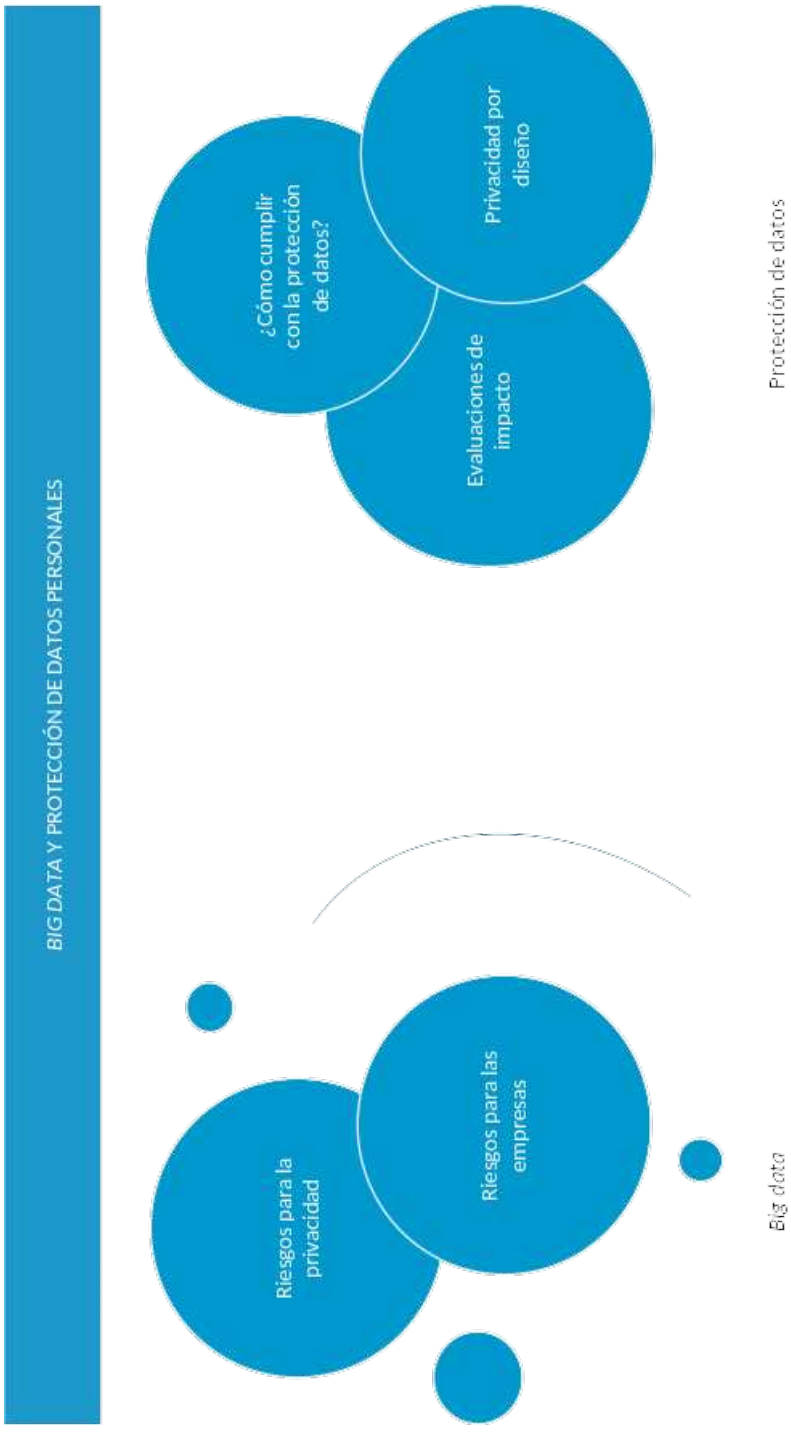
Gobierno del Dato y Toma de Decisiones

Tema 9. Big data y protección de datos personales

Índice

Esquema



© Universidad Internacional de La Rioja (UNIR)

9.1. Introducción y objetivos

En este tema vamos a analizar los retos que el *big data* plantea a la privacidad y protección de datos y conocer cuáles son las tendencias que se están articulando para dar respuesta a dichos retos.

