1. *Gap Analysis* na prática

1.1. Orientações iniciais

** As respostas devem ser conduzidas e orientadas com o auxílio de um profissional da área de Segurança da Informação e/ou Tecnologia da Informação;*

** O profissional que for conduzir e orientar o Gap Analysis poderá incluir ou excluir questionamentos de acordo com suas pretensões e entendimento acerca das atividades da empresa. Contudo, quanto mais perguntas forem realizadas, mais pontual será o resultado da análise;*

** A tabela abaixo apresenta uma visão geral acerca dos principais questionamentos necessários à identificação das lacunas de segurança existentes nas empresas.*

GAP ANALYSIS			**DATA DE EMISSÃO:**
Das formas de sistematizar os riscos e aplicar medidas mitigatórias			
Questionamento	**Instrução**	**Respostas**	**Como adequar**
1) A alta gestão da empresa já possui uma visão geral acerca da LGPD e consciência sobre a necessidade da adequação e da implementação de uma nova cultura de privacidade e proteção de dados?	Já houve a fase de conscientização dos gestores?		Realizar a palestra de conscientização.
2) Existe na empresa uma área específica e responsável pela segurança das informações pessoais dos titulares?	Há equipe e/ou profissional da área de segurança da informação na empresa?		Contratar um profissional interno ou externo.
3) A empresa já possui uma definição das políticas internas de privacidade e proteção de dados?	Há código de boas práticas e condutas?		Elaborar esses documentos.
4) Houve a criação do Comitê Multidisciplinar pela empresa?	Verificar se foi criado.		Criar Comitê Multidisciplinar.
5) Houve a indicação do DPO *(Data Protection Officer)* ou Encarregado de Dados)?	Foi indicado?		Indicar.

6) Existe uma política de atendimento aos direitos dos titulares com procedimentos bem definidos?			Editando uma política.
7) A empresa garante o atendimento a todos os direitos dos titulares dispostos na lei?	Descrever quais sim e quais não.		
8) A empresa possibilita a gestão de acesso aos dados pelos titulares de forma facilitada?	De que forma o usuário pode acessar e alterar seus dados?		
9) Há um plano de gerenciamento de crise. Existe algum procedimento específico para a ocorrência de um incidente de segurança e/ou vazamento de dados?			
10) A empresa possui um mapa de fluxo de dados que reflete as operações de tratamento de dados que realiza?			
11) Existe orçamento disponível pela empresa para a implementação das medidas técnicas requeridas pela lei?	Responder sim ou não.		
12) Existe orçamento disponível pela empresa para a implementação das medidas de segurança da informação requeridas pela lei?	Responder sim ou não.		
13) Houve a realização do mapeamento dos dados?	Os dados manipulados pela empresa foram mapeados e classificados?		
14) Após o mapeamento, a empresa consegue compreender se existem riscos relacionados ao tratamento de dados pessoais que realiza?			
15) As operações de tratamento de dados pessoais realizadas pela empresa são sempre registradas formalmente?			

16) A empresa atende a todos os princípios elencados na lei?	Indicar quais atende e quais não atende plenamente?		Como atender?
17) As operações de tratamento de dados que a empresa realiza estão amparadas pela base legal adequada?	Sim ou não?		
18) Qual a finalidade do principal tratamento de dados realizado com potencial risco?	Indicar a finalidade		
19) Quais os principais riscos identificados?	Detalhar quais os riscos identificados.		Ex: ausência de consentimento? Falta de transparência ao utilizar o dado? Risco na coleta em meios físicos? Ausência de técnicas de descarte seguro? Inobservância às leis vigentes?
20) Qual o grau do risco identificado?	*Alto, médio, baixo?*		
21) Quais as ações imediatas adotadas pela empresa para mitigar os riscos detectados?	*Relacionar todas as medidas adequadas para alcançar a conformidade.*		*Ex: Implementação de uma Política de Governança de Dados (políticas de privacidade, gestão de acesso aos dados, adoção de medidas técnicas e administrativas em relação ao tratamento de dados em meios físicos e digitais, obtenção de consentimento válido, eliminação da coleta de dados em papel.*
22) Quais são os riscos inerentes identificados?	*Trata-se da ocorrência de possíveis irregularidades encontradas que poderão comprometer parcialmente ou totalmente o desenvolvimento das atividades da empresa.*		*Ex: ausência de Política de Privacidade, de Política de Cookies, inobservância ao atendimento aos direitos dos titulares, utilização de dados sem finalidade legítima.*
OBS: O questionário completo e demais orientações para o *Gap Analysis* estão disponíveis em nosso Módulo II - Curso de LGPD na Prática			

