# Marina de Miranda: Anotações rápidas sobre a LGPD

Em mais de uma oportunidade, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD) cita a *"[...] salvaguardas e mecanismos de mitigação de risco"*.


De fato, as referidas ações mostram-se muito importantes, pois se prestam a evitar os riscos aos direitos dos titulares dos dados pessoais. Contudo, só é possível mitigar aquilo que já se "conhece" e é aqui que a gestão de riscos ganha destaque.

A exemplo do que ocorre na implantação de programas de integridade e de *compliance*, no campo da LGPD, a gestão de riscos compreende a identificação, a análise e o gerenciamento dos riscos, seja por meio da prevenção ou pela previsão de medidas a serem aplicadas caso ele venha a se concretizar.

Trata-se, portanto, de uma forma de "prever" os possíveis cenários e se preparar para eles, o que, em termos de proteção de dados pessoais, constitui ferramenta indispensável a ser incorporada à rotina de trabalho de qualquer organização (pública ou privada) e aos demais sujeitos à LGPD [1].

E de que modo a incorporação da gestão de riscos acontece na prática? Ou melhor, como estruturar um processo de gestão de riscos?

Entre inúmeras metodologias existentes, a Associação Brasileira de Normas Técnicas (ABNT) expediu a NBR ISO 31000:2018 como critério norteador para a gestão de riscos.

Ainda é possível contar com a NBR ISO 31004:2015, que é um guia para a implementação da norma anterior, e a NBR ISO 31010:2012, a qual dispõe sobre técnicas para o processo de gestão de riscos.

Ademais, considerando o enfoque voltado à proteção de dados e à segurança da informação, é imprescindível também aliar o processo de gestão de riscos às normas ABNT NBR ISO/IEC 27001:2013; 27002:2013 e 27003:2020, as quais versam, respectivamente, sobre requisitos, controles e orientações para sistemas de gestão da segurança da informação.

Contudo, como pretendemos abordar a estruturação do processo de gestão de riscos a partir de uma noção mais prática, utilizaremos outros materiais como bases de estudo, mais especificamente o Guia de Gestão de Riscos do Supremo Tribunal Federal e o Guia Prático de Gestão de Riscos para a Integridade da Controladoria-Geral da União.

É claro que, a depender da organização, a estrutura de um processo de gestão de riscos pode variar, mas, de modo geral, as etapas a seguir descritas podem ser consideradas como verdadeiros pilares e, portanto, merecem atenção.

E vale mais uma ressalva, com exceção da comunicação que, segundo a ISO 31000:2018, deve estar presente em todo o processo de gestão, tendo em vista que o compartilhamento de informações é essencial para o bom andamento dos trabalhos, as demais etapas seguem necessariamente uma ordem.

O primeiro passo é selecionar o objeto da gestão, ou seja, qual processo organizacional será analisado, podendo o termo "processo" ser definido, nesse caso, como toda e qualquer atividade dentro da organização que realiza qualquer tipo de tratamento de dados [2].

Mas, atenção! A escolha do objeto pressupõe o conhecimento de toda a "engrenagem". Para isso, mostra-se prudente fazer um mapeamento de todos os processos, de modo que seja possível determinar, em síntese, como ele acontece, quem são os responsáveis por cada estágio e sua periodicidade. Aliás, cabe registrar que o mapeamento serve de base para a construção do ciclo de vida dos dados [3].

Em um segundo momento, é importante fixar os objetivos do processo e da própria organização, bem como compreender os contextos interno e externo no qual a empresa está inserida, os quais podem ser compreendidos como fatores que, de alguma forma, impactam o processo e/ou a própria organização.

A etapa seguinte diz respeito à identificação dos riscos que perpassa pela descrição das causas, dos eventos de risco e das possíveis consequências. Nesse ponto, a fim de compreender o quadro de maneira mais profunda, é interessante apontar tanto o risco inerente quanto o risco residual.

Segundo o Guia Prático de Gestão de Riscos para a Integridade da Controladoria-Geral da União, o risco inerente corresponde àquele ao qual ainda não se aplicou qualquer ação capaz de reduzir a probabilidade da sua concretização e/ou do seu impacto, já o risco residual se refere ao risco que "restou" após a implementação das ações mencionadas.

Certo, uma vez identificados os riscos, cumpre analisá-los. É nesse momento que ocorre a avaliação da probabilidade (de ocorrer o evento de risco) e do impacto (grau de magnitude das consequências decorrentes do evento) a fim de obter o nível de risco e, por conseguinte, construir a matriz de riscos, também conhecida como matriz de calor.

O próximo passo corresponde ao tratamento dos riscos, em que, finalmente, são definidas as medidas, as salvaguardas e os mecanismos para mitigação dos riscos. De forma geral, a depender do nível de risco, o tratamento pode se resumir a evitar, reduzir, compartilhar ou aceitar o risco.

Nessa fase, a fim de efetivar o tratamento, é importante elaborar um plano de ação com a indicação do tipo de tratamento, as medidas a serem implantadas, o responsável pela concretização e o prazo para tanto.

É evidente que não basta desenvolver e implementar o processo de gestão de riscos, é preciso acompanhá-lo, motivo pelo qual o monitoramento constitui a última etapa, pois é a partir da observação contínua que o desempenho das ações implementadas poderão ser verificadas, bem como que o surgimento de novos riscos serão constatados.

Um último registro: este artigo não tem como pretensão oferecer uma fórmula mágica ou uma receita de bolo, visto que, assim como toda a implantação de um programa de conformidade com a LGPD, a gestão de riscos é igualmente complexa.

Sendo assim, por meio deste texto, buscou-se tão somente indicar um possível roteiro de pesquisa e estudo para, então, finalmente, o leitor colocar os seus aprendizados em prática.

**Referências bibliográficas**

— BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em outubro de 2020.
— _____. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO (CGU). Guia Prático de Gestão de Riscos para a Integridade: orientações para a administração pública federal direta, autárquica e fundacional. Brasília:  MT e CGU, 2018.
— _____. SUPREMO TRIBUNAL FEDERAL (STF). Guia de Gestão de Riscos. Brasília: STF, Secretaria de Gestão Estratégica, Escritório de Gestão Aplicada, 2019.

[1] Conforme artigo 1º da Lei nº 13.709/2018.

[2] Segundo a LGPD, considera-se artigo 5º […] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[3] Para saber mais sobre ciclo de vida dos dados,  acesse: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pd.

**Date Created**
23/10/2020