Este tema también aborda las implicaciones que desde el punto de vista de la privacidad y la protección de datos tienen los tratamientos de datos masivos dentro del entorno *big data analytics*, para ello establecemos los objetivos siguientes:

- Identificar brevemente los retos para las empresas.
- Describir las posibles implicaciones que el *big data* puede tener sobre la privacidad de las personas y qué aspectos de la normativa hay que tener en consideración en un proyecto *big data.*
- Analizar el concepto de seguridad por diseño, iniciativa que pretende dar respuesta a los restos planteados y facilitar un equilibrio entre los requerimientos del negocio y los derechos de los ciudadanos.
- Introducirnos en las evaluaciones de impacto, herramienta que ayuda a evaluar los riesgos que para la privacidad tienen los productos y servicios, y a identificar controles mitigadores.

© Universidad Internacional de La Rioja (UNIR)

9.2. ¿Amenaza el big data a la privacidad?

Big data: crecimiento exponencial de la disponibilidad y el uso automatizado de la información, se refiere a conjuntos de datos digitales gigantes en poder de las corporaciones, los gobiernos y otras grandes organizaciones, que luego son analizados exhaustivamente utilizando algoritmos informáticos.

El *big data* se basa tanto en la creciente capacidad de la tecnología para apoyar la recogida y el almacenamiento de grandes cantidades de datos como en la capacidad de analizar, conocer y sacar el máximo partido de todo el valor de los datos (en particular, el uso de aplicaciones de análisis).

Es evidente el gran potencial que presenta el *big data* para la innovación, algunos lo han considerado como el *oil* del siglo XXI. Gracias al avance tecnológico existente, unido a la facilidad de recolectar información, será fuente de importante desarrollo del conocimiento al poder aplicar la correlación sobre grandes volúmenes de datos, de manera que el valor de la información que se pueda llegar a obtener sea inimaginable.

Dentro de este debate, no son pocos los que reconocen en el análisis de datos y el conocimiento basado en la correlación un nuevo paradigma en el pensamiento humano que desplazaría a un segundo plano la búsqueda de relaciones de causa y efecto. Sea o no una revolución, lo cierto es que está aquí y existe un amplio consenso sobre las posibilidades que el *big data* ofrece y ofrecerá en el futuro, que hoy ya se pueden ver en su amplia aplicación en la investigación, entre otras, la investigación de la física de partículas o la investigación genética.

© Universidad Internacional de La Rioja (UNIR)

La expectativa de que el *big data* pueda, en última instancia, conducir a decisiones mejores y más informadas ya ha facilitado su incorporación en diferentes sectores muy diversos, entre ellos, la salud, las comunicaciones móviles, las redes inteligentes, la gestión del tráfico, la detección de fraudes o la comercialización y venta al por menor, tanto *online* como *offline*.

Hoy en día existe un gran desconocimiento del volumen real de datos que pueden estar almacenados por las diferentes organizaciones, gobiernos, empresas… y del uso y finalidades que se le pueda dar a esta información; pero existe el consenso de considerar que su incremento será exponencial.

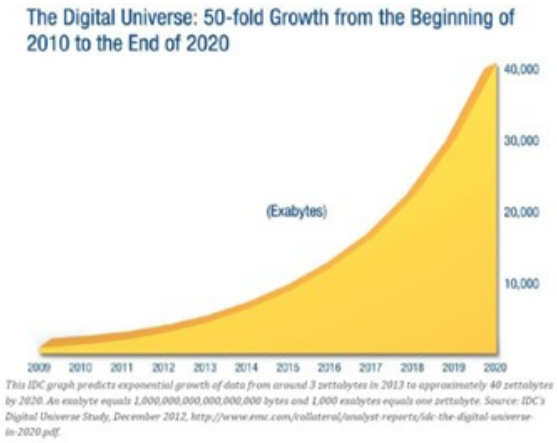


Figura 1. Crecimiento del universo digital 2010-2020. Fuente: Zhenhua's Wiki, s.f.

