
Afinal, que caminho preciso percorrer para me adequar à Lei Geral de Proteção de Dados Pessoais?
BAPTISTA LUZ
ADVOGADOS

autores

Gabriela Brum Davoli

Amanda Azevedo De Oliveira

Gustavo Henrique Luz Silva

revisores

Felipe Gabriades

Fernando Bousso

Pedro H. Ramos

Rafael Pessoa

Renato Leite Monteiro

projeto gráfico

Laura W. Bandeira Klink

Fabio Salmoni

Maio de 2020

BAPTISTALUZ

Afinal, que caminho preciso percorrer para me adequar à **Lei Geral de Proteção de Dados Pessoais?**

Este paper busca organizar melhores práticas comumente utilizadas pelo Baptista Luz Advogados em projetos de adequação e conformidade de organizações à **Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018) e demais normas setoriais de proteção de dados. Possui caráter meramente informativo e não substitui e nem deve ser entendido como aconselhamento jurídico ou técnico.

Índice clicável

Prefácio

Estamos passando por um dos períodos mais desafiadores e, ao mesmo tempo, mais interessantes para o ambiente de negócios. 2020 reservou às empresas não só uma nova forma de pensar o relacionamento com seus clientes, mas também o seu papel na sociedade. E nunca foi tão importante fazer essa reflexão.

Desde nossa fundação, um dos pilares principais da nossa atuação no Baptista Luz Advogados é o conhecimento aberto, uma das formas de aplicar o Direito como instrumento de inovação e transformação da sociedade. É evidente que há propriedade intelectual no conhecimento jurídico; mas há também uma necessidade de desmistificar o papel desse conhecimento num mundo em que a informação, antes restrita aos causídicos, agora é livremente disponível na internet. No atual contexto, são as pessoas que fazem a diferença.

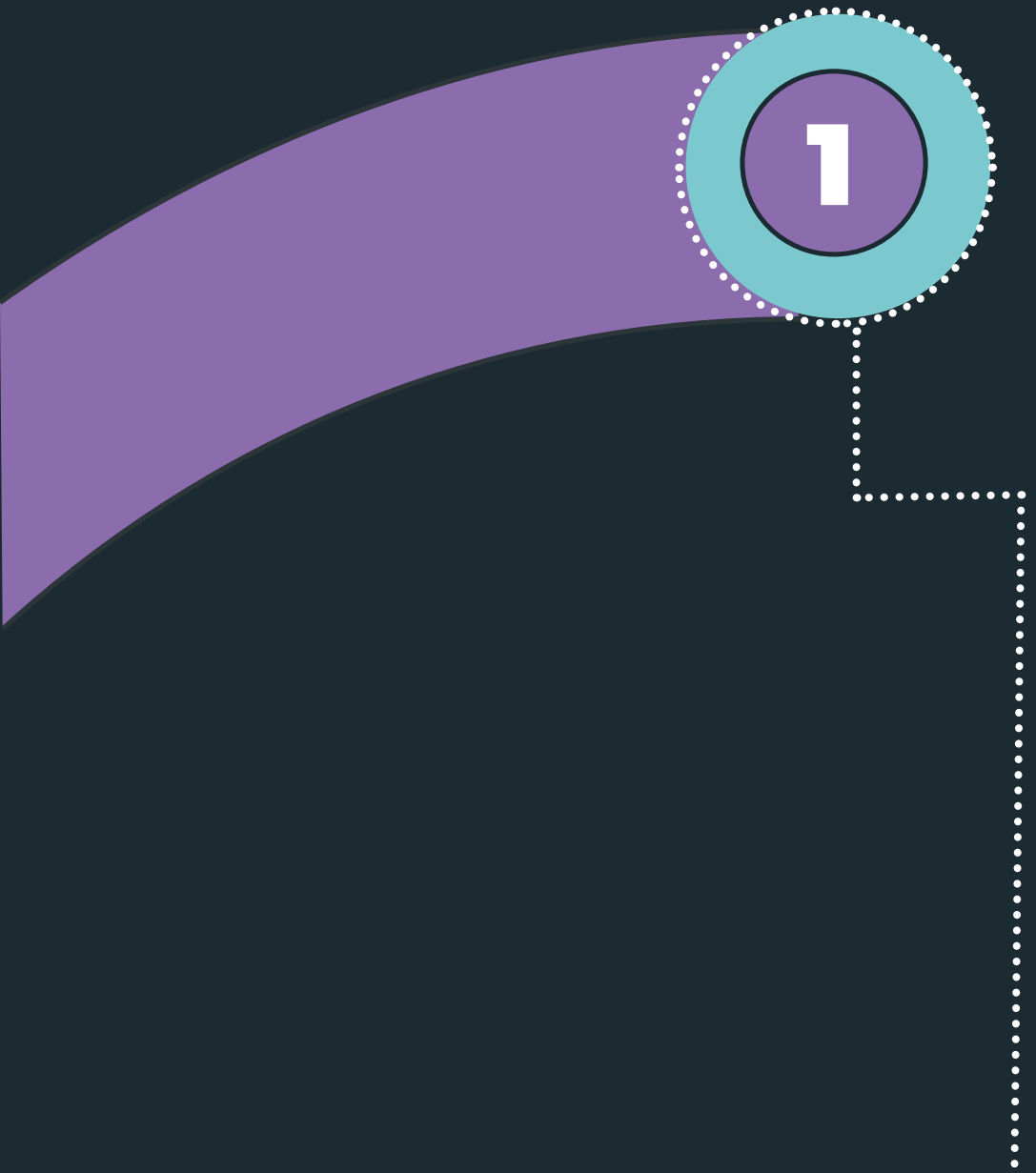
E por essa razão estamos sempre publicando tanto conteúdo, dos mais diferentes temas envolvendo direito e inovação, e sem reservas em relação à profundidade desses conhecimentos. Em vários momentos, tornamos públicos inclusive modelos de documentos e estudos que usamos no escritório. E tudo isso porque entendemos que quanto mais conhecimento aberto, mais o mercado amadurece como um todo, mais oportunidades surgem, mais nosso papel social se fortalece e mais as pessoas aumentam suas capacidades e o poder de transformação junto às empresas em que atuam.

E é por isso que apresentamos, com este trabalho, nosso conhecimento sobre projetos de adequação em proteção de dados, que adquirimos a partir de mais de 80 projetos desenvolvidos desde 2017 com pequenas e grandes empresas, brasileiras e multinacionais, de setores inovadores e tradicionais. No momento sensível em que estamos, que combina crise econômica, incertezas políticas e, principalmente, ausência de segurança jurídica devido a sucessivos adiamentos da LGPD e do atraso na constituição da ANPD, parece que esse é o movimento correto e necessário quando pensamos na contribuição que podemos dar a um debate propositivo sobre como as empresas podem melhor se preparar para uma legislação que, agora, parece cada vez mais próxima de sua vigência definitiva.

Não temos a pretensão de que o conhecimento aqui compartilhado seja definitivo – muito pelo contrário! Nós mesmos estamos sempre construindo e adaptando nossa metodologia constantemente, além de sempre adequá-la para cada tipo de empresa (sob pena de entregarmos experiências genéricas e desconexas com a realidade dos clientes). Além disso, esse trabalho é também um convite ao debate, para que mais pessoas discutam projetos de adequação de forma aberta e propositiva, preenchendo lacunas que, hoje, carecem de orientação de autoridades reguladoras.

Boa leitura!

Time de Proteção de Dados do Baptista Luz Advogados | Maio de 2020



Introdução

1.1 O que é a LGPD?

A Lei nº 13.709/2018 (a "Lei Geral de Proteção de Dados Pessoais" ou a "LGPD"), sancionada em agosto de 2018 e vigente a partir de agosto de 2020, traz várias regras e obrigações relacionadas à privacidade e proteção de dados pessoais[1], tanto em meios online quanto offline, sendo aplicável a praticamente qualquer organização, seja ela pública ou privada, com ou sem fins lucrativos, independentemente do setor econômico a que pertença.

Embora ainda haja diversos pontos a serem regulamentados, muitos deles pela Autoridade Nacional de Proteção de Dados (a "ANPD"), a LGPD já proporciona relevante expectativa de segurança jurídica às organizações e à população, já que regula o tratamento[2] de dados pessoais, define as hipóteses[3] que autorizam tais tratamentos e aumenta o rol de direitos dos titulares de dados, prevendo, por exemplo, o direito de acesso facilitado às informações referentes à forma de uso dos dados, o direito de apagamento dos dados em determinadas situações, o direito à portabilidade dos dados, o direito à revisão de decisões automatizadas, o direito à revogação do consentimento, entre outros.

