RGM
TECNOLOGIA

Workshop LGPD

Medidas Administrativas de Segurança da Informação

Agenda

- A segurança da informação
- Quando analisar a segurança da informação
- Medidas administrativas de segurança da informação
- Como utilizar o LGPD Governance (PCP) para inventariar e analisar as medidas administrativas de segurança da informação

RGM TECNOLOGIA

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

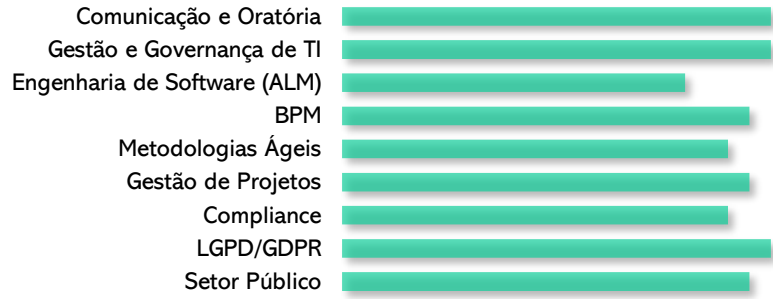
Certificações

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

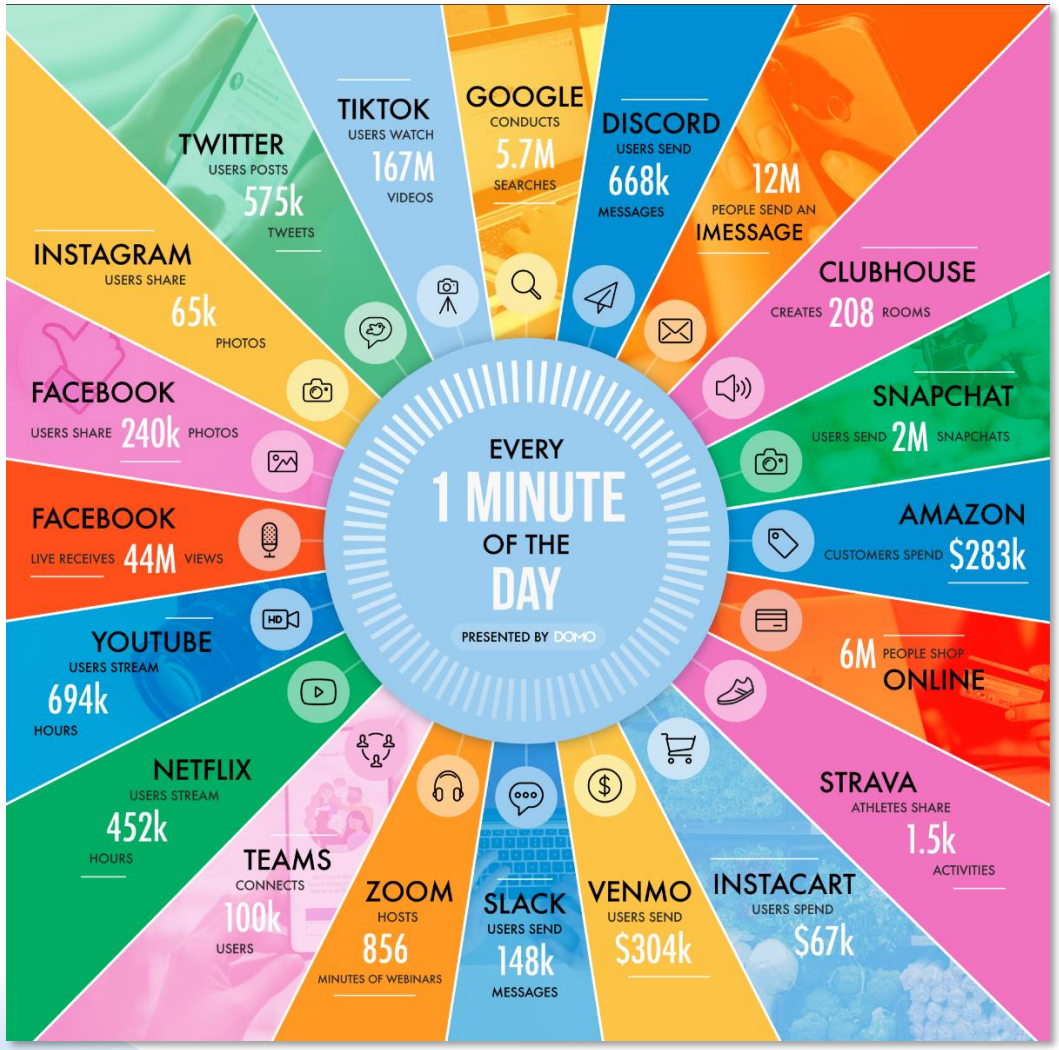
Software Engineering
Professional Scrum Product Owner (PSPO I)
Professional Scrum Master (PSM I)
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF
IBM Certified Solution Designer (RUP)
Certified Expert in BPM

