

LGPD – Lei Geral de Proteção de Dados

Qual é o caminho ?

INSTITUTO SENAI DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

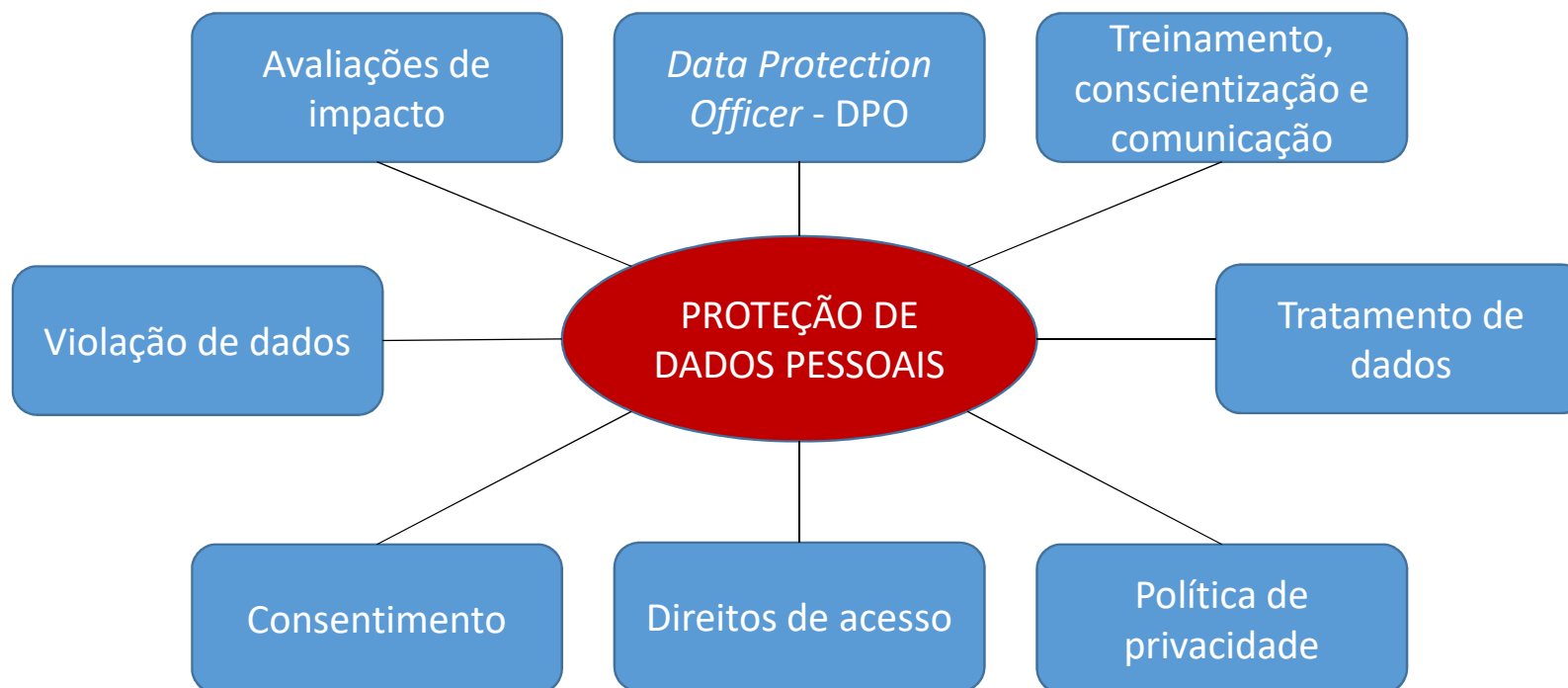
A LEI SE APLICA A TODAS AS EMPRESAS E ORGANIZAÇÕES

