INTE
GRI
DADE

PROTEÇÃO
DE DADOS

Pratique integridade, faça a diferença.

ROADMAP

ICTS protiviti

FIEMG

INTRODUÇÃO

- O Desenvolvimento de um *roadmap* busca trazer direcionamento para implantação de ações voltadas à implementação e sustenção do Programa de Privacidde nas organizações, bem como mitigar riscos relacionados ao tratamento de dados pessoais e evitar o uso indevido e/ou vazamento de informações.

- O *roadmap* é a estruturação dos planos de ação para adequação da organização às exigências da LGPD e deve ser elaborado considerando todas as atividades de correção ou adequação identificadas na etapa de diagnóstico. As ações devem ser estruturadas de acordo com a priorização de execução e devem ser definidos os prazos para realização, bem como os responsáveis por cada atividade estabelecida.

- Para que o desenvolvimento do *roadmap* esteja de acordo com as necessidades da organização, seu modelo de negócios e sua área de atuação, é fundamental que um diagnóstico seja realizado com o detalhamento e a acuracidade necessários para a análise adequada de todos os processos das diferentes áreas da organização.

- O diagnóstico deverá contemplar as análise de todas das atividades com tratamento de dados pessoais em relação às exigências da LGPD, identificação dos *gaps*, atribuição das bases legais, definição das ações de adequação e o estabelecimento de controles específicos para atividades críticas da organização.

INTRODUÇÃO

- É fundamental que o responsável pelo projeto de adequação consiga envolver toda a organização, de forma a promover o engajamento em todas as fases, ou seja, do levantamento de informações à execução das ações de adequação estabelecidas.
- O desenvolvimento de uma matriz de esforço e benefício será fundamental para identificar ações críticas, sendo possível estabelecer a prioridade na implementação. Será importante, também, para auxiliar no direcionamento dos recursos necessários para implementação e no estabelecimento um Programa de Privacidade para garantir a sustentação e continuidade das ações que manterão a organização em conformidade com a LGPD.
- Com roadmap estruturado, todas as ações para adequação estarão organizadas e os próximos passos estarão planejados de forma a possibilitar o conhecimento de todo o esforço necessário para que a organização esteja em conformidade com a LGPD e também será possível definir tempo, custo e pessoal a ser alocado nesse processo.
- A implementação deverá considerer o acompanhamento ou monitoramento da execução, bem como da efetividade das ações de adequação.
- Todas as etapas do processo devem ser devidamente registradas para atendimento ao princípio da Responsabilização e Prestação de Contas, previsto no artigo 6º da LGPD, e possibilitar a “demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados e, inclusive, da eficácia dessas medidas”.

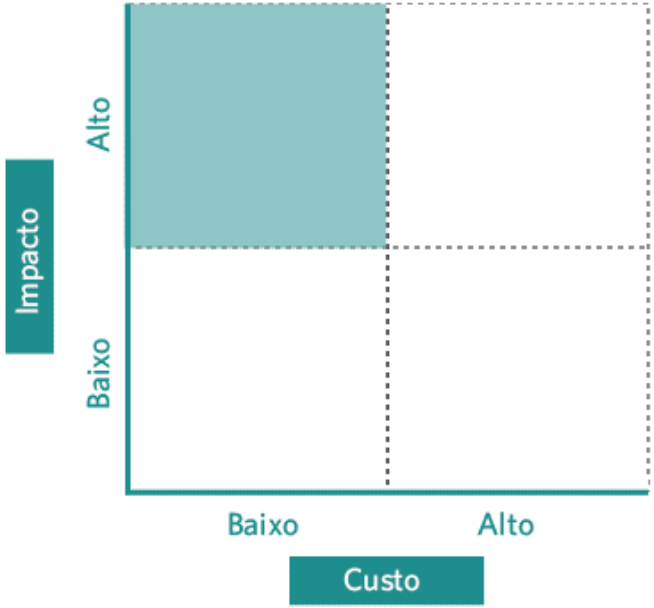
O QUE É NECESSÁRIO ANTES DE INICIAR?

