PRO-AUDIT

# DESMISTIFICANDO A LGPD

Março/2020

# ❖ Introdução

A essa altura, você provavelmente já ouviu falar sobre a Lei Geral de Proteção de Dados (LGPD). Aprovada em agosto de 2018, a LGPD é a resposta brasileira a um movimento global de países que reconheceram a necessidade para as novas relações que se estabelecem em uma sociedade cada vez mais movida a dados.
Esse movimento começou há décadas em outros países e blocos econômicos e ganhou força em 2018, com a vigência da nova regulação de proteção de dados da União Europeia - a General Data Protection Regulation (GDPR).

Agora, o Brasil não só superou o atraso nessa pauta, como soube se valer desse atraso, aprovando uma regulação equilibrada, que conjuga a garantia e direitos com o fomento à inovação. A LGPD, assim como a GDPR, tem a função de proteger a privacidade e outras liberdades fundamentais dos cidadãos, ao mesmo tempo em que promove o estímulo a modelos de negócios e políticas públicas que são viabilizadas através do tratamento de dados pessoais e/ou a monetização dessas informações.

Apesar de uma nova regulação causar receios em relação aos custos de conformidade (o "Custo Brasil"), a LGPD representa uma janela de oportunidades. Primeiro, porque as organizações terão que colocar "ordem na casa", na medida em que terão que conhecer melhor todas as suas bases de dados e lhes atribuir uma finalidade específica. É um exercício que poderá trazer insights para se repensar o próprio modelo de negócio e até mesmo para lançar novos produtos e serviços. Segundo, a adequação à legislação de dados pessoais pode melhorar a reputação da empresa, na medida em que o tratamento adequado dos dados pode ser explorado no seu plano de comunicação para reforçar a confiança com o titular da informação. Terceiro porque a lei traz uma série de exigências relacionadas à segurança da informação no sentido não só de prevenir o "vazamento" de dados, mas, também, de remediá-los da forma mais eficientes caso ocorram. Certamente, organizando esses quesitos, será mais fácil identificar e remediar qualquer tipo de incidente. Tratam-se de medidas cujo saldo final pode agregar valor e competitividade a uma organização.

Em agosto de 2020, todo negócio que fizer o uso de dados pessoais já deverá estar em conformidade com as novas premissas. Por isso, o processo de adequação precisa se iniciar agora. Para te ajudar com isso, este material traz um sobrevoo sobre a LGPD, explicando uma visão mais prática para você, como gestor da empresa, precisa fazer para se adequar às exigências e canalizá-las como um benefício para sua organização.

# ❖ Expertise

Atuamos em Tecnologia da Informação, a 35 anos. E nos últimos 14 anos, focamos nossa atuação em **Governança** (Implementação de Boas Práticas), **Otimização** (Fazer Mais com Menos), **Compliance** (Adequação às Leis e Normas) e **Quality Assurance** de Projetos.


Em início de 2018, por força de contrato de parceria com a IBM, recebemos capacitação e tivemos que adequar nossos padrões de trabalho a GDPR e a normas de Compliance. E em seguida, veio a LGPD. Ela foi aprovada em agosto e logo comecei a questionar nossos clientes e ninguém sequer sabia que a Lei existia ou tinha ouvido falar.

Preparei um material/apresentação, sobre a Lei. E divulguei. Simples e prático. Está sendo enviado junto com este artigo. Mas a resposta dos clientes foi a mesma*, não sabemos e vamos esperar*.

Nós temos expertise em Compliance, com vários processos de adequação à Lei de Software e Lei de Informática, principalmente. Atuamos em conformidade com padrões da IBM e Microsoft. E compreendemos o todo, e não apenas parte do problema. Nossa atuação está balizada nisso. Sempre damos ao cliente a solução mais racional e clara aos clientes atendidos. Nossa visão de trabalho é atuar com uma auditoria (Assessment Compliance) do processo do comitê/DPO e focado em Quality Assurance do processo como um todo.

Outro ponto chave de nossa atuação sempre foi a visão de que a TI, como setor, deve propiciar a disseminação de conhecimento, compartilhando, orientando e fazendo a empresa como um todo crescer tecnologicamente, trazendo inovação, melhorias e agilidade aos negócios.

