El análisis de riesgos en el marco del RGPD

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.

De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña organización que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

La herramienta Facilita de la Agencia Española de Protección de Datos (AEPD) está destinada a aquellas organizaciones que realizan tratamientos de datos personales que, a priori, tiene un escaso nivel de riesgo para los derechos y libertades de las personas cuyos datos tratan.

En el resto de casos, se deberá realizar un análisis básico de riesgos o una Evaluación de Impacto en la Protección de Datos (EIPD) si el riesgo es alto.

El formato que se presenta a continuación puede servir como análisis básico de riesgos o como plan de gestión de los riesgos, una vez realizada la EIPD.

Nombre de activo	Fase	Riesgo		Medida	Responsable	Recursos	Plazo
		Amenaza	Nivel				

** Nota explicativa:*

- *Nombre del activo utilizado para realizar el tratamiento de datos personales en alguna de sus fases. Pueden ser los propios datos, hardware, software, comunicaciones, personas, proveedores, localizaciones, …*
- *Fase del ciclo de vida de los datos personales: Recogida, almacenamiento, uso, cesión o acceso a datos por terceros, destrucción*
- *Riesgo resultado del impacto y la probabilidad*
  - *Amenaza que provoca el riesgo*
  - *Resultado cuantitativo del riesgo*
- *Medida de seguridad*
- *Responsable (persona, unidad organizativa, …) de diseñar, implantar, mantener y/o mejorar la medida de seguridad*
- *Recursos necesarios para gestionar la medida de seguridad*
- *Plazo de inicio y fin de la medida de seguridad*