INTE
GRI
DADE

PROTEÇÃO
DE DADOS

Pratique integridade, faça a diferença.

ICTS protiviti® FIEMG

GUIA FAÇA VOCÊ MESMO:

diagnóstico, planejamento e desenvolvimento

INTRODUÇÃO

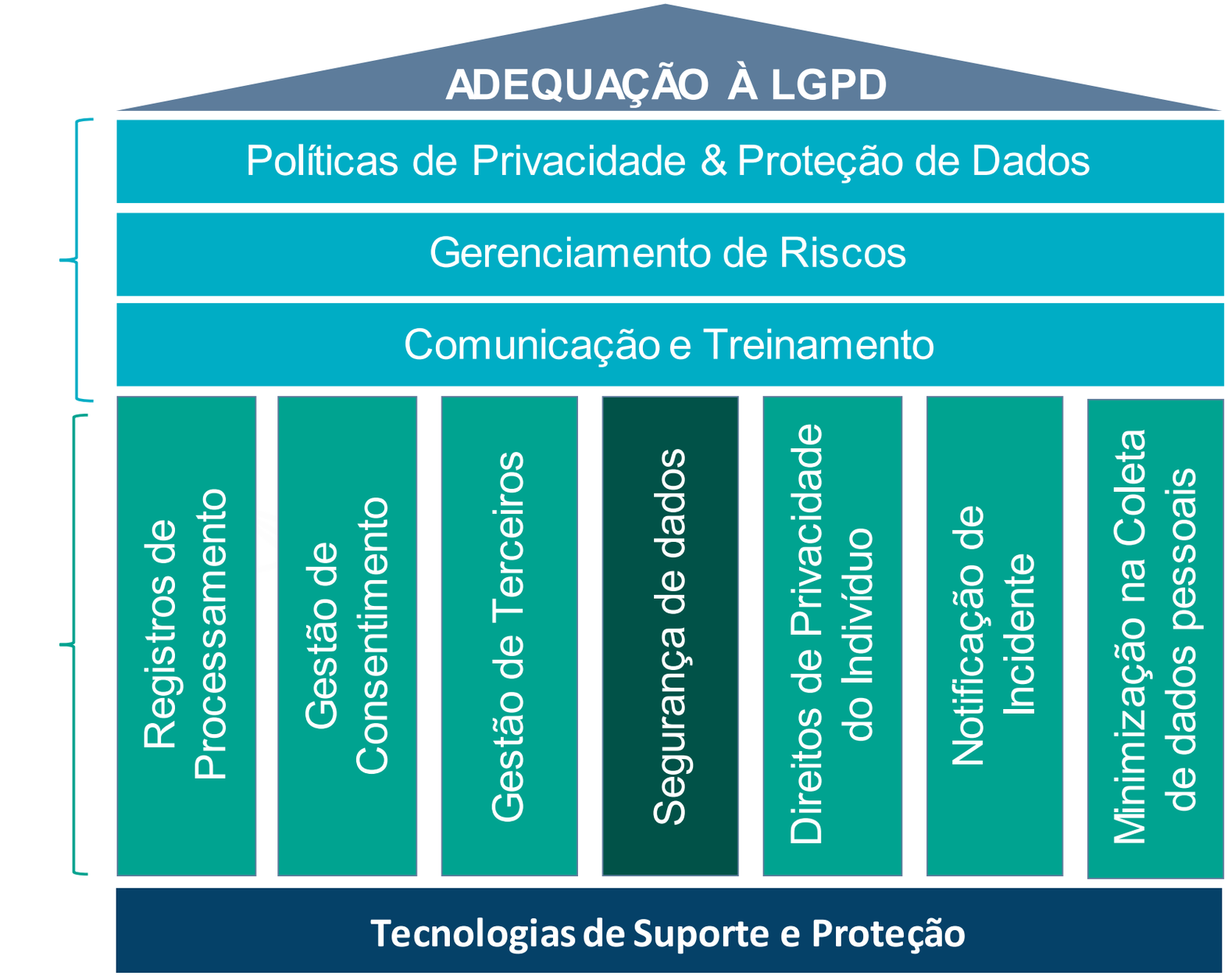
Realizar a adequação do ambiente organizacional às regras de proteção de dados vigentes desde a promulgação da lei 13.709/18, também conhecida como Lei Geral de Proteção de Dados (LGPD), é um dos principais desafios das organizações atualmente.
Tendo isso em vista, desenvolvemos um guia prático para ajudar as organizações à:

Alcançar um nível mínimo de conformidade com a LGPD;
Iniciar/adequar os processos e operações compatíveis com LGPD;
Reduzir o risco de sanções, penalidades ou processos legais relacionados à LGPD.

Vale ressaltar, que este é um guia orientativo para que gestores, responsáveis pelo tema proteção de dados pessoais, possam ter um direcionamento das ações necessárias para colocar em prática um programa de conformidade à lei em questão.
É importante que tais gestores dediquem esforço para implantação, com foco no modelo de negócios da organização e setor de atuação, sempre avaliando seus riscos, com suas peculiaridades e disponibilidade de investimentos que possui.

Sucesso na implantação!

PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS



PROGRAMA DE PRIVACIDADE
PASSOS PARA A CONFORMIDADE

Estabelecer um inventário formal das atividades de tratamento de dados e sistemas de apoio que recolhem, processam e armazenam dados pessoais.

Implementar ações estruturantes para adequação à LGPD, como a elaboração da Política de Privacidade e Relatórios de Impacto, Gestão do consentimento, Atendimento ao direito dos titulares e Gestão de Terceiros.

Monitorar a conformidade com a LGPD, por meio da adoção de indicadores e avaliação periódica dos processos de privacidade implementados.

Revisar o programa anualmente para atualizar documentos, políticas e processos, garantindo a adequação à LGPD.

INTE
GRI
DADE

PROTEÇÃO
DE DADOS

Pratique integridade, faça a diferença.

ICTS protiviti® FIEMG

GUIA DE ADEQUAÇÃO À LGPD

ETAPAS:

Diagnóstico, Planejamento e Desenvolvimento

Mapear áreas e
unidades de negócios

Realizar um inventário de
atividades de tratamento

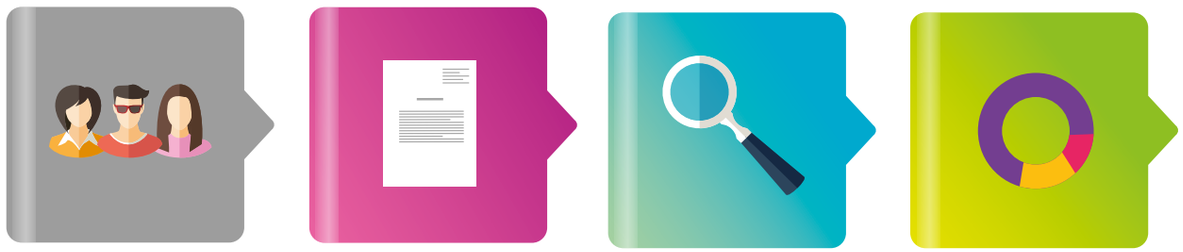
Apontar os riscos e gaps
relacionados a LGPD

Definir o plano de ação
para adequação da empresa

INTEGRIDADE

MAPEAR ÁREAS E UNIDADES DE NEGÓCIOS

ICTS protiviti® FIEMG



Identificação das áreas que realizam tratamento de dados pessoais dentro da empresa (ex. RH, Marketing, TI, Jurídico, Compras);

Levantamento dos ativos de TI (Sistemas, ferramentas etc.), bem como seu armazenamento como nuvem, on premisse ou estação de trabalho;

Mapeamento dos principais fornecedores para os quais a empresa envia ou recebe dados pessoais.