Mapa de habilidades



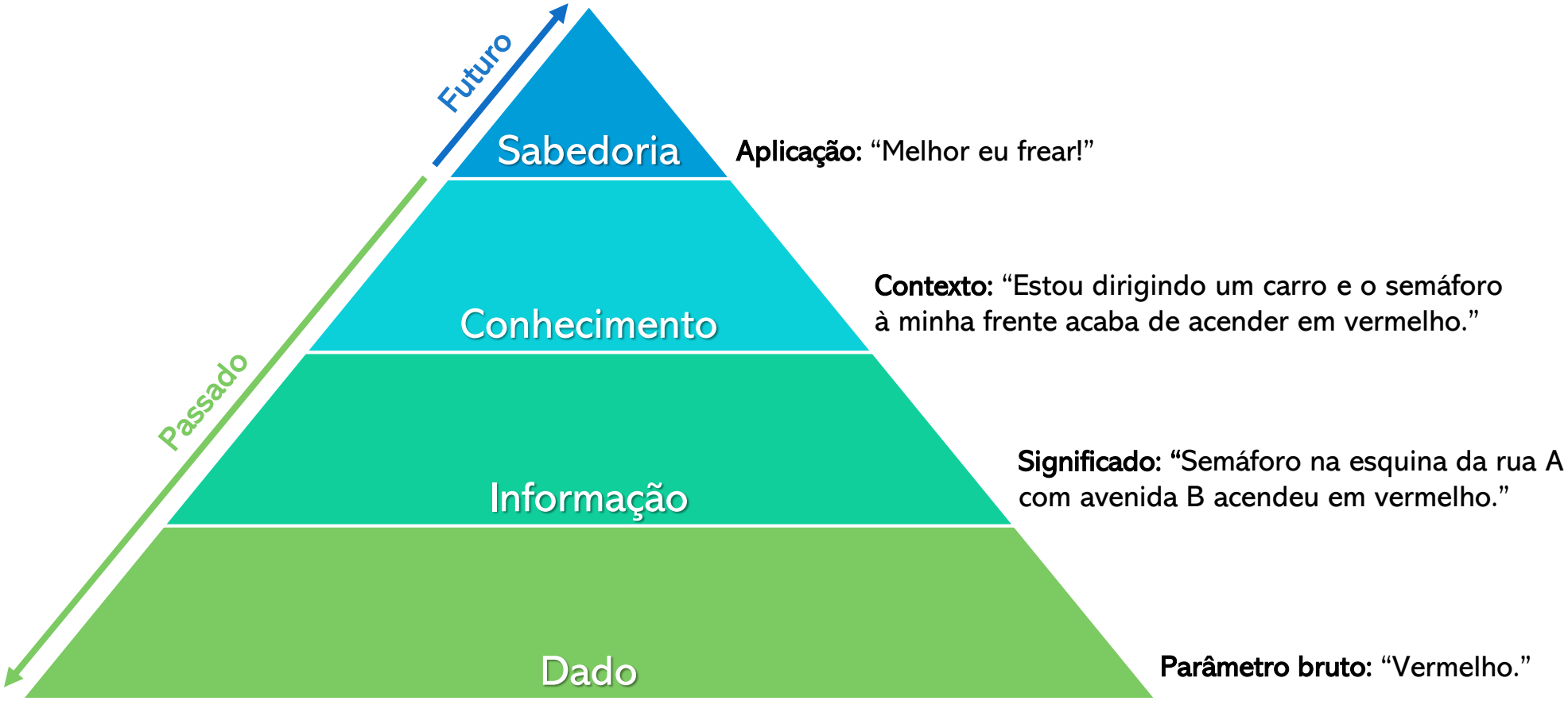
A segurança da informação

Volume de dados pessoais



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

Gestão do conhecimento



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

Princípios a serem observados

- **LGPD - 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.