Além disso, a lei prevê **dez princípios**, que são a espinha dorsal do tratamento de dados pessoais e que devem ser respeitados e levados em consideração em qualquer atividade de tratamento. Veja na próxima página:

LGPD tem como principais fundamentos:

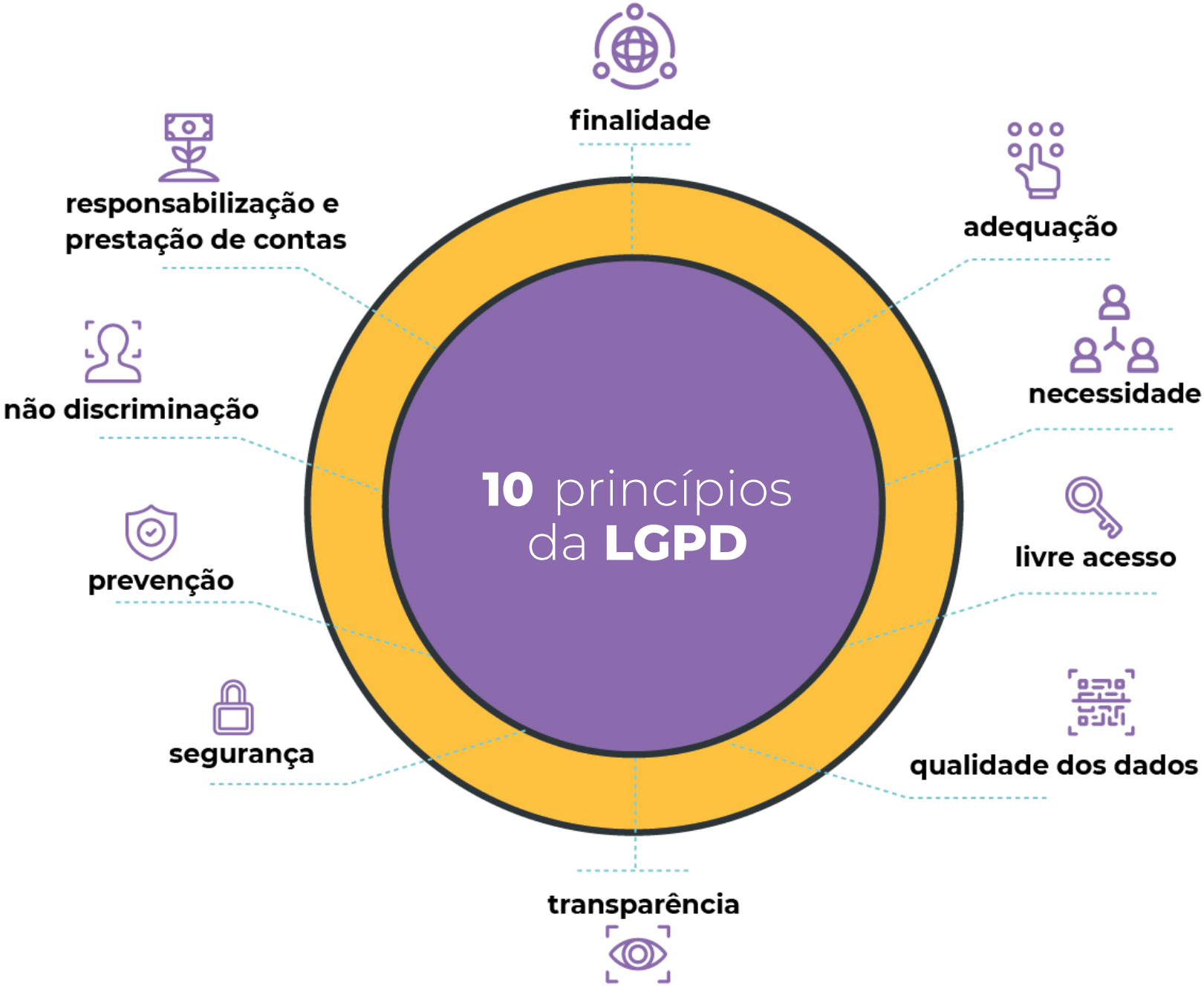
- a proteção e o respeito à privacidade de pessoas físicas;
- a autodeterminação informativa – "devolvendo" às pessoas o controle sobre seus próprios dados;
- o desenvolvimento econômico, tecnológico e a inovação; e
- a proteção e defesa do consumidor.

[1] **Dados Pessoais:** qualquer informação relacionada a uma pessoa natural identificada ou que possa vir a ser identificada (identificável) (art. 5º, I, da LGPD); essa definição deve ser entendida de modo a incluir, ainda, números identificativos, dados de localização, identificadores eletrônicos, dados sensíveis (definidos no art. 5º II da LGPD), ou qualquer dado que, quando combinado com outras informações, seja capaz de identificar uma pessoa natural, torná-la identificável ou, ainda, individualizá-la.

[2] **Tratamento:** toda operação realizada com Dados Pessoais, como as que se referem a atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X, da LGPD).

[3] **Bases legais** para o Tratamento de Dados Pessoais: arts. 7º e 11 da LGPD.

[4] **Direitos dos titulares de dados:** estão contidos no Capítulo III – Dos direitos do titular (arts. 17 a 22 da LGPD) e em artigos esparsos ao longo da Lei, como o art. 9º.


finalidade
adequação
necessidade
livre acesso
qualidade dos dados
transparência
segurança
prevenção
não discriminação
responsabilização e prestação de contas
10 princípios da LGPD

1.2 Por que se adequar à LGPD?

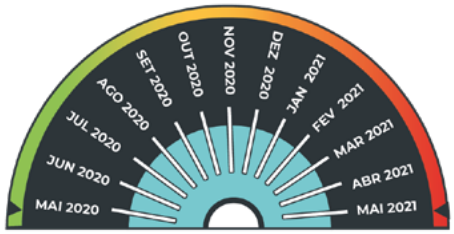
Em se considerando a complexidade da LGPD e, consequentemente, de um projeto de adequação, foi determinado um prazo de carência para que a lei pudesse ser efetivamente aplicada, de modo que as organizações pudessem, assim, adaptar-se às novas normas. Por iniciativa do Poder Executivo, via MP 959/2020, o prazo atual da entrada em vigor da LGPD é 3 de maio de 2021.

A LGPD prevê diversas penalidades que podem ser aplicadas às organizações no caso de uso ilegal ou inadequado de dados - que vão desde advertências até multas de 2% do faturamento anual, limitadas a R$ 50.000.000,00, por infração.

Falta 1 ano até a plena vigência da LGPD, e a adequação e conformidade à lei não devem ser encaradas somente como a melhor forma de diminuir riscos regulatórios, mas sim como elementos essenciais para o aprimoramento dos vários modelos de negócio de organizações dos mais diversos nichos de mercado, de modo a permitir a extração de valor das informações que estejam sob o seu controle, permitindo, assim, inovar por meio do projeto de adequação. Não são poucos os exemplos que demonstram que as organizações podem tornar os seus processos internos mais eficientes, cortando custos, ganhando tempo e até mesmo desenvolvendo novos produtos e serviços, tudo no contexto de adequação a leis de proteção de dados.

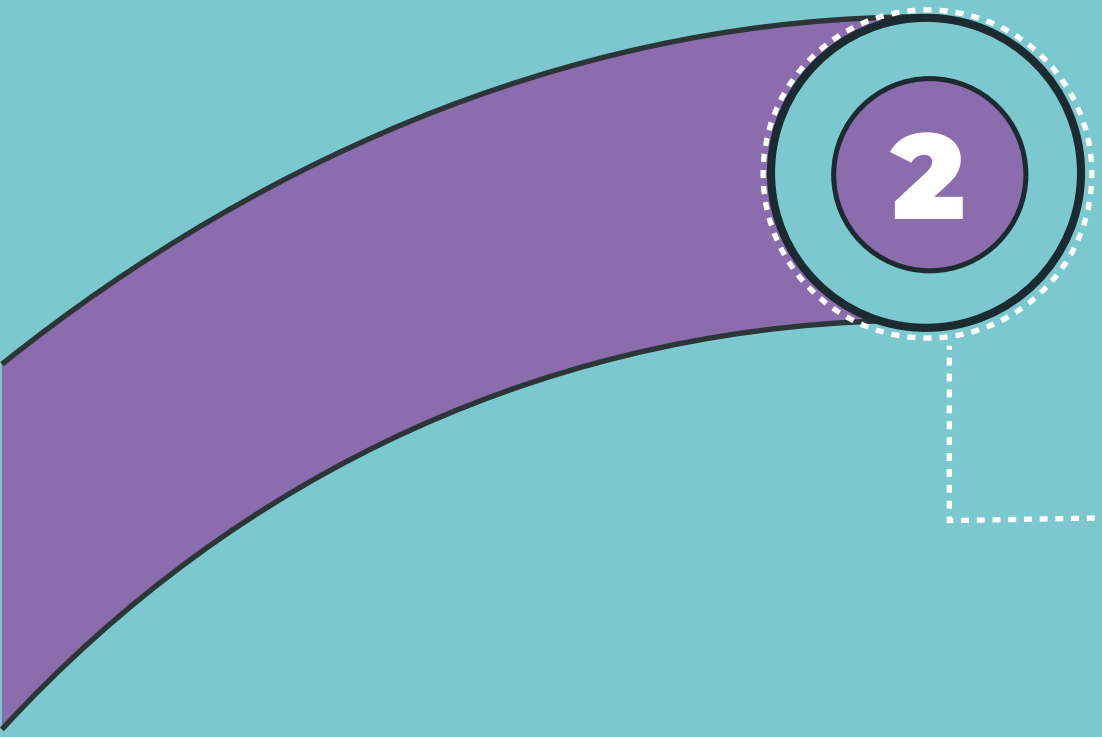
As organizações podem e devem encarar o processo de adequação à LGPD como uma forma de agregar valor aos seus negócios e produtos, pois, ainda que a cultura de privacidade e proteção de dados esteja "engatinhando" no Brasil, a crescente conscientização da população sobre a necessidade de se ter controle sobre seus dados pessoais é uma tendência mundial, que fará cada vez mais parte da realidade de todos. Encarar a correta proteção de dados como um elemento de confiança pode ser, portanto, um diferencial competitivo num universo de descrença sobre a forma com a qual as organizações lidam com dados pessoais em geral.