# ❖ Mercado e LGPD

Inevitável, nesses últimos tempos, receber uma enxurrada de informações sobre LGPD. E por atuar em Compliance e já ter atuado um pouco com a GDPR (norma Europeia), compreender que existem informações verídicas, que legalmente deveremos nos adequar, mas que também há um sensacionalismo comercial para colocar todo mundo "contra a parede" para se adequar rápido, de qualquer jeito e implantar controles, softwares e etc.... Contratar DPO, criptografar dados, e assim vai...

Não estou "pregando" desobediência civil. Longe disso. Estou definindo que Compliance, se faz com COÊRENCIA.

Estudamos muito a LGPD. Vários eventos, treinamentos, palestras e webinar. Todos em geral tem um único objetivo, vender algo. Ou software, ou serviços de DPO, ou segurança, ou alguma coisa...

Demoramos um pouco para compreender, aonde agregariamos mais aos nossos clientes. Qual a melhor forma de atuar em LGPD? Como posso trazer mais resultados aos nossos clientes pela minha atuação?

Então resolvemos escrever esse artigo, pois compreendemos que NOSSA orientação, experiência e visão sobre LGPD, pode propiciar algo de positivo aos nossos clientes. A intenção do texto não é ser técnico, é mais como um bate papo detalhando as nossas percepções sobre a Lei e sua aplicação.

E com relação a isso, só peço se o artigo lhe ajudou que divulgue aos seus contatos de outras empresas. Desde já fico ao dispor para eventuais dúvidas e/ou questionamentos.

Acompanhe conosco **e**
**boa leitura!**

Março/2020

# ❖ O que é a Lei?

Não entrarei nos detalhes técnicos e legais, mas sim em uma PERSPECTIVA que tenho sobre a Lei em si:

1. NOVIDADE: A Lei não trouxe NENHUMA novidade, ela está trazendo a OBRIGAÇÃO de Boas Práticas de Governança, existente a 20 ou 30 anos, que são claras na ISO 27000, com COBIT e ITIL. Ou seja, na realidade as empresas já deveriam ter esses procedimentos internalizados.
   O que eu costumo ouvir: *"Segurança da informação é pertinente, é importante. Mas não é prioritário*". E não é prioritário por que envolve custos que reduzem o resultado no final do ano.

   **Então é uma coisa que é sempre postergada. Só que com a Lei, isso acabou**.

2. CONTINGÊNCIA: Nas nossas experiências, dentro das nossas qualificações, trato muito de plano de continuidade de negócios, contingência e redundância. Tenho claro o que vejo no mercado, que 8 entre 10 empresas que tem plano de continuidade implementado, NUNCA testaram. A ISO 27000, por exemplo, você encontra ela em praticamente todas as circulares do Banco Central e especialmente a circular de Ciber Segurança, em que há o enfoque em necessidade do plano de continuidade, mas são detalhes que todo mundo conhece de trás para a frente, mas são relegados a segundo, terceiro ou último plano dentro das empresas.

   **Mas o mais preocupante é que 90% das empresas NÃO tem esse plano.**

3. TRABALHO JURÍDICO: Então inicialmente, foi abordado e analisado por vários especialistas jurídicos e grandes advogados/escritórios. Pouquíssimos deles reconheceram o seu percentual de participação na adequação. Muitos advogados acharam que pelo termo LEI era um assunto jurídico e quando tentaram implementar tiveram problemas gravíssimos. Por que eles ofereciam a conformidade da Lei aos seus clientes e na verdade, na execução não conseguiam chegar ao final.

   **Um comentário que vimos de um advogado, reflete essa realidade: "O técnico menos capacitado sabe mais de TI que o mais capacitado dos advogados". E isso espelha o requisito que a Lei exige em segurança de informação.**

4. ENVOLVIMENTO: No que tange a adequação da Lei, entendo que a uma participação muito maior das áreas de negócio/processo propriamente ditas, ajustes de procedimentos processuais do que procedimentos de segurança ou ajustes de tecnologia da informação.

