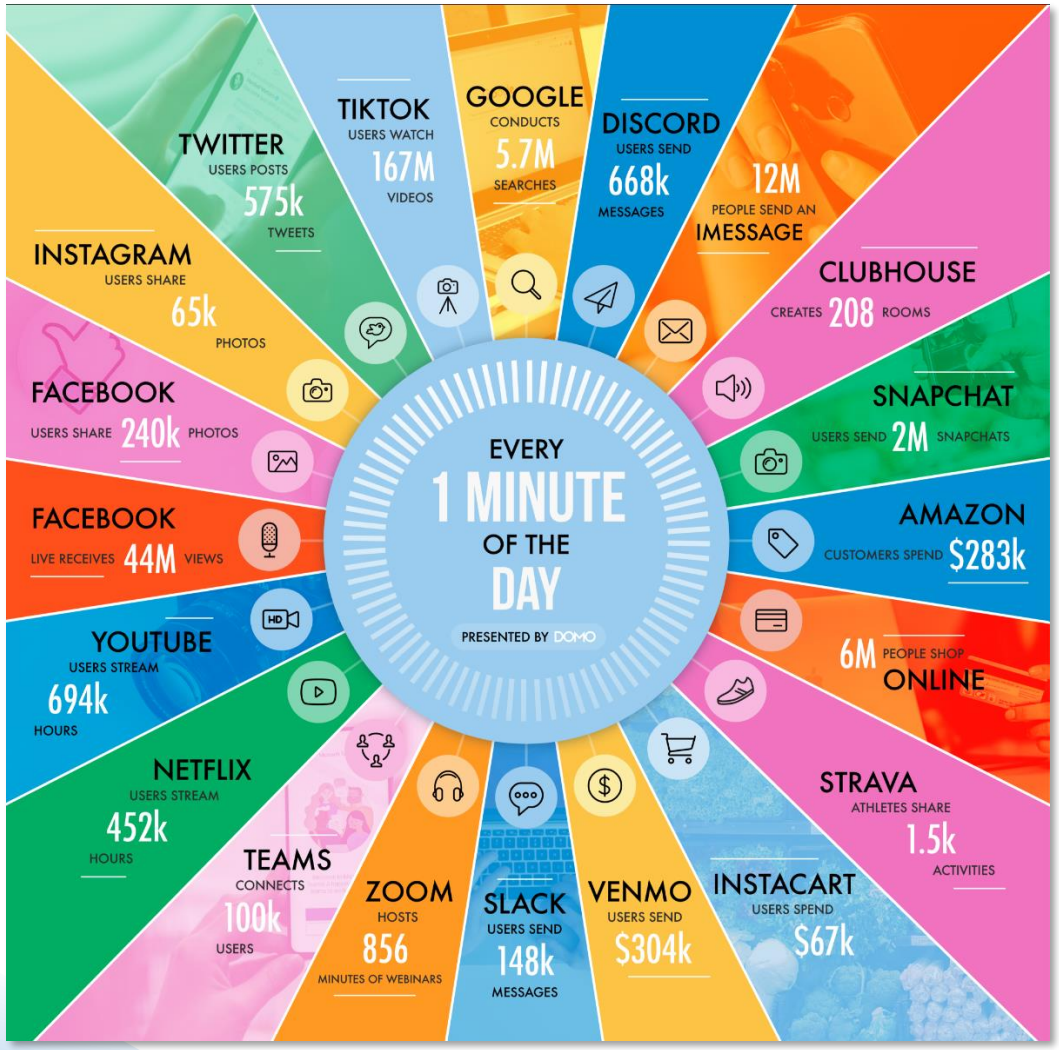
RGM TECNOLOGIA

Agenda da trilha

I. Privacidade e dados
II. Gestão do conhecimento
III. As principais características da LGPD
IV. Os papéis previstos na LGPD
V. A LGPD aplicada à gestão pública