REALIZAR UM INVENTÁRIO DE ATIVIDADES DE TRATAMENTO

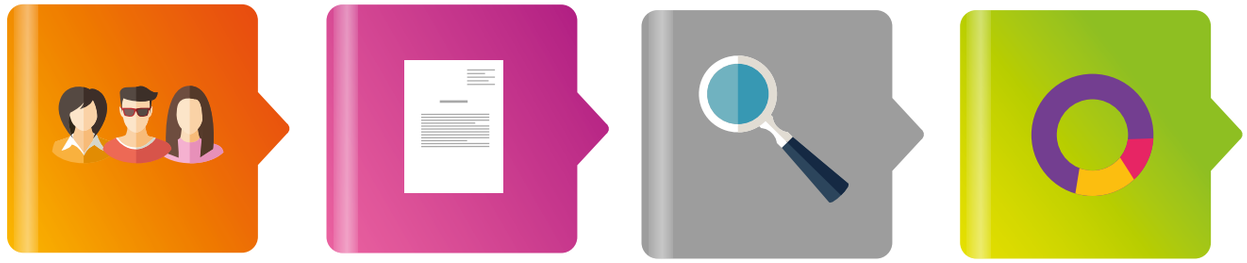
Realizar entrevistas com os responsáveis pelos processos nas áreas corporativas e de negócio que tratam dados pessoais, tais como tais como TI, RH, Financeiro, Jurídico, Comercial etc..

Formalizar as atividades que tratam dados pessoais, por meio da elaboração dos registros de atividades de processamento de dados pessoais *(ROPAs - Record of Processing Activities);*

Atribuir bases legais para os registros de tratamento, com o apontamento dos gaps jurídicos;

Mapear e desenhar os fluxos de tratamento de dados pessoais, considerando quem é o titular de dados, quais dados pessoais são utilizados, qual a finalidade do tratamento, em quais sistemas os dados transitam, se estes são compartilhados com outras áreas da organização, órgãos reguladores, fornecedores etc..

REALIZAR UM INVENTÁRIO DE ATIVIDADES DE TRATAMENTO



Quem envia o dado?

Como esse dado chega até sua área?

Diretamente do titular ou via terceiro

Planilha por e-mail, documento no drive, Papel, pen drive.

Qual a finalidade do tratamento?

Como o dado é armazenado?

No e-mail, desktop, rede/diretórios,

arquivo físico, sistemas

A quem é destinado esse dado?

Como se dá o envio ou acesso a esse dado?

Órgãos públicos, terceiros, fornecedores,

outras áreas de empresa

Envio/acesso fora do país Maios de envio e controle de acesso:

sistema, e-mail, senhas, criptografia

Como o dado é arquivado, descartado

apagado após o tratamento?

Permanece no sistema? Há backup?

É deletado, rasgado ou destruído?

REALIZAR UM INVENTÁRIO DE ATIVIDADES DE TRATAMENTO

ICTS protiviti® FIEMG

O registro de processamento de atividade (ROPA), deve conter minimamente as seguintes informações de forma clara:

Identificador da atividade: inserir um identificador numérico ou alfanumérico único para cada atividade;
Nome da atividade: inserir o nome da atividade;
Nome da Empresa;
Nome da área: inserir o nome da área da organização que a atividade é realizada;
Responsável: indicar o responsável pela atividade;
Descrição: descrever de forma detalhada a atividade;
Finalidade: inserir o resumo da finalidade da atividade de tratamento dos dados;
Titular: informar os tipos de titulares (ex: cliente, fornecedor, empregado, aluno etc.);
País do Titular: Indicar o país a que pertence os titulares dos dados;
Volumetria de Titulares: indicar nas faixas estabelecidas, qual o volume/quantidade de titulares de dados envolvidos na atividade de tratamento. A classificação deverá seguir conforme o range abaixo:

1 a 100 dados pessoais – Baixo
101 a 10.000 dados pessoais – Médio
10.001 a 100.000 dados pessoais – Alto
Acima de 100.000 de dados pessoas – Extremo

REALIZAR UM INVENTÁRIO DE ATIVIDADES DE TRATAMENTO

Tipos de dados pessoais: relacionar os tipos de dados pessoais e/ou sensíveis envolvidos na atividade de tratamento (ex: nome, identidade, placa de carro, e-mail, endereço IP, geolocalização, filiação partidária etc.);

