

# La privacidad de los datos y los riesgos

**Author :** gochoadealda

**Categories :** [Auditoría, Certificación y Calidad de Sistemas Informáticos](#)

**Date :** 1 diciembre, 2018

En el post anterior vimos que cambios ha supuesto la nueva ley de privacidad y protección de los datos, la RGPD a las empresas europeas. Que obligaciones tienen y que intencionalidad tiene la nueva ley.

En este post nos centraremos en los riesgo que atañen a la privacidad de los datos y analizaremos diferentes formas de enfrentarnos a los mismos, mostrando una breve introducción a la herramienta FACILITA.

Un riesgo es toda aquella posibilidad de que se produzca un contratiempo o una desgracia, que alguien o algo sufra algún tipo de perjuicio o daño. En cuanto a la privacidad, el riesgo que a todos se nos viene a la cabeza es el de la filtración de información sensible, clasificada o confidencial. Por tanto, ¿si queremos evitar que estos riesgos se cumplan que debemos hacer? Una de las formas más comunes y eficaces de combatir los riesgos es mediante el proceso conocido como Gestión de riesgos.

La gestión de riesgos son el conjunto de actividades y/o tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.[1] Esta gestión de riesgos implica por lo tanto la identificación de los riesgos, la evaluación o categorización de los mismos y por último la elaboración de planes de acción para mitigar los mismos.

La gestión de riesgos se divide generalmente en 3 fases principales:

1. Identificación de Amenazas
2. Evaluación de los riesgos
3. Tratar los riesgos

Todas estas fases están sometidas a una monitorización continua, de esta forma de trata de conseguir que por el camino no se cometan errores que puedan repercutir gravemente más tarde.

## **Fase 1: Identificar Amenazas y Riesgos**

El riesgo viene dado por la exposición a amenazas, por tanto, desde la perspectiva de la privacidad, es fundamental comprender qué es una amenaza y cómo se pueden identificar escenarios de riesgo para los datos personales a partir de la misma.

Una amenaza implica cualquier factor de riesgo con potencial para provocar daños o

perjuicios. En el caso de la privacidad de los datos, las amenazas son principalmente de tres tipos:

- **Acceso ilegítimo a los datos:** Relacionado con la confidencialidad, son los casos en los que personas acceden a datos a los cuales no deberían poder acceder, sobre los que no tienen permisos.
- **Modificación No autorizada de los datos:** Relacionada con la integridad, cuando los datos con los que se trabaja tienen riesgo o han sido dañados o corrompidos, esto es modificaciones sobre los datos sobre las que no se tiene conocimiento o no han sido solicitadas o aprobadas.
- **Eliminación de los datos:** Relacionado con la disponibilidad, estamos ante aquellos casos en los que se pierden o desaparecen datos.

Otra forma diferente de definir un riesgo sería verlo como una posibilidad de que se cumpla una amenaza y por lo tanto esta trajese consigo consecuencias negativas. El nivel de riesgo se mide en función de la probabilidad de que se cumpla y del impacto que este tendría en caso de cumplirse. Lo que nos lleva a la segunda fase.

## **Fase 2: Evaluar los riesgos**

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos es el mecanismo mediante el cual se valora el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se cumpla.

El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se vuelve realidad, por ejemplo, un impacto sería despreciable o leve si no tuviera consecuencias sobre los usuarios (teniendo en cuenta que lo que estamos valorando es la privacidad) o, por el contrario, un impacto sería significativo o grave si el daño ocasionado sobre los derechos y libertades del usuario fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo. Los riesgos se suelen categorizar en función de escalas que midan estos impactos y la probabilidad de que sucedan, ejemplos de estas categorías podrían ser Alto, Medio, Bajo o Grave, Común y Leve.

## **Fase 3: Tratar los riesgos**

Con ello llegamos a la última fase del proceso de gestión de riesgos. En esta fase se elaboran metodologías y mecanismos que permitan reducir la probabilidad y/o el impacto de los riesgos en caso de llegar a producirse, de forma que el valor asociado a el riesgo en cuestión pueda reducirse.

Básicamente sería elaborar un plan de acción en el cual apoyarnos para no caer en estos riesgos o en caso de que se produzcan tener mecanismos que reduzcan el impacto de los mismos.

Para terminar, toca hablar de la herramienta FACILITA. FACILITA es una herramienta que ha creado la Agencia Española de Protección de Datos (AEPD) para ayudar a las empresas a

realizar el tratamiento de datos personales, con un riesgo asociado bajo, de forma sistemática. Agilizando así todo el proceso y haciendo así más sencillo el cumplimiento para con la RGPD.

Su uso es muy sencillo, se basa en en tan solo tres pantallas con preguntas muy concretas que permite a aquel que la utiliza determinar su situación en cuanto al tratamiento de datos. En función de las respuestas que se den a las preguntas propuestas obtendremos uno de dos posibles resultados: Si se adapta a los requisitos exigidos para utilizar FACILITA o si se debe realizar un análisis de riesgo más concienzudo. En caso de que la herramienta pueda usarse, el resultado del empleo de la misma será la obtención de diversos documentos adaptados a la empresa o cliente concretos, cláusulas contractuales, cláusulas informativas, registro de actividades de tratamiento y un anexo con medidas de seguridad orientativas consideradas mínimas.

## Referencias

<https://www.aepd.es/herramientas/facilita.html>

<https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>

[ISACA: GDPR Data Protection Impact Assessments](#)