# ❖ LGPD – Percepções:

Para que meu raciocínio fique mais claro, procurei traduzir a minha abordagem da Lei, sua adequação e busca de Compliance em visões:

## ADEQUAÇÃO

A LGPD não é um projeto, uma implementação ou um serviço de adequação que tem início, meio e fim.
É uma norma, um Lei que deve ser seguida, obedecida e atendida.
No mundo empresarial, um PROCESSO PERMANENTE. Quem conhece e tem implementado a NBR ISO9001(sistema de qualidade), tem a visão de processo, controle e auditoria.
A LGPD é muito próxima a isso. Ela inicia com uma implementação/adequação, mas que vai ser tornar um processo recorrente, de controle, informações/evidências, auditorias.
A diferença principal é que no caso da ISO, chamamos o auditor, agendamos auditorias e buscamos a Certificação ISO. E o pior que pode acontecer é a Não-Certificação.
Na LGPD, a existência de processo, evidências, controles e documentações podem evitar Multas, sanções e Paradas Operacionais.
Mas reforço, devem ser encaradas como mesmo enfoque. Um processo, um sistema completo de gerenciamento. No caso da ISO9001, QUALIDADE. No caso da LGPD, PRIVACIDADE.

Acreditamos, com convicção de que a LGPD deve ser desenvolvida internamente e que 50% da implementação é ajuste de processo. E não vai existir software e hardware que faça isso. Isso é feito pelas pessoas, com treinamento, orientação e documentação. Processo a processo. Analisando 1 a 1.

## ESTUDOS DA LEI

Estudar LGPD para implantar em uma empresa é igual a aprender a dirigir decorando o código nacional de trânsito. Se até pelada de rua tem regra, como eu vou implementar a conformidade de uma organização a uma lei tão extensa, como a LGPD, se eu não defino estas regras?
Privacidade e Compliance são coisas que poucas pessoas conhecem. Então como eu vou começar a falar da noite pro dia sobre privacidade, cobrar privacidade dos funcionários se eles não sabem o que é. Eu preciso dar para eles uma referência. E essa referência vai ser baseada em que?

Na política de privacidade/segurança e no código de ética e conduta da empresa.

## NÃO É SÓ TI

Seguindo a visão A, a LGPD não é um processo de TI. É um processo da EMPRESA.
Primeiro, por que não são somente dados lógicos que podem "descumprir" a Lei. Uma ficha de cadastro, de cliente ou de funcionário podem causar mais estrago que um dado armazenado, se isso "vazar".
Então, se não é somente dado armazenado em servidores de banco de dados e arquivos, as ações não podem ser direcionadas apenas a TI.
Outro erro recorrente é jogar tudo para o lado jurídico. A participação que vejo do jurídico é de, no máximo, 15% do processo todo.
É baseado em orientação e interpretação da Lei, documentar a base legal da coleta, análise e ajuste de contratos, eventuais procedimentos judiciais e de consultoria frente a termos, procedimentos e implicações legais. Além de alinhamento da política de privacidade, de segurança e o código e conduta/ético. Não vejo o jurídico atuando mais que isso no processo de conformidade.
Basicamente vai atuar em 3 situações:

1. ocorreu um vazamento e precisamos verificar o que houve de fato.
2. houve um vazamento sim, a empresa verificou e se denunciou.
3. denúncia de cliente, fornecedor ou concorrente querendo quebrar as pernas da empresa. Isso aconteceu muito na Europa, de maio de 2018 a maio de 2019, o site da autoridade europeia recebeu mais de 60 mil denúncias.

## DIVISÃO POR ÁREAS

As áreas de negócio são responsáveis por 50% do processo da conformidade com a Lei.
O Jurídico, como já citei, representa uns 15% do processo.
O TI (Tecnologia da Informação) já presta seu serviço de infraestrutura, o que vai ter que fazer é adequar procedimentos e processos a alguns requisitos de lei que tem relação com mapeamento de dados, estruturação e proteção. Isso representa uns 15%.
A SI (Segurança da Informação) fortalecendo os 8 itens da norma 27000, que a Lei exige. E que ninguém tem implementado. Existem algumas implementadas, mas o conjunto não é encontrado.
Partindo da mais básica, política de segurança, todo mundo tem.
Mas se você for dentro da empresa e questionar qualquer funcionário, até mesmo ao nível de gerência, eles sabem o que está lá e seguem no seu dia-a-dia? Estamos falando RH, de Produção, de Comercial, de Marketing, de Compras, de todos que coletam e efetivamente trocam e processa informação privada da empresa.
Cabe a SI, uma parte de 20% do processo todo.

