RGM
TECNOLOGIA

Workshop LGPD

Plano de Ação para adequação à LGPD

Agenda

- O que é o Plano de Ação
- Seções e estrutura do Plano de Ação
- Quando o Plano de Ação é elaborado
- Como utilizar o LGPD Governance (PCP) para cadastrar e gerenciar o Plano de Ação

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

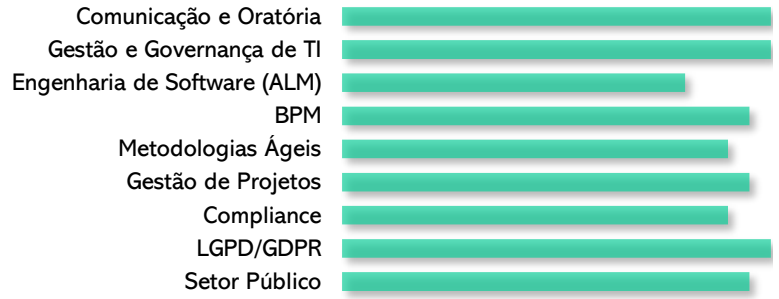
Certificações

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



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

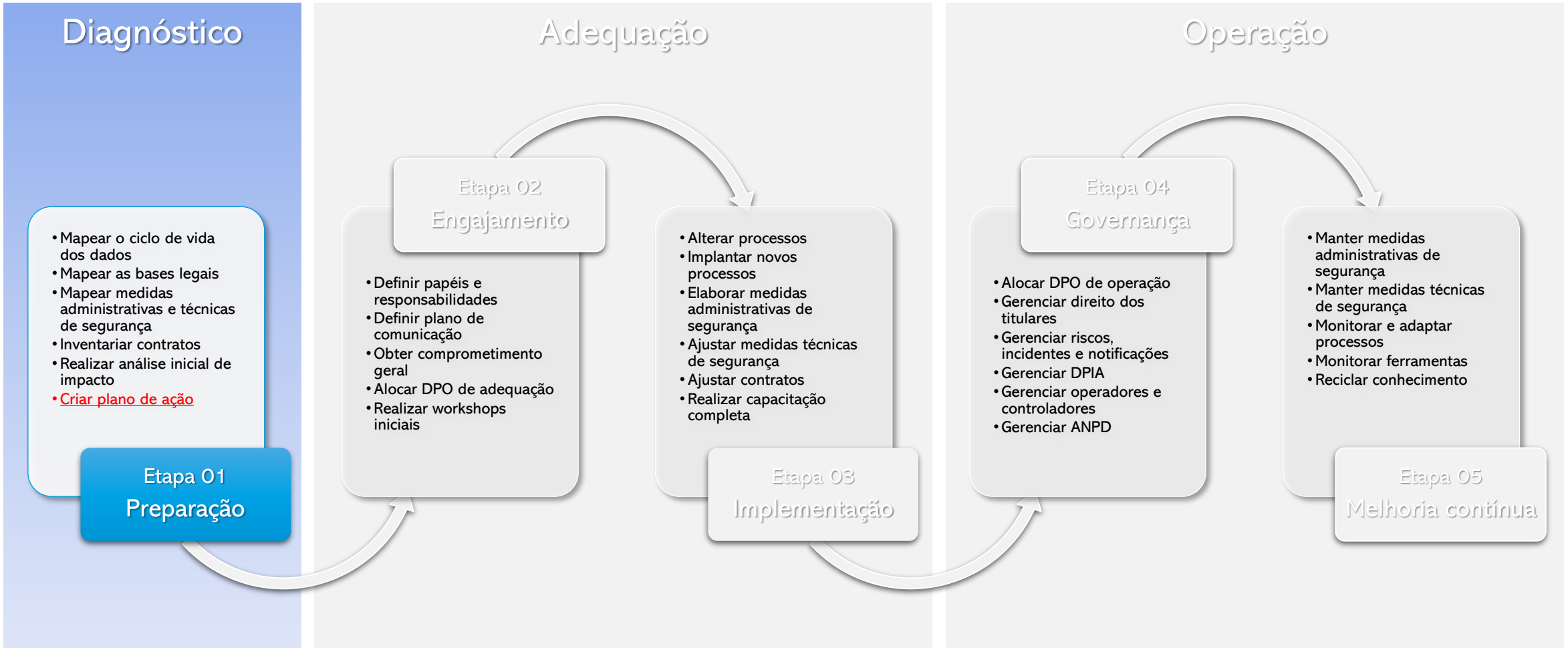
Deverá se implementar medidas administrativas e técnicas de **segurança da informação**, para garantir a **Confidencialidade**, **Integridade** e **Disponibilidade** dos Dados Pessoais que você usa

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**

RGM TECNOLOGIA

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

O Plano de Ação para adequação à LGPD

O caminho até o Plano de Ação

RGM TECNOLOGIA

O caminho até o Plano de Ação
1/6

1) Como usamos os dados pessoais?

- Informações levantadas:
  - Quais rotinas de tratamento executamos com dados pessoais
  - Quais documentos abrigam esses dados pessoais e onde eles são tratados (ativos)
  - Qual a origem e destino dos dados pessoais em tratamento
  - Quais operadores utilizamos
  - Com que compartilhamos dados pessoais
  - Qual a categoria e classificação de cada dado pessoal em uso
- Potenciais problemas encontrados:
  - Coletamos dados pessoais e não usamos (princípio da necessidade)
  - Compartilhamos dados indevidamente
  - Utilizamos operadores erroneamente

RGM TECNOLOGIA

O caminho até o Plano de Ação
2/6

2) Quais bases legais justificam o uso dos dados pessoais?