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

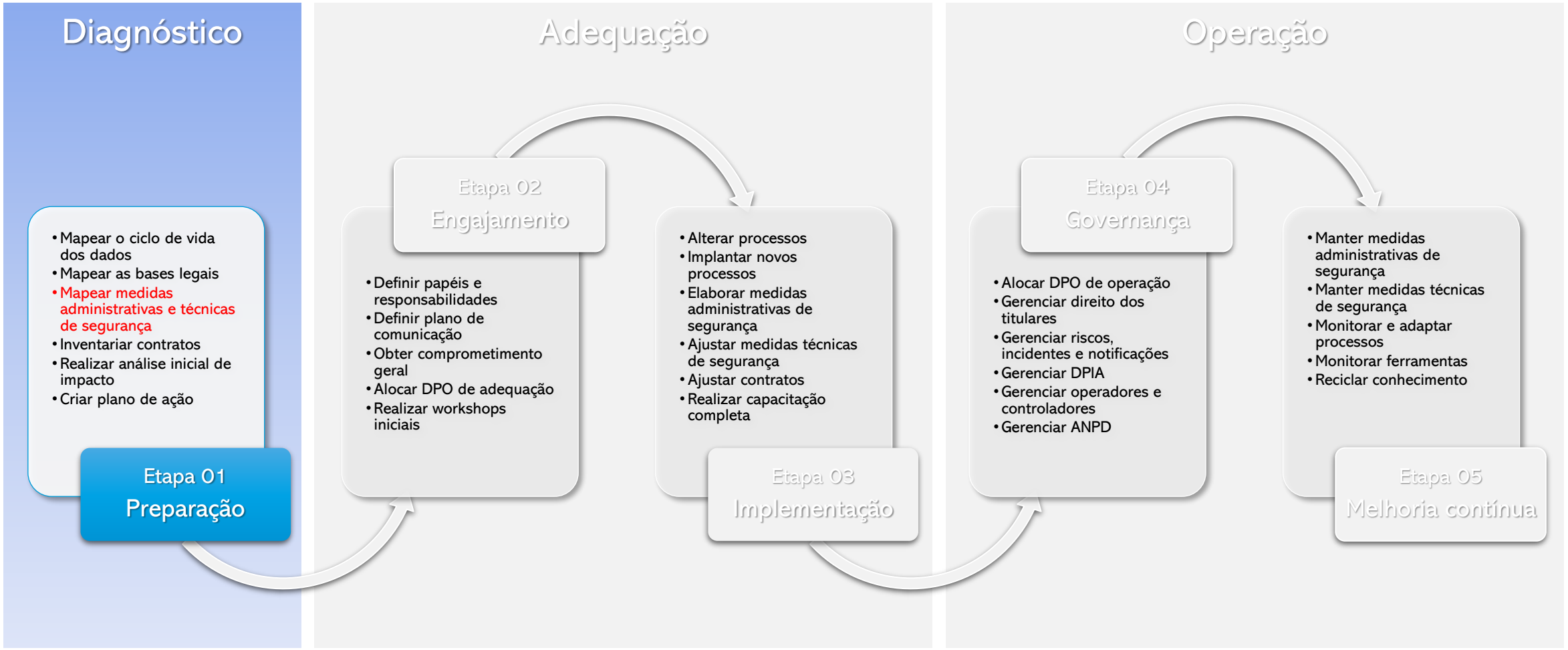
Deve-se considerar que o maior interessado na privacidade é o Titular dos Dados. São os interesses dele que importam mais

RGM TECNOLOGIA

Quando analisar a segurança da informação

Como implementar um SGPD

Como implementar um SGPD



Diagnóstico
1. Preparação

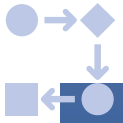
- **Principal objetivo da etapa:**
  - Elaborar *o Plano de Ação* com atividades claras e objetivas que deverão ser executadas posteriormente para garantir a adequação do controlador à LGPD.

- **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?