Para conhecer o conteúdo programático do Curso e fazer a sua inscrição, basta clicar no link abaixo:

https://www.implementandoalgpd.com.br/curso-lgpd-modulo-ii-plano-de-adequacao-a-lgpd/

**** O início das aulas é imediato!***

* Após a conclusão das respostas ao questionário, a empresa terá informações suficientes à adoção das melhores estratégias no sentido de adequar seus processos às disposições da lei;

* Lembramos que a adequação às disposições da LGPD é focada na análise dos riscos existentes e nas formas de mitigá-lo;

* O risco é evidenciado na probabilidade da materialização de uma evento negativo relacionado à operação de tratamento de dados realizada;

* Todo o processo de adequação da empresa deve levar em conta os riscos evidenciados conforme o levantamento realizado na etapa de mapeamento e classificação dos dados, bem como nas informações gerais obtidas na fase de elaboração dos *gaps;*

** P*ara uma análise *evidenciada no risco existente em cada processo, deve-se levar em consideração o risco do evento danoso se materializar e o seu impacto caso se materialize;*

** Ao identificar o grau do risco existentes em cada processo que a empresa realiza, esta poderá:*

*- **aceitar**[1] o risco existente, caso ele não represente grandes impactos à sua atividade ou seja relativamente insignificante;*

---

[1] A empresa poderá **aceitar** riscos sempre que as operações de tratamento de dados pessoais que realiza já estiverem em conformidade com as leis e regulamentos que orientam a sua atividade, em especial com a LGPD.

*- **mitigar**[2] o risco, caso entenda pela definição dos controles necessários à prevenção, de modo a reduzir a probabilidade de ocorrência, ou, quando da ocorrência, minimizar o impacto;*

*- **zerar**[3] o risco existente de modo a interromper os eventos que potencialmente dão causa à sua ocorrência;*

*- **Terceirizar**[4] o risco por meio, por exemplo, da contratação de um seguro para este fim.*

** De posse de todas as informações deverá ser elaborada uma matriz de riscos relacionada a cada processo da empresa, de modo que seja possível avaliar o potencial do risco encontrado.*

Essa atividade deverá ser realizada pela área de segurança da informação e/ou tecnologia da informação.

** Será por meio da elaboração da matriz que haverá suporte para que a empresa decida por aceitar o risco, mitigar, terceirizar ou zerar o seu impacto.*

1.4. Observação geral

A Lei Geral de Proteção de Dados não tem por objetivo que os incidentes não aconteçam, o que a lei impõe é que, em caso de ocorrência, os impactos de seu vazamento sejam minimizados.

Desse modo, o que a lei requer é que sejam adotadas todas as medidas necessárias no que diz respeito às técnicas e segurança da informação, minimizando o risco de ocorrência e seus potenciais impactos.

---

[2] Poderá a empresa mitigar os riscos quando verificar que estes são moderados ou altos, mas que por meio da implementação das medidas necessárias, pode-se reduzir o seu risco ou grau de impacto.

[3] A empresa também poderá optar por **zerar** o risco por meio da interrupção de um tratamento potencialmente arriscado onde os custos para mitigá-lo não justificam a continuidade da atividade.

[4] Também poderá terceirizar o risco por meio da contratação de um seguro específico para este fim ou transferindo a responsabilidade do tratamento à outra empresa contratualmente.