Se dispone de tecnologías con capacidad de analizar ingentes cantidades de datos no estructurados de diferentes fuentes a altas velocidades de procesamiento. A lo que se habrá de añadir el Internet de las cosas, facilitado por el nuevo estándar de Internet Protocol versión 6 (IPv6) y una potencial conexión IPv6 que, tal y como señala Wikipedia, admite 340 282 366 920 938 463 463 374 607 431 768 211 456 direcciones (2128 o 340 sextillones) —cerca de 6,7 × 1017 (670 mil billones)— por cada milímetro cuadrado de la superficie de la Tierra.

© Universidad Internacional de La Rioja (UNIR)

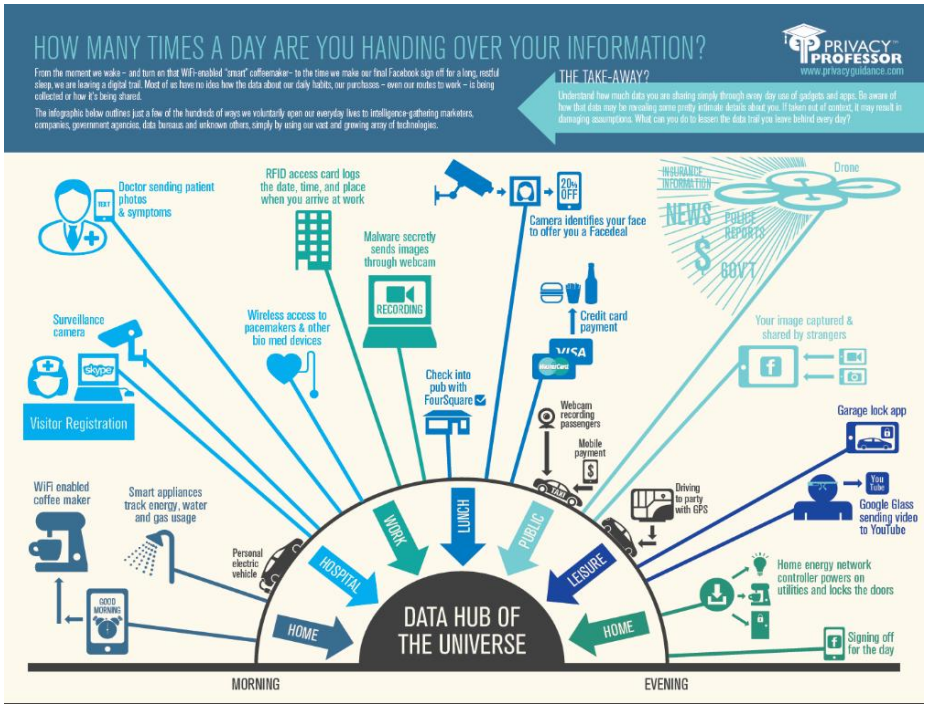


Figura 2. Centro de datos del universo. Fuente: Protiviti Chile, 2018.

Del big data al big brother

Actualmente, hay un amplio debate sobre la potencial amenaza que, desde el punto de vista de la protección de datos y el derecho a la intimidad, presenta esta acumulación ingente de datos y sus potenciales usos, vislumbrándose grandes y significativos riesgos.

No se cuestiona una tecnología que ya está ofreciendo importantes avances en áreas de amplio consenso, en relación con el beneficio que genera a la sociedad, como es el caso de la ciencia; pero sí se cuestiona el uso que de la tecnología se pueda derivar y la afectación que esto pueda tener para los ciudadanos.