- Conhecer a LGPD e compreender a necessidade de adequação pelas organizações
- Conscientizar a Alta Administração
- Conscientizar os colaboradores da organização
- Avaliar o nível de adequação da organização à LGPD
- Realizar do levantamento e mapeamento dos processos que tratam dados pessoais
- Executar a análise dos processos e identificação de *gaps* em relação às exigências da LGPD
- Realizar a avaliação de riscos relacionados à proteção de dados
- Estabeler as ações de adequação e/ou correção e definição dos planos de ação, com base nas prioridades da empresa, e por meio da estruturação de uma matriz de esforço benefício

MATRIZ DE ESFORÇO E BENEFÍCIO

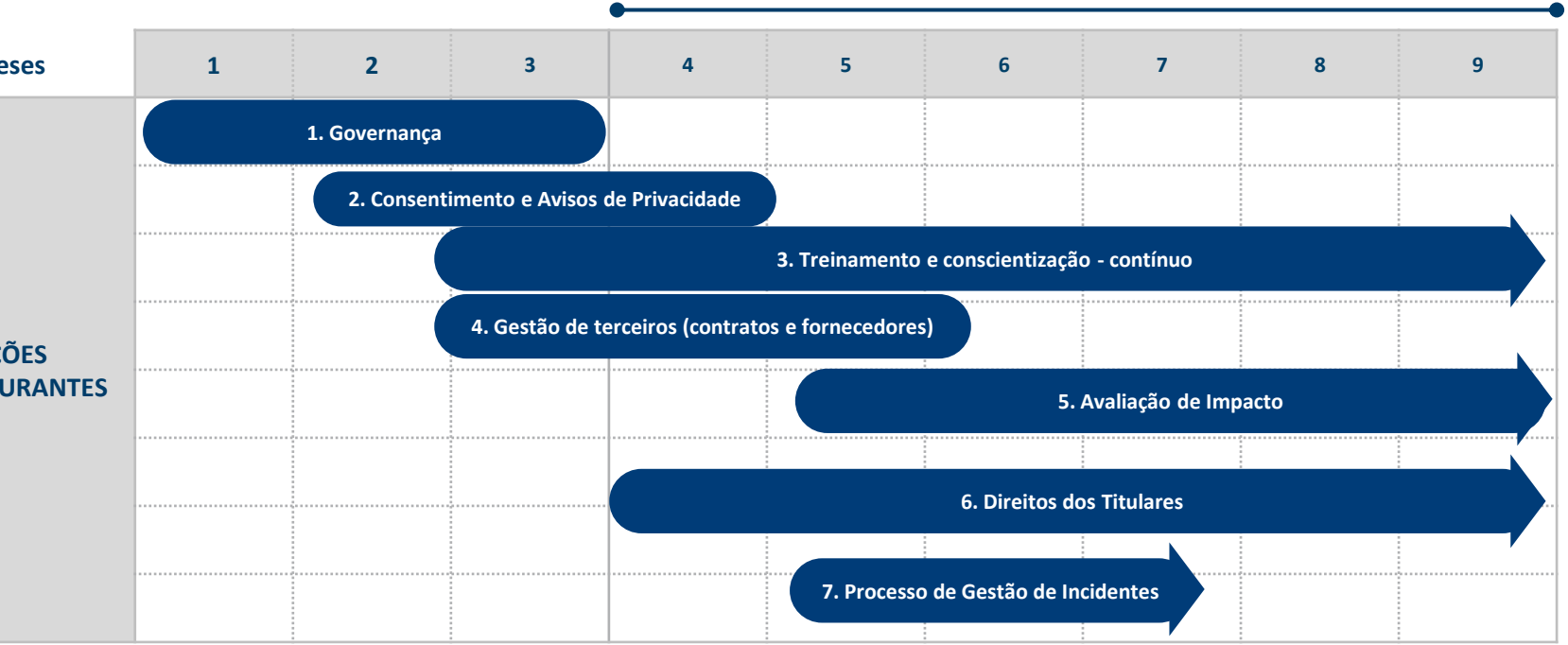
- Para estabeler as ações de adequação e/ou correção de maneira criteriosa e priorizada é fundamental que a organização estruture uma matriz de esforço/ complexidade e benefício.
- Considerando que as organizações são diferentes, atividades que parecem similares podem ter esforço e complexidade diferentes a depender da estrutura e disponibilidade de recursos da organização.
- Além disso, a organização deve estabelecer de maneira priorizada as ações para reduzir os riscos relacionadas a LGPD:
  - Estruturar uma análise pareto (20% das ações cobrem 80% do problema).
  - Projetar as ações para cobrir riscos críticos no início da implantação.