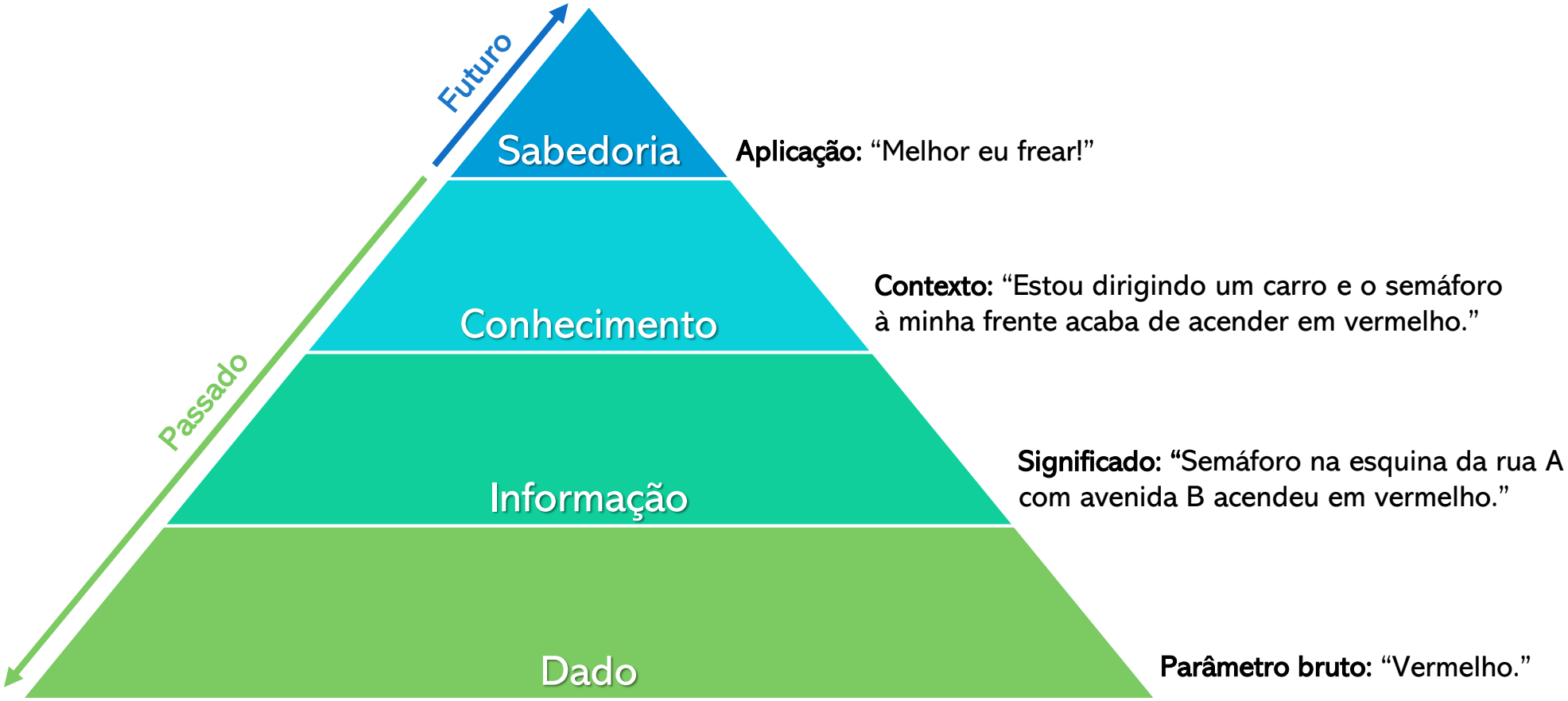
RGM TECNOLOGIA

Volume de dados pessoais

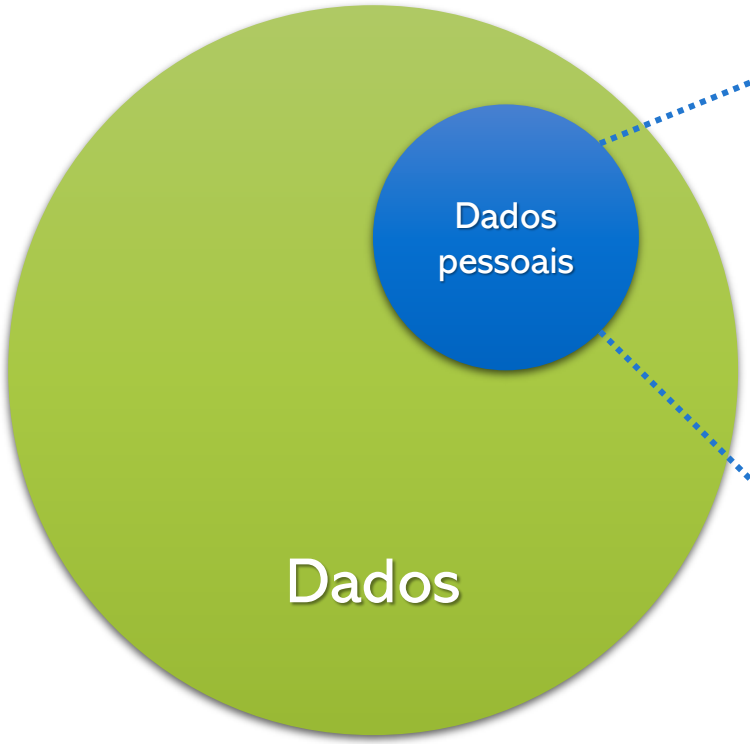


Fonte: Data Never Sleeps 9.0
(https://www.domo.com/learn/infographic/data-never-sleeps-9)

Gestão do conhecimento



Dados pessoais



Nome
CPF
RG
Sexo
Data de nascimento
Endereço
E-mail
....

Dado pessoal: *informação relacionada a pessoa natural identificada ou identificável.*
(LGPD, Art. 5º)

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. 5°, inciso X)

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

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

RGM TECNOLOGIA

A Lei Geral de Proteção de Dados

Histórico da LGPD

- Constituição Federal (Art. 5º)
- Lei de Acesso à Informação (Lei nº 12.527/2011)
- Lei de Crimes Cibernéticos (Lei Carolina Dieckmann - Lei nº 12.737/2012)
- Marco Civil da Internet (Lei nº 12.965/2014)
- *General Data Protection Regulation* - GDPR (União Europeia - 2016)
- *California Consumer Privacy Act of 2018* – CCPA (Estados Unidos - 2018)
- Lei da Desburocratização (Lei n.º 13.726/2018)
- Resolução 4658 BACEN (2018)

RGM TECNOLOGIA

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

RGM TECNOLOGIA

FOLHA DE S.PAULO

Justiça já tem 600 decisões envolvendo lei de proteção de dados

Pedidos vão de exclusão de nomes na internet a remoção de informações no RH após demissão

Na Senacon, foram abertas 12 averiguações envolvendo proteção de dados desde setembro. Só no último mês, o órgão autuou quatro bancos, e a lista tende a crescer. Foram aplicadas multas a Itaú (R$ 9,6 milhões), Pan (R$ 8 milhões), BMG (R$ 5,1 milhões) e Cetelem (R$ 4 milhões).

Danos morais

Eletropaulo indenizará idosa por vazar dados pessoais a estranhos

A própria empresa notificou a consumidora do vazamento de dados decorrente da ação de criminosos.

terça-feira, 6 de julho de 2021

Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados

Decisão é uma das primeiras referentes à nova lei, que entrou em vigor no dia 18.

Valor — Por Valor Online

30/09/2020 20h00 · Atualizado há 6 dias

BL CONSULTORIA DIGITAL

HOMEPAGE › PRIVACIDADE & PROTEÇÃO DE DADOS

LGPD / NOTICIAS SOBRE DIREITO DIGITAL / PRIVACIDADE & PROTEÇÃO DE DADOS

Instituição de Ensino é condenada por infração à LGPD

MPDFT AJUÍZA 1ª AÇÃO CIVIL PÚBLICA COM BASE NA LGPD

Publicado: 22/09/2020 às 7:27

Compartilhar Tweet

Iniciativa é contra empresa de informática especializada em comercializar dados cadastrais de usuários

O Ministério Público do Distrito Federal e Territórios ofereceu a primeira ação civil pública com pedido de tutela, baseada na Lei Geral de Proteção de Dados Pessoais, nesta segunda-feira, 21 de setembro. A lei, que entrou em vigor na sexta-feira, enquadra como lesiva a conduta de uma empresa sediada em Belo Horizonte (MG).

Homem pagará indenização de R$ 15.000,00 por divulgar dados pessoais sensíveis da ex-companheira. (LGPD).

A intimidade e a privacidade devem ser resguardadas, isso porque se constituem em direitos fundamentais da pessoa.

PRIVACIDADE

Ransomhack: um futuro problema envolvendo a LGPD?

Para evitar este e outros incidentes de segurança, o caminho é um só: investimento em cibersegurança

LGPD: sanções começam este ano

Em vigor desde o ano passado, LGPD começa a aplicar sanções a partir de agosto de 2021. Empresas precisam planejar sua governança de dados

Escopo da LGPD

Para atender a LGPD, controladores e operadores deverão realizar um **projeto de adequação à Lei**, buscando atender requisitos **operacionais**, **jurídicos** e **tecnológicos**

Você precisará **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

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

Será necessário ainda 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**

RGM TECNOLOGIA

Princípios a serem observados

- **Art. 6º** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

  I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

  II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

  III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

  IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

  V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

  VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

  VII - **segurança**: utilização de medidas 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 difusão;

  VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

  IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

  X - **responsabilização** e prestação de contas: 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.