Es en este marco donde la presencia de gobiernos y empresas con ingentes cantidades de datos sobre los ciudadanos se perciben como una amenaza no solo sobre la privacidad, sino también sobre su libertad.

© Universidad Internacional de La Rioja (UNIR)

Potencialmente podrían facilitar un conocimiento amplio e íntimo de los individuos, a los que, además, se les podría someter a decisiones automatizadas con base en dicho conocimiento. La amenaza es un potencial *big brother* que sepa todo sobre nosotros, facilitado por un mundo hiperconectado en el que el acceso a multitud de fuentes de datos y su tratamiento permita descubrir el perfil más íntimo de las personas —el yo más íntimo— en el que quedarían integrados: pensamientos, deseos, ilusiones, conductas, etc.

La amenaza se fundamentaría, en primer lugar, en la **trazabilidad de nuestros actos y conductas en Internet,** donde existe una continua captación de datos sobre nuestras interacciones, que además podría reflejar nuestras conductas más íntimas, gracias a una falsa percepción de anonimato por parte del individuo. En este contexto sería posible **ligar las acciones del yo virtual con el yo real,** algo que con la incorporación de altas capacidades de tratamiento y fuentes adicionales de información se presupone muy posible.

Esta amenaza se materializaría en las decisiones que, con base en este conocimiento de las personas, se podrían fundamentar, bien a través de un conocimiento particular de cada individuo o bien a través de la aplicación de patrones o perfiles. Una decisión que podría tener carácter predictivo, basada en un histórico de datos y su acomodo en perfiles establecidos. Incluso se podrían aplicar decisiones sobre hechos no realizados pero que por inferencia sí se producirían, lo que podríamos llamar una «seguridad preventiva», tal y como se trataba, por ejemplo, en la película *Minority Report*.

Este debate mediático se puede seguir fácilmente por los recurrentes artículos o entradas en blogs presentes en Internet.

© Universidad Internacional de La Rioja (UNIR)

Al margen de este debate apocalíptico, la discusión habría que centrarla en cómo crear un equilibrio que garantice la privacidad y protección de datos de los ciudadanos al mismo tiempo que da respuesta a las necesidades de las empresas.

Hoy por hoy, en las empresas el *big data* está siendo utilizado para identificar tendencias generales y correlaciones. Por ejemplo, en el campo del *marketing* y la publicidad el *big data* puede ser utilizado para analizar o predecir preferencias personales, el comportamiento de las personas y las actitudes de los clientes individuales y así traducir estos en medidas o decisiones que se toman sobre los clientes, como pueden ser descuentos personalizados, ofertas especiales y anuncios dirigidos basados en perfiles.

El reto está en que estos usos se desarrollen sin comprometer los derechos de los ciudadanos, el derecho a la privacidad y a la protección de datos personales; es decir, sin atentar contra los derechos y libertades de los individuos.

Retos para las empresas y organizaciones

Las tecnologías de análisis de grandes datos son, sin duda, una gran oportunidad para las empresas, al facilitar la búsqueda de la obtención de patrones y correlaciones que pueden no ser evidentes y sí útiles para el negocio.

© Universidad Internacional de La Rioja (UNIR)

Un ámbito que adquiere especial protagonismo, como ya hemos comentado, es el área de *marketing*, en la búsqueda no solo de conocer mejor a los clientes en lo referente a sus preferencias y comportamientos de compra, sino también para facilitar la toma de decisiones sobre los mismos. Esto puede llegar a suponer una **ventaja competitiva** con relación a:

