# Roteiro Definitivo para o Plano de Adequação à LGPD

06 de abril de 2021

# Adequação à LGPD

***- Organização***

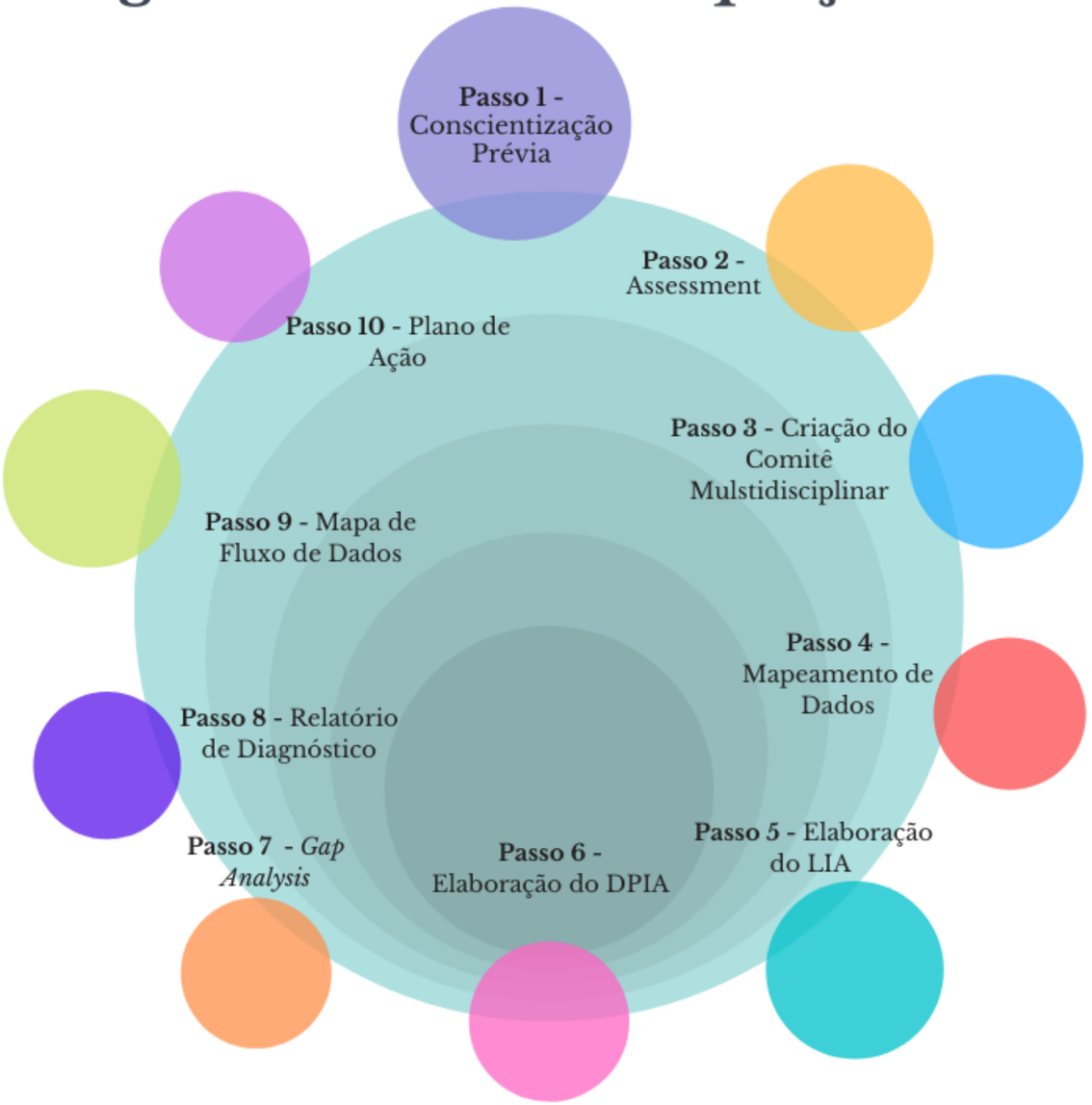
***- Preparação***

***- Desenvolvimento***

***- Implementação e Governança***

***- Monitoramento***

# Roteiro geral Plano de Adequação à LGPD




A&V CO.

## O que é Plano de Adequação à LGPD?

Um Plano de Adequação à LGPD é a fase de realização das medidas preparatórias para a implementação do Programa de Conformidade com lei.

Ou seja, ele é um projeto que contém todas as diretrizes necessárias à implementação do Programa de Governança em Privacidade e Proteção de Dados.