Recursos de informação relacionados: relacionar os recursos (sistemas, aplicações, documentos físicos, tipos de documento digital – pdf, word, excel, txt) que contenham dados pessoais e são utilizados na atividade de tratamento;

Agente de Tratamento: Indicar qual o papel da organização, enquanto agente de tratamento dos dados: Controlador ou Operador;

Países de tratamento: identificar os países que estarão envolvidos na atividade executada;

Origens dos dados: identificar a forma como o dado do titular é coletado (se coletado diretamente do titular ou enviado por fornecedor/parceiro);

Método de transferência (origens): indicar os sistemas/aplicações de onde os dados dos titulares são transferidos;

Destinos dos dados: indicar para onde os dados são transferidos/compartilhados; Método de transferência (destinos): indicar os sistemas/aplicações para onde os dados pessoais serão transferidos;

REALIZAR UM INVENTÁRIO DE ATIVIDADES DE TRATAMENTO

ICTS protiviti® FIEMG

Acesso ou utilização dos dados: identificar as áreas ou partes envolvidas no processo que terão acesso aos dados dos titulares utilizados na atividade (ex: parceiros de negócios, auditores internos ou externos, agências externas, outras áreas da organização, autoridades etc.)

Localização de partes envolvidas: relacionar os países onde estão localizadas áreas ou partes envolvidas na atividade;

Órgão de Controle: identificar as entidades ou órgãos públicos ou não que podem fiscalizar, autuar ou regulamentar a atividade;

Fornecedores: identificar os fornecedores que estejam envolvidos com a atividade;

Atividades de tratamento relacionadas: indicar, se houver, outras atividades da organização que façam parte do processo ou tenham relação com a atividade de tratamento que está sendo documentada (ex: execução da folha de pagamentos pelo RH tem relação com a atividade da área financeira de efetivar pagamentos de empregados, a atividade de cobrança da área Financeira tem relação com a atividade de vendas da área Comercial etc.);

Retenção de dados: Informar o prazo pelo qual os dados utilizados na atividade são mantidos na Organização;

Atribuição de base legal: atribuir a base legal para tratamento de acordo com a finalidade da atividade.

INTEGRIDADE

DIAGNÓSTICO – APONTAR OS RISCOS E GAPS RELACIONADOS A LGPD

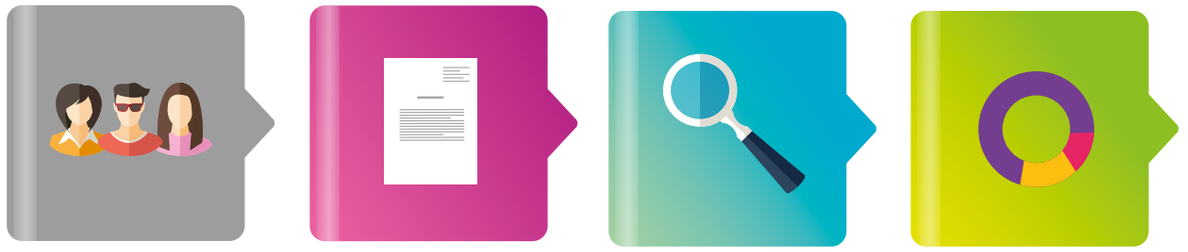
ICTS protiviti®

FIEMG

- Vazamento de dados pessoais
- Tratamento indevido de dados dos titulares

DIAGNÓSTICO – APONTAR OS RISCOS E GAPS RELACIONADOS A LGPD

Mapear os principais riscos relacionados à LGPD e, para cada risco, definir a probabilidade e impacto da materialização do Risco.