- Informações levantadas:
  - Quais hipóteses de tratamento de dados podem ser utilizadas para justificar o uso dos dados pessoais
  - Quais fundamentos legais externos podem ser utilizados para justificar o uso dos dados pessoais
  - Quais consentimentos obtemos (ou não) dos Titulares de Dados
- Potenciais problemas encontrados:
  - Fazemos uso de dados pessoais sem justificativa legal
  - Não conhecemos nossas bases ou fundamentos legais
  - Não estamos gerenciando adequadamente o consentimento dos Titulares

RGM TECNOLOGIA

O caminho até o Plano de Ação
3/6

3) O quão seguro é o uso dos dados pessoais?

- Informações levantadas:
  - Quais medidas técnicas implementamos em nossos ativos
  - Qual o nível de confiabilidade de nossos ativos
- Potenciais problemas encontrados:
  - Baixo nível de confiabilidade dos ativos de informação
  - Falta de implementação de medidas técnicas suficientes para garantir a segurança dos dados pessoais

O caminho até o Plano de Ação
4/6

4) Como estão estabelecidas nossas políticas e nossos contratos?

- Informações levantadas:
  - Quais políticas temos definidas e qual o conteúdo dessas políticas
  - Como está implementado o Comitê de Privacidade
  - Quem é nosso DPO
  - Quais cláusulas contratuais de privacidade e segurança temos definidas e qual o escopo dessas cláusulas
  - Como gerenciamos formalmente o relacionamento entre Controlador x Operador x Titulares de Dados
- Potenciais problemas encontrados:
  - As políticas não são suficientes e/ou não foram disseminadas adequadamente
  - Não temos responsáveis formais para gerenciar a privacidade e o uso de dados pessoais
  - Não formalizamos cláusulas contratuais de privacidade e segurança de dados
  - O relacionamento entre o Controlador e seus Operadores e/ou Titulares de Dados é informal

RGM TECNOLOGIA

O caminho até o Plano de Ação
5/6

5) Quais controles de governança temos implementado?

- Informações levantadas:
  - Como mantemos nossas políticas
  - Como gerenciamos riscos e incidentes de privacidade e segurança da informação
  - Como conseguimos efetuar notificações à ANPD
  - Como gerenciamos nossos consentimentos
  - Como atendemos Titulares de Dados
  - Como emitimos o DPIA
- Potenciais problemas encontrados:
  - As políticas não são controladas formalmente
  - Não gerenciamos riscos e incidentes de forma adequada e/ou completa
  - Não conseguimos notificar a ANPD e/ou Titulares de Dados em caso de incidentes
  - Não gerenciamos consentimentos adequadamente
  - Não conseguimos garantir o atendimento aos Direitos dos Titulares de Dados
  - Não somos capazes de emitir o DPIA

RGM TECNOLOGIA

O caminho até o Plano de Ação
6/6

6) Quais são os nossos riscos de privacidade e segurança?

- **Riscos operacionais**:
  - Executamos rotinas operacionais em desacordo com a LGPD
  - Temos problemas com nossas políticas
  - Temos problemas com papéis e responsabilidades
  - Temos problemas com controles de governança da LGPD (novos processos)
- **Riscos jurídicos**:
  - Não conseguimos justificar legalmente nossos tratamentos de dados
  - Temos problemas com contratos e cláusulas de privacidade e segurança da informação
  - Temos problemas de formalização da relação Controlador x Operadores x Titulares de Dados
- **Riscos tecnológicos**:
  - Temos níveis baixos de confiabilidade em nossos ativos de informação
  - Não conseguimos visualizar a Hierarquia do uso de Dados Pessoais
  - Não conseguimos implementar com facilidade os controles de governança da LGPD (novos processos)

RGM TECNOLOGIA

O que é o Plano de Ação

- **É o documento que compila todo o resultado da etapa de Preparação e define todas as ações que ainda precisam ser concluídas para garantir a adequação do Controlador à LGPD.**
  - i. **Aspectos operacionais e administrativos**: Ações que alteram rotinas operacionais e administrativas do Controlador, adequando aspectos geralmente mais associados a papéis e responsabilidades, medidas administrativas e fluxo de informação e processos;
  - ii. **Aspectos tecnológicos**: Ações que alteram requisitos de Tecnologia da Informação do Controlador, adequando aspectos geralmente mais associados parâmetros de TI de Ativos de Informação eletrônicos e medidas técnicas de segurança;
  - iii. **Aspectos jurídicos**: Ações que alteram parâmetros jurídicos, legais e/ou contratuais do Controlador, adequando aspectos geralmente mais associados a contratos, bases legais, autorizações e responsabilidades legais;
  - iv. **Aspectos evolutivos:** Sugestões para se expandir a abrangência do SGPD em implantação para outras áreas ou departamentos do Controlador.

Riscos e atividades do Plano de Ação

- O Plano de Ação deve:
  - Elencar os Riscos encontrados até então no projeto e já detalhar as estratégias de gestão de cada risco;
  - Elencar todas as atividades de adequação que deverão ser executadas até então separadas por categoria
    - **Atividades operacionais**
    - **Atividades jurídicas**
    - **Atividades tecnológicas**
  - As atividades deverão ser direcionadas aos responsáveis ideias, que sejam capazes de executá-las
  - Ser conhecido e aprovado por todos, para evitar surpresas
  - Ser completo, abrangendo todo o escopo da LGPD

RGM TECNOLOGIA

Demonstração prática

RGM
TECNOLOGIA

Obrigado!

Adilson Taub Jr.

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

RGM Tecnologia

www.rgm.com.br

SCAN ME