Papéis previstos da LGPD

Titular de Dados

- Pessoa física identificável
- É quem a LGPD busca garantir a privacidade
- Proprietária dos dados em tratamento

Controlador

- Pessoa física ou jurídica que é o maior responsável pelos dados dos Titulares
- É quem define as regras de segurança

Operador

- Pessoa física ou jurídica que realiza o tratamento de dados (ou parte dele) a pedido do Controlador
- Deve se adequar às regras definidas pelo Controlador

Encarregado (DPO)

- Ponto focal da LGPD dentro de um Controlador ou Operador
- Garante a adequada execução das rotinas de segurança
- Atende os Titulares e a ANPD

ANPD

- Órgão do Poder Executivo Federal que regulamentará a LGPD e garantirá sua execução
- Audita Controladores e Operadores
- Aplica sanções

RGM TECNOLOGIA

Sanções previstas

- **Art. 52**. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

  I - **advertência**, com indicação de prazo para adoção de medidas corretivas;

  II - **multa simples**, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, **limitada, no total, a R$ 50.000.000,00** (cinquenta milhões de reais) por infração;

  III - **multa diária**, observado o limite total a que se refere o inciso II;

  IV - **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;

  V - **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;

  VI - **eliminação dos dados pessoais** a que se refere a infração;

  X - **suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

  XI - **suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

  XII - **proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados**.

A LGPD na gestão pública

- A operação de órgãos públicos, da administração direta ou indireta, invariavelmente realiza tratamento de Dados Pessoais e esses tratamentos devem ser realizados exclusivamente para o cumprimento das atribuições legais do serviço público (Art. 23)
- A LGPD é totalmente aplicável à gestão pública
  - Empresas públicas (ou de sociedade mista) são consideradas empresas privadas para os parâmetros da LGPD (Art. 24)
- Exceto multas financeiras, todas as demais sanções previstas na LGPD poderão ser imputadas a entes públicos (Art. 52)
- Entes públicos podem executar o papel de Controlador ou Operador, a depender de suas responsabilidades em um determinado processo de negócio ou fluxo de informação

RGM TECNOLOGIA

Trilha 02
Implementando um SGPD

RGM TECNOLOGIA

Agenda da trilha

I. Escopo de adequação à LGPD
II. O que é um SGPD
III. Gestão do tratamento de dados pessoais
   a. Processos de negócio
   b. Ativos de informação, artefatos e dados pessoais
   c. Finalidades e hipóteses de tratamento de dados pessoais
   d. Segurança da informação (e a ISO/IEC 27.001)
   e. Medidas administrativas de segurança
   f. Medidas técnicas de segurança

RGM TECNOLOGIA

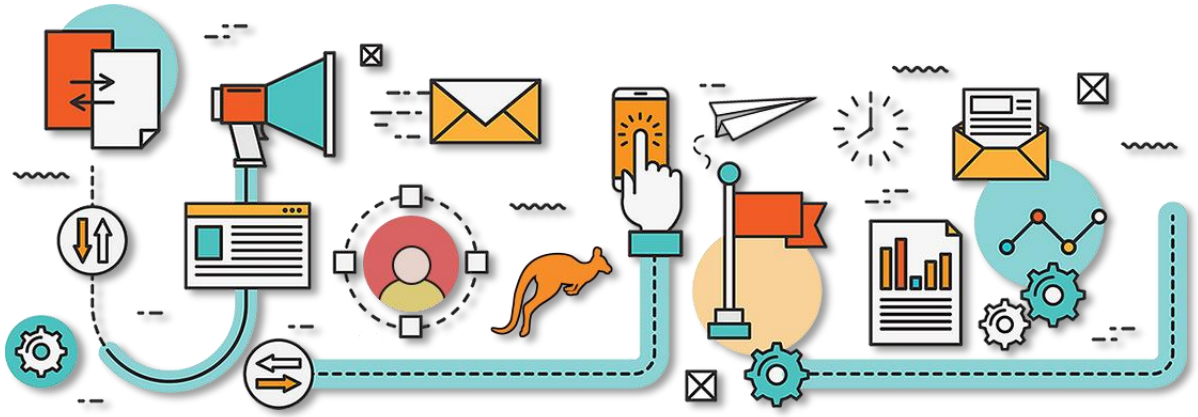
Adequação à Lei Geral de Proteção de Dados

RGM TECNOLOGIA

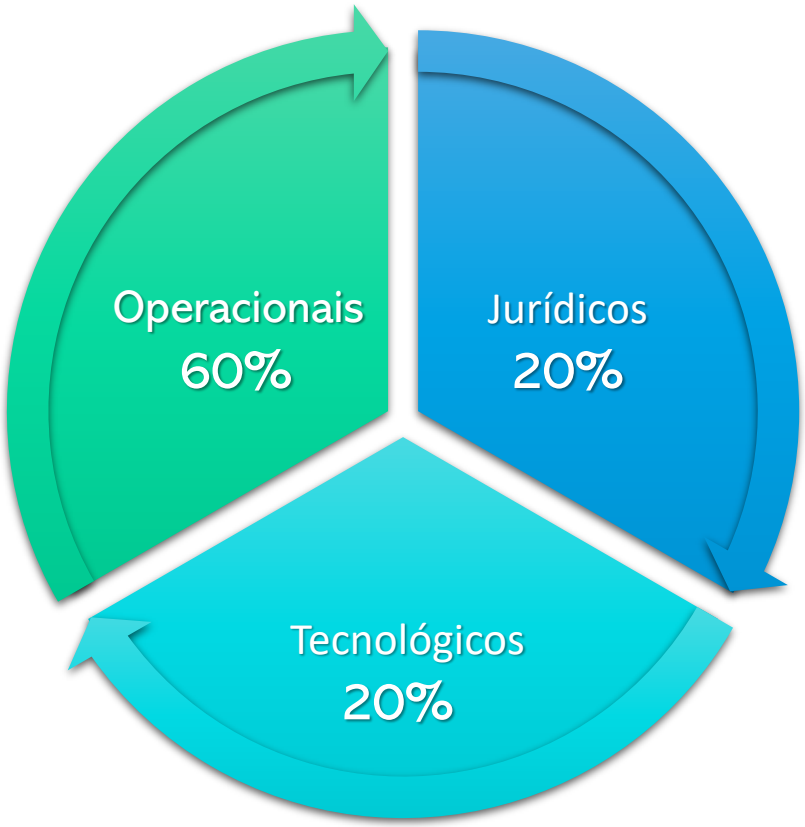
O que é um SGPD

- **Sistema**: Conjunto de elementos, concretos ou abstratos, intelectualmente organizados que interagem de tal forma que o resultado do todo não pode ser alcançado individualmente por suas partes.