9 MOTIVOS PARA APLICAÇÃO DA LEI

Todas as empresas devem estar adequadas à LGPD até ago/2020

- | |
|---|
| 1. Todos os segmentos tratam dados - Indústria, saúde, educação, agências de publicidade, prestadores de serviços de todos os segmentos; |
| 2. Todos os departamentos, parceiros e terceirizados tratam dados - RH, logística, aplicativos, agências de publicidade, escritórios contábeis; |
| 3. Tratar dados é uma atividade essencial para a competição. Dados são ativo financeiro; |
| 4. O mercado já exige a conformidade com as bases legais; |
| 5. A Lei estabelece Princípios - transparência, finalidade, necessidade, dentre outros; (Reputação). |
| 6. Os titulares passam a ter direitos - confirmação, consentimento, informação sobre compartilhamento... |
| 7. Medidas de segurança, governança e boas práticas - Inversão do ônus da Prova; |
| 8. Criação da figura do "encarregado" que responderá às demandas e arcará com as responsabilidades; |
| 9. Haverá agentes fiscalizadores e punições. |

VISÃO GERAL DA LEI - PROTEÇÃO DE DADOS PESSOAIS



RAZÕES PARA SE PREOCUPAR COM A LGPD

CIO

Q MENU

Home > Tendências

5 razões pelas quais você deve se preocupar com a LGPD

Profissionais ainda têm dúvidas sobre o que poderão fazer ou não quanto às novas regras

De 30/04/2019 às 16h43
Ontem às 16h43



<https://cio.com.br/5-razoes-pelas-quais-voce-deve-se-preocupar-com-a-lgpd/>

1. Não se trata apenas de multas - é sobre a reputação também

É preciso ter consciência de que o descumprimento não está apenas relacionado em pagar a multa de até 2% do faturamento das empresas (com valor máximo de até R\$ 50 milhões) - estamos falando sobre a reputação da marca

2. A LGPD mudará a maneira de fazer negócios; seus processos atuais podem se tornar ilegais

No mundo além dos muros da corporação, a maneira de realizar os negócios será modificada. As informações voltam a ser de propriedade do indivíduo e as empresas deverão mostrar que possuem interesse em utilizar esses dados e como o farão. Muitos dos processos atuais se tornarão ilegais.

3. É provável que você precise de alterações no contrato com seus fornecedores e clientes

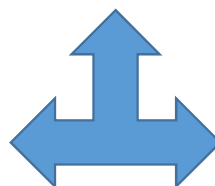
As empresas deverão se adequar às regras, por meio de ações como alterações de seus contratos com prestadores e, principalmente, clientes. Vale lembrar que a lei “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