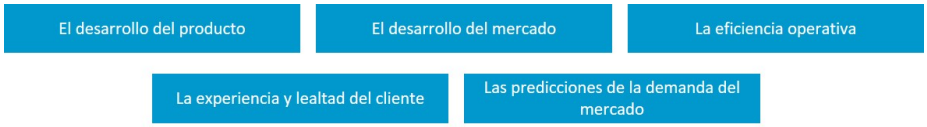
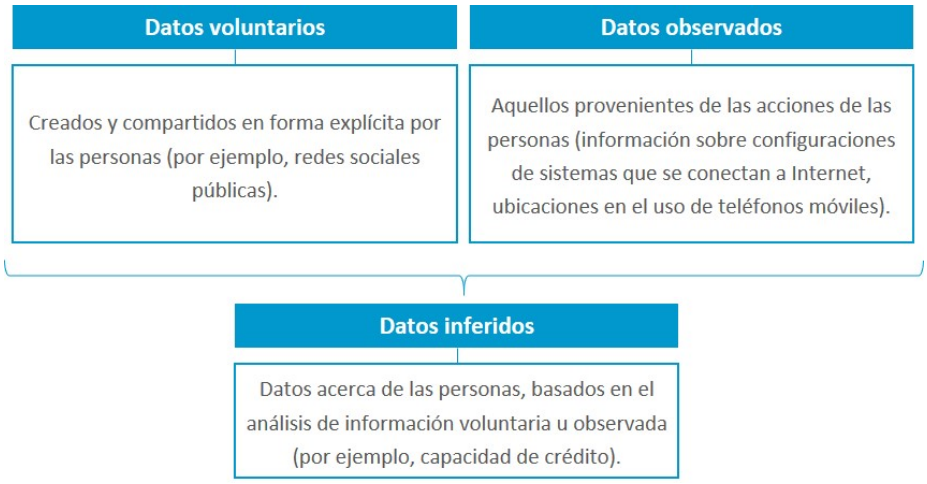


Figura 3. Ámbitos beneficiados. Fuente: elaboración propia.

En este contexto los datos personales que manejan las empresas son:



© Universidad Internacional de La Rioja (UNIR)

Ideas clave

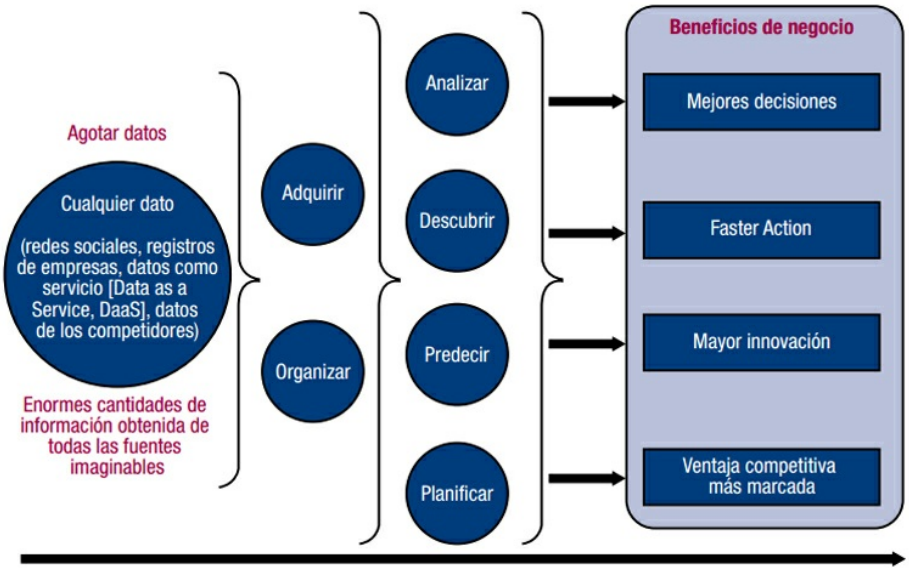


Figura 4. *Big data,* impactos y beneficios. Fuente: ISACA, 2013.

Estas fuentes dispares fácilmente nos van a llevar a pensar que el tratamiento de estos datos no es indiferente para las regulaciones en protección de datos y que cumplir con las obligaciones de la normativa debe ser un objetivo clave en los procesos de *big data*.