- Um **Sistema de Gestão/Gerenciamento de Proteção de Dados (SGPD)** é um conjunto de *papéis*, *atividades*, *documentos*, *controles* e *ferramentas* que, juntos, buscam gerenciam, organizam e garantem a **segurança de dados.**



Aspectos tratados em um SGPD



Operacionais

- Ciclo de vida dos dados pessoais
- Finalidades de tratamento de dados
- Medidas *administrativas* de segurança (políticas)
- Processos previstos na LGPD
- Gestão de riscos operacionais

Jurídicos

- Hipóteses de tratamento de dados pessoais
- Fundamentos legais
- Gestão jurídica de contratos
- Gestão de riscos legais

Tecnológicos

- Gestão de ativos de informação
- Medidas *técnicas* de segurança
- Disponibilização de ferramentas para apoio ao SGPD
- Gestão de riscos tecnológicos

RGM TECNOLOGIA

Como implementar um SGPD

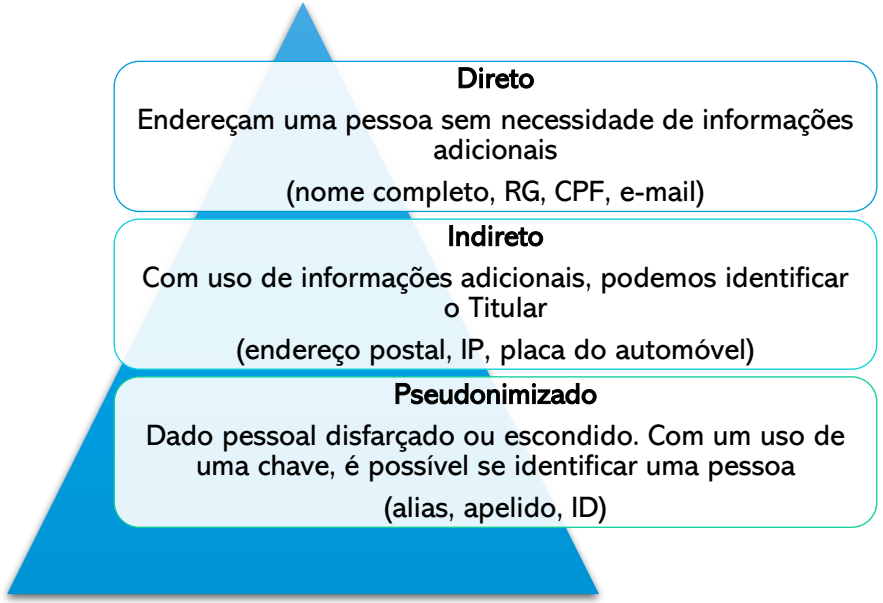
Ciclo de vida dos dados pessoais

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;



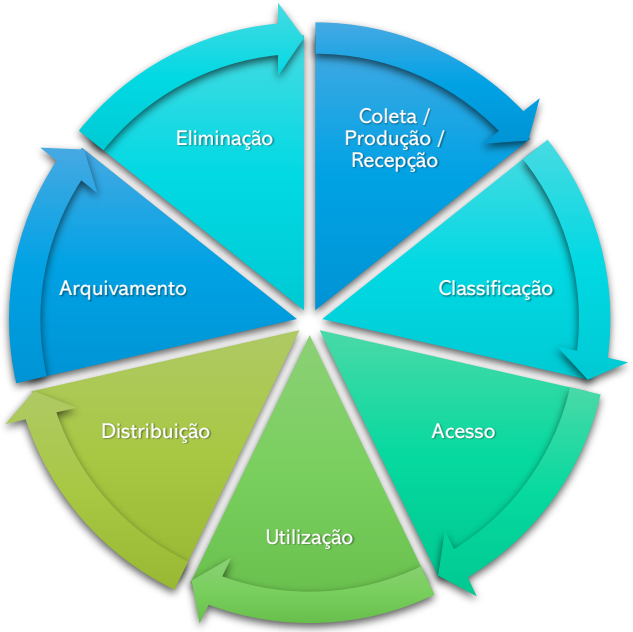
Dados anonimizados não fazem parte do escopo da LGPD, por não ser possível identificar o Titular
(não há chave para reverter a anonimização)

Ciclo de vida dos dados pessoais

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

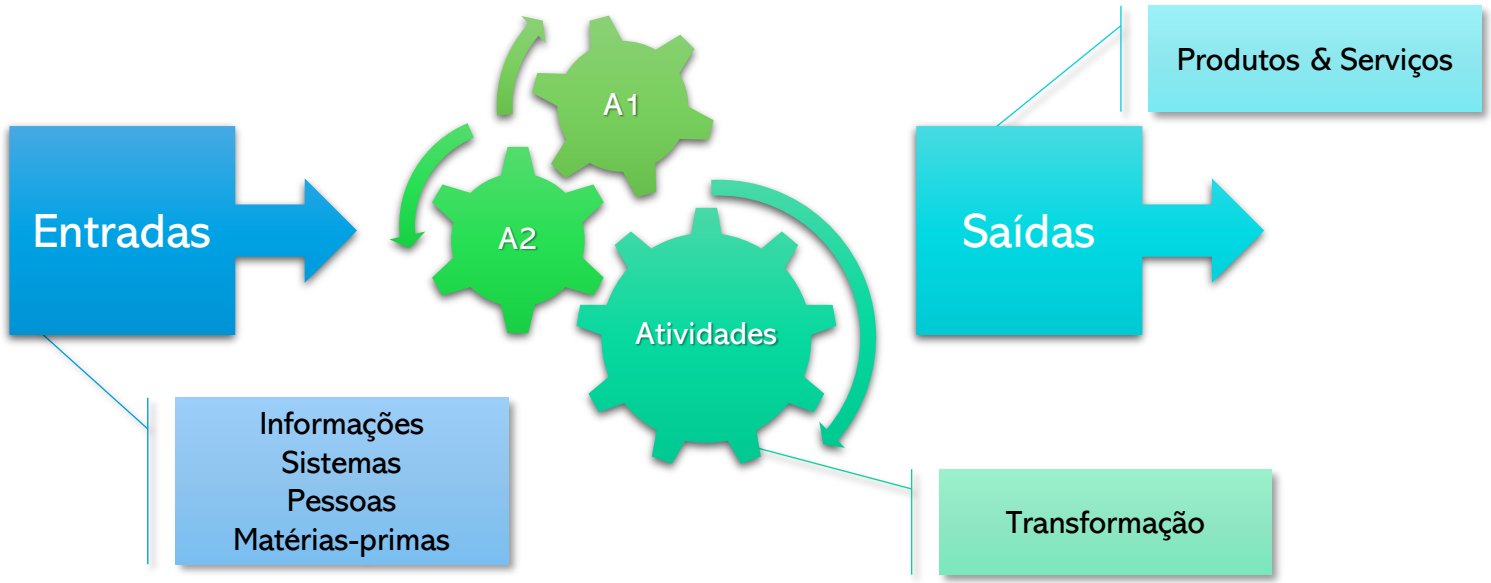
  (...)

  X - **tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;



Processos de negócio

- Processos são conjuntos de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos ou serviços (saídas), que têm valor para um grupo específico de clientes.