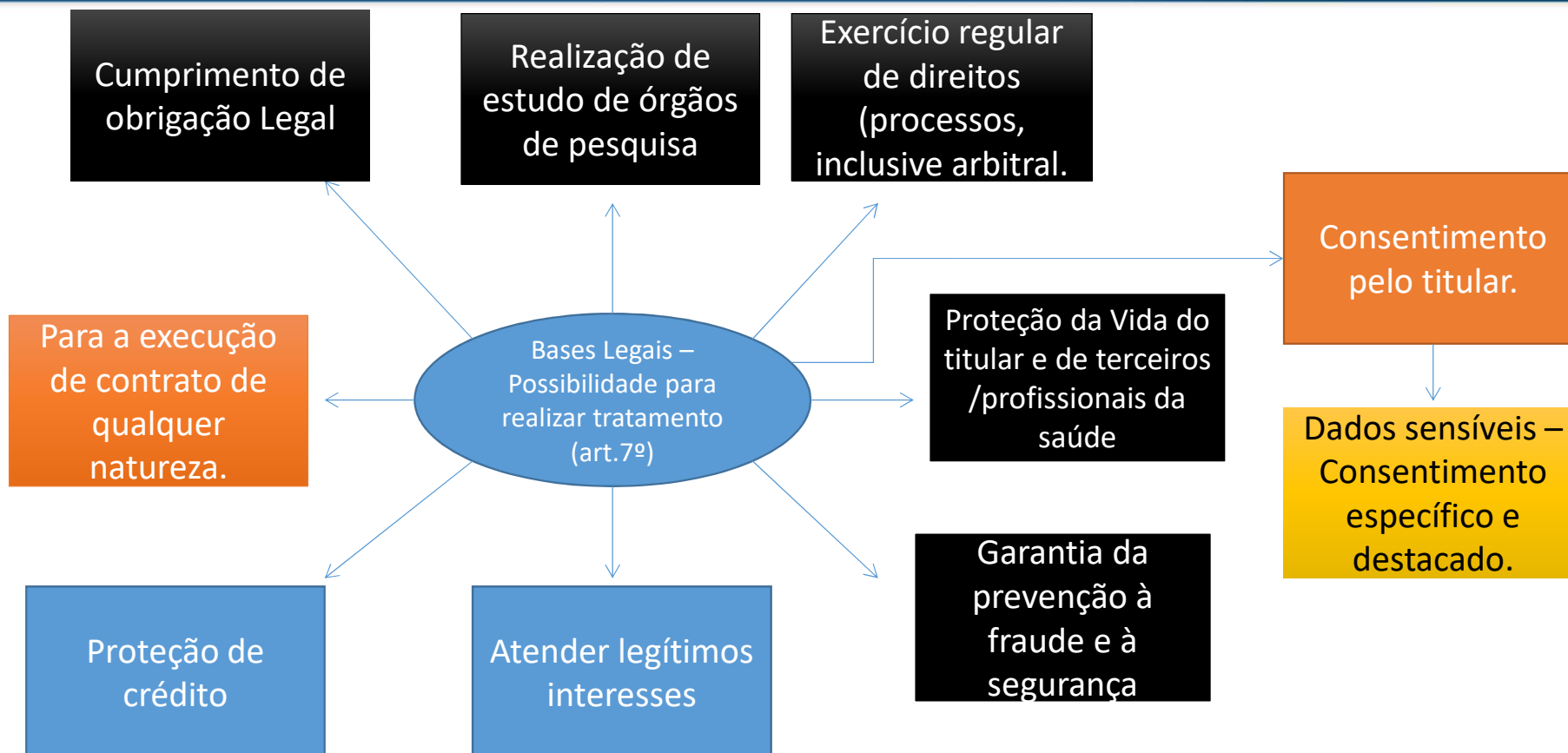
Dados (art. 5º, I) Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável, de forma direta ou indireta.

O que é tratamento (art.5º, X).
Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, controle, modificação....

Anonimizado (art. 5º, III e XI).
Não possibilita a associação, direta ou indireta a um indivíduo.

Dado Sensível (art. 5º,II) Religião, opinião política, saúde, vida sexual, biométrico, genético...

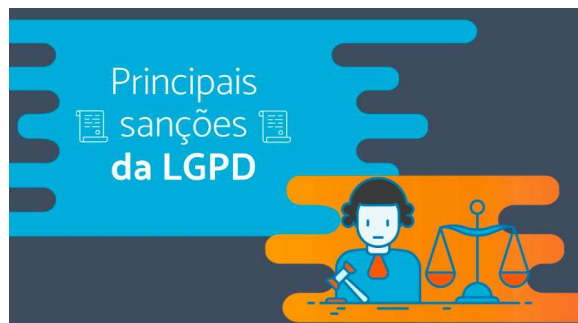
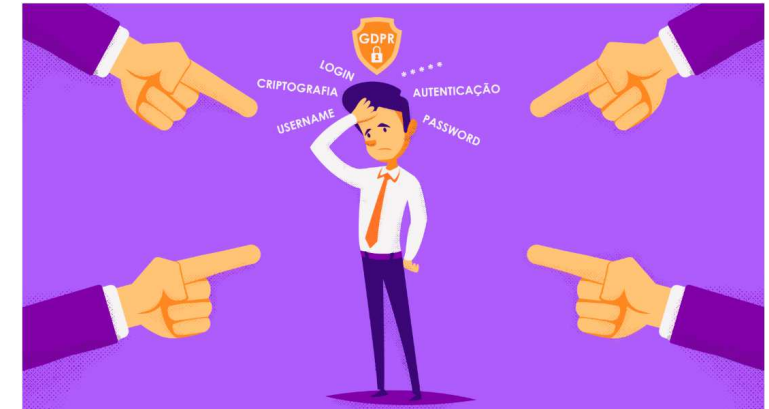