## EVIDÊNCIAS

Temos que nos preocupar, ou dar foco a criação das evidências de atendimento aos mecanismos de controle da Lei.
Quando não temos um caminho, como é o caso a LGPD, temos que construir.
Para eu poder tratar o processo de conformidade é importante tração um plano estruturado, que no nosso entendimento, começa pela criação de um comitê multisetorial/disciplinar que tratará as ações e balizará a condução do processo.
E um desses membros, deve ser encaminhado a ser o DPO (encarregado pela privacidade na empresa), que é o "pai da criança".
Em seguida deve ser criada uma política de segurança "coringa"/genérica, que irá nortear as ações do comitê e o restante do processo. Isso é o básico.
É importante fazer o detalhamento/planejamento do processo em sequência de ações.

## DIREITOS DO TITULAR

Pela nova Lei o titular dos dados tem direito de: acessar, revisar, alterar e até solicitar exclusão da base de dados.
Mas como eu posso evidenciar a exclusão da informação de alguém?? Você tem um contrato meu assinado, e digo que "quero que destrua esse contrato". Como evidenciar que destruiu esse contrato? Não tem como, por que o contrato foi destruído. E aí você destrói a evidência.
Como você prova que executou esse processo?? Assim como em um processo de ISO9001, formalizando o procedimento em um documento. Por que a agência (ANPD) também vai ter boa fé de chegar e dizer, "mas você destruiu". Você pega o documento, nós temos um processo, o responsável é fulano, ele faz assim, é destruído dessa forma e é descartado desse jeito.
Existe um processo.

Muito diferente de você chegar e dizer "eu descarto". E a evidência? Não tenho. Como você faz? Eu aperto delete.

Segurança da informação é antes de tudo a criação de evidências.

## PRAZO

Por conta da Lei, o prazo é para se cobrar das empresas a conformidade. Se a Lei começasse a valer hoje, as empresas que não estivessem em conformidade NÃO seriam multas ou sofreriam sanções. A não conformidade não gera multa. Somente se houver o vazamento e você não estiver em conformidade, aí teremos multas e sanções.
Ai qual o risco que a empresa corre. Como hoje ninguém pode ficar calado, senão vai estar indo contra a Lei, a autodenúncia é OBRIGATÓRIA, e por isso estamos vendo tantas notícias de que houve vazamentos ultimamente. Então, você não pode ficar quieto. Diz: "sofri um vazamento! ". O que vai acontecer? O MP (Ministério Público) vai bater na porta e solicitar: "Me mostra as evidências de atendimento a Lei". AI você não tem NADA. É a diferença entre uma multa de 2 milhões e 500 mil. Isso é óbvio, pois a própria Lei diz que existem 11 medidas atenuantes e as medidas atenuantes mais poderosas é a implementação de procedimentos e políticas que eliminem os riscos de vazamento.
Ouvi, de clientes, o posicionamento de que a aplicação da Lei poderia ser prorrogada. OK. Mas o fato disso acontecer não nos isenta de sua aplicação e que a empresa tem que se adequar.
A visão de que uma prorrogação de prazo, seria "ganhamos tempo", é muito simplista. Pois se houver vazamento e não houverem evidências da adequação, a multa é grande. Se você apresenta evidências de que estão fazendo o processo de forma correta e coerente, há a possibilidade de contestar o valor e trazer essa multa para um valor irrisório. Podendo chegar até a uma penalidade simples, sem valores financeiros, dependendo do tipo de vazamento.
Qual a vantagem de se trabalhar logo no assunto?
Se levar em conta que já existe um acordo entre Mercosul e União Europeia, estreitando parcerias/linhas comerciais, só vai participar quem estiver ajustado e em conformidade com a LGPD/GDPR. E Não estamos falando de nada de outro mundo. Estamos falando de boas práticas, reconhecidas, testadas e amparadas.