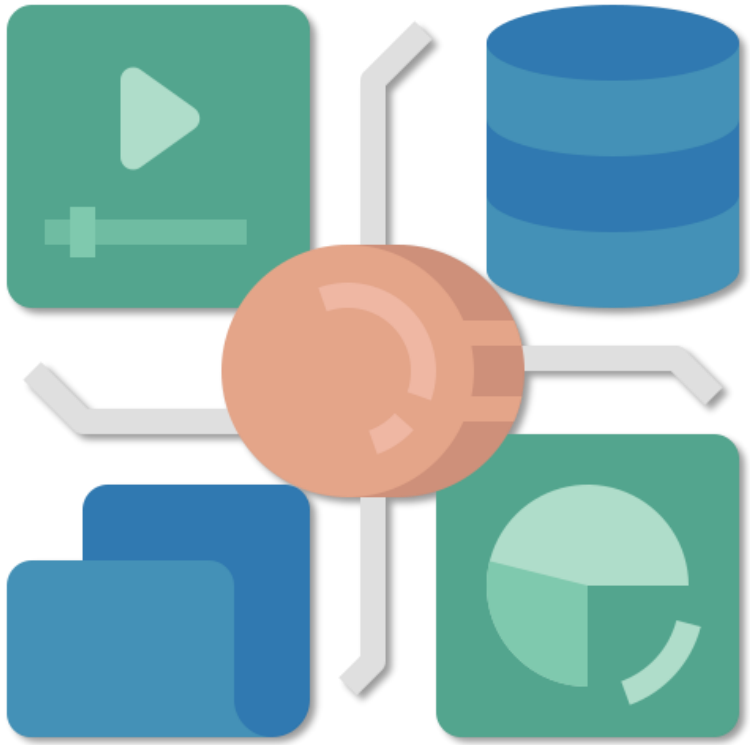
- Todo trabalho importante realizado nas organizações faz parte de algum processo
- Não existe um produto ou serviço oferecido por uma organização sem um processo organizacional
- Este porém pode ou não estar documentado

Principais atributos de um processo:

- Objetivo do processo
- Papéis envolvidos
- Ativos utilizados nas atividades
- Regras e premissas para execução
- Entradas
- Fluxo
- Saídas

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 e classificação de dados pessoais

- 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
- Dentro de um determinado **Artefato**, um **Dado Pessoal** pode 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)

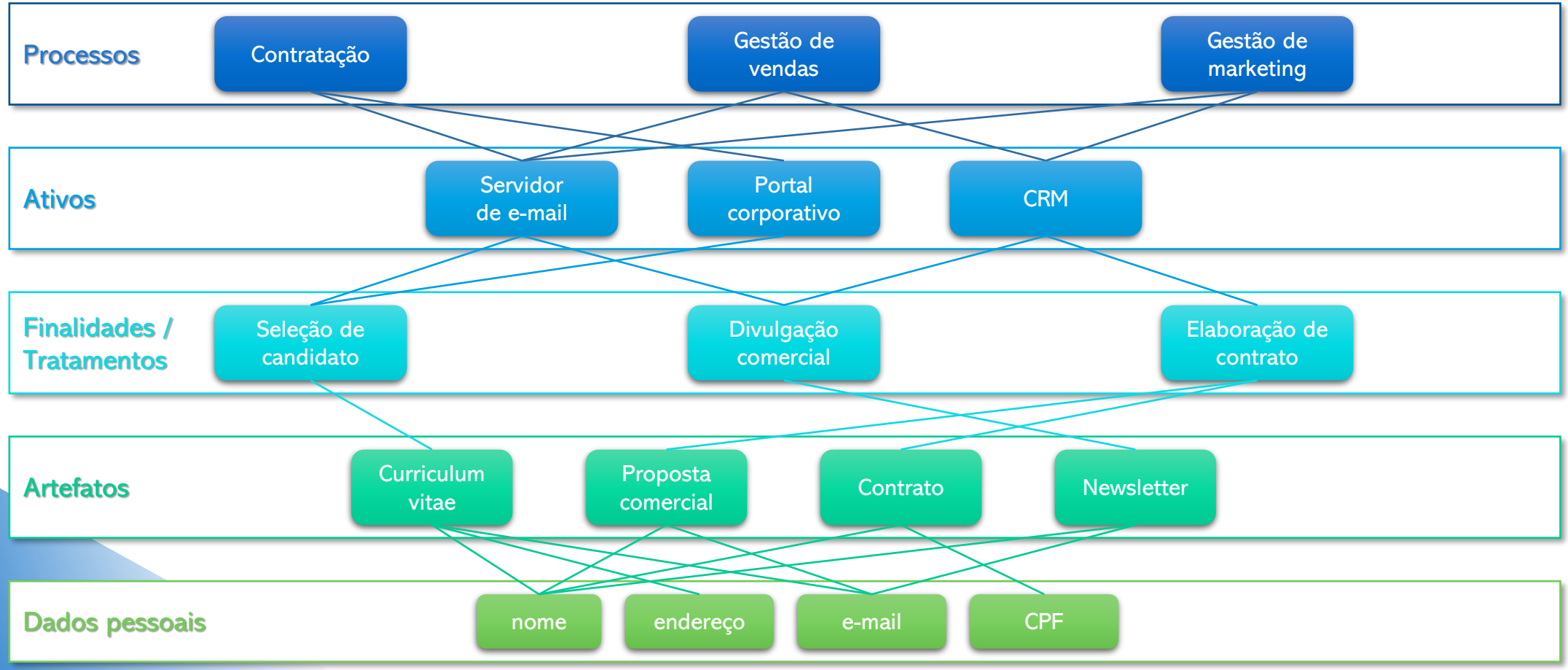
RGM TECNOLOGIA

Finalidades de tratamento de dados pessoais

- Cada processamento de um Dado Pessoal (que ocorre por um motivo específico), pode ser considerado uma **Finalidade de Tratamento de Dados Pessoais**.
  - Deve demonstrar detalhes do tratamento de Dados Pessoais realizados ali, como por exemplo: Se usa Operador, se Compartilha Dados, prazo de armazenamento das informações, se trata Dados Pessoais de crianças ou adolescentes.
- Cada Finalidade de Tratamento de Dados Pessoais deve ter uma Hipótese de Tratamento associada, de acordo com os Artigos 7º e 11º da LGPD:
  - Cumprimento de obrigação legal ou regulatória
  - Execução de políticas públicas (exclusivo para entes públicos)
  - Realização de estudos e pesquisas (exclusivo para órgãos de pesquisa)
  - Execução de contrato (*exclusivo para o Art. 7º*)
  - Processos judiciais
  - Proteção da vida
  - Tutela de saúde (por profissionais, serviços ou autoridades de saúde/sanitárias)
  - Proteção de crédito
  - Promoção das atividades do controlador (*exclusivo para o Art. 7º*)
  - Consentimento explícito

RGM TECNOLOGIA

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

RGM TECNOLOGIA

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

RGM TECNOLOGIA

Segurança da informação e dos dados pessoais

Responsabilidade sobre segurança

- É responsabilidade do Controlador garantir a segurança dos **Dados Pessoais** e evitar (ou gerenciar adequadamente) incidentes de privacidade:
  - *"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."* (LGPD, Art. 46)
  - *"Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."* (LGPD, Art. 47)
  - *"Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares."* (LGPD, Art. 49)

RGM TECNOLOGIA

Segurança e privacidade de dados

A garantia da privacidade dos dados é obtida através da implementação de controles de segurança.