PROBABILIDADE DE OCORRÊNCIA

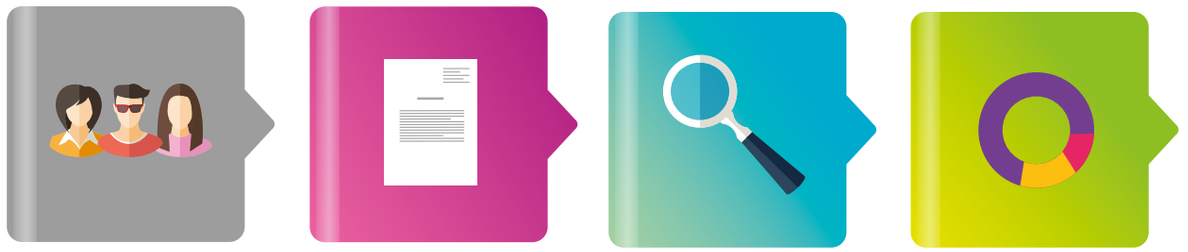
É a chance de um gap ser explorado ou a ocorrência de um evento ou conjunto de eventos materializar um risco

IMPACTO DA MATERIALIZAÇÃO DO RISCO

É a consequência para a organização:
Mensurável, quantitativo
(perda de receita, valor de mercado;
Não mensurável, qualitativo
(reputação, valor da marca).

A combinação entre a probabilidade e o impacto qualifica o risco potencial ao qual a organização está exposta, em termos de criticidade.

DIAGNÓSTICO – APONTAR OS RISCOS E GAPS RELACIONADOS A LGPD



RISCOS

Definir riscos críticos para adequação à LGPD. Abaixo, dois riscos devem ser identificados no processo de adequação, em linha com os princípios da lei:

Risco de vazamento de informações;
Risco de tratamento indevido de dados.