SANÇÕES ADMINISTRATIVAS

Considerações que a Autoridade Nacional de Proteção dos Dados deve levar:

- Reincidência
- Boa fé
- Condição econômica
- Proporcionalidade
- Pronta adoção de medidas corretivas
- Mecanismos e procedimentos internos de proteção de dados
- Política de boas práticas e governança
- Cooperação do infrator
- Grau do dano, gravidade
- Vantagem obtida ou pretendida



Sanções:

- Eliminação de dados pessoais
- Bloqueio do tratamento de dados
- Multa de até 2% do faturamento do grupo no Brasil (limitado a R\$ 50 milhões por infração)
- Advertência
- Publicização da infração

Envolver executivos e revisar organograma

Identificar projetos e áreas afetados face a legislações setoriais

Criar um programa de governança em conformidade com a LGPD

Estruturar e nomear um DPO

Elaborar e rever documentos jurídicos na venda de bens e serviços, compartilhamento de dados, terceirização, consentimentos , *disclaimers*, dados de menores, contratos trabalhistas

Garantir o exercício dos titulares mediante a confirmação da implementação de medidas técnicas e organizacionais

Realizar treinamentos internos para a nova cultura

LGPD X ISO

ISO27001

- . Requisitos
- . Gerenciamento Riscos
- . Aplicação de Controles
- . Plano Implementação
- . Revisão Gerenciamento

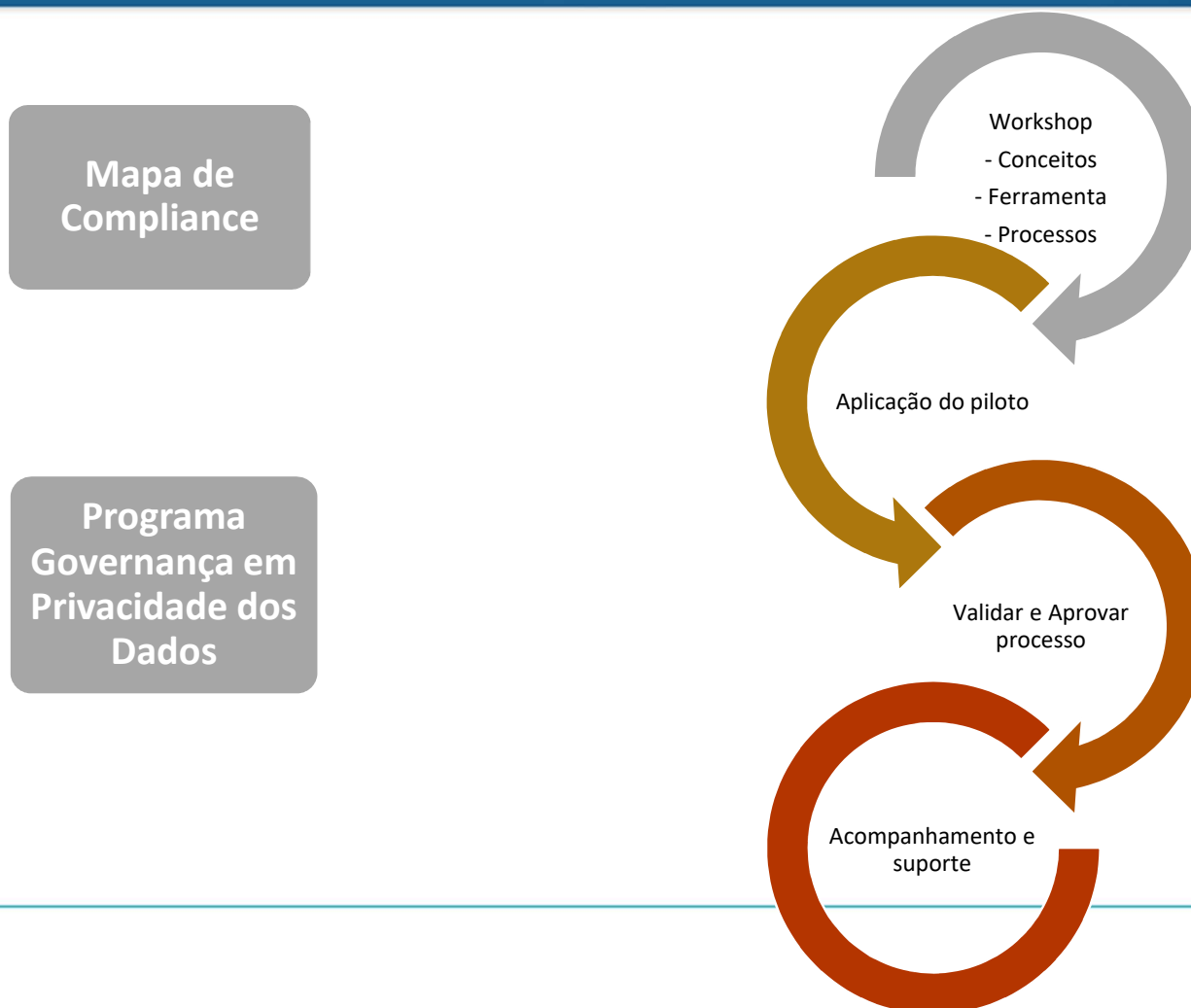
- | | |
|-------------|---------------------------|
| . Projeto | . Controles de Segurança |
| . Escopo | . Conformidade Terceiros |
| . Objetivos | . Incidentes de Segurança |
| . Políticas | . Conscientização |
| . Auditoria | . Treinamento |