Privacy by design & Privacy by default

- A privacidade dos Dados Pessoais não deve ser algo opcional, e um padrão que define parâmetros para ajudar a alcança-la é o *Privacy by design* ou, em tradução livre, a *Privacidade desde a concepção*.
- Trata-se de um modelo teórico que, por si só, não resolve os problemas de proteção de dados, muito menos garante a adequação à LGPD, mas define 7 princípios valiosos para se manter em mente durante a execução dos projetos de adequação à LGPD:

Princípio #1: Prevenir e não remediar

Aja proativamente e pense antes do fato, não depois

Princípio #2: Privacidade como padrão (*privacy by default*)

Não exija nenhuma ação do seu titular de dado para que a privacidade de seu produto, serviço ou solução seja "ativada"

Princípio #3: Privacidade incorporada ao projeto

A privacidade não deve ser tratada como um componente adicional de seu produto, serviço ou solução, ela é algo intrínseco ao projeto

Princípio #4: Soma positiva

A privacidade deve agregar valor ao seu produto ou serviço e não apenas ser uma obrigação ou escolha

Princípio #5: Segurança de ponta-a-ponta

A proteção de dados deve ser algo presente desde o início das atividades de tratamento de dados até quando os dados são destruídos

Princípio #6: Visibilidade e transparência

A privacidade deve ser algo visível e transparente para todos do projeto, que devem saber as regras, práticas e tecnologias envolvidas na proteção

Princípio #7: Solução centrada no usuário

Deve-se considerar que o maior interessado na privacidade é o Titular dos Dados. São os interesses dele que importam mais

RGM TECNOLOGIA

Medidas administrativas de segurança
(1/2)

- Implementar controles ou soluções que maximizem os níveis de segurança dos **Dados Pessoais**, pavimentando assim o caminho para garantir a privacidade dos Titulares de Dados, se inicia com o estabelecimento de compromissos e guias que enderecem as boas práticas e os princípios que devem surgir já na governança corporativa do Controlador e Operador (Art. 50 da LGPD).
- O comprometimento com a privacidade são documentados/obtidos através das **Medidas Administrativas de Segurança**:
  - **Política de privacidade**: Foco externo, demonstra as regras públicas de como o ente trata os Dados Pessoais e busca garantir a privacidade dos Titulares de Dados
  - **Política de segurança**: Foco interno, estabelece as regras a serem aplicadas pelo ente na implementação das Medidas Técnicas de Segurança
  - **Cláusulas contratuais (e gestão de contratos)**: Estabelece diretrizes, limites e responsabilidades sobre os tratamentos de Dados Pessoais realizados no relacionamento entre as partes;
  - **Treinamento, capacitação e conscientização**: Prepara os colaboradores do ente a lidar com a privacidade, compartilha responsabilidades e documenta a ciência de todos perante os compromissos adotados pelo Controlador ou Operador

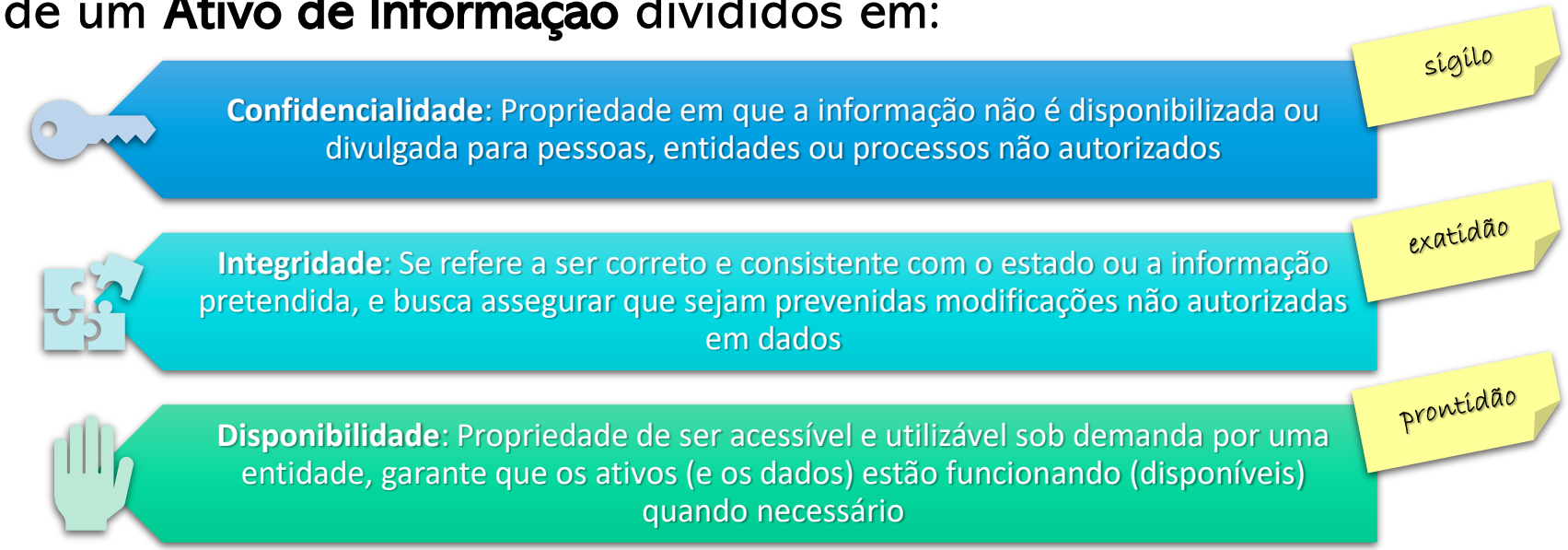
RGM TECNOLOGIA

Medidas administrativas de segurança
(2/2)

- As **Medidas Administrativas de Segurança** devem:
  - Estar integradas à governança corporativa
  - Estabelecer relação de confiança com o Titular de Dados, por meio de atuação transparente e que assegure mecanismos de participação do Titular de Dados, incluindo canais para que eles exerçam seus direitos
  - Definir mecanismos de supervisão do SGPD
  - Estabelecer um ciclo de vida de atualização/manutenção das Medidas de Segurança adotadas
  - Definir regras para a realização da gestão de riscos de segurança e privacidade
  - Definir os parâmetros da gestão de incidentes e notificações
  - Estabelecer regras para compartilhamento e transferência de Dados Pessoais
  - Definir o papel e as responsabilidades do DPO
  - Definir responsabilidades e regras a serem cumpridas pelo Controlador e seus Operadores
  - Ser exequíveis