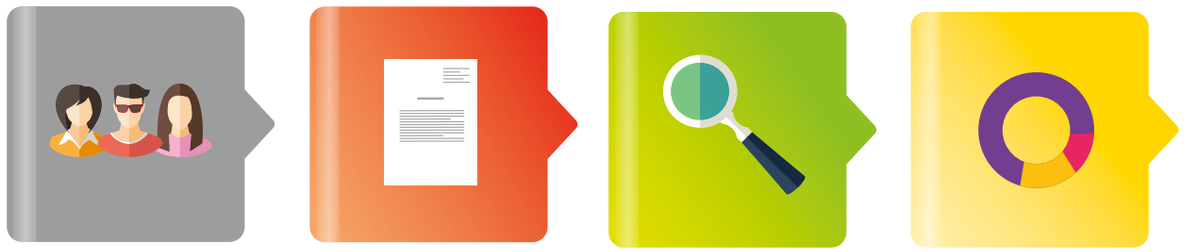
IMPACTOS

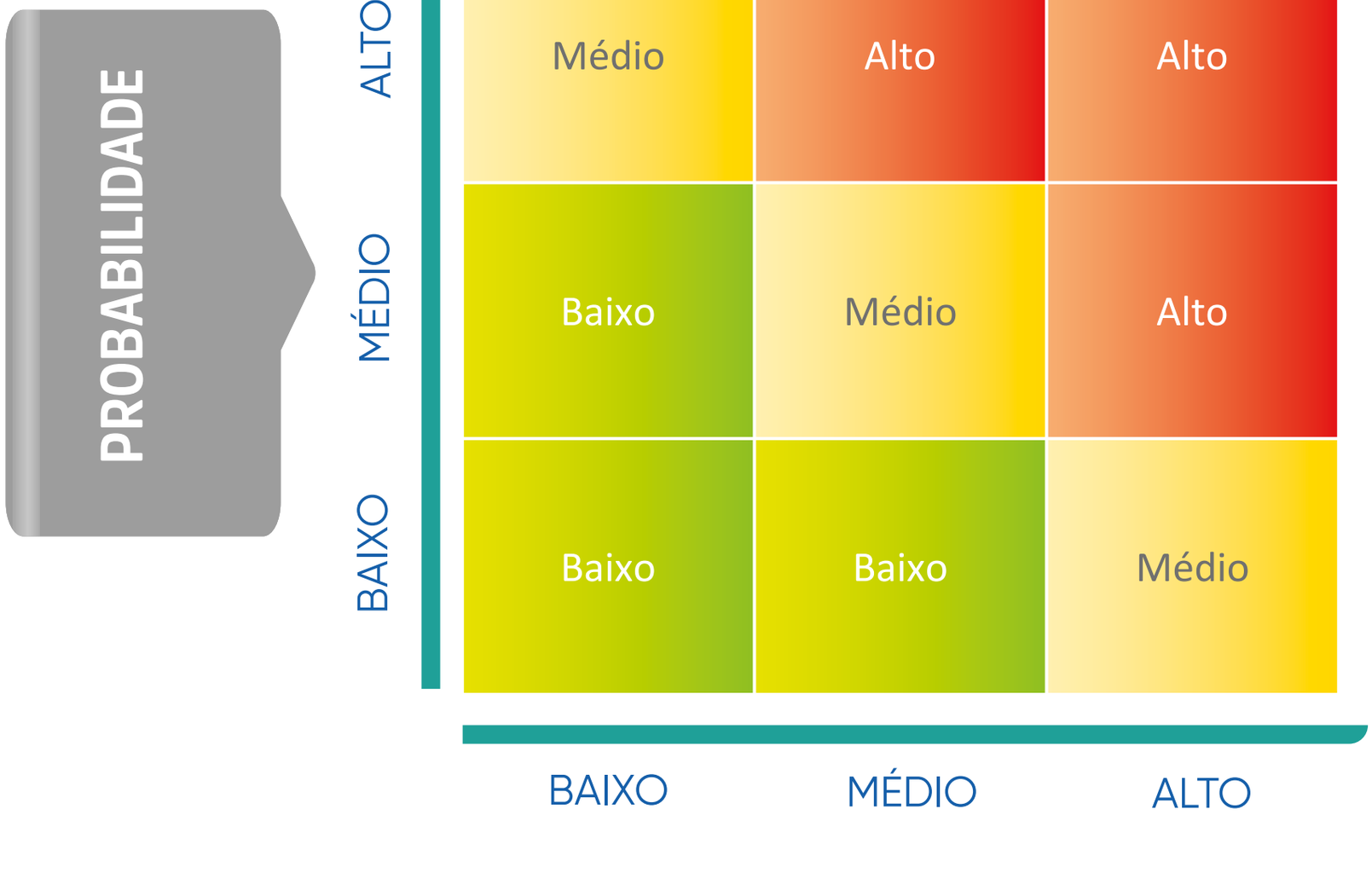
Sanções aplicadas pela ANPD;
Aumento do contencioso, devido a eventuais ações movidas pelos titulares de dados;
Atuação ativa de órgãos reguladores;
Danos à reputação da organização.

A combinação entre a probabilidade e o impacto qualifica o risco potencial ao qual a organização está exposta, em termos de criticidade.

DIAGNÓSTICO – APONTAR OS RISCOS E GAPS RELACIONADOS A LGPD

A partir da classificação de probabilidade e impacto, os riscos e gaps identificados devem ser posicionados na matriz e receber a classificação de relevância.





DEFINIÇÃO DO PLANO DE AÇÃO

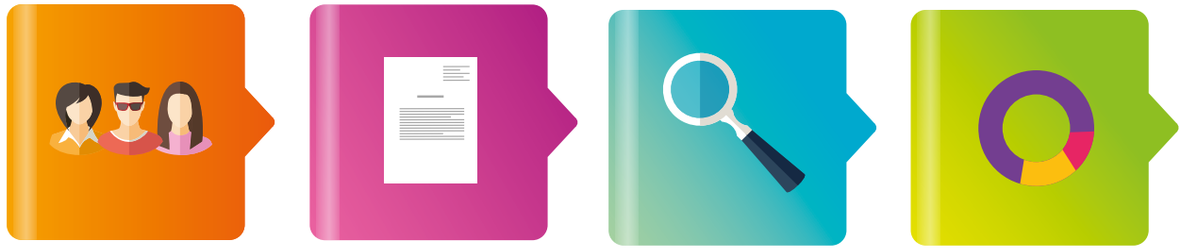
Cada atividade mapeada deve ser detalhadamente analisada no contexto da proteção de dados, para identificação das divergências entre o processo atual e as exigências da LGPD, identificando os gaps de cada processo.

Para cada gap identificado, deve ser estabelecido um plano de ação. Deve ser, também, avaliado o esforço x benefício para se definir a prioridade de implementação destas ações.