Será por meio das atividades contidas no Plano de Adequação que a empresa terá condições de implementar o seu Programa, e mais que isso, que dará efetividade a ele.

As informações extraídas nessa fase de planejamento e preparação, servirão de suporte para a adoção das melhores estratégias de implementação das medidas requeridas pela lei.

Todas as atividades desenvolvidas nesta fase, assim compreendida, também, a avaliação da maturidade da empresa em relação às operações envolvendo o tratamento de dados pessoais, possibilitarão à empresa uma análise mais assertiva acerca das medidas que precisará adotar para o atendimento às disposições da lei.

Assim, todas essas medidas identificadas e necessárias para a conformidade com a lei estarão dispostas no Plano de Ação e, a partir dele que, finalmente, será possível implementar o Programa de Governança em Privacidade e Proteção de Dados.

Essas medidas serão estabelecidas na última fase do Plano de Adequação - Passo 10: o Plano de Ação.

## O que é o Programa de Governança em Privacidade e Proteção de Dados?

O Programa de Governança é a fase execução de todas as medidas necessárias à conformidade da empresa que foram verificadas na fase de realização do Plano de Adequação.

Ex: elaboração e ajustes dos contratos, elaboração das políticas, implementação das medidas técnicas e de segurança da informação, elaboração do guia de boas práticas, criação do Plano de Resposta a incidentes e etc..

5 coisas que você precisa saber antes de iniciar o seu Plano de Adequação na prática?

- A adequação à LGPD é uma jornada multidisciplinar (Jurídico, TI e SI);
- Não existe LGPD na prática sem entendimento da teoria;
- Sempre se dará no caso concreto! Não existe fórmula, solução mágica que se encaixe a todas as empresas de forma idêntica;
- Não existe número de fases específico para implementação;
- Não existe implementação de uma cultura de privacidade e proteção de dados dentro da empresa sem a conscientização da alta gestão e de todos os colaboradores acerca do tema;

# Passo 1 - Conscientização prévia

**- Conscientização e apresentação do tema para a Alta Gestão - (para consultorias);**

**- Conscientização dos Colaboradores;**

**- Apresentação do tema para os titulares de dados.**

# Como fazer na prática?

## Alta Gestão

Apresentação do tema para os gestores da empresa, com enfoque nos principais pontos da LGPD, aspectos mais relevantes, maiores impactos para as empresas.

## Colaboradores

Toda a arquitetura relacionada à implementação de uma nova cultura de privacidade e proteção de dados passa pela conscientização dos colaboradores! Além disso, todos os processos envolvendo tratamento de dados pessoais passam pelos colaboradores.

## Titular de Dados

Além de atender ao princípio da boa-fé, transparência, demonstra aderência ao disposto no art.50, I,"e" (relação de confiança com o titular).

# Passo 2 - *Assessment* - Avaliação inicial

**- Pré-*Assessment*/fase de conhecimento geral acerca das atividades da empresa (questionário);**

**- Da realização do *Assessment* (diagnóstico/avaliação);**

**- Mapeamento de Dados e *Gap Analysis***

## O que é o Pré-*Assessment*?

**É uma  visão geral e estratégica acerca das operações envolvendo o tratamento de dados pessoais pela empresa de acordo com o segmento da empresa, ou seja, essa pré-avaliação consiste em uma análise acerca do modelo de negócio desenvolvido pela empresa.**

## Pré-*Assessment*

**- Envio de questionário para conhecer a empresa.**

**- Qual o segmento da empresa?**
**-- Quantos áreas envolvem tratamento de dados?**
**- Número aproximado de terceiros envolvidos no tratamento de dados pessoais?**
-

## Objetivos do Pré-*Assessment*?

**- Adoção da melhor estratégia de implementação;**

**-- estimar horas a serem trabalhadas;**

**- precificar.**

## Quando ele deve ser realizado?

Esta pré-avaliação deverá ocorrer **antes do envio da proposta para a empresa** solicitante.

# Posteriormente, ocorrerá a fase de avaliação/diagnóstico = *Assessment*

# Atividades compreendidas no *Assessment:*

## Pré-*Assessment*

Para a consultoria conhecer a empresa, porte e segmento.

## Mapeamento de Dados

O mapeamento de dados deve ser realizado por áreas e por processos.

## *Gap Analysis*

Diagnóstico de maturidade da empresa em relação à segurança das informações das quais realiza o tratamento de dados pessoais.

