Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (interuniversitario: UOC, UAB, URV, UIB)

EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Nombre del estudiante:	Eladio Cortizas de Castro
Nombre del Profesor/a colaborador/a:	Antonio José Segovia Henares
Nombre del Profesor/a:	Carles Garrigues Olivella
Fecha:	5 de junio de 2019

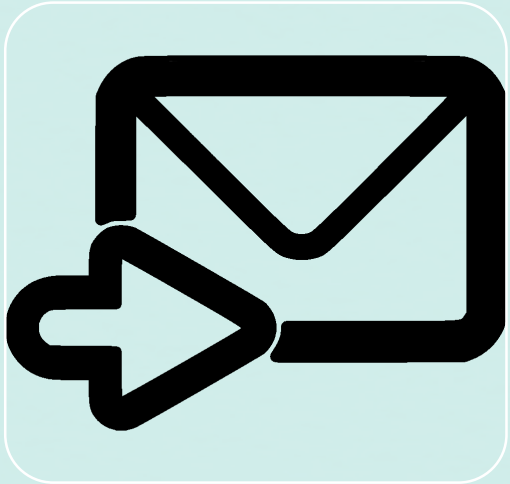
Índice

- Dato personal
- Principios
- Derechos
- Brecha de seguridad
- Evaluación de impacto relativa a la protección de datos
- Análisis de Riesgos

Dato personal

Es todo aquel dato referente a las personas que permite identificarlas. Tanto directamente como indirectamente.

Huella dactilar



Dirección postal

Dirección IP

Principios

Principio de responsabilidad proactiva (accountability): Se documentará todo lo relacionado a la gestión de la protección de datos personales.

Principio de protección de datos por defecto y desde el diseño: Se deberán adoptar medidas técnicas y organizativas que garanticen el cumplimiento de la norma en las primeras fases del diseño, de forma que se garantice la intimidad y los principios de protección de datos desde el primer momento.

Principio de licitud, lealtad y transparencia: La información debe facilitarse de forma comprensible, simple, inteligible y accesible. Incluso pueden usarse iconos normalizados.

Principio de limitación de la finalidad: Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

Principio de minimización de los datos: Los datos personales recogidos deben ser los mínimos necesarios para la finalidad establecida. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

Principio de exactitud de los datos: Los datos personales serán exactos y, si fuera necesario, actualizados. Para ello se tomarán todas las medidas técnicas y organizativas necesarias.

Principio de limitación del plazo de conservación de los datos: Los datos personales deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los mismos

Derechos

Supresión: Supresión de los datos personales que le conciernan. También refuerza el "derecho al olvido" en el entorno on-line.

Oposición y decisiones individuales automatizadas: Oponerse al tratamiento de sus datos personales y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en él o le afecte.

Portabilidad: Recibir los datos personales en un formato estructurado. Estos datos se podrán transmitir, a otra organización.

Limitación: El interesado podrá solicitar que la organización evite la modificación, borrado o supresión de sus datos.

Acceso: Toda persona tiene derecho a acceder a los datos recogidos que le conciernan.

Rectificación: Rectificar los datos personales inexactos o incompletos

Consentimiento claro y afirmativo claro

Brecha de seguridad

Son errores, fallos o violaciones intencionales que, producidos en o contra un sistema informático, derivan en la destrucción, pérdida o alteración de datos personales, comunicación o acceso en favor de terceras personas no autorizadas. Las brechas de seguridad deberán ser comunicadas por el responsable a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose un plazo máximo de 72 horas.

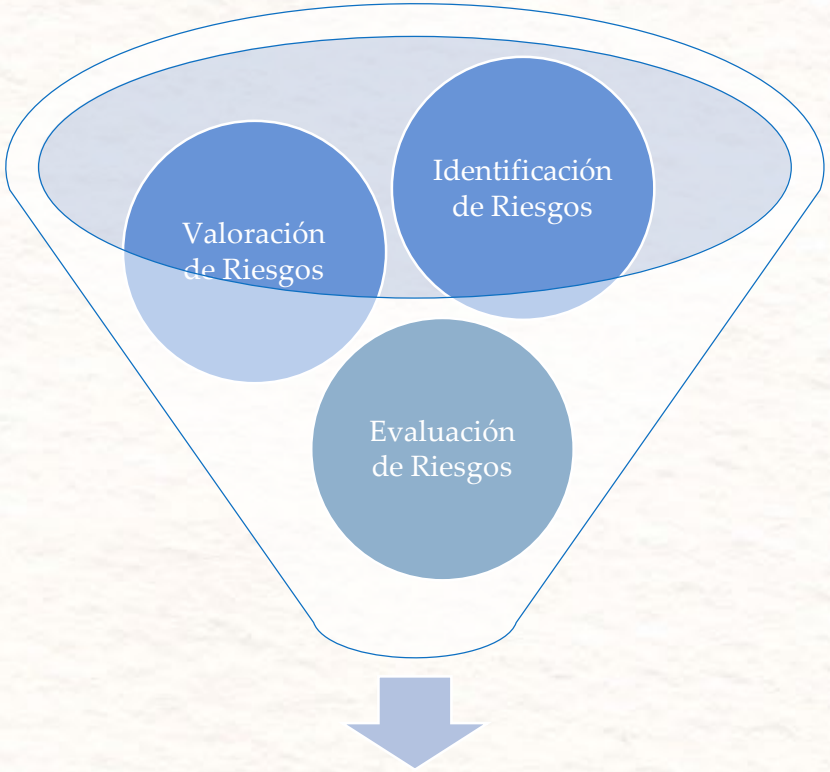
Evaluación de impacto relativa a la protección de datos EIPD

- Evaluación de impacto: El cálculo o estimación de los efectos que un conjunto de acciones puede provocar antes, durante o después.
- Evaluación de impacto relativa a la protección de datos: Antes de ponernos a tratar datos personales hagamos una reflexión sobre sus consecuencias. Esta reflexión será mediante una metodología sistemática, repetible y documentada.

La EIPD también se puede emplear como instrumento de rendición de cuentas para cumplir los requisitos del RGPD.

Análisis de Riesgos

Es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.



Tratamiento de Riesgos

MUCHAS GRACIAS