Os planos de ação devem ser estabelecidos considerando:

Estruturar os planos de ação identificando esforço x complexidade x benefício.
Estabelecer de maneira priorizada as ações para reduzir os riscos relacionadas a LGPD.
Estabelecer responsáveis pela implantação das ações de adequação incluindo função do Encarregado, considerando inclusive distribuição de atividades entre as áreas envolvidas.
Estruturar um cronograma de trabalho para implantação das ações.
Definir os investimentos necessários para aquisição de ferramentas, gestão de processos e treinamento de profissionais da organização.

ELABORAÇÃO DA MATRIZ RACI



Matriz RACI é uma ferramenta que facilita a gestão de tarefas, ações ou projetos, pois descreve a função dos diversos participantes, no processo. A matriz RACI será fundamental na execução e monitoramento dos planos de ação, pois demonstram os papéis e as responsabilidades de todos os envolvidos nas ações implantação da LGPD da organização.

RACI refere-se, em inglês a: *Responsible, Accountable, Consulted e Informed*, que traduzindo para o português significam:

RESPONSIBLE = Responsável
ACCOUNTABLE = Aprovador
CONSULTED = Consultado
INFORMED = Informado

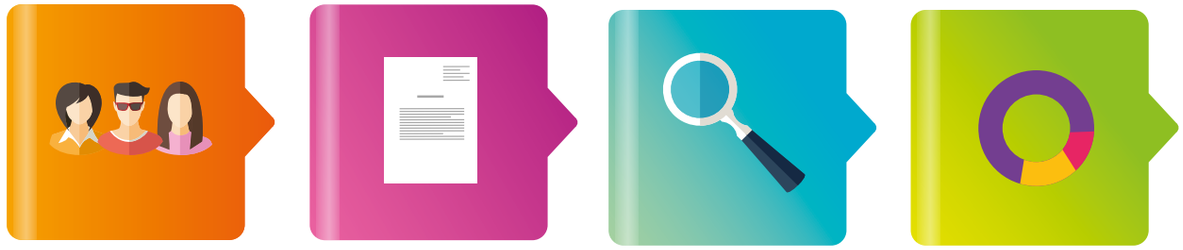
Cada uma das palavras acima refere-se ao tipo de responsabilidade no processo de adequação, ou seja:

R: pessoa responsável pela execução da atividade.
A: pessoa que aprova a execução da atividade, seja a autorização do início, o acompanhamento da execução ou a validação da conclusão.
C: pessoa que apoia a execução da atividade, contribuindo com seu conhecimento técnico ou teórico sobre o tema.
I: pessoa que precisa ser informada da execução das atividades, seja na conclusão de algum processo ou na ocorrência de fatos relevantes.

DOCUMENTOS RESULTADOS DA ETAPA DE "DIAGNÓSTICO", SEUS RESPECTIVOS MODELOS PARA PREENCHIMENTO:

1. ROPA – Registro de atividades de processamento de dados pessoais
2. Fluxos de processamento de dados pessoais
3. Matriz de gaps, riscos e Plano de ação
4. Modelo de matriz RACI

CRONOGRAMA ESTIMADO



	1	2	3	4	5	6	7	8	9	10	11	12
INVENTÁRIO DE ATIVIDADES PRINCIPAIS	Registros de Processamento											
	Fluxos de dados											
		Atribuição das Bases Legais										
TEMAS ESTRUTURANTES					Registro de Processamento - atualização							
						Avaliação de Impacto						
							Gestão do Consentimento					
								Gestão de Cookies				
									Gestão de Terceiros			
										Direito dos Titulares		
												Notificação de Incidentes
MODELO DE GOVERNANÇA												

Definir e nomear DPO

Definir *Usuários Multplicadores* e realizar treinamentos

Treinamento Corporativo

* Cronograma estimado e deverá ser adequado de acordo com cada organização, modelo de negócios e setor de atuação.

INTEGRIDADE

PROTEÇÃO DE DADOS

Pratique integridade, faça a diferença.

ICTS protiviti® FIEMG