## TRADUÇÃO

Temos que ter claro, que a LGPD não é uma Lei. Ela copiou um Regulamento que tem uma base técnica, que pela tradução se PERDEU. Quando houve a tradução da GDPR, General Data Protector Regulament, para Lei Geral de Proteção de Dados, colocando a palavra "LEI" e "DADOS" dentro da mesma oração houve uma polarização entre o jurídico e a TI. Quando você fala em regulamento, tudo muda. Então a primeira coisa a fazer é entender o que a LGPD é. E o que você vai contratar. Senão ouvindo o termo LGPD você vai entender que é jurídico ou é técnico. É fundamental, antes de partir para contratação saibam do que está se falando. E contratem de forma correta. **PERCENTUALMENTE!**
Muitas empresas passaram a adaptar a finalidade de seu produto, serviço ou software a adequação de LGPD. Vi algumas empresas de segurança, transformar (comercialmente) um sistema de gestão de risco em um sistema de gestão de conformidade com a LGPD. Tem empresas que faziam gestão de governança de TI e passaram a fazer gestão de implementação de LGPD.
Se você receber a visita de alguém com uma "bala de prata", pede pra mostrar qual "lobisomem" ela matou. Deixa eu ver qual é teu relatório, que tipo de processo você fez e onde.

## VAZAMENTO

Se ocorrer um vazamento você vai pagar a multa. E está claro que hoje, na presente situação, a LGPD é muito mais uma questão de gestão de risco do que atendimento a Lei.
Vazamento de dados, nem sempre é decorrente de um ciber-ataque.
Existiram 2 grande cases, situações emblemáticas na Europa, que nada tem a ver com invasão. Primeiro um funcionário de uma companhia aérea que perdeu um pen drive com informações de folha de pagamento. Encontraram, abriram as informações e a agência reguladora aplicou uma multa de 100mil libras para a companhia. O segundo caso foi de um hospital de Portugal que os médicos denunciaram o hospital por que qualquer um tinha acesso ao prontuário do paciente e tomaram uma multa de 400mil Euros por conta disso.
Não é preciso haver um ciber-ataque, isso é um equívoco. As pessoas acham as vezes que é preciso ter uma invasão. NÃO!!
Nestes 2 casos, se tivesse havido conscientização, orientação e treinamento, teria sido impedido.
Como é de praxe, surgiram vários oportunistas, que tiveram uma leitura própria da LGPD, para oferecer um produto, software ou serviço. Que efetivamente não considero adequado.
Entendo que é um processo de Compliance contínuo. Não uma implementação, mas um processo recorrente, revisado semestralmente ou anualmente, validado, consolidado, testado e auditado. Pois a Lei diz o que você NÃO pode fazer, mas o que você não pode fazer vai depender do que você faz.
Então se você é um hospital, você tem o prontuário do paciente. Mas se você é uma indústria, não vai ter prontuário, então o que se aplica a você não se aplica ao outro. São áreas diferentes. Não só os procedimentos são diferentes, mas na medida que você faz um diagnóstico situacional e meta análise da situação da empresa com relação aos requisitos da Lei, há variação do grau de maturidade entre as empresas. E a adequação muda, para cada ambiente muda. NÃO HÁ RECEITA DE BOLO!

## VISÃO DE PROCEDIMENTO

Não há como presumir. Tem que investigar.
Efetivamente entrar em cada processo.
A Lei cita 8 itens da norma 27000, e recentemente saiu a 27701, gestão de sistema de Privacidade de Dados. E para você obter essa certificação você precisa estar certificado na 27000. Ou seja, Privacidade é em si ela não existe. Se você não tem segurança, você não tem privacidade. E para deixar claro, certificar-se na ISO27000/701, não lhe garante adequação a LGPD.
O Compliance como propomos é uma auditoria. Ela vem por trás, validando e verificando, se está sendo feito de forma correta.
E voltando ao princípio de que a implementação é feita internamente, como o comitê vai validar que o processo que eles criaram e implementaram é correto? Existe um conflito de interesse ai. Seguindo a visão da ISO9001, quem implementa ou executa o processo não pode auditar.