Portanto, um projeto de adequação e conformidade à Lei Geral de Proteção de Dados Pessoais, além de diminuir os altos riscos de violação de preceitos regulatórios, é a melhor forma de demonstrar ao mercado, ao seu público-alvo e a stakeholders que a organização se importa com questões de privacidade, com a proteção e o uso adequado de dados pessoais e com o respeito aos direitos garantidos aos titulares, certamente trazendo benefícios à imagem e à reputação da organização.



De acordo com o Consumer Pulse Survey[5] 2019 , estudo global desenvolvido pela *Accenture Interactive*, **69%** dos consumidores alegaram que abandonariam o uso de marcas que utilizam seus dados pessoais de forma invasiva e **73%** dos consumidores afirmaram estarem dispostos a fornecer seus dados caso as marcas fossem mais transparentes em relação às formas de tratamento dos seus dados.

[5] TIEMAN, Scott; PÉREZ MOIÑO, Javier. Consumer Pulse Survey 2019. Accenture Interactive, 2019. Disponível em: <https://www.accenture.com/_acnmedia/PDF-110/Accenture-See-People-Not-Patterns.pdf Acesso em 17.01.2020>. Acesso em: 17 jan. 2020.



Como se adequar?

2. Como se adequar?

O primeiro passo para dar início a um projeto de adequação à LGPD deve ser definir qual metodologia de adequação será a mais apropriada para a sua organização. Essa avaliação depende diretamente das necessidades, da estrutura, do modelo de negócio, da maturidade da organização em relação aos temas de privacidade e proteção de dados pessoais e do tempo necessário, e disponível, até a adequação.

É importante ter em mente que não existe um selo que ateste a conformidade completa às regras de proteção de dados, algo como "LGPD Compliant". As iniciativas de adequação devem ser encaradas como processos constantes, que perdurarão por toda a vida da organização, uma vez que, a cada dia, novos serviços e produtos são desenvolvidos, processos internos são alterados, novas pessoas são contratadas e novas práticas são adotadas.

É por isso que a LGPD determina que as organizações devem ser capazes de demonstrar que adotaram todas as medidas cabíveis, dentro de critérios objetivos de tempo, custo e tecnologia disponível para estarem o mais próximo possível da conformidade *(accountability)*.

Com essas questões em mente, podemos citar os seguintes modelos de projeto de adequação*:

- **a consolidação** de um Programa de Governança em Privacidade e Proteção de Dados Pessoais;
- **a elaboração** de análises Privacy by Design & Privacy by Default dos principais serviços e produtos da organização; e
- **a metodologia tradicional,** completa, que engloba as principais e a grande maioria das atividades de tratamento de dados de todas as áreas da organização ou das áreas que trazem mais risco, numa análise risk based approach (lidando primeiro com o que representa maior grau de risco aos titulares e à organização).

*as indicações possuem caráter informativo e não devem ser entendidas como aconselhamento jurídico ou técnico.

Abordaremos de forma pontual as duas primeiras metodologias neste tópico e, tendo em vista a sua extensão, abordaremos a metodologia tradicional ao longo dos demais tópicos deste *paper*.

É importante ter claro que diversas outras técnicas e metodologias (inclusive versões simplificadas ou estendidas destas) podem ser utilizadas para se chegar aos mesmos objetivos, sendo sempre aconselhável a realização de uma análise "caso a caso" em sintonia com o perfil da organização para a seleção do modelo de projeto mais adequado.

2.1 Programa de governança em privacidade e proteção de dados pessoais

O desenvolvimento e a consolidação de um Programa de Governança em Privacidade e Proteção de Dados Pessoais deve ser compatível com as necessidades da organização. Um programa dessa natureza pode servir para estabelecer as melhores práticas para o tratamento de dados pessoais dentro desta, levando em consideração o volume de operações, a escala e a estrutura da organização, assim como o risco de potenciais danos aos titulares. O objetivo de estruturar um programa de governança em privacidade e proteção de dados é definir padrões para as atividades que dependam do uso de dados pessoais na organização, documentá-los e tornar possível a verificação periódica da aderência das práticas da organização a esses padrões.

De forma sucinta, um Programa de Governança em Privacidade e Proteção de Dados Pessoais pode seguir a seguinte estrutura:

a demonstrar o comprometimento da organização em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais;

b ser aplicável a todo o conjunto de dados pessoais que estejam sob controle da organização, independentemente do modo de coleta;

c adequar-se à estrutura, à escala e ao volume das operações, bem como à sensibilidade dos dados tratados;

d estabelecer políticas e salvaguardas adequadas com base em processo de avaliações sistemáticas de impactos e riscos à privacidade;

e ter o objetivo de estabelecer relação de confiança com o titular de dados pessoais por meio de atuação transparente e que assegure mecanismos de participação;

f estar integrado à estrutura geral de governança da organização, estabelecendo e aplicando mecanismos de supervisão internos e externos;

g contar com planos de resposta a incidentes e remediação; e

h ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Além disso, no contexto do desenvolvimento do Programa, a organização pode também elaborar e implementar:

Declaração de Missão e Visão de Privacidade:

composto por frases curtas que descrevam sucintamente a razão e a função da proteção de dados no contexto de suas atividades.

Exemplos: Protect your life online with privacy (Firefox); Everyday apps. Designed for your privacy (Apple);

Políticas Internas:

desenvolvimento e implementação de políticas internas e aperfeiçoamento daquelas já existentes.

Exemplos: política de privacidade (interna e externa), de direitos, de segurança da informação, de incidentes, de continuidade dos negócios, de relação com fornecedores, de treinamentos, de Recursos Humanos, de elaboração de relatório de impacto à proteção de dados, dentre outras.

Ações Educativas e de Conscientização:

para difundir e reforçar as políticas e as práticas de privacidade e proteção de dados pessoais da organização.

Exemplos: métodos formais, como workshops e treinamentos para colaboradores e equipes estratégicas, e informais, como a criação de grupos de discussão sobre temas e acontecimentos do mundo da privacidade e proteção de dados, além de informes constantes e ativos sobre temas afins e práticas da organização.

Procedimentos de Relacionamento com Fornecedores e Parceiros:
aprimoramento dos processos internos de contratação, com atenção à natureza e aos riscos envolvidos nos serviços contratados.

Exemplos: criação de checklists para seleção de fornecedores, criação de manual com regras de contratação e padrões mínimos de segurança da informação e proteção de dados para orientação de fornecedores, dentre outros mecanismos.

2.2 Análises Privacy by design & privacy by default

Caso a consolidação do Programa de Governança em Privacidade e Proteção de Dados Pessoais não seja possível ou, ainda, não se adeque ao modelo de negócio da organização, as análises *Privacy by Design* e *Privacy by Default* podem ser uma boa alternativa, permitindo a verificação pontual da aderência de produtos, serviços, soluções e processos específicos às regras de proteção de dados.

Uma análise *Privacy by Design* consiste na avaliação de produtos, serviços e atividades de tratamento de dados pessoais levando em consideração os princípios e as regras da LGPD **desde a sua concepção até a sua implementação e o seu pleno funcionamento**, a fim de **(i)** identificar as medidas necessárias à adequação desses produtos e serviços à LGPD e, consequentemente, **(ii)** mitigar riscos decorrentes do tratamento de dados pessoais aos direitos e às liberdades dos titulares de dados.

Na prática, questões de privacidade e proteção de dados devem ser observadas pela organização durante toda a fase de desenvolvimento de novos projetos que possam impactar os titulares de dados de alguma forma, por meio do tratamento de seus dados pessoais.

Além do disposto na LGPD, outros elementos também devem ser levados em conta nesta fase, dentre eles: **(i)** o estado da arte em medidas técnicas, de segurança e organizacionais; **(ii)** os custos de implementação; **(iii)** as finalidades e a extensão das atividades de tratamento de dados pessoais envolvidas; e **(iv)** os possíveis riscos a direitos e liberdades individuais[6].

Em poucas palavras, o principal objetivo da metodologia *Privacy by Design* é garantir que qualquer processo de uso de dados pessoais respeite, no mínimo, os princípios previstos na LGPD. Segue sugestão de tabela para iniciar uma adequação nestes moldes*:

princípio	aderência	medidas necessárias
finalidade	*sim/não*	*ações a serem tomadas e responsáveis*
adequação		
necessidade		
livre acesso		
qualidade dos dados		
transparência		
segurança		
prevenção		
não discriminação		
responsabilidade e prestação de contas		

* A tabela é apenas um ponto de partida, outras análises mais específicas podem decorrer do seu preenchimento, como análises de bases legais, revisão de contratos com fornecedores e revisão do exercício de direito dos titulares.

[6] Vide Guidelines 4/2019 on Article 25 (Data Protection by Design and By Default) do European Data Protection Board (EDPB).

Já a análise Privacy by Default decorre da análise Privacy by Design na medida em que direcionará a configuração dos produtos e serviços, sempre partindo de formatos mais protetivos e menos invasivos para, apenas após interações livres dos titulares de dados, alcançar modelos de mais ampla utilização de dados pessoais. Nesta análise, é fundamental avaliar a quantidade de dados tratados, os que são estritamente necessários para o funcionamento e oferecimento do serviço/produto, a duração das atividades de tratamento, o período de retenção de dados pessoais etc[7].