Exemplo de matriz, no qual podem ser populadas as ações para desenvolvimento*:



* Fonte: https://m.sebrae.com.br/sites/PortalSebrae/artigos/matriz-de-foco-como-priorizar-as-acoes-de-maior-impacto,3dfeaa7dab90d510VgnVCM1000004c00210aRCRD

ROADMAP PADRÃO (1 DE 2)



ROADMAP PADRÃO (2 DE 2)

Meses	1	2	3	4	5	6	7	8	9
AÇÕES ESPECÍFICAS	8. Mapeamento das atividades de processamento de dados pessoais - ROPAs				9. Atualização dos ROPAs				
					10. Implantação e testes de controles de atividades críticas				
MANUTENÇÃO DO PROGRAMA					11. Manutenção do Programa				

ROADMAP - Ações Estruturantes (1/3)

Etapas	O que recomendamos?	Direcionamento
1. Governança	• Definir quem será o Encarregado e realizar capacitação em privacidade e proteção de dados; • Comunicar e conscientizar as áreas sobre seus papeis e responsabilidades em relação ao Programa de Privacidade; • Viabilizar e patrocinar a implementação dos processos relacionados a LGPD na organização; • Revisar demais documentos corporativos (contratos e políticas) para contemplar diretrizes de Privacidade e Proteção de Dados.	Estabelecer o papel de Encarregado pelo tratamento de dados pessoais e incorporar formalmente as atividades na descrição de cargo.
2. Consentimento e Avisos de Privacidade	• Estruturar diretrizes de registro de consentimento considerando: dado coletado, finalidade, nome do controlador, terceiros envolvidos no tratamento e condições de revogação; • Estruturar um processo/infraestrutura de gestão de consentimento, para gerenciar o *opt-in* e *opt-out* (solicitação de cadastramento e descadastramento) em todas as plataformas, registrando as evidências das solicitações (*opt-in/opt-out*) dos titulares; • Comunicar e realizar a gestão de Cookies em todas as plataformas e sites, via barra de Cookies, possibilitando a permissão ou não do usuário em relação à coleta de determinados cookies; • Incluir as informações relacionadas a consentimento e cookies nas políticas e avisos relacionados à proteção de dados e privacidade, ou criar políticas específicas para os temas.	Implantar barra de Cookies contendo preferências, direitos e solicitações, contatos de privacidade (Encarregado) e política de privacidade

ROADMAP - Ações Estruturantes (2/3)

Etapas	O que recomendamos?	Direcionamento
3. Treinamento e Conscientização	• Elaborar e executar treinamento da política de Privacidade e Proteção de Dados para todos os colaboradores, promover a cultura e privacidade na empresa e disseminar as diretrizes e comportamentos e esperados; • Disponibilizar verba para cursos, livros e materiais de capacitação em Privacidade e Proteção de dados para o Encarregado e/ou equipe designada para suporte ao Programa de Privacidade.	Criar rotina de treinamentos da Política de Privacidade para todos colaboradores. Recomenda-se curso de *Exin Essentials* para Encarregado e profissional de TI.
4. Gestão de Terceiros (Contratos e Fornecedores)	• Revisar termos contratuais com fornecedores (se aplicável) para incluir os aspectos de Segurança da Informação, Privacidade e Proteção de Dados; • Definir processo de gestão de fornecedores para classificação de riscos relacionados ao tratamento de dados pessoais; • Criar procedimento de *Due Diligence* visando mitigação de riscos relacionados a Privacidade e Proteção de Dados para fornecedores críticos; • Revisar documentação trabalhista, políticas internas, códigos de conduta e acordos de não divulgação;	Revisar os contratos com os prestadores de serviços relacionados às atividades de maior relevância.