GDPR/LGPD

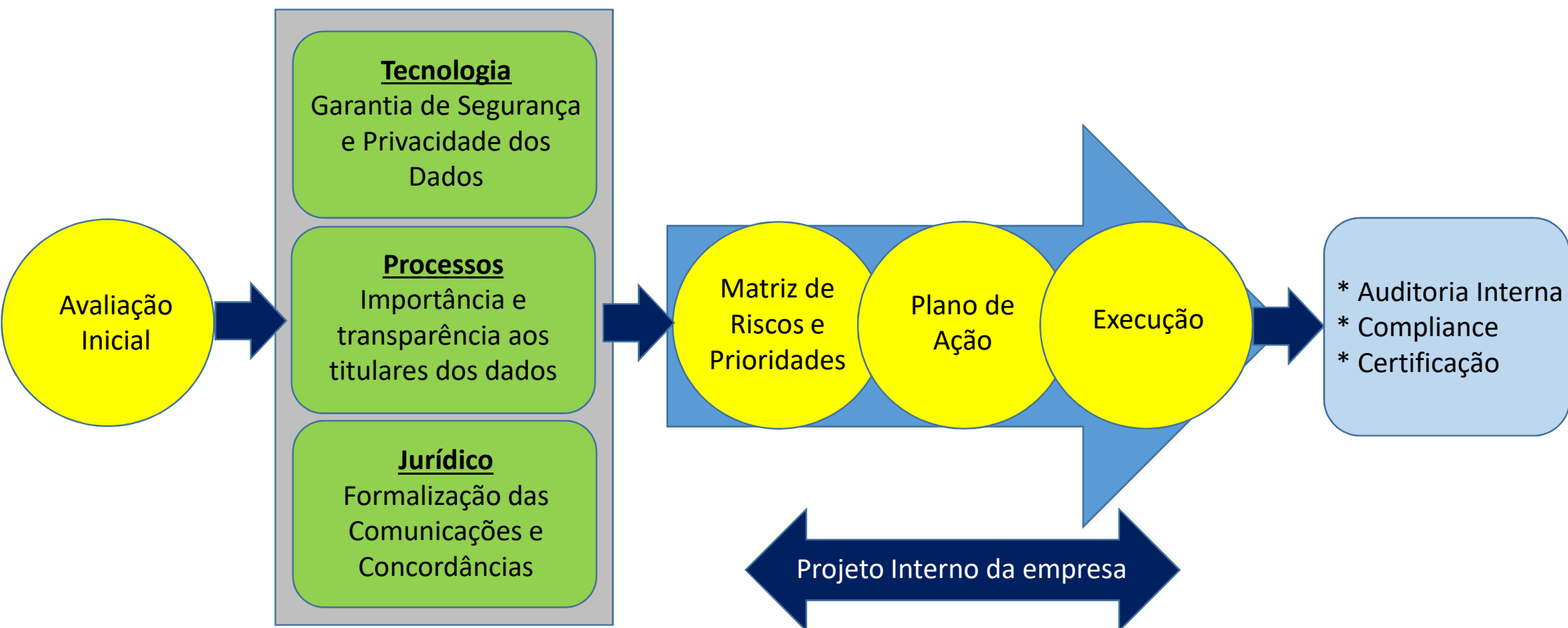
- . Proteção dados pessoais
- . Atividades
- . Direitos Titular dos Dados
- . DPIA
- . Transf. de Dados Pessoais