## ENCARREGADO DE DADOS

Outro ponto chave, é o surgimento espontâneo de vários cursos de DPO. Em várias entidades. Ou seja, se promiscuiu de uma forma absurda. E isso vai acabar sendo um tiro no pé, na medida que não há competência histórica para se oferecer esse tipo de treinamento de certificação.
Mas vamos lá. **DPO(Data Protector Officer),** não é uma PROFISSÃO e é nisso que estamos pecando. Todos vendem a idéia que isso será uma profissão e não é. É tão somente uma FUNÇÃO! Tanto é que qualquer funcionário, ou membro do comitê pode ser DPO. E não é estudar para uma prova e obter uma certificação que o gabarita para ser DPO da empresa. Reforce-se que a competência na conformidade com a Lei, não tem nem a ver com a Lei e nem com a TI. Ninguém fala das áreas de negócio. Como acreditar na certificação de alguém que não fala nesse aspecto do negócio. Vemos associações oferendo cursos para certificação de DPO, pessoas assumindo o título de DPO sem nunca ter exercido o cargo ou função. Vemos advogados assumindo como "Doutor Fulano de Tal, DPO". Ele nunca estudou segurança da informação. Acredito de uma forma bem simples, que as pessoas deveriam conhecer um pouco mais o assunto para poder fazer um juízo.
Existem hoje, mais de 200 sugestões de alteração da Lei. Ai você paga muito para fazer treinamento e a prova de certificação, e ai se aprovam 50 alterações na Lei. Sua certificação foi por água a baixo. Não é mais válida. O DPO é um fiscalizar, que atua junto ao processo de auditoria, dando a chancela de conformidade e apresentando as informações a ANPD.
Na LGPD o DPO é Encarregado de Proteção de Dados e tem uma função muito diferente do DPO da GDPR. Fique atento!!

## INCIDENTE DE DADOS

É preciso ter em mente que as empresas estarão sempre passíveis a incidentes, por mais que se engajem no processo de adequação à LGPD e da promoção de seus valores.
Existem riscos de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais. Por esse motivo, a LGPD oferece ferramentas para mitigar esses incidentes. Se ocorrer uma violação de dados, essa deverá ser comunicada a ANPD e aos titulares dos dados atingidos em um prazo razoável, o que deverá ser precisado em regulação posterior. Em relação às possíveis penalidades aplicáveis, a LGPD prevê advertências (com indicação de prazo para adoção de medidas corretiva), a necessidade de tornar pública a infração, o bloqueio dos dados pessoais envolvidos no tratamento indevido e até mesmo a eliminação desses dados. Isso sem falar nas multas, que poderão representar até 2% do faturamento da empresa limitada, com o limite de R$ 50 milhões por infração.
De qualquer forma, a postura habitual da empresa em relação aos seus tratamentos de dados será levada em consideração para o estabelecimento de penalidades pela Autoridade Nacional de Proteção de Dados (ANDP). Esse é um outro motivo pelo qual é tão importante implementar um bom programa de Compliance/conformidade.