# Passo 3 - Criação do Comitê Multidisciplinar

**- Indicação prévia dos nomes daqueles que farão parte do Comitê Multidisciplinar;**

**- Definição do DPO (*Data Protection Officer*) ou Encarregado de Dados, com elaboração do termo para formalização);**

**- Indicação final dos colaboradores que farão parte do Comitê Multidisciplinar.**

## Reunião 1

### Composição prévia do Comitê Multidisciplinar

- Apresentação do tema e conscientização alta gestão;

- Definição do time inicial, verificação da indicação do DPO;

# Reunião 2

## Composição definitiva do Comitê Multidisciplinar

- Definição do time definitivo;

- Apoio, organização, atribuições e responsabilidades .

- Nomeação do DPO (*Data Protection Officer)* ou Encarregado de Dados.

# Passo 4 - Mapeamento de Dados - *Data Mapping LGPD*

**- Etapa obrigatória por força do art. 37 da LGPD;**

**- Necessária para o levantamento de todas as informações que serão imprescindíveis ao desenvolvimento do Plano de Adequação e, posteriormente, à implementação do Programa de Governança em Privacidade e Proteção de Dados.**

# O mapeamento deve ser feito:

*Por áreas!

*Por Processos!

*Sempre de acordo com o contexto do tratamento de dados que a empresa realiza

Muito importante: cada área deve compreender com clareza quais as leis, decretos, regulamentos que orientam a atividade à qual a sua área e atividade em geral da empresa se vincula.

## Questionário

1) Quem é a empresa Controladora?
2) Quem é o *DPO (Data Protection Officer)* ou Encarregado de Dados?
3) Qual o segmento da empresa? *(Indústria, aviação, saúde, turismo)*
4) Qual a área mapeada? *(RH, marketing, portaria, financeiro, vendas)?*
5) Qual o processo mapeado? *(folha de pagamento, recrutamento, venda em plataforma online?*
6) Quais as normas aplicáveis ao tratamento? *(Leis, decretos, regulamentos que orientam a atividade da empresa)*
7) Quais os tipos de dados coletados e tratados nesta área e processo? *(Nome,CPF, e-mail, biometria)?*
8) Qual a finalidade do tratamento?*(Qual a razão para utilização do dado)?*
9) De que forma os dados são utilizados? *(Online/meios físicos)?*
10) Qual a base legal utilizada?

# Passo 5 - Mapa de Fluxo de Dados

**- Meio visual de compreender todo o fluxo de dados que a empresa trata em cada área e em relação à cada processo**

**- Por onde os dados transitam?**

# O Mapa de Fluxos de Dados é importante para:

- Verificação visual simplificada

- Atendimento aos direitos dos titulares de modo mais efetivo

*COLETA

*ARMAZENAMENTO

*COMPARTILHAMENTO

*DESCARTE

# Passo 6 - *Gap Analysis*

- ***Gap Analysis*** **ou análise de lacunas ou brechas é o entendimento acerca do cenário real e atual** que a empresa possui em relação à privacidade e proteção dos dados dos quais realiza o tratamento;

- É um procedimento necessário para **diagnosticar a maturidade** da empresa em relação aos processos envolvendo o tratamento de dados pessoais que a empresa realiza;

- Servirá como espécie de **raio-x (antes e depois)** - Princípio da prestação de contas. Comparativo de como era e como estão os processos após a implementação das medidas.

# Análise das lacunas/brechas de segurança

- Deve ser realizado/conduzido por um profissional da área de segurança da informação e/ou TI.

- Método indicado? Questionário específico para verificação do nível de maturidade dos processos que a empresa realiza.

# Alguns questionamentos

**O que é importante saber para a realização desta análise?**

**Importante: após a realização do *Gap Analysis* deverá haver a elaboração do Relatório de Diagnóstico, com base na matriz de risco elaborada.**

**Ex: 1** A alta gestão da empresa já possui uma visão geral acerca da LGPD e consciência sobre a necessidade da adequação e da implementação de uma nova cultura de privacidade e proteção de dados?

**Ex: 2** Existe na empresa uma área específica e responsável pela segurança das informações pessoais dos titulares?

**Ex: 3** Há um plano de gerenciamento de crise. Existe algum procedimento específico para a ocorrência de um incidente de segurança e/ou vazamento de dados?

**Ex: 4** Quais os principais riscos identificados?

# Passo 7 - Relatório de Diagnóstico

- Documento contendo todas as conclusões das fases mapeamento de dados + *Gap Analysis.*

# Exemplos do que deve constar no relatório:

A **primeira referência** aborda o **cenário atual da empresa em relação à privacidade e proteção de dados** em um contexto geral.

