INFORME ANÁLISIS DE RIESGOS

¿QUÉ ES?

Se trata de un estudio previo que se debe realizar con todo nuevo tratamiento de datos personales. La principal finalidad es establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de las personas afectadas.

¿EN QUÉ CONSISTE?

En este informe se identifican los riesgos y amenazas a los que están expuestos los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. A continuación, se deberán desarrollar las soluciones o medidas correspondientes para mitigar y/o eliminar los riesgos detectados y decidir cuáles de ellas se van a aplicar.

DESCRIPCIÓN DE LOS TRATAMIENTOS

La descripción de los tratamientos sujetos al análisis de riesgos, permite conocer el ciclo de vida de los datos, el uso que se va a dar a los mismos y cualquier elemento que interviene en esa utilización. Se debe determinar para cada tratamiento si es riesgo es bajo o alto. El riesgo será alto siempre que realicemos los siguientes tratamientos:

- Elaboración de perfiles de “aspectos relacionados con el desempeño del interesado en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos”.
- Toma de decisiones automatizada con efecto legal o similar (produzca exclusión o discriminación).
- Monitorizar o controlar a los interesados.
- Tratar categorías especiales de datos.
- Datos relativos a las personas vulnerables (menores, ancianos...).
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas (huella dactilar, reconocimiento facial…).
- Cuando el procesamiento en sí mismo “impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato”.

NECESIDAD DEL INFORME

El Reglamento 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD establece la necesidad de realizar un análisis de riesgos con la finalidad de implantar medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Una descripción adecuada de las actividades de tratamiento es fundamental para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo.

También es el momento adecuado para definir las medidas de control y seguridad para garantizar los derechos y libertades de los interesados con el objetivo de cumplir con el principio de responsabilidad proactiva y que un tratamiento se inicie respetando las exigencias de privacidad según el riesgo a la que está expuesto.

PRINCIPALES RIESGOS

Protección de la información:

- Integridad de los datos personales:
  - Riesgo: Modificación o alteración de datos personales no intencionada

- Disponibilidad de los datos personales:
  - Riesgo: Pérdida o borrado no intencionado de datos personales

- Confidencialidad de los datos personales:
  - Riesgo: Acceso no autorizado a los datos personales

Riesgos asociados al cumplimiento:

- Garantizar el ejercicio de los derechos de los interesados:
  - Riesgo: Ausencia de procedimientos para el ejercicio de derechos

- Garantizar los principios relativos al tratamiento:
  - Riesgos: Ausencia de legitimidad para el tratamiento de los datos personales; Tratamiento ilícito de datos personales

MEDIDAS DE CONTROL PARA REDUCIR LOS RIESGOS

Modificación o alteración de datos personales no intencionada:

- Segregación de funciones mediante perfiles de acceso.
- Controles de monitorización de amenazas en red.

Pérdida o borrado no intencionado de datos personales:

- Copias de seguridad.
- Almacenamiento en dos ubicaciones diferentes.

Acceso no autorizado a los datos personales:

- Mecanismos de control de acceso
- Segmentación de la red

Ausencia de procedimientos para el ejercicio de derechos:

- Procedimientos y canales para el ejercicio de derechos

Ausencia de legitimidad para el tratamiento de los datos personales:

- Cláusulas informativas y base legitimadora para el tratamiento de datos

Tratamiento ilícito de datos personales:

- Monitorización del uso de datos personales