El incumplimiento de la normativa no solo puede tener repercusiones económicas, **un riesgo económico** importante mediante sanciones, sino también un **riesgo reputacional** que convierta una ventaja competitiva en una amenaza al ser una «ventaja» ilícita. Las empresas deberán, por tanto, gestionar los riesgos derivados del cumplimiento normativo en protección de datos.

Pero, es más, vivimos en un mundo que está ampliamente globalizado, Internet facilita que ciudadanos de un extremo del mundo interactúen con entidades ubicadas en el polo opuesto del planeta y, seguramente, sometidos a regulaciones en materia de privacidad y protección de datos muy diferentes. Por tanto, las empresas deberán gestionar esta disparidad legislativa y la potencial inseguridad jurídica que pueda introducir en sus operaciones.

© Universidad Internacional de La Rioja (UNIR)

Esta disparidad de regulación en un ámbito capaz de generar ventajas competitivas sin fronteras somete a obligaciones bien diferentes para sus actores, en función de la legislación aplicable. Esta desigualdad, en cuanto las reglas de juego, puede incidir negativamente sobre aquellas entidades que estén sometidas a marcos regulatorios más estrictos. Esta es una de las críticas importantes que se vierten sobre la legislación de la Unión Europea en materia de protección de datos.

La normativa de la UE es especialmente garantista en cuanto a los derechos de los ciudadanos se refiere y reconoce el derecho de autodeterminación informativa como un derecho fundamental, un derecho instrumental, básico para la libertad del individuo.

Este hecho, frente a legislaciones más laxas como la de EE. UU., puede ser considerado como una barrera para entidades europeas en la lucha por un mercado global y todo un **riesgo para su competitividad** en Internet (comercio electrónico, redes sociales, etc.). Además, esta disparidad internacional también puede ser un **riesgo jurídico** para las grandes corporaciones de carácter multinacional.

Por último, asistimos a una creciente necesidad por parte de las empresas de datos y de su análisis para la toma de decisiones estratégicas y la evaluación de sus resultados, lo que puede tensar los procesos internos de autorregulación en la materia y la asunción de comportamientos no éticos o no legales en pro de beneficios económicos. Dos ejemplos de ello:

- Sucumbir a la tentación inmediata de proceder a la captación de todo tipo de dato sin finalidad concreta alguna y con la expectativa de un uso futuro, bajo la expectativa de que se pueda extraer información y conocimiento y ayudar en la toma de decisiones.
- La utilización de datos de carácter personal para finalidades diferentes de aquella para la que los datos fueron recabados, no amparadas por la ley.

© Universidad Internacional de La Rioja (UNIR)

A ello también habría que añadir un **riesgo social,** de manera que la generalización de determinadas prácticas poco transparentes pudiera desencadenar un rechazo social a determinados usos, que *a priori* no debería tener una connotación negativa, y a un fomento de legislación más restrictiva. Para ello, solo debemos reflexionar sobre las noticias que en los últimos tiempos han aparecido en los medios sobre Google o sobre el espionaje indiscriminado de gobiernos a sus ciudadanos.

El caso de Google es especialmente interesante, ya que es uno de los líderes en servicios de *marketing* basados en técnicas de *analytics*. Es posible que sus prácticas, debido a su posición dominante en el mercado, no tengan un impacto directo sobre el uso que los usuarios hacen de sus servicios, pero seguramente se intensifica la preocupación de las autoridades de protección de datos, que buscarán reforzar los mecanismos para garantizar el cumplimiento de la normativa. Esta circunstancia, entre otras, ha contribuido al nuevo marco regulador de la protección de datos personales en la UE. Veamos dos ejemplos:

- Google se enfrenta a una demanda por haber espiado el contenido de millones de mensajes enviados y recibidos por estudiantes estadounidenses que utilizan aplicaciones de la compañía para la *suite* de educación. Además, está acusada de haber utilizado esa información para construir perfiles encubiertos utilizados para enviar publicidad dirigida a los estudiantes.