Na prática, esse tipo de análise deve servir para garantir que, sempre que titulares de dados pessoais estiverem diante de opções relacionadas às formas de tratamento de seus dados pessoais por uma organização, tais opções devem estar, por padrão, configuradas de modo a privilegiar a sua privacidade acima de outros fatores que não encontrem respaldo específico na legislação.

Ambas as metodologias podem ser implementadas com a ajuda de um time multidisciplinar, envolvendo, por exemplo, jurídico, área técnica, de produtos, engenharia de dados, segurança da informação, UX, entre outras.

Como exemplo de aplicação das análises Privacy by Design e Privacy by Default, a Apple recomenda em artigo de seu Kit de Desenvolvimento de Software, na parte de Interface com Usuário, que os desenvolvedores de aplicações para seus dispositivos sempre protejam os dados pessoais e as preferências dos usuários sobre como os seus dados são usados[8].

As recomendações, em suma, são:

- solicite acesso apenas quando sua aplicação precisar dos dados pessoais;
- seja transparente sobre como os dados pessoais serão utilizados;
- dê ao usuário controle sobre os dados e proteja os dados coletados;
- deixe as configurações mais protetivas como padrão; e
- use a quantidade mínima de dados necessária à aplicação.

Em resumo, as análises *Privacy by Design* e Privacy by Default direcionam o desenvolvimento e o aprimoramento de produtos e serviços por parte das organizações de forma compatível com as regras de proteção de dados pessoais, criando um ambiente de segurança regulatória e respeito à privacidade dos titulares de dados pessoais, tudo de forma proativa.

[7] Ibidem.

[8] https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy

3

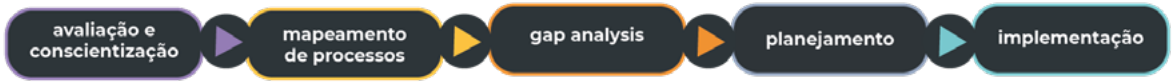
Melhores práticas para um projeto de adequação

Apresentadas algumas opções técnicas e metodológicas de adequação, resta entender o que mais pode ser feito por uma organização para compatibilizar as suas práticas e rotinas às novas regras.

E quando se fala em adequação às exigências da LGPD, uma das metodologias mais completas tem como essência e orientação os fundamentos que norteiam a realização do *Data Protection Impact Assessment* (DPIA). É considerado o método mais moderno para a identificação de riscos de violação de preceitos regulatórios em proteção de dados pessoais.

Os principais objetivos do DPIA são identificar e mapear os riscos, e organizar e encontrar formas de minimizar os eventuais impactos à privacidade e proteção de dados causados pelas práticas de tratamento de dados da organização.

A aplicação dessa metodologia se dá em cinco fases distintas e complementares. Cada fase é extremamente interligada à seguinte, sendo certo que o desenvolvimento mais adequado, mas não exclusivo, das atividades de uma fase depende diretamente da conclusão ou maturidade das atividades das fases anteriores.



Essa metodologia, também conhecida como a metodologia tradicional, apesar de ser mais extensa e complexa, pode ir além de garantir a conformidade de processos materialmente relevantes para uma organização no contexto de privacidade e proteção de dados; acima de tudo, ela é estruturada para ser o primeiro passo ao desenvolvimento de uma cultura de privacidade e proteção de dados dentro da organização de forma generalizada.

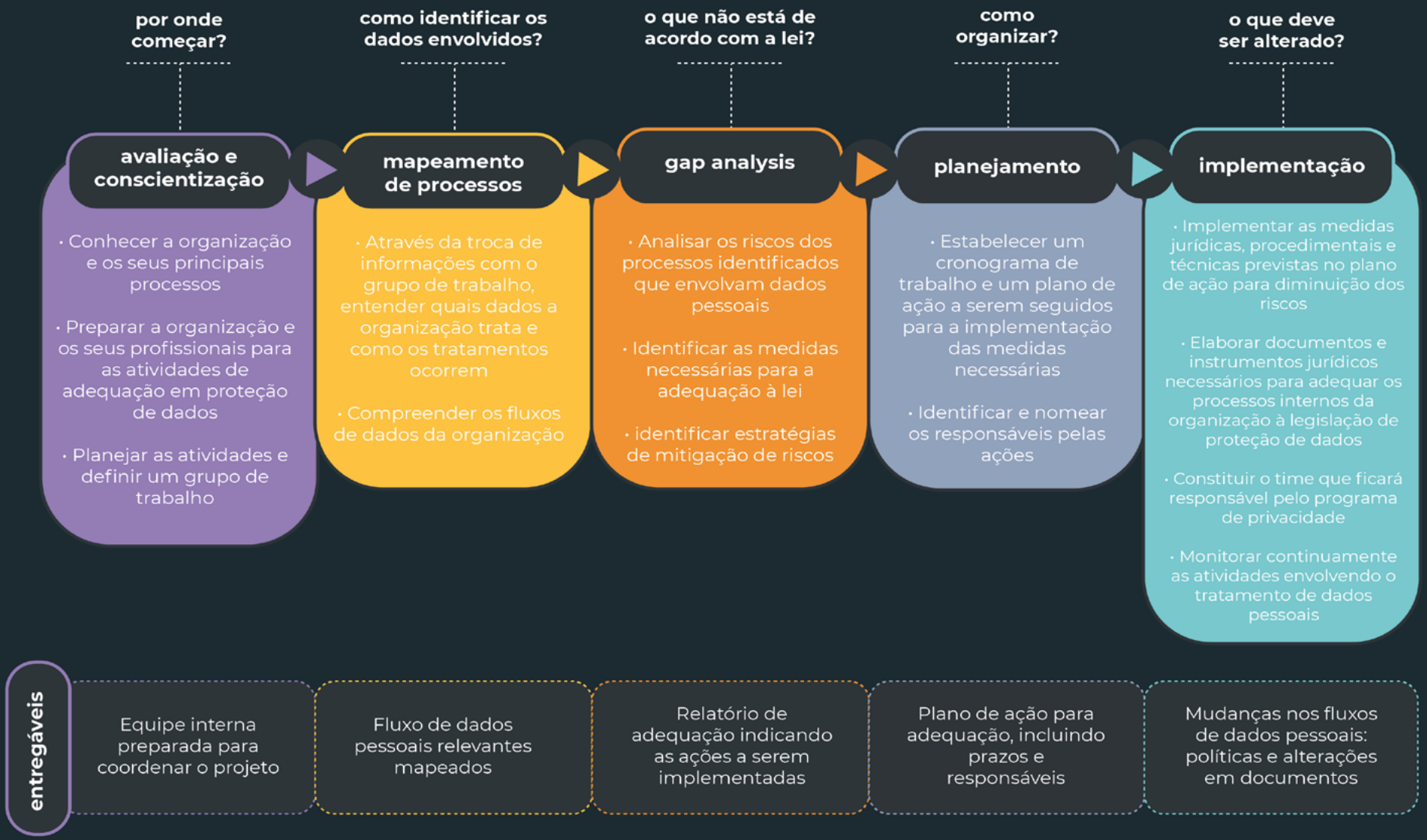
A ideia é que o seu desenvolvimento possibilite a entrega de um programa organizacional maduro e transversal, capaz de demonstrar o comprometimento da organização com o tratamento adequado de dados pessoais em todas as suas frentes de atuação e a implementação de medidas adequadas para a diminuição de riscos regulatórios, ao mesmo tempo que permitirá à organização extrair valor de seus processos, torná-los mais eficientes, inovar e reinventar seus serviços, produtos, procedimentos e plataformas.

Para descomplicar, a seguir apresentamos detalhadamente o passo a passo de cada uma das fases dessa metodologia de processo de adequação à LGPD.

[9] Este manual se limita a comentar o viés jurídico de um projeto de adequação à LGPD, o que não impede que haja, também, em paralelo ou em outro momento, anterior ou posterior, uma análise técnica que englobe sistemas, aspectos de tecnologia e segurança da informação.

BAPTISTALUZ

Em 30s...



3.1. Por onde começar?

AVALIAÇÃO E CONSCIENTIZAÇÃO

O que é?
É o momento de conscientizar e preparar a organização para as atividades do projeto de conformidade com as regras de proteção de dados.

Qual o objetivo?
Familiarizar a organização e seus colaboradores com a metodologia de trabalho e conscientizá-los de que a LGPD deve balizar todo e qualquer negócio e processo que lide com dados pessoais.

Qual o resultado esperado?
Realização de palestras e workshops apontando as principais preocupações sobre proteção de dados, as principais regulações e os efeitos disso na organização. Realizar reuniões de kick-off para definir o time interno que auxiliará no projeto de adequação e familiarizá-los com os detalhes da metodologia do projeto.

Antes de colocar a mão, de fato, nos dados e processos, é preciso preparar a organização de forma eficaz para o processo de adequação que será realizado, inserindo na sua estrutura a importância da cultura de privacidade e proteção dos dados pessoais.

Então, o primeiro passo é conhecer e entender a organização, sua maturidade regulatória e seu modelo de negócio, e, fundamentalmente, entender como ela trata dados pessoais.

Em seguida, é o momento de planejar o escopo de atividades, com foco nas questões jurídicas pertinentes, na determinação dos principais stakeholders (interessados) que estarão envolvidos no processo e na definição das responsabilidades.

NA PRÁTICA

Quem são os principais stakeholders?