# ❖ Finalizando ou começando...

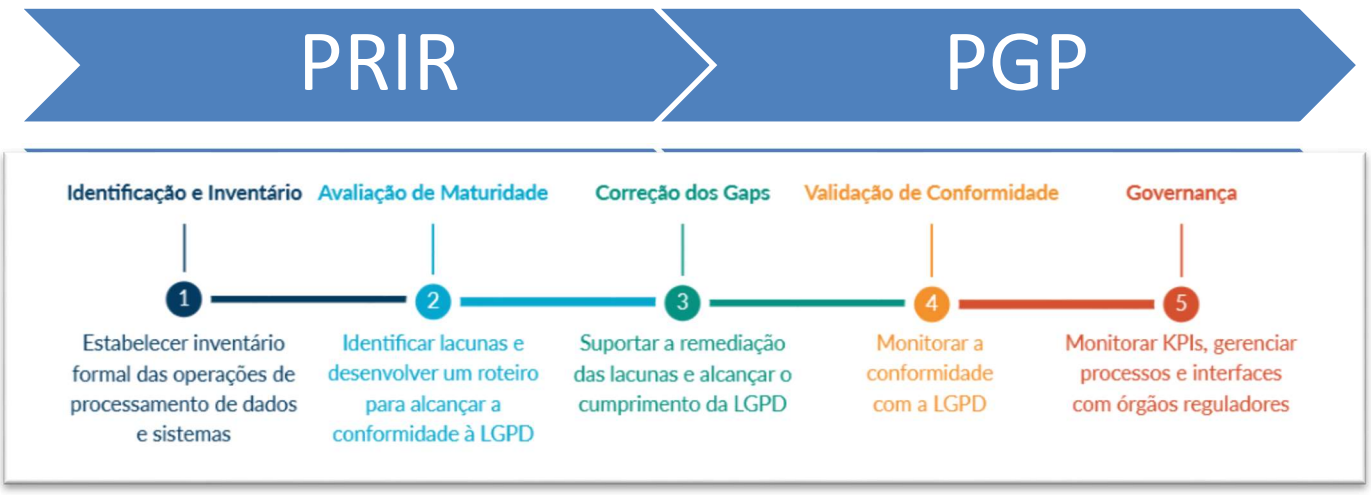
Para encerrar, já pedindo excusas pelo artigo tão longo, gostaríamos de deixar uma sugestão de processo de adequação.

Para iniciar um projeto de Compliance/Conformidade, é importante estar aberto à necessidade de criar uma nova cultura de privacidade na sua empresa, alinhadas com os princípios da LGPD, considerando sobretudo a possibilidade de realizar treinamentos para os colaboradores. Tão importante quanto as soluções tecnológicas, é o elemento humano para que, holisticamente, a organização tenha uma mudança de mentalidade.

De maneira geral, será preciso entender a própria organização e o tratamentos de dados envolvidos em suas atividades para avaliar os riscos envolvidos. Em seguida será preciso estabelecer uma estratégia de gerenciamento desses riscos. Trata-se, portanto, de um tripé: cognição, mensuração e controle dos riscos.
Assim, tendo em mente todo o conjunto de normas que se aplica às atividades desenvolvidas pela sua empresa, será importante criar um programa de governança de privacidade, que deverá envolver toda a instituição.

É recomendável que se estabeleça um comitê interno de privacidade, que precisa ser escalonável para atender as diferentes áreas da empresa e os respectivos dados pessoais tratados. Nesse sentido, a diretoria, a gerência, o jurídico/compliance, as áreas de tecnologia da informação, recursos humanos, marketing, etc. terão diferentes atribuições para a execução de um trabalho coletivo. Enquanto o jurídico precisará desenvolver atividades como a revisão dos contratos, políticas de proteção de dados e códigos de conduta. O RH, por exemplo, deve colaborar com a implementação do programa em relação aos dados dos funcionários e alinhar com eles suas expectativas de privacidade.

A seguir, apresentaremos uma possível metodologia a ser adotada para dar início a um processo de conformidade:



PRO-AUDIT

# ❖ CONCLUSÃO...

A LGPD tem um enorme impacto econômico e regulatório. Isso porque é quase impossível pensar em uma empresa que não realize nenhum tipo de tratamento de dados pessoais. Para um processo de implementação eficiente, é imprescindível que a empresa esteja aberta à criação de uma nova cultura de privacidade, engajando e criando sinergia entre os mais diversos setores nessa tarefa.
É claro que uma mudança de cultura traz consigo anseios e dificuldades. No entanto, além da mera adequação à lei para evitar multas e punições, a implementação de um plano de conformidade representa a oportunidade de experimentar bons "efeitos colaterais", que decorrem da reorganização dos processos internos e novos insights sobre os produtos e serviços oferecidos. A partir da conformidade com o novo marco legal, se pode projetar a sua empresa a um novo patamar, alinhado com a nova realidade do mercado e as crescentes expectativas dos clientes em relação à proteção de seus dados.

**ESPERAMOS TER AJUDADO!**

**E NOS COLOCAMOS AO SEU DISPOR**

**Pro-Audit Consultoria e Serviços**
**Leandro Áureo Azambuja**
Gerente de Projetos e P&D&I
Microsoft Certified Professional
Compliance Specialist
leandro@pro-audit.eti.br