

Programas de cumplimiento normativo



El **Compliance** o programas de cumplimiento normativo son el conjunto de procedimientos y protocolos adoptados en la empresa con la finalidad de detectar y prevenir los posibles incumplimientos de cualquier normativa ya sea externa -leyes, reglamentos, etc.- como interna -políticas, códigos éticos, etc.-. Así, el riesgo de **Compliance** se configura como el **riesgo de sufrir sanciones o daño reputacional como consecuencia del incumplimiento del marco normativo de la empresa**.

Debido al creciente número de regulaciones y al innegable incremento de la sensibilidad social respecto de la ética de los negocios, el **Compliance** en muchos casos ha dejado de ser una opción voluntaria para las empresas y ha pasado a ser un **requisito a integrar dentro de la estrategia y estructuras internas**.

El **Compliance** trata, en definitiva, de establecer un conjunto de **herramientas de gestión para prevenir** que cualquier operación que se lleve a cabo por quienes actúan en nombre de la empresa sea contraria a las normas establecidas.



Módulo 2: plan de adecuación a la normativa de protección de datos

Nueva normativa: derechos y obligaciones

Desde el 25 de mayo de 2018 es exigible a todas las empresas que tratan datos personales el cumplimiento con los principios, requisitos y exigencias contenidos en el Reglamento General de Protección de Datos. Asimismo, el pasado mes de diciembre entró en vigor la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, que trae a las empresas **nuevas obligaciones** con las que cumplir.

La nueva normativa prevé **multas** de hasta el 4% de la facturación global anual o 20 millones de euros para quienes incumplan.

Nuevo enfoque: la responsabilidad proactiva

El nuevo principio de responsabilidad proactiva obliga a las empresas a:

- Realizar un constante esfuerzo, no solo por cumplir la normativa de protección de datos, sino por ser capaz de demostrarlo → Esto exigirá a la empresa que documente todas las medidas y decisiones que se adopten en relación con esta materia.
- Sujetar su actuación al principio de protección de datos desde el diseño → Pensar en términos de protección de datos desde la fase inicial del tratamiento.
- Cumplir el principio de protección de datos por defecto → Debiendo aplicar las medidas apropiadas para garantizar que, por defecto, solo se traten los datos necesarios para los fines específicos que se persiguen con el tratamiento.

Los **Planes de Adecuación** a la Normativa de Protección de Datos permiten implantar todos los requisitos exigibles por esta normativa a través de las siguientes **fases o tareas**:

1. Análisis GAP
2. Registro de actividades de tratamiento
3. Establecimiento de la política de privacidad
4. Definición de roles y responsabilidades
5. Análisis de riesgos y evaluación de impacto en protección de datos
6. Formación concienciación interna
7. Diseño del protocolo de gestión de reclamaciones y ejercicio de derechos.
8. Protocolo de gestión de las incidencias y violaciones de seguridad
9. Revisión, mantenimiento y mejora continua

Para más información y asesoramiento en la materia, contacta con PKF Attest