COMO O IST TIC PODE ATUAR



VISÃO GERAL PARA ADEQUAÇÃO DA LGPD



ROADMAP DE AVALIAÇÃO INICIAL

Contexto

Levantamento dos Requisitos

Identificação dos entrevistados, áreas, seleção dos requisitos e componentes que envolvem as atividades objeto de interesse.

Avaliação

Não Conformidades

Apontamento de não conformidades encontradas e definição de ações para remediação.

Resultados

Relatório

Divulgação do Plano de Ação e recomendações de tecnologias a serem implementadas.

Análise

Entrevistas

Entrevistas em forma de questionário com pessoas-chave e análise aprofundada dos processos e ambiente tecnológico.

Prazo:
01 a 02 semanas

Checklist para Compliance da LGPD

1) Conscientização e comunicação

Garanta que seus funcionários entendam a LGPD e comuniquem-se com o serviço e a equipe sobre o motivo pelo qual você está coletando os dados.

2) Análise de dados pessoais

Analise uma lista de todos os dados confidenciais armazenados e processados.

3) Procedimentos de Revisão

Ter uma política de privacidade adequada e revisá-la regularmente.

4) Direitos de acesso

Listar quais direitos de acesso devem ser concedidos e como as alterações devem ser tratadas.

5) Consentimento do Cliente

Garanta que seus clientes consentam com o processamento de seus dados.

6) Violações de dados

Implementar um procedimento para lidar com violações de dados.

7) Avaliações de impacto

Efetuar uma avaliação de impacto da proteção de dados.

8) Responsáveis pela proteção de dados (DPO's)

Determine se você precisa de um responsável pela proteção de dados (DPO).