RGM TECNOLOGIA

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

RGM TECNOLOGIA

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. 7° para dados normais
- Utilizar os incisos definidos no Art. 11° 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*

RGM TECNOLOGIA

Etapa de Preparação

Passo 1.3 Analisar as Medidas Administrativas

Analisar o alinhamento corporativo

- Verificar como o assunto "privacidade" é tratado na Governança Corporativa
- Entender como é aplicado os conceitos de "*privacy by design*" e "*privacy by default*" na empresa
- *Envolvimento do time jurídico*

Analisar as Políticas de Privacidade

- Documentos com foco EXTERNO que estabelecem os compromissos da empresa
- Analisar a exequibilidade e completude dos compromissos firmados
- Avaliar o nível de disseminação das políticas
- Envolvimento do time jurídico

Analisar as Políticas de Segurança

- Documentos com foco INTERNO que detalham regras e estratégias para a melhor gestão e segurança dos Ativos de Informação
- Analisar se essas políticas são compatíveis com as políticas de privacidade e de governança
- *Envolvimento do time de TI*

Analisar contratos

- Inventariar contratos que enderecem o tratamento de Dados Pessoais
- Analisar cláusulas contratuais com Titulares e Operadores
- Listar e associar terceiros envolvidos em tratamentos de Dados Pessoais
- *Envolvimento do time jurídico*

RGM TECNOLOGIA

Medidas administrativas de segurança da informação

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

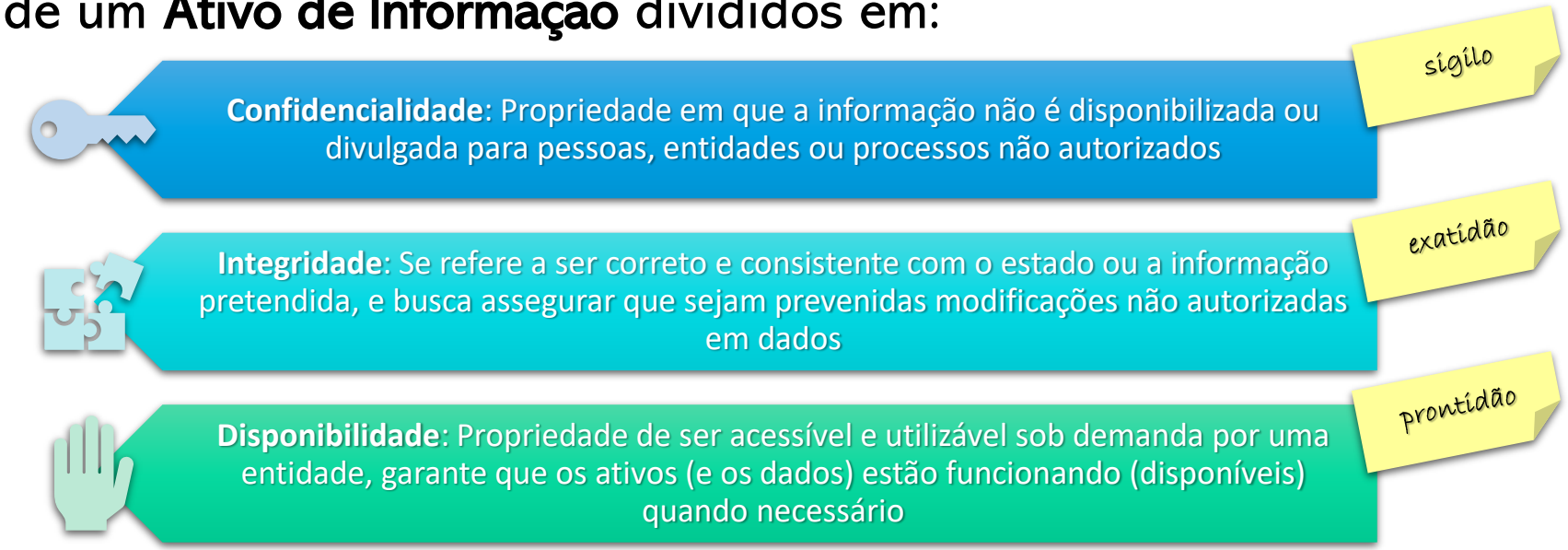
RGM TECNOLOGIA

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

Demonstração prática

RGM
TECNOLOGIA

Obrigado!

Adilson Taub Jr.

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

RGM Tecnologia

www.rgm.com.br

SCAN ME