Medidas técnicas de segurança
(1/2)

- Como os Dados Pessoais são tratados nos **Ativos de Informação**, devemos implementar **Medidas de Segurança** para maximizar o nível de Confiabilidade dos **Ativos de Informação.**
- De acordo com a norma **ISO/IEC 27.001**, as medidas visam aumentar os níveis de segurança de um **Ativo de Informação** divididos em:



Medidas técnicas de segurança
(2/2)

Medidas técnicas de Confidencialidade

- Criptografia de dados
- Estrito controle de acesso físico e lógico: *Assegurar o nível de acesso apropriado e somente para as pessoas autorizadas*
- Classificação de dados: *Definir a que público os dados podem ser comunicados (Públicos? Sensíveis? Confidenciais?)*
- Treinamento de pessoal
- Segregação de funções: *Evitar que funções conflitantes sejam executadas pela mesma pessoa*
- Política de "mesa limpa"

Medidas técnicas de Integridade

- Padronizar caminho de acesso: *Por exemplo, não permitir atualização de dados "diretamente na Base de Dados"*
- Gravação de logs de usuários: *Garantir que possa ser determinado quem modificou a informação*
- Segregação de Função, posições e autoridade: *Ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências*
- Mudanças em sistemas e dados devem ser são autorizadas
- Padronizar terminologia: *Por exemplo, um incidente é sempre chamado de "incidente", logo, o termo "chamado" não pode ser inserido na base de dados*

Medidas técnicas de Disponibilidade

- Implementação de uma robusta solução de *backup* e *restore*
- Realizar rotinas de teste de restauração de ambientes
- Políticas de armazenamento gerenciado de dados: *Por exemplo, não permitir o armazenamento de dados em máquinas pessoais, dar preferência a sistemas de armazenamento centralizados, como servidores em rede interna ou cloud*
- Implementação do Gerenciamento de Disponibilidade da ITIL

RGM TECNOLOGIA

Gestão de riscos, incidentes e notificações de privacidade

Riscos de segurança da informação

- Risco é toda a situação em que há probabilidade de os resultados serem diferentes do esperado devido a um motivo. Isto nos dá a chance de evitar um dano ou consequência adversa. É a *probabilidade* de uma ameaça explorar uma vulnerabilidade e causar um dano ou consequência.
- Riscos ainda não são fatos.
- Exemplo de risco:
  - "*Podemos ter perda de dados no sistema de Gestão Tributária por não termos backups atualizados. Se houver um problema do disco rígido do banco de dados, não haverá como garantir a recuperação das informações de arrecadação do IPTU do último mês. Isso tornará o Portal da Transparência desatualizado e poderá gerar problemas contábeis associados aos valores de receitas orçamentárias, dificultando a prestação de contas ao TCE.*"

RGM TECNOLOGIA

Classificando riscos de segurança

- Um risco tem uma *Probabilidade* de ocorrer (percentual) e um *Impacto* previsto (baixo, médio ou alto). A combinação desses atributos mostra a *Criticidade* que devemos considerar ao tratá-lo. Uma sugestão é utilizar uma Matriz de Criticidade, como a seguir:

Probabilidade	Impacto: Baixo	Impacto: Médio	Impacto: Alto
100%	Alta	Urgente	Urgente
90%	Moderada	Urgente	Urgente
80%	Moderada	Alta	Urgente
70%	Moderada	Alta	Urgente
60%	Moderada	Alta	Alta
50%	Baixa	Alta	Alta
40%	Baixa	Moderada	Alta
30%	Baixa	Moderada	Moderada
20%	Baixa	Baixa	Moderada
10%	Baixa	Baixa	Moderada

Gerenciando riscos de segurança
(1/2)

- Gerenciar riscos visa diminuir a possibilidade do risco se tornar um fato e, consequentemente, gerar os impactos esperados (ou não mapeados).
- É uma atividade constante do Controlador e do operador, a ser liderada pelo DPO
  - "*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.*" (LGPD, Art. 46)
  - "*Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.*" (LGPD, Art. 50)
- Deve-se definir uma estratégia para tratar cada risco. Os tipos possíveis de Estratégia para gestão de um risco são:
  - **Evitar**: O Controlador tomará medidas para impedir que o risco se torne um fato e gere um incidente
  - **Mitigar**: O Controlador tomará medidas para diminuir a probabilidade do risco ser disparado
  - **Compartilhar/Transferir**: O Controlador dividirá a responsabilidade de gestão do risco com um terceiro
  - **Aceitar**: O Controlador não tem como tomar medidas preventivas contra o risco e vai aceita-lo como ele é

Gerenciando riscos de segurança
(2/2)

- **Risco**: "*Podemos ter perda de dados no sistema de Gestão Tributária por não termos backups atualizados. Se houver um problema do disco rígido do banco de dados, não haverá como garantir a recuperação das informações de arrecadação do IPTU do último mês.*"
- **Descrição do impacto**: "*Tornar o Portal da Transparência desatualizado e gerar problemas contábeis associados aos valores de receitas orçamentárias, dificultando a prestação de contas ao TCE.*"
- **Probabilidade**: 60% | **Impacto**: Alto | **Criticidade**: Alta
- **Tipo de estratégia**: Mitigar
- **Descrição da estratégia**: Atualizar o processo de *backup* do servidor XPTO, incluindo backup incremental diário em ambiente externo na nuvem. Realizar atividades quinzenais de teste de *restore* do servidor.
- **Responsável por gerenciar o risco**: João da Silva
- **Status**: Detectado [*Disparado, Encerrado, Cancelado*]
- **Data de cadastro:** 10/04/2022

Relatório de impacto de proteção de dados

- O Relatório de Impacto de Proteção de Dados, também conhecido como **Data Protection Impact Assessment** (DPIA), é um documento definido na LGPD que demonstra que o Controlador gerencia riscos de privacidade:
  - *"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."* (LGPD, Art. 5º, inciso XVII)
  - Deve ser emitido/gerenciado pelo DPO
  - Será a primeira evidência a ser analisada pela ANPD
  - Deve conter "*a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.*" (LGPD, Art. 38, parágrafo único)

RGM TECNOLOGIA

Quando emitir o DPIA

De acordo com a LGPD

- Sempre que o tratamento de dados *representar alto risco à garantia dos princípios gerais de privacidade dos Titulares de Dados*
  - Obrigação dos Controladores (LGPD, Art. 50, parágrafo 2º, inciso I, alínea d)
  - Solicitação da ANPD para exceções à LGPD (LGPD, Art. 4º, parágrafo 3º)
  - Solicitação da ANPD para justificar Legítimo Interesse (LGPD, Art. 10, parágrafo 3º)
  - Solicitação da ANPD para agentes do Poder Público (LGPD, Art. 32)
  - Solicitação da ANPD ao Controlador (LGPD, Art. 38)