MAPA DE COMPLIANCE														
LGPD - Lei Geral de Proteção dos Dados (Lei 13.709 de 14 de agosto de 2018)	Macrocontrole	CONTROLES DE SEGURANÇA DA INFORMAÇÃO												
		Política e regulamentação de	Acesso aos dados pessoais	Classificação da informação	Privacidade Técnica	Privacidade Organizacional	Processamento de Aplicações (Seguro)	Comunicação de Negócio	Uso de Segurança (Backup)	Segurança de Redes de Informação	Segurança de Processamento de Informação	Segurança de Dados	Processo Organizacional	
Direitos: Titularidade dos dados pessoais	Dados pessoais e da pessoa singular	X	X	X					X	X		X	X	
1. Aplicação e abrangência da lei	Análise de aplicação territorial e lógica	X	X	X								X	X	
2. Requisitos para tratamento dos dados pessoais	Base legal para tratamento de dados pessoais	X	X									X	X	
3. Direitos do Titular	Direitos da pessoa singular	X	X	X	X			X	X	X		X	X	
4. Consentimento do Titular	Autorização de uso de dados pessoais	X	X	X	X			X	X	X		X	X	
5. Uso com finalidade específica	Limitação de uso	X	X	X	X			X	X	X		X	X	
6. Tempo de tratamento	Limitação de uso	X	X	X	X			X	X	X		X	X	
7. Coleta mínima e adequada	Limitação de uso	X	X	X	X			X	X	X		X	X	
8. Livre acesso pelos Titulares	Direitos do Titular	X	X	X	X			X	X	X		X	X	
9. Adequação	Limitação de uso	X	X	X	X			X	X	X		X	X	
10. Garantia de segurança pelo Controlador	Segurança da Informação (controles)	X	X	X	X	X	X	X	X	X	X	X	X	
11. Estruturação da segurança de dados pessoais	Proteção técnica	X	X	X	X	X	X	X	X	X		X	X	
12. Comunicação a autoridades	Comunicação a autoridade, marcado	X	X	X	X			X	X	X		X	X	
13. Anonimização de dados	Proteção de dados	X	X	X	X							X	X	
14. Governança privacidade de dados pessoais	Governança	X	X	X	X	X	X					X	X	
15. Transferência internacional de dados	Transferência de dados	X	X	X	X	X	X	X	X			X	X	
16. Tratamento de dados crianças e adolescentes	Crianças e adolescentes	X	X	X	X					X		X	X	
17. Encargamento do tratamento de dados pessoais	Gerência dos dados pessoais	X	X							X		X	X	
18. Registro de proteção de dados pessoais	Gerência de risco de dados pessoais	X	X									X	X	
19. Penalidades	Responsabilidades e penalidades	X	X							X	X		X	
20. Autoridade Nacional	Autoridade Nacional	X	X			X						X	X	
21. Política de Dados Pessoais	Regulamento de Dados Pessoais	X	X					X	X	X		X	X	
22. Direito ao esquecimento	Direito ao esquecimento	X	X	X	X			X	X	X		X	X	
Controles de Segurança da Informação														
Preparação		11	14	8	12	8	10	4	13	16	8	1	13	6

RESULTADOS ESPERADOS - AVALIAÇÃO INICIAL (COMPLIANCE)

- ✓ A empresa conseguirá ter uma visão de sua situação atual com relação aos itens e requisitos da LGPD;
- ✓ A empresa conseguirá alocar os recursos necessários de forma mais eficaz e eficiente dentro de suas atividades para estar em conformidade com a referida norma;
- ✓ A empresa conseguirá dimensionar o tempo a ser dispensado de suas pessoas dentro de um determinado prazo e dessa forma ter uma previsão mais correta de qual seu custo total nesse processo;
- ✓ Por meio do Plano de Ação, será possível visualizar o esforço necessário para implementação do programa de governança em privacidade de dados.

Programa de Governança em Privacidade dos Dados

- Tratamento de Dados
- Acesso e Portabilidade
- Tratamento de Dados Poder Público
- Transferência Internacional dos Dados
- Declaração de Aplicabilidade e boas práticas
- Tratamento de Incidentes
- Gestão de Riscos
- Análise de infraestrutura
- Comunicação para todas as áreas
- Treinamento e Conscientização
- Jurídico



RESULTADOS ESPERADOS - PROGRAMA DE GOVERNANÇA EM PRIVACIDADE DOS DADOS

- ✓ A empresa conseguirá implementar boas práticas de governança para a gestão de privacidade dos dados requisitados pela LGPD;
- ✓ A empresa adotará os procedimentos para o tratamento dos dados, incluindo os processos de reclamações e petições de titulares e obrigações envolvendo incidentes com o tratamento de dados;
- ✓ Estruturar as normas de segurança e padrões técnicos de infraestrutura;
- ✓ Implementar ações educativas com treinamento e conscientização;
- ✓ A empresa incluirá os mecanismos internos de monitoramento e supervisão para fazer a gestão e mitigação de riscos relacionados ao tratamento de dados pessoais.

- ✓ O que eu preciso fazer na minha empresa ?
- ✓ A certificação ISO não é obrigatória para atendimento a LGPD, porém é um meio seguro para implementar e demonstrar o *COMPLIANCE*.
- ✓ Desenhar o mapa de “Governança e Segurança”.
- ✓ Rever os contratos internos e externos.
- ✓ Conscientização.
- ✓ Se você não se adequar, estará fora do mercado (reputação).

Sistema Fiep

<i>FIEP</i>
<i>SESI</i>
<i>SENAI</i>
<i>IEL</i>

nosso i é de indústria.