axis CORPORATE

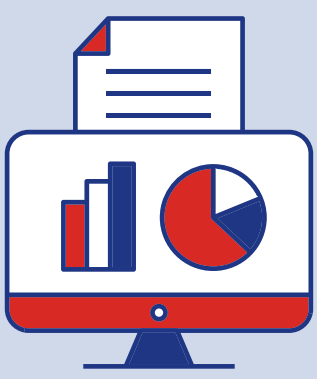
Modelo de gobierno

Una operativización sin riesgos, ágil y acorde a la ley

Tras el primer año en funcionamiento de los diferentes modelos de gobierno para cumplir con la RGDP, es el momento de hacer balance. El DPO, delegado de protección de datos, ha de evaluar si su modelo goza de buena salud o por el contrario corre el riesgo de ser sancionado.
Un modelo de gobierno estándar no garantiza a la organización la inexistencia de ineficiencias y/o gaps normativos, tal y como se demuestra con las sanciones recientemente emitidas. El DPO ha de asegurarse de que su modelo cumple y se adapta a las necesidades reales de su compañía y, para ello, debe poner foco en las siguientes fases:

1 Criterios RGPD

Recomendamos poner foco en la obtención de los datos, para operativizar la sistemática

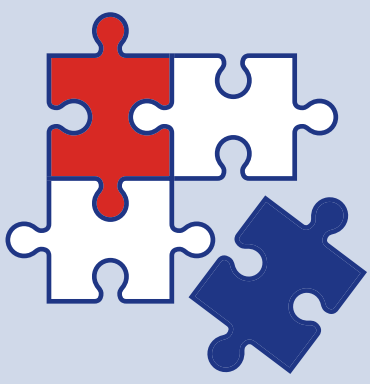


- Inventario de tratamientos
- Recogida de información
- Uso de la información basada en consentimientos
- Ampliación en los derechos de los usuarios
- Resolución de consultas por parte del DPO
- Reporting interno y a AEPD
- Cumplimiento del principio de accountabilty

2 GAP en las herramientas de mercado

El DPO ha de asegurarse de que las herramientas utilizadas cubren de manera íntegra y ágil los requerimientos legales y de gestión

- Infraestructura de gestión de derechos y consentimientos
- Gestión integral de las PIAs
- Registros de actividades de tratamiento
- Seguimiento de medidas y proyectos RGPD
- Políticas de ciberseguridad
- Planes de contingencia



3 Operativa / Gestión RGPD

Derivado de las necesidades de gestión, se requiere de una operativización efectiva de los elementos *core* en la actividad de RGPD

- Gestión PIAs
- Ejercicio de derechos
- Comunicación de brechas de seguridad
- Respuesta a requerimientos AEPD
- Respuestas a consultas DPO

4 Control y Gobierno

El DPO debe velar para que en todas las compañías del grupo se efectúe un control del gobierno adecuado, según las métricas marcadas

- Concienciación sobre la privacidad en la compañía
- Comités PIA/ Privacidad
- Visión integral RGPD
- Implantación de un entorno de control
- Identificación de necesidad

Tipos de sanciones e incidencia

Tras un año en funcionamiento del modelo GDPR, se han emitido diversas sanciones, desde 800€ hasta 250.00€, con foco en los siguientes aspectos:

70% Art. 5 “Principios relativos al tratamiento”. La mayoría de las sanciones emitidas (70%) están relacionadas con la necesidad de que el tratamiento de los datos personales garantice una seguridad adecuada de éstos (integridad y confidencialidad).

25% Art 6. “Licitud del tratamiento”. El tratamiento debe de cumplir 1 de las 6 condiciones establecidas en el reglamento.

5% Art 32. “Seguridad del tratamiento”. Aplicar medidas técnicas y organizativas apropiadas.

Contar con una PIA que evalúe los principios relativos al tratamiento, la licitud de este y las necesidades técnicas y organizativas, garantiza el establecimiento de tratamientos válidos y corrige tratamientos que ya se están haciendo.