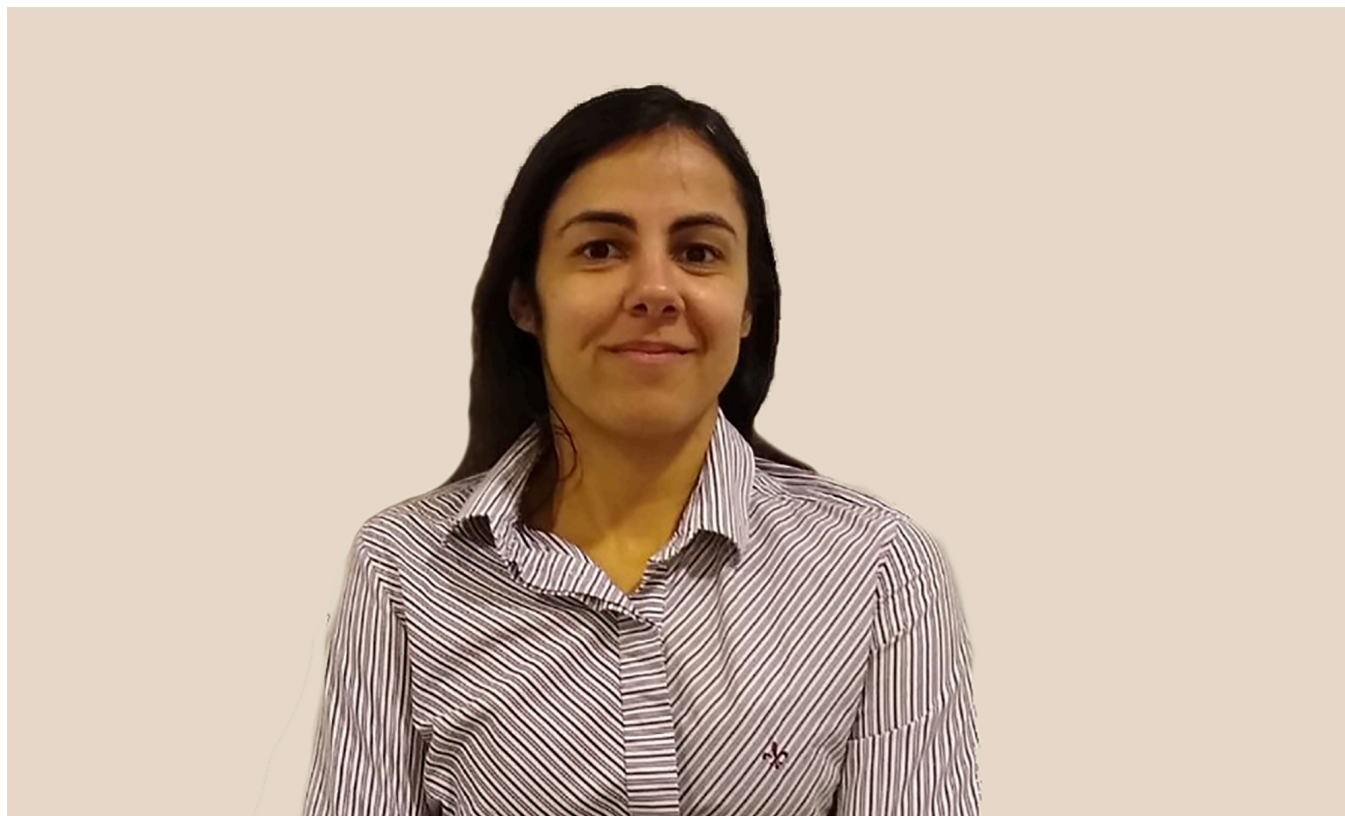


Por Vania Freitas (*)



Desde a divulgação da LGPD (Lei Geral de Proteção de Dados Pessoais), em agosto de 2018, as empresas têm enfrentado diversos desafios para a adequação de sua operação aos requisitos demandados pela Lei. Dentre eles, destacamos o mapeamento das atividades e processos que tratam de dados pessoais, a elaboração de relatório de impacto de atividades críticas, a conscientização dos profissionais internos e terceiros por meio de treinamentos, o atendimento aos direitos dos titulares, o controle em sistemas e aplicações que tratam dados pessoais e a prevenção de incidentes, entre outras.

Além dos pontos trazidos acima, cabe ressaltar a necessidade de um encarregado de proteção de dados pessoais, também conhecido pela sigla DPO (Data Protection Officer), profissional responsável, entre outras atividades, pela intermediação com a ANPD (Autoridade Nacional de Proteção de Dados) e pela interação com o titular de dados. Esta função pode ser exercida por um profissional interno ou uma empresa terceirizada, e seu acesso deve estar disponível pelos meios de comunicação da empresa, pela política de privacidade ou outro meio apropriado. Para pequenas e médias empresas, a figura do encarregado não é obrigatória, mas isso não dispensa a empresa de atender aos titulares de dados quando houver demanda.

Há ainda a mudança de mentalidade dos profissionais da organização como um dos principais desafios enfrentados pelas empresas, pois, para uma adequação consistente, a equipe interna deve estar preparada para as atividades do dia a dia da Lei.

Após a etapa de diagnóstico e implantação do Programa de Privacidade, esforço que deve abranger todas as áreas da empresa, se faz necessário realizar o monitoramento das ações executadas com o objetivo de manter essa atividade como um organismo vivo.

Para a realização do monitoramento e definição da governança de privacidade, as empresas precisam trabalhar com as figuras que estão diretamente ligadas à operacionalização do programa,

como as áreas de Tecnologia e Segurança da Informação, Jurídico, Compliance, Comunicação e Recursos Humanos. Essas áreas chaves, por sua vez, têm a responsabilidade de difundir o tema privacidade para as demais, de forma que todos saibam os conceitos da LGPD e a sua aplicabilidade no dia a dia das atividades de trabalho, monitorando assim os riscos e permitindo que a empresa consiga demonstrar maior conformidade e aderência aos requisitos da LGPD.

Sob todos esses aspectos, podemos dizer que um programa de privacidade de dados vai muito além do cumprimento da legislação, sendo necessário colocar em prática um plano estruturado para cada empresa a partir de metodologias específicas que visam a implantação, o monitoramento, a manutenção e o aperfeiçoamento do programa de privacidade.

Além disso, estar em conformidade com a LGPD também é relevante para o contexto geral de mercado, como o ambiente de negócios ao qual a empresa está inserida, a visibilidade perante o mercado e clientes, a força da marca, dentre outros benefícios como a transparência perante o titular de dados e, principalmente, a segurança do tratamento de suas informações e dos dados pessoais.

(*) **Vania Freitas** é gerente de Data Privacy na [ICTS Protivit](#), empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.