

## nota informativa

---

Ciudad de México, 23 de noviembre de 2022

# 5 principios para un programa de compliance en privacidad-datos

**La normatividad en materia de protección de datos personales establece una serie de obligaciones complejas que deben observar las empresas que tratan datos personales.**

Las multas impuestas en 2021 por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) por infracciones a la legislación en materia de protección de datos personales superaron los 90 millones de pesos.

La normatividad en materia de protección de datos personales establece una serie de obligaciones complejas que deben observar las empresas que tratan datos personales dentro del marco de sus operaciones. Cada una de estas obligaciones conlleva una serie de actividades que son fáciles de pasar por alto cuando la empresa desconoce la relevancia, alcance y repercusiones del tema.

En términos del artículo 28 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, las empresas deben adoptar medidas para garantizar el debido tratamiento de los datos personales, privilegiando los intereses y expectativas razonables de privacidad de los titulares.

Dentro de las medidas que contempla la legislación, se encuentra la elaboración de políticas y programas de privacidad obligatorios y exigibles al interior de la organización de las empresas. Estas políticas y programas son un conjunto de directrices que emiten las empresas para promover, vigilar y asegurar el cumplimiento de la legislación aplicable, permitiéndoles mitigar situaciones que pudiera exponerlas a algún tipo de riesgo o responsabilidad, así como acreditar la debida diligencia en el desarrollo de sus funciones.

En nuestra experiencia, para asegurar el correcto diseño, implementación y operación de un programa de compliance en materia de privacidad y protección de datos personales, se deben seguir los siguientes pasos:

**1. Inventario de los tratamientos.** Es indispensable evaluar los distintos procesos de la empresa, con el fin de identificar los tratamientos de datos personales que realiza (perfiles de titulares, datos tratados, finalidades del tratamiento, transferencias, entre otros).

**2. Diagnóstico de nivel de cumplimiento.** Es necesario identificar los mecanismos de cumplimiento existentes o aquellos que aún requieran ser implementados para dar cumplimiento a los principios y deberes que establece la normativa (información, consentimiento, finalidad, proporcionalidad, responsabilidad, lealtad y calidad).



**3. Diseño del programa de compliance.** Los mecanismos de cumplimiento deben ser idóneos y acordes con las operaciones de la empresa (avisos de privacidad, políticas de cookies, mecanismos para la obtención del consentimiento, catálogo de funciones y obligaciones del personal, cláusulas o acuerdos con clientes y proveedores involucrados en el tratamiento de los datos personales, entre otros).

**4. Implementación del programa de compliance.** Resulta necesario llevar a cabo acciones de concientización y capacitación del personal involucrado en el tratamiento de los datos personales, para garantizar la adecuada instrumentación y cumplimiento del programa (ej.: oficial, delegado o comité de protección de datos personales).

**5. Revisiones periódicas.** El programa debe evaluarse periódicamente con el propósito de medir su nivel de cumplimiento, así como identificar cualquier actualización que fuera necesaria con motivo de cambios legislativos u operativos de la empresa (auditorías internas o externas).

De esta forma es posible cerrar posibles brechas de incumplimiento que pudieran exponer a las empresas a multas de hasta 320,000 veces el valor de la Unidad de Medida y Actualización (\$30 millones de pesos aproximadamente), las cuales pudieran llegar a adicionarse por un monto igual en casos de reincidencia y duplicarse tratándose de infracciones que involucren el tratamiento de datos sensibles.

---

## Área TMT y Compliance de ECIJA México

Socios.mexico@ecija.com