ROADMAP - Ações Estruturantes (3/3)

Etapas	O que recomendamos?	Direcionamento
5. Avaliação de Impacto	• Definir e formalizar critérios para elaboração de *DPIA (Data Protection Impact Assessment)* - ou RIPD (Relatório de Impacto à Proteção de Dados); • Elaborar *DPIA* para todas as atividades com atribuição de base legal de legítimo interesse; • Definir um processo de endereçamento e cronograma de execução de planos de ação para mitigação dos riscos levantados nos Relatórios de Impacto.	Realizar os relatórios de impacto para o legítimo interesse atribuído pelo advogado às atividades de tratamento.
6. Direitos dos Titulares	• Estabelecer processo para o tratamento dos direitos dos titulares de dados quanto a: confirmação, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, revogação de consentimento, compartilhamento, explicação, oposição e revisão de decisão automatizada; • Definir critérios para avaliação das solicitações de dados pelo titulares e bases legais para aceitar e declinar solicitações; • Designar indivíduos e/ou áreas responsáveis para suportar as solicitações dos titulares de dados pessoais; • Definir procedimentos e avaliar a aquisição de ferramentas para registro e gestão de solicitações, assegurando que sejam geradas as evidências quem possam se fazer necessárias em momento posterior.	Adotar ferramenta para gestão do atendimento aos direito dos titulares, considerando toda a dinâmica envolvida (recomenda-se ferramenta Plataforma de Gestão de Consentimento - CMP).
7. Gestão de Incidentes	• Estruturar um processo de gerenciamento de incidentes relacionados à proteção de dados pessoais em linha com as diretrizes definidas pela ANPD	Utilizar como fonte as diretrizes definidas pela ANPD

ROADMAP - Ações Específicas

Etapas	O que recomendamos?	Direcionamento
8. Mapeamento das atividades de processamento de dados pessoais - ROPAs	• Realizar o mapeamento das atividades que envolvem tratamento de dados pessoais, por meio de entrevistas ou workshops de levantamento junto aos donos dos processos e áreas foco. • Estruturar o inventário com todas as atividades de tratamento de dados pessoais. • Elaborar os relatórios de atividade de processamento, os ROPAs (Records of Processing Activities), ou Registros de atividades de processamento. Tal documento dever conter o descritivo da atividade, sua finalidade, elementos de dados coletados, dono do processo e base legal para o tratamento de dados pessoais.	Utilizar como base o anexo A1 – "Modelo de ROPA".
9. Atualização dos ROPAs	• Estabelecer processo de atualização contínuo dos ROPAs, dada as mudanças constantes na organização. A atualização se faz necessária, visto que processos, atividades e sistemas são inseridos, alterados e substituídos e a atualização se faz necessária dada este fato. • Comunicar e garantir a interação junto às áreas de negócios para as atualizações ocorram no tempo adequado.	Comunicar e interagir continuamente com as áreas de negócios para que as atualizações sejam feitas no timing adequado
10. Implantação de controles de atividades críticas	• Estruturar e implantar controles de mitigação de riscos em atividades que são críticas para o negócio. • Suportar as áreas de negócios na implantação dos controles definidos para atividades de tratamento de dados pessoais críticas • Definir rotina de testes dos controles, promovendo a mitigação contínua dos riscos relacionados a proteção de dados pessoais.	Definir controles para utilização dos dados pessoais em linha com as finalidades definidas pelos ROPAs.

ROADMAP – Manutenção do Programa

Etapas	O que recomendamos?	Direcionamento
11. Manutenção do Programa	• Definir rotinas de atualização dos ROPAs • Manter e avaliar indicadores de atendimento aos direitos dos titulares • Avaliar continuamente o processo de consentimento e se as atividades de tratamento que utilizam o consentimento como base legal, estão sendo realizadas com base em linha com as exigências da LGPD. • Realizar continuamente, programas de conscientização junto aos colaboradores para apresentar os riscos, impactos e benefícios que a LGPD traz. • Realizar processo contínuo de avaliação do *Privacy by Design* (privacidade desde a concepção) e Privacy by Default (privacidade por padrão). • Avaliar se Data Discovery de dados é necessário para complementar o inventário de atividades de processamento. • Estabelecer rotina de revisão das políticas e normas de privacidade e segurança de informações. • Avaliar de forma contínua e/ou periódica os fornecedores e terceiros que tratam dados pessoais em nome da empresa, e se este também tem um programa de privacidade de dados e cybersegurança para atender à LGPD.	Estruturar processos e rotinas para manutenção e elevação da maturidade do programa em linha as exigência da LGPD.

INTEGRIDADE

PROTEÇÃO DE DADOS

Pratique integridade, faça a diferença.

ICTS protiviti

FIEMG