A **segunda abordagem** se refere à **existência de pontos crítico**s relacionados à privacidade e segurança na empresa

**Terceira abordagem** diz respeito aos **aspectos relacionados às melhorias que poderão ser implementadas para garantir a privacidade e a proteção dos dados** dos usuários titulares dos dados.

Na quarta referência o relatório mencionará os **objetivos da empresa quanto à privacidade e proteção dos dados** dos usuários.

Após, haverá menção a **todas as leis e regulamentos que orientam a atividade realizada pela empresa** nas atividades relacionadas ao tratamento de dados.

E, por fim,  a **referência a todas as medidas que devem ser implementadas a curto, médio e longo prazo.**

**Será com base no Relatório de Diagnóstico que teremos informações para as estratégias do Plano de Ação.**

# Passo 8 - LIA *(Legitimate Interest Assessment)*

- Teste de ponderação ou proporcionalidade;

- É um teste destinado à verificação da viabilidade da utilização da base legal do Legítimo Interesse.

**Quando o teste deve ser realizado?**

**Sempre que o Controlador utilizar a base legal do Legítimo Interesse para justificar alguma operação envolvendo o tratamento de dados pessoais.**

***Importante: o objetivo do teste é fazer um balanceamento entre os interesses legítimos do controlador e os direitos e liberdades fundamentais dos titulares de dados.***

## O que avaliar no LIA?

- Qual a finalidade do tratamento?

- Quais os dados tratados?

- Legitimidade do Interesse (finalidade legítima e situação concreta);

- Necessidade (minimização e existência de outras bases legais);

**- Balanceamento (legítima expectativa, direitos e liberdades fundamentais);**

**- Salvaguardas (transparência e mecanismos de oposição opa-out, mecanismos de mitigação de riscos).**

***Importante: a reprovação em uma das fases inviabiliza a legitimação do tratamento por meio desta base legal.***

# Passo 9 - DPIA *(Data Protection Impact Assessment)*

**- Relatório de Impacto à Proteção de Dados Pessoais.**

**- Art. 5º. Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: 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 riscos.**

**- Art.10 § 3º. A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.**

**Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.**

***IMPORTANTE: é recomendável que o Controlador elabore o DPIA sempre que legitimar o tratamento de dados por meio da base legal do legítimo interesse ou quando estiver tratando dados pessoais sensíveis.***

***Que tal pecarmos pelo excesso?***

# Passo 10 - Plano de Ação

**- Plano contendo todas as informações necessárias à adoção das medidas a serem implementadas.**

**O Plano de Ação é uma forma de organizar a sequência de ações de modo planejado para a obtenção dos resultados esperados, seguindo uma metodologia com metas e objetivos bem delineados, de modo a verificar, de forma clara e objetiva, quais são as tarefas a serem desenvolvidas, apontando as prioridades, necessidades prévias, bem como os responsáveis por desenvolver cada das tarefas nele dispostas, bem como acompanhar o andamento do projeto, a fim de que se possam obter os resultados desejados.**

**Em outras palavras, o objetivo do Plano de Ação é de um planejamento estratégico de trabalho, visando a elaboração de um trabalho em equipe de forma ordenada, respeitando os prazos e cumprindo cronogramas estabelecidos.**

**Será no Plano de Ação  que todas as informações levantadas nas fases anteriores serão traduzidas em medidas de urgência baixa, média e alta.**

**No Plano de Ação haverá a determinação acerca das medidas que deverão/poderão ser implementadas a curto, médio e longo prazo, bem como a definição da melhor estratégia.**

***IMPORTANTE: todas as medidas necessárias e descritas no Plano de Ação é que darão suporte à implementação do Programa de Governança em Privacidade e Proteção de Dados.***

***Lembre-se: todas as atividades do Plano de Ação são de preparação, enquanto o Programa de Governança em Privacidade e Proteção de Dados é a fase de efetiva execução de todas essas medidas, é nesta fase que a conformidade ganha a forma.***

# Querem uma live sobre o Programa de Governança com *checklist e* passo a passo?

O que eu preciso?

1.Que vocês se inscrevam na news do Implementando a LGPD!

2. Que indiquem a live para 10 pessoas e que essas 10 pessoas se inscrevam na news!

3. Que se inscrevam no nosso canal aqui no Youtube e ativem o sininho!

4. Que nos sigam no Facebook e no Instagram!

# Todos os links estarão no descritivo do vídeo!

@Implementandoalgpd
www.implementandoalgpd.com.br