  Al hilo de la cuestión en Estados Unidos, se plantean nuevas preguntas acerca de la compatibilidad entre las leyes de protecciones de los niños en Estados Unidos y el uso de *big data*.

- El reconocimiento de estas prácticas se deja entrever en la modificación de los términos de servicios (ToS).

Puedes consultar los términos de servicio de Google en: https://policies.google.com/terms?hl=es

---

© Universidad Internacional de La Rioja (UNIR)

Los términos del servicio de Google indican, por ejemplo, que:

> «Google usará los derechos que le confiere esta licencia únicamente con el fin de: Gestionar y mejorar los servicios […]. Esto incluye el uso de sistemas automatizados y de algoritmos para analizar tu contenido y poder hacer lo siguiente:
>
> - Comprobar si hay spam, software malicioso o contenido ilegal.
> - Ofrecerte servicios personalizados, como recomendaciones, resultados de búsqueda, contenido y anuncios personalizados» (Google, s.f.).

A lo que se suman las actuaciones de las agencias de protección de datos de los Estados miembros de la Unión Europea, que se saldaron con sanciones.

En el caso de España, en diciembre de 2013, Google fue objeto de apertura de expediente sancionador por parte de la Agencia Española de Protección de Datos por vulnerar gravemente los derechos de los ciudadanos. En el procedimiento se declaran ilegales los tratamientos de datos personales realizados por Google con su nueva política de privacidad, donde los argumentos motivadores de la sanción serían los siguientes:

- Se considera constatado que Google no da a los usuarios información suficiente sobre qué datos recoge y para qué fines los utiliza, combina los obtenidos a través de distintos servicios, los conserva durante un tiempo indefinido y obstaculiza el ejercicio de los derechos ARCO (acceso, rectificación, cancelación-supresión y oposición).
- Esta combinación de los datos que recoge por medio de diferentes servicios excede ampliamente de las expectativas razonables de la mayoría de los usuarios, que no son conscientes de ello y pierden el control de su propia información personal.

© Universidad Internacional de La Rioja (UNIR)

- La resolución considera que se recoge y trata ilegítimamente información con datos de carácter personal de todos los usuarios que acceden a sus servicios (usuarios dados de alta y visitantes). Estaríamos hablando de más de un centenar de servicios dirigidos a usuarios residentes en España. Además, no se informa con claridad a los usuarios de Gmail de que se realiza un filtrado del contenido del correo y de los ficheros anexos para insertar publicidad.

Por tres infracciones a la LOPD se impuso a Google una sanción de 300 000 euros por cada una, requiriéndole que cumpla con la ley sin dilación.

¿Cuáles son los riesgos y los desafíos planteados por el big data para el derecho a la protección de los datos personales y la privacidad?

Desde el punto de vista de la protección de datos y el derecho a la intimidad, presenta grandes y significativos riesgos.

El grupo de trabajo WP29 (en adelante, WP29) es un órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud del artículo 29 de la Directiva 95/46/CE. En él están presentes las autoridades de protección de datos de los países miembros de la Unión Europea, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que con carácter consultivo es independiente. Este órgano y sus competencias ampliadas con la entrada en vigor del RGPD pasa a denominarse Comité. Tiene entre sus funciones:

- Aconsejar a los Estados en relación con la protección de datos.
- Promover la aplicación de la directiva de protección de datos en todos los Estados miembros de la UE.
- Facilitar a la Comisión dictamen sobre las leyes comunitarias que afectan al derecho a la protección de datos personales (órgano consultivo).

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En el documento «Opinion 03/2013 on purpose limitation» elaborado por el WP29, identifica cinco importantes amenazas en materia de protección de datos derivadas del *big data:*

- **La magnitud de la recopilación de datos,** la capacidad de seguimiento y elaboración de perfiles de los individuos, teniendo en cuenta la variedad y el detalle de los datos recopilados y la combinación de