- Diretorias | C-Level
- Gerências
- Jurídico | Compliance | Regulatório | Riscos
- Tecnologia da Informação | Segurança da Informação
- Recursos Humanos
- Procurement
- Marketing | Data Science | Business Inteligence
- Produtos | Serviços | Aplicativos

O time interno que auxiliará, junto com os assessores externos, o projeto de adequação deve ser composto por representantes de todas as áreas da empresa, ou macro áreas. Estes serão o ponto de contato, os gestores e os responsáveis por incentivar o adequado levantamento de informações que permitirá conhecer os processos de cada área que lidam com dados pessoais. Com o time formado, dá-se sequência à conscientização e preparação da organização e de seus profissionais para as atividades de adequação a serem desenvolvidas.

O objetivo da preparação de pessoal é aproximar a maior quantidade de pessoas e demonstrar, de forma objetiva, a real importância do tema na vida de todos, seja no contexto das atividades da organização, seja nas diversas situações corriqueiras observadas na vida privada dos colaboradores. Isso permitirá que a organização em geral e todos os diretamente envolvidos na iniciativa de adequação possam "falar a mesma língua" daquele momento em diante.

Então, gaste o tempo que for necessário nessa fase – ela é fundamental para o sucesso do projeto!

Para encerrar essa primeira etapa, deve ser feita uma reunião de kick-off com a equipe responsável pelo projeto de conformidade de proteção de dados da organização, para que seja realizado um treinamento na metodologia de trabalho e finalizado o cronograma inicial.

A partir deste momento, a equipe de trabalho deve estar apta a passar adiante os conhecimentos até então adquiridos para o resto da organização, de forma a contribuir para a disseminação do tema e para facilitar a penetração dos conceitos e objetivos pertinentes ao projeto em todas as áreas que serão envolvidas nos trabalhos.

Vale frisar!

A qualidade do desenvolvimento dessa etapa vai ecoar durante todo o projeto, portanto, é fundamental que ao término dela a organização e seus colaboradores estejam familiarizados com a metodologia e conscientes de que a LGPD e demais normas de proteção de dados aplicáveis não são apenas novas obrigações legais - na verdade, são a nova forma de fazer negócios e estabelecer confiança com os titulares dos dados pessoais.

NA PRÁTICA

Como conscientizar?

- Palestras
- Workshops

Para o máximo possível de colaboradores da organização, de todos os níveis, da diretoria aos prestadores de serviço, apontando as principais preocupações sobre proteção de dados, as principais regulações e os efeitos e impactos delas na organização.

3.2. Como identificar os dados utilizados?

MAPEAMENTO DE PROCESSOS

O que é?
É o momento em que são identificadas as atividades de tratamento de dados materialmente relevantes da organização.

Qual o objetivo?
Conhecer e mapear detalhadamente as atividades de tratamento de dados materialmente relevantes, os fluxos de tais atividades, as suas relações contratuais com os fornecedores e parceiros, os documentos internos relevantes às atividades e solicitação de documentação complementar necessária para entender os processos.

Qual o resultado esperado?
Registro dos fluxos de dados pessoais na organização, identificação de relações contratuais e levantamento de documentos internos relacionados às atividades.

Com a organização preparada para as atividades de adequação à LGPD, o próximo passo é identificar e analisar as atividades de tratamento de dados pessoais. E, para isso, é preciso conhecer não só os dados tratados, mas também o fluxo desses dados dentro e fora da organização.

O que é fluxo de dados pessoais?

Também chamado de *data lineage*, nada mais é do que o caminho dos dados pessoais nas respectivas atividades de processamento, dentro e para fora da organização.

Nesse momento, o essencial é conhecer e mapear os processos materialmente relevantes da organização e, a partir daí, identificar exposições e contingências em relação às regulamentações aplicáveis.

Além de documentar os tipos de dados pessoais utilizados e seu ciclo de vida, é preciso conhecer também, no mínimo: **(i)** as finalidades de tratamento; **(ii)** as eventuais situações de compartilhamento de dados pessoais com terceiros; e **(iii)** os meios (digitais ou analógicos) utilizados para o tratamento de dados pessoais.

NA PRÁTICA

Quais informações são essenciais e como obtê-las.

- Formulários
- Questionários
- Entrevistas com representantes de diferentes áreas
- Mapeamento de fornecedores e parceiros
- Contratos, instrumentos jurídicos relevantes e documentos relacionados às atividades

Depois de mapeados os processos materialmente relevantes, é hora de entender as atividades da organização com maior profundidade por meio do levantamento de informações adicionais, esclarecimentos sobre os processos mapeados e eventuais documentos pertinentes (como políticas e contratos, por exemplo).

O objetivo aqui é garantir que não haja qualquer obscuridade, principalmente nas atividades que impliquem maior grau de risco aos titulares de dados.

Para finalizar essa etapa, deve ser atribuída, a cada atividade de tratamento de dados pessoais, a base legal mais apropriada, conforme as hipóteses previstas na LGPD, a depender dos dados pessoais envolvidos, da sua origem, bem como da finalidade de tratamento em cada caso.

NA PRÁTICA:
como é um mapeamento?

nome do processo	dados pessoais utilizados	quantidade aproximada de pessoas	país onde as pessoas estão localizadas	categoria dos titulares dos dados	finalidade de processo
Cadastro pessoal na recepção do prédio.	nome, RG, CPF e foto	1000 pessoas	Brasil	Colaboradores e visitantes	Identificação das pessoas que circulam no prédio

Origem dos dados	Local de armazenamento	fluxo interno dos dados	transferência a terceiros	período de retenção	base legal
Diretamente dos titulares	Armazenado em servidores próprios	Os dados são fornecidos pelos titulares e são armazenados nos servidores locais	Não há	Não há critério	legítimo interesse

Desenvolver a etapa do mapeamento pode ser algo trabalhoso, sendo certo que compreender e registrar esses fluxos informacionais é algo complexo, principalmente por não existir, ainda, uma delimitação legal ou regulatória daquilo que obrigatoriamente deve ser registrado.

Atualmente, há no mercado diversas ferramentas que podem facilitar os trabalhos desenvolvidos nessa fase do projeto de adequação, por exemplo: *OneTrust | TrustArc | DPOrganizer*, entre tantas outras, que visam a automatizar algumas das etapas necessárias à realização de um mapeamento completo e posterior levantamento de documentos.

Cada ferramenta tem suas peculiaridades e decidir qual a mais adequada depende de uma série de fatores a serem analisados pela organização e assessorias técnica e jurídica. Neste ponto, é importante ressaltar que o mapeamento, assim como as demais fases do projeto de adequação, deve desenvolver-se sempre sob o enfoque jurídico, e não apenas técnico. Em geral, a combinação de esforços de times jurídicos e técnicos é a mais recomendada para o desenvolvimento de um projeto saudável que consiga lidar de forma multidisciplinar com todos os possíveis desafios desse tipo de trabalho.

ATENÇÃO: Não confundir!

Mapeamento de dados
Lei Geral de Proteção de Dados (LGPD, art. 37).

Registro das atividades de tratamento de dados pessoais, ou seja, de que forma os dados pessoais são utilizados: da coleta ao descarte, especialmente quando baseado no legítimo interesse.

Inventário de dados
Decreto do Marco Civil da Internet (art. 13, III, Decreto nº 8.711/16)

Documento detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do responsável pelo acesso e o arquivo acessado.

Data Discovery

Não previsto em lei específica, mas sim em padrões como ISO 27001 e 27002

Trata-se de uma medida mais técnica que visa efetivamente descobrir onde os dados pessoais se encontram, principalmente dentro dos sistemas responsáveis pelos seus tratamentos. Não é apenas saber quais são os fluxos de dados pessoais, mas quais são efetivamente os dados dos titulares, como seu nome, CPF, RG, e-mail, e onde estes estão armazenados. O Data Discovery é essencial, por exemplo, para atender a algumas requisições de direitos, como o de pedir uma cópia dos dados que a organização possui sobre alguém, e a retificação e eliminação destes.

Tempo é dinheiro!

O período de mapeamento de dados constuma ser um dos mais relevantes do projeto, e também que mais consome tempo e recursos da empresa.

Materialidade e relevância precisam ser conceitos estratégicos nessa fase, priorizando processos que são importantes para os objetivos institucionais e estratégicos da empresa, suas perspectivas futuras e o cenário político e judicial em torno do tema. As decisões corretas sobre o que é e o que não é materialmente relevante nessa fase podem ser decisivas para o tempo e custo dos projetos.

3.3. O que não está de acordo com a lei?

ANÁLISE DOS GAPS

O que é?
É o momento em que devem ser analisadas as atividades de tratamento mapeadas com o objetivo de identificar todas as lacunas em contraste com as regras de proteção de dados aplicáveis. Em suma, identificar, dentro da organização, o que não está de acordo com a LGPD e as regras setoriais cabíveis.

Qual o objetivo?
Analisar os riscos de violação a preceitos regulatórios e aos direitos dos titulares dos dados de cada atividade de tratamento de dados pessoais mapeada, levando em consideração o modelo de negócio, os recursos tecnológicos, a governança e a cultura da organização, com o fim de indicar as medidas de adequação à lei e de diminuição de riscos, tanto dos titulares de dados quanto da organização.

Qual o resultado esperado?
Definição de bases legais adequadas para as atividades de tratamento de dados da organização e elaboração de Relatório de Adequação, apontando as medidas necessárias para que processos-chave sejam adequados, além de uma sugestão de plano de ação baseado numa matriz de risco.

O **Relatório de Adequação** é o documento que resulta da análise das atividades de tratamento de dados pessoais e de seus riscos, visando permitir a indicação das medidas jurídicas, organizacionais e técnicas necessárias para a adequação à LGPD e às normais setoriais aplicáveis. É o principal documento dessa fase e nele devem estar descritas, no mínimo:

(i) as atividades de tratamento de dados pessoais e os riscos aos titulares e à organização, considerando a LGPD e outras normas de proteção de dados aplicáveis;

(ii) as recomendações de medidas corretivas e preventivas;

(iii) a priorização destas medidas, considerando o nível de criticidade da atividade de tratamento de dados e a complexidade da sua implementação; e

(iv) a proposta de plano de ação em formato de matriz de risco, baseada no nível de criticidade de cada medida sugerida.

Plano de Ação

Nível de criticidade	Tema	Atividade	Responsável	Prazo	Status
Muito Alto	Revisões Contratuais	[descrição 01]	B/LUZ	20/02/2020	Em andamento
Muito Alto	Gestão de Direitos Titulares	[descrição 02]	Cliente	10/02/2020	Concluída no prazo

Um dos maiores erros na apresentação desse relatório são **recomendações genéricas e sem considerar a realidade da empresa**. O relatório não deve ser somente uma leitura da lei, mas sim uma avaliação das exigências legais frente ao negócio da empresa, os processos mapeados e o que é essencial para o modelo de negócio. Essa diferença é fundamental para uma abordagem de parceria com o negócio, que é muito diferente de uma abordagem meramente de auditoria.

Para que essas descrições sejam possíveis, o Relatório poderá detalhar:

I. As atividades da organização mapeadas que envolvam dados pessoais.

É importante identificar em cada uma delas:

(i) a sua finalidade dentro do funcionamento da organização;

(ii) os titulares dos dados, se são colaboradores, crianças ou idosos, por exemplo;

(iii) o perfil dos dados pessoais tratados, ou seja, se são sensíveis ou não;

(iv) a forma de tratamento, que sistemas são utilizados e se há compartilhamento; e

(v) as recomendações específicas visando à adequação de cada atividade, preferencialmente divididas pelas áreas da organização.

É fundamental que sempre seja dada especial atenção aos pontos que possam trazer maior risco aos titulares dos dados, como o tratamento de dados sensíveis e a existência de titulares de categorias especiais (como crianças e adolescentes, por exemplo).

II. Os requisitos para o tratamento de dados pessoais previstos na LGPD e que se apliquem aos processos identificados

Para que sejam feitas as recomendações específicas de cada atividade, precisam ser levados em consideração os princípios, as bases legais (e respectivas regras) de tratamento de dados e o quanto as práticas da organização estão respeitando os requisitos previstos na lei.

III. O exame das relações existentes entre a organização e os titulares de dados pessoais tratados

É preciso avaliar os tipos de relações existentes entre a organização e os titulares de dados pessoais tratados por ela, incluindo as formas por meio das quais podem eles exercer os seus direitos, bem como o procedimento correto no caso da existência de litígios e reclamações referentes a esse tratamento.

NA PRÁTICA

Digamos que a organização compartilhe os dados dos titulares com terceiros - por exemplo: área de auditoria interna de um hospital que compartilha os dados cadastrais e dados de saúde das pessoas com empresas externas de auditoria, para fins de verificação da qualidade do serviço. Neste caso, devem ser implementados processos de anonimização ou pseudonimização dos dados sensíveis para que estes possam ser acessados pela prestadora de serviços sem que os pacientes do hospital possam ser individualmente identificados.

IV. O exame das relações existentes entre a organização e terceiros

Ainda, para a identificação das lacunas existentes nas atividades de tratamento de dados pessoais, é importante que sejam examinadas as diferentes relações da organização com fornecedores, parceiros, prestadores de serviço etc. Muitos processos do cotidiano da organização dependem desse tipo de relação, de modo que é essencial que essa análise seja feita para fins de garantir uma maior conformidade com a Lei.

NA PRÁTICA

A organização identifica que o contrato firmado com um importante parceiro comercial não menciona, entre suas cláusulas, o cuidado necessário com o tratamento dos dados pessoais dos titulares. Nessa situação, recomenda-se que o documento seja revisto e seja negociada com esse parceiro a inclusão de uma cláusula nesse sentido.

3.4. Como organizar?

PLANEJAMENTO

O que é?
É o momento de estabelecer um cronograma priorizado para a execução dos trabalhos necessários ao cumprimento das recomendações do relatório de diagnóstico.

Qual o objetivo?
Estabelecer por onde e como deve ser iniciada a implementação.

Qual o resultado esperado?
Plano de ação e cronograma de implementação detalhados, com indicação de responsáveis e dos diferentes níveis de criticidade de cada medida.

A partir das conclusões do Relatório de Adequação, deverá ser desenhado um Plano de Ação, que servirá como base para a fase de Implementação do projeto.

Com tantas atividades que precisam ser adequadas dentro da organização, é necessário estabelecer um critério de prioridade para a definição de um ponto de partida. Para essa definição, uma boa saída é a utilização da metodologia "risk-based approach" (lidando primeiro com o que representa maior grau de risco aos titulares e à organização).

Paralelamente a essa metodologia, é válido avaliar, em conjunto com a equipe interna e/ou assessores externos, os custos de implementação das medidas necessárias e a reserva de budget para tanto. É preciso colocar na balança o valor da implementação de determinada recomendação e o grau de risco que a atividade de tratamento de dados pode trazer para decidir, assim, por onde começar.

Também facilita a organização das atividades a partir da delimitação das responsabilidades dos envolvidos na implementação. Uma boa forma de fazer isso é utilizar a metodologia RACI, segundo a qual a atribuição das tarefas é realizada conforme a contribuição de cada parte para a execução das medidas recomendadas, como da forma ao lado descrita:

R
Responsible - aquele que efetivamente realizará a implementação da ação.

A
Accountable - aquele que responde pela implementação.

C
Consulted - aquele que será consultado sobre como fazer a implementação.

I
Informed - aquele que será informado da realização da atividade, sem necessariamente ser envolvido em sua execução.

[10] Não é necessário que todas as atividades tenham os quatro níveis de desenvolvimento.

Desse modo, podem ser listadas as recomendações prioritárias para a diminuição de riscos e os responsáveis pela realização de cada fração das atividades necessárias, inclusive quem deve ser consultado para dar suporte à execução de cada uma delas[10]

atividade	risco	finalidade	recomendação	R	A	C	I
Monitoramento das atividades dos colaboradores através de captura da tela minuto por minuto	Alto	Garantir que o colaborador acesse apenas sites relacionados a sua atividade laboral	Adotar medidas de minimização, através da implementação de tecnologias que proíbam o acesso a determinados sites	Departamento de TI	Departamento de TI	Jurídico / Compliance	Departamento de Recursos Humanos

Nesse caso, o risco jurídico envolvido no processo descrito seria alto em função de não estar sendo respeitado o princípio da necessidade (minimização) previsto na LGPD. Para garantir que o colaborador acesse apenas sites relacionados a sua atividade laboral, não é necessário que ele tenha sua tela capturada a cada minuto.

A implementação de algum mecanismo tecnológico que proíba o acesso a determinados sites, como redes sociais, caberia, por exemplo, ao departamento de tecnologia de informação da organização. Tudo isso, claro, com o devido alinhamento aos departamentos de compliance e jurídico de modo a permitir a incorporação dos requisitos legais e regulatórios aplicáveis à ferramenta eventualmente utilizada.

Idealmente, a organização também pode atribuir diferentes níveis de responsabilidade dentro da matriz RACI para os vários departamentos e profissionais que serão envolvidos em cada atividade necessária à adequação, indicando de forma clara a extensão da participação de cada componente da organização nessa fase do projeto.

3.5. O que deve ser adequado?

IMPLEMENTAÇÃO

O que é?
É o momento em que são implementadas as medidas visando à conformidade legal, organizacional e técnica, bem como à prevenção de riscos.

Qual o objetivo?
Executar as atividades previstas no plano de ação.

Qual o resultado esperado?
Elaboração e atualização de produtos, serviços, processos, práticas, plataformas, contratos e documentos necessários para adequar as atividades de tratamento da organização à LGPD.

Entre tais medidas e providências, geralmente podem estar as seguintes:

I. Programa de Governança em Privacidade e Proteção de Dados Pessoais

Desenvolvimento e implementação de uma estrutura corporativa abrangente de proteção de dados, incluindo papéis e responsabilidades de diferentes atores para garantir a manutenção da cultura de privacidade na organização. Para permitir a continuidade de tal programa, deve-se estabelecer um time, interno ou externo, de funcionários ou assessores, que ficará a cargo de gerenciar, supervisionar e revisar todo o programa de governança em privacidade e proteção de dados (privacy team). A figura do Encarregado, ou Data Protection Officer (DPO), pode ou não fazer parte desse time, pois este pode ser executor de atividades mais estratégicas e/ou de auditoria.

II. Revisão de contratos e instrumentos jurídicos contratuais

Adequação dos contratos da organização às atuais necessidades regulatórias e aos princípios gerais de proteção de dados, como:

(i) contratos com fornecedores e parceiros;

(ii) contrato intragrupo, que prevê o tratamento de dados dentro do grupo econômico da organização;

(iii) instrumentos jurídicos para validar a transferência internacional de dados, quando for o caso; e

(iv) documentos internos, como termos de confidencialidade, contratos de trabalho e aqueles referentes a informações dos colaboradores, com o intuito de reforçar a importância do tema da privacidade.

NA PRÁTICA

Digamos que um determinado fornecedor seja responsável pelo fornecimento do software de folha de pagamento da organização e que, no contrato firmado entre as partes, não haja cláusula estabelecendo um nível adequado de proteção aos dados pessoais coletados. Será necessário o aditamento do contrato para incluir cláusula específica ou anexo de proteção de dados pessoais e segurança da informação para, entre outras questões, garantir que os dados sejam utilizados pelo fornecedor apenas quando necessário para a execução do objeto do contrato, proibindo quaisquer formas adicionais de uso, como o seu compartilhamento com terceiros.

III. Desenvolvimento e aperfeiçoamento de políticas e processos

Adequação de políticas internas e externas da organização incluindo as Políticas e processos relacionados à/ao:

(i) Tratamento de Dados Pessoais;

(ii) Segurança da informação, continuidade dos negócios e resposta a incidentes;

(iii) Exercício de direitos dos titulares;

(iv) Relação com fornecedores e parceiros;

(v) Recursos humanos;

(vi) Ciclo de vida dos dados;

(vii) Uso de *cookies* e tecnologias similares;

(viii) Relatório de Impacto à Proteção de Dados Pessoais;

(ix) Revisão periódica do programa de governança; e

(x) Treinamentos e conscientização.

NA PRÁTICA

Exercício de direitos dos titulares

Deve ser avaliado se existe uma ferramenta que permita aos titulares exercer os seus direitos de uma forma fácil, como um canal de contato entre os titulares e a organização, onde possam ser feitas requisições (como de exclusão ou correção de um determinado dado). Caso não exista nenhuma ferramenta que cumpra essa função, é recomendado que seja implementado algo do gênero, preferencialmente algum mecanismo tecnológico e interativo, como um *privacy dashboard:*

Relação com fornecedores e parceiros

Recomenda-se a elaboração de um questionário para futuros fornecedores para obtenção de informações e documentos que ajudarão a entender o nível de padrões de segurança da informação e de conformidade com a legislação. Devem ser feitos questionamentos como: (i) se a empresa dispõe de uma política de privacidade publicamente disponível; (ii) quais são as medidas técnicas que a empresa utiliza para proteção de dados; (iii) a qualidade do programa de segurança da informação da empresa; e (iv) a qualidade do programa de privacidade geral da empresa.

As políticas devem ter como principal objetivo fornecer informações aos titulares sobre o tratamento de dados pela organização e sobre as suas práticas de proteção e segurança, bem como definir diretrizes internas para estabelecer processos como, por exemplo, responder a um incidente de segurança da informação ou atender a requisições de direitos dos titulares.

Uso de cookies e tecnologias similares

Caso a organização tenha um website que utilize cookies e tecnologias de rastreamento similares, é necessário que se tenha uma forma de controle e de obtenção de informações sobre o funcionamento de tais tecnologias. É recomendável que sejam implementadas ferramentas técnicas que possibilitem a obtenção e a gestão do consentimento dos usuários do website e o efetivo controle sobre o uso de cookies, em conjunto com a publicação de uma política que explique para os titulares o que são os cookies, para que servem, quais tipos são utilizados pela organização e quais as finalidades, entre outras informações, que tragam maior transparência aos titulares sobre toda a extensão do uso de referidas tecnologias.

IV. Análises Privacy by Design & Privacy by Default

No caso de serviços e produtos ainda em fase de concepção e produtos já existentes, mas que precisem ser repensados para incorporar princípios de proteção de dados, é recomendado que sejam feitas análises de Privacy by Design & Privacy by Default.

Como já abordado no item 2.2, tais análises tratam de incorporar salvaguardas de privacidade e proteção de dados pessoais durante o desenvolvimento ou revisão de soluções, para que sejam adotadas todas as medidas aptas a proteger os dados pessoais.

V. Avaliações de impacto à proteção de dados pessoais

Devem ser realizadas avaliações para o planejamento de atividades de tratamento de dados pessoais que possam gerar riscos às liberdades e aos direitos fundamentais dos titulares, como no caso de atividades em que a base legal mais adequada seja a do legítimo interesse, quando poderá ser necessário, por exemplo, realizar testes de balanceamento e proporcionalidade, conhecidos como Testes de Legítimo Interesse.

Avaliações desse tipo têm como principal objetivo apontar as medidas, as salvaguardas e os mecanismos de diminuição de riscos para situações específicas que requeiram especial atenção da organização.

NA PRÁTICA

Imagine que uma determinada organização está elaborando um novo produto, como o desenvolvimento de um aplicativo de delivery que, em parceria com diversos restaurantes, faz a entrega dos pedidos dos usuários. Para esse tipo de aplicativo, é necessário ter, ao menos, alguns dados pessoais da pessoa que deseja pedir e receber o produto.

Uma análise de Privacy by Design contribuirá para que o projeto do aplicativo seja formulado em respeito aos princípios da LGPD, identificando, por exemplo, quais dados são realmente necessários e como eles devem ser tratados de forma compartilhada entre a organização e os restaurantes parceiros evitando que sejam transferidos dados como o e-mail, telefone e número de documento do cliente, uma vez que desnecessários para a realização da entrega. Dessa maneira, o design da aplicação já incorporaria os princípios de proteção dos dados desde a sua concepção.

Uma organização deseja dar especial atenção a uma determinada atividade, como a de compartilhamento de dados de saúde de pacientes com uma empresa de tecnologia que, por sua vez, possua uma solução de inteligência artificial para detectar padrões de determinadas doenças. Os dados de saúde são dados sensíveis, de forma que o seu tratamento compartilhado pode apresentar um risco alto para a organização e para o próprio titular dos dados.

A elaboração de um relatório de impacto deve revelar de forma detalhada todos os riscos desse tratamento e, especialmente, o impacto que esse tipo de atividade teria para a privacidade e os direitos dos titulares de dados, bem como apresentar todos os possíveis mitigadores de tais riscos, visando à sua implementação antes de disponibilizar o serviço ou realizar o compartilhamento.

VI. Orientações para a implementação de medidas de adequação

A organização pode manter interações multidisciplinares e multidepartamentais ao longo de todo o projeto, especialmente na fase de implementação. Para tanto, é essencial que áreas operacionais, jurídicas, técnicas e de segurança possam "falar a mesma língua" para definir as práticas mais adequadas a cada situação, efetivamente compreendendo os gaps e tomando as medidas necessárias para remediá-los.

VII. Orientações para que a organização disponha de planos de resposta a incidentes de segurança da informação

O Plano de Resposta a Incidentes tem por objetivo permitir que a organização possa responder adequadamente a incidentes e tomar as ações de remediação adequadas, bem como estabelecer comunicações com a ANPD e com os titulares eventualmente afetados por incidentes, nas situações em que estes possam acarretar riscos ou danos relevantes.

NA PRÁTICA

Os principais envolvidos na execução das etapas de implementação das medidas de adequação devem dispor de meios aptos a manter uma comunicação eficiente durante os seus trabalhos. A interação multidisciplinar nesses contatos é um elemento essencial ao correto tratamento de questões que envolvam a revisão de procedimentos internos, relações com parceiros e funcionalidades de sistemas, por exemplo.

O plano de resposta deverá conter, no mínimo:

1. Definição de incidente

2. Definição de ações que os colaboradores devem adotar antes, durante e após o incidente

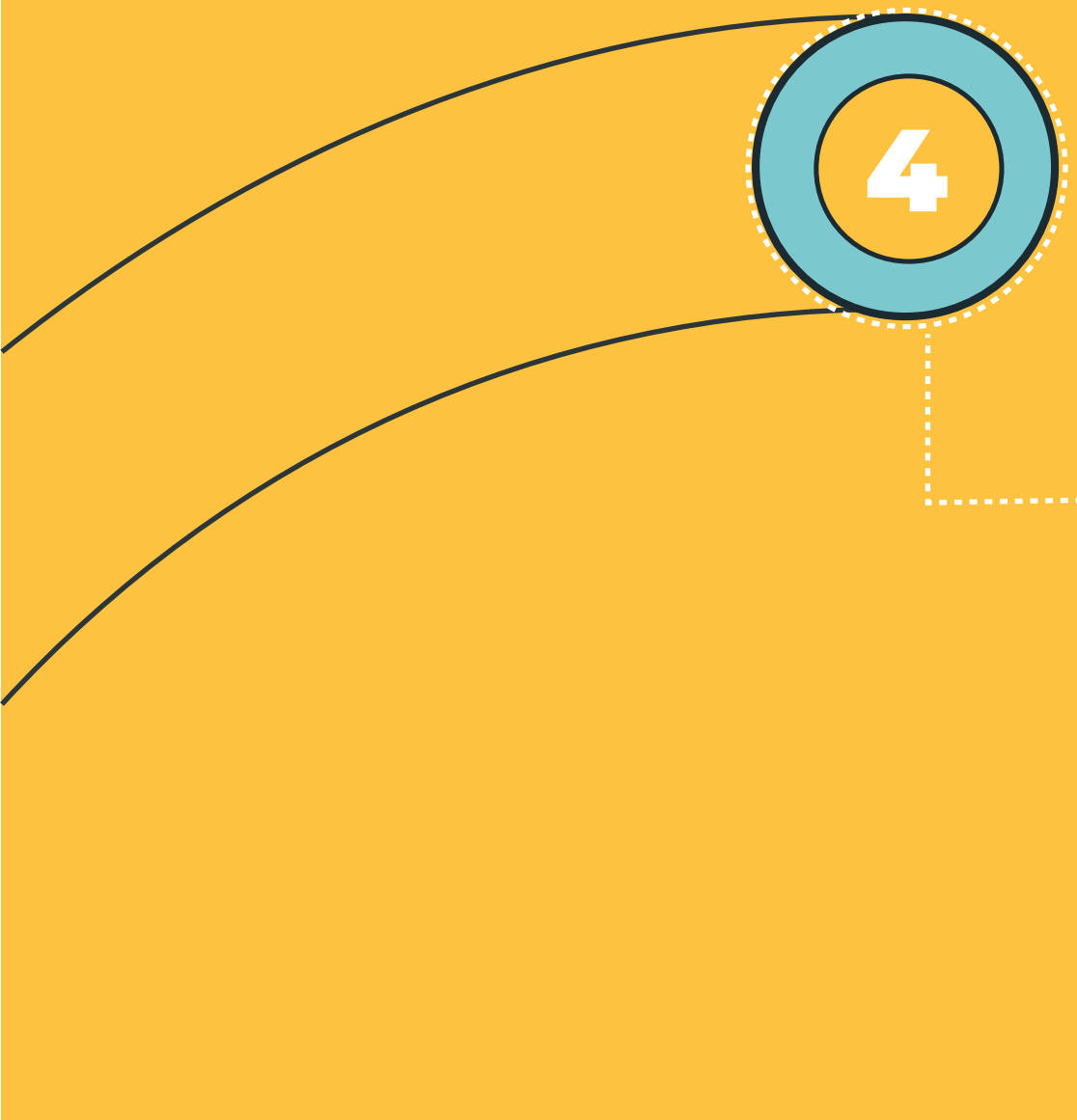
3. Definição de procedimentos e equipe de resposta

4. Descrição da natureza dos dados pessoais afetados

5. Indicação sobre informações dos titulares envolvidos

6. Indicação do nível de risco e de gravidade do incidente

7. Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados e mitigação dos danos aos titulares.



Terminada a implementação, qual é o próximo passo?

Terminada a implementação, qual é o próximo passo?

MONITORAMENTO

O que é?
Manutenção do Programa de Governança em Privacidade e Proteção de Dados Pessoais.

Qual o objetivo?
Garantir que a organização mantenha suas atividades em nível adequado de conformidade com a regulação de proteção de dados, mesmo diante de eventuais alterações na sua forma de fazer negócios, da adoção de novas tecnologias e criação de novos produtos e serviços.

Qual o resultado esperado?
Atualização e manutenção da conformidade e do Programa de Governança em Privacidade e Proteção de Dados.

A adequação de uma organização à LGPD e a demais regulamentações que tratam de privacidade e proteção de dados não se encerra após a implementação completa do plano de ação mencionado.

A organização é um organismo vivo e o cenário jurídico nacional sobre privacidade e proteção de dados também está em constante desenvolvimento, de modo que é fundamental internalizar uma **contínua busca por adequação e atualização,** sobretudo por meio da manutenção do Programa de Governança em Privacidade e Proteção de Dados Pessoais.

Assim, é essencial contar com profissionais internos e/ou externos que sejam capazes de lidar com todos os desafios trazidos pela legislação de proteção de dados. Deve ser constantemente posta em evidência a necessidade da existência de uma cultura de privacidade nas mais diversas atividades diárias da organização, o que pode ser reforçado com treinamentos, acompanhamento regulatório, conscientização sobre as políticas internas e sua aplicabilidade, análises *Privacy by Design* e *Privacy by Default*, gerenciamento de incidentes de segurança, dentre outras ferramentas.

5

Considerações Finais

Em um cenário econômico cada vez mais guiado e orientado por dados pessoais, a tarefa de adequação à LGPD revela-se obrigatória para viabilizar o desenvolvimento de negócios e cada vez mais fidelizar clientes e colaboradores.

A execução de um projeto de adequação não busca apenas eliminar riscos regulatórios e eventuais sanções, mas fundamentalmente alinhar a atuação da organização aos padrões globais de respeito à privacidade e proteção de dados pessoais. É um projeto contínuo, que demanda atualizações periódicas e monitoramento constante.

O projeto de adequação deve ser entendido como uma forma de agregar valor aos negócios, produtos e serviços, em íntima sintonia com a crescente conscientização dos consumidores sobre o valor de suas informações pessoais, sendo possível que as organizações aproveitem esse momento para estabelecer um enorme diferencial competitivo e demonstrar que realmente se importam em proteger dados pessoais sob o seu controle.

Quanto antes a cultura de privacidade e proteção de dados for internalizada e disseminada dentro das organizações, mais fácil será navegar, crescer e se transformar no novo cenário econômico que se desenha.

BAPTISTA LUZ
ADVOGADOS

contato@baptistaluz.com.br

Acesse **baptistaluz.com.br** para conhecer nossos setores de expertise e ler mais sobre os temas sobre os quais geramos conteúdo com abordagem prática.

nossas **unidades**

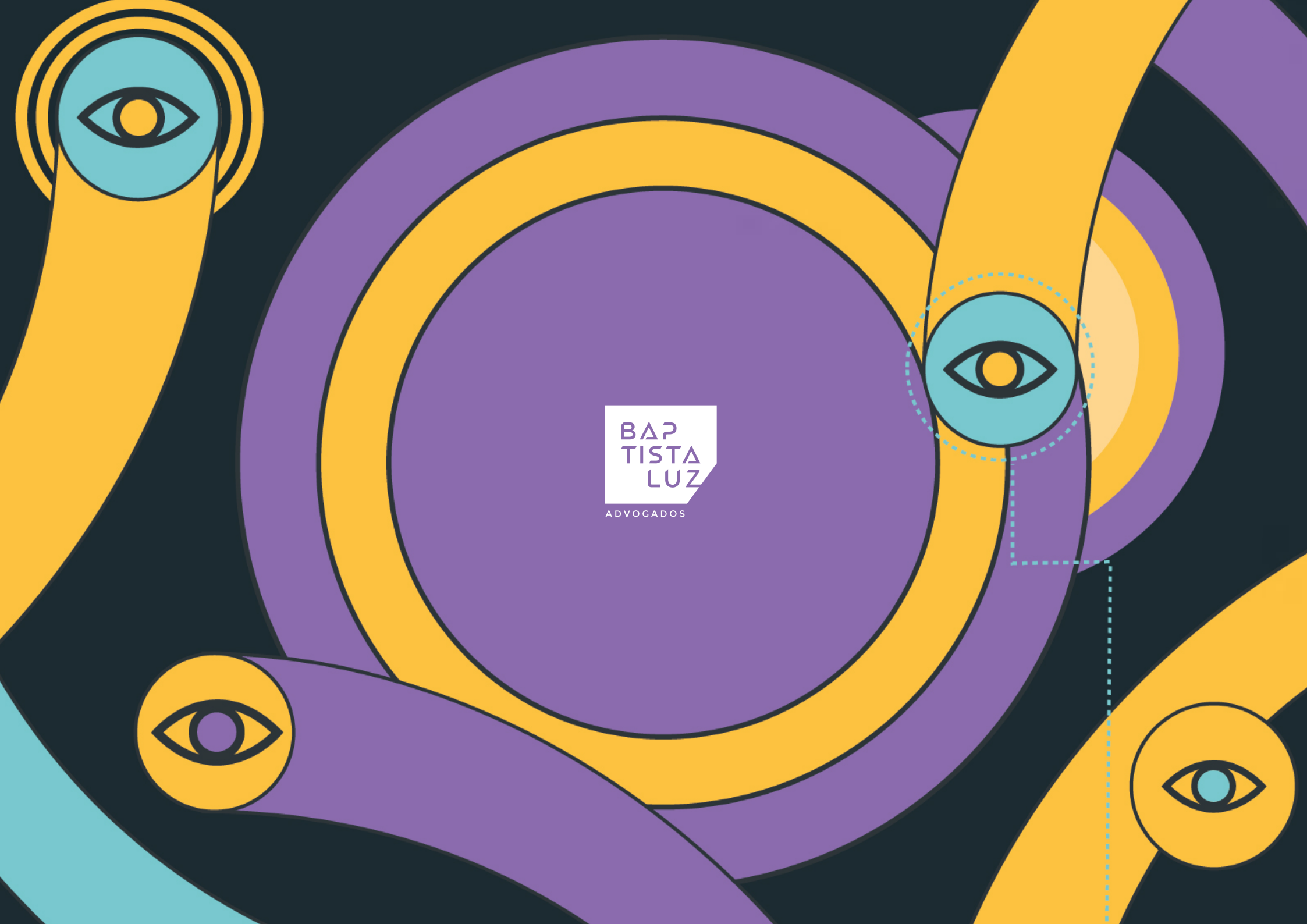
SÃO PAULO
Rua Ramos Batista, 444 / 2° Andar
Vila Olímpia / São Paulo / SP
Tel +55 11 3040 7050

PORTO ALEGRE
R. Carlos Trein Filho, 599 / 11° andar
Auxiliadora / Porto Alegre / RS
Tel +55 51 3207 9057

FLORIANÓPOLIS
Rua Bento Gonçalves, 183 / Sala 1001 /
Centro / Florianópolis / SC
Tel +55 48 3225 6468

LONDRINA
Rua Ayrton Senna da Silva, 300 / Sala n° 1801
Gleba Palhano / Londrina / PR
Tel +55 43 3367 7050

MIAMI
1110 Brickell Ave / Ste 200
Miami / FL 33131


BAPTISTA LUZ
ADVOGADOS