Melhores práticas para o DPO

- Sempre quando houver:
  - Grande volume de tratamento de dados
  - Tratamento de Dados Sensíveis
  - Tratamento de Dados de Crianças e Adolescentes
  - Tratamento de Dados por Legítimo Interesse do Controlador
  - Compartilhamento de Dados Pessoais com terceiros
  - Tratamento de Dados Pessoais realizados de forma automatizada, sem verificação humana
  - Riscos de privacidade detectados com criticidade URGENTE ou ALTA

RGM TECNOLOGIA

Incidentes de segurança e privacidade

- Sempre que houver uma ocorrência (fato), ilícita ou acidental, proveniente ou não de um risco previamente detectado, que gere *destruição*, *perda*, *alteração*, *comunicação* ou qualquer forma de *tratamento inadequado ou ilícito* sobre informações, temos um *incidente de segurança.*
- Quando as informações associadas ao incidente são Dados Pessoais, temos um *incidente de privacidade.*

Gestão de incidentes e notificações

- Um incidente de privacidade deve ser comunicado à ANPD:
  - *"O Controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional."* (LGPD, Art. 48)
- Cabe ao Controlador e sua análise de impacto (inclusive o DPIA), analisar se o incidente pode acarretar risco ou dano relevante aos titulares. Essa análise ainda não foi regulamentada, mas podemos considerar os seguintes parâmetros para essa classificação:
  - Volume da Dados Pessoais, Volume de Titulares de Dados associados e características dos Dados Pessoais (Dados Sensíveis, por exemplo)
- Canal oficial previsto pela ANPD
  - A ANPD definiu que, por enquanto (mar/22), o canal para enviar notificações ao órgão é pelo SEI, e inclusive providenciou um formulário padrão para a criação do artefato (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca)

RGM TECNOLOGIA

Composição de uma Notificação

- Ao notificar a ANPD quando da ocorrência de um incidente que possa acarretar risco ou dano relevante aos Titulares, deve ser informado o seguinte:
  - A descrição da natureza dos dados pessoais afetados
  - As informações sobre os titulares envolvidos
  - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial
  - Os riscos relacionados ao incidente
  - Os motivos da demora, no caso de a comunicação não ter sido imediata
  - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

(LGPD, Art. 48)

Gestão dos direitos dos titulares de dados

Os direitos dos titulares de dados
(1/2)

- Livre acesso, de forma clara, objetiva e transparente, à informações sobre o tratamento de seus dados:
  - confirmação de existência do tratamento e quais dados estão sendo utilizados [15 dias de SLA]
  - finalidade específica do tratamento
  - forma e duração do tratamento
  - identificação e contato do controlador
  - uso compartilhado de dados pelo controlador e a finalidade
  - responsabilidades dos agentes de tratamento

  (LGPD, Art. 6° incisos IV e VI, Art. 9° e Art. 18)

- Integridade, atualização e exatidão de seus dados (LGPD, Art. 6°, inciso V e Art. 18, inciso III)
- Revogação de seus consentimentos de forma gratuita e facilitada (LGPD, Art. 8°, parágrafo 5°)
- Solicitação de término do tratamento de seus dados (LGPD, Art. 15, inciso III)
- Titularidade de seus dados e direito a sua privacidade e intimidade (LGPD, Art. 17)
- Revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais (LGPD, Art. 20)

RGM TECNOLOGIA

Os direitos dos titulares de dados
(2/2)

- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei (LGPD, Art. 6 inciso III, Art. 18, inciso IV e Art. 60)
- Portabilidade dos dados a outro fornecedor de serviço ou produto (LGPD, Art. 18, inciso V)
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei (LGPD, Art. 18, inciso VI)
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (LGPD, Art. 18, inciso VII)
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (LGPD, Art. 18, inciso VIII)
- Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais (LGPD, Art. 60)

RGM TECNOLOGIA

Gestão de direitos dos titulares de dados

A confirmação de existência, o acesso a dados pessoais e aos seus direitos devem ser providenciados ao Titular, mediante requisição (LGPD, Art. 18 e Art. 19)

Gestão de consentimentos dos titulares de dados

O que é o consentimento na LGPD

- É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica (LGPD, Art. 5º, inciso XII)

- Pode ser utilizada como uma das hipóteses que justificam a realização de um determinado tratamento de dados, inclusive o tratamento de dados sensíveis e o compartilhamento internacional de dados (LGPD, Art. 7º, inciso I; Art. 11, inciso I e Art. 33, inciso VIII)

Quando usar o consentimento

É obrigatório quando...

- Não houver outra hipótese que justifica o tratamento de dados
- Ocorrer a realização do tratamento de dados de uma criança ou adolescente (Art. 14, parágrafo 1º).
  - Nesse caso, deve ser concedido pelo responsável
- Houver o compartilhamento de dados pessoais por pessoas jurídicas de direito público a pessoa de direito privado (Art. 27, inciso I)
  - Exceto em casos excepcionais

É dispensável quando...

- Houver outra hipótese que justifica o tratamento de dados
- O Controlador está tratando de dados tornados manifestadamente públicos pelo titular (LGPD, Art. 7º, parágrafo 4º)
  - Mesmo quando dispensável (pelos dados serem públicos, ou por se utilizar outra hipótese de tratamento), o consentimento não desobriga o Controlador dos demais parâmetros da LGPD (LGPD, Art. 7º, parágrafo 6º)

RGM TECNOLOGIA

Gestão de consentimentos

- **Escopo do consentimento**
  - Deve ser específico (para cada finalidade) e não poderá conter vícios (LGPD, Art. 8º, parágrafos 3º e 4º e Art. 7º, parágrafo 5º)
  - Se o tratamento de dados for justificado pelo consentimento, o Controlador deverá fornecer ao Titular de Dados uma cópia eletrônica integral de seus dados pessoais (Art. 19, parágrafo 3º)
- **Obtenção e registro**
  - Deve ser obtido por escrito ou qualquer outro meio que demonstre a vontade do Titular de Dados (LGPD, Art. 8º)
  - Se obtido por escrito, deverá ser através de cláusula específica e destacada para isso (LGPD, Art. 8º, parágrafo 1º)
  - Cabe ao Controlador comprovar que o consentimento foi dado pelo Titular (LGPD, Art. 8º, parágrafo 2º e Art. 9º, parágrafo 1º)
  - Cabe ao Controlador avisar o Titular de Dados sobre as consequências se houver negativa quanto ao consentimento (Art. 18, inciso VIII)
- **Revogação**
  - O Controlador deve permitir a revogação de consentimentos por parte do Titular de Dados, de forma fácil e grátis, mas ele continua válido para os tratamentos realizados antes da revogação (LGPD, Art. 8º, parágrafo 5º e 6º; Art. 9º, parágrafo 2º; Art. 15, inciso III e Art. 18, incisos VI e IX)

RGM TECNOLOGIA

Obrigado!

Adilson Taub Jr.

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

RGM Tecnologia

www.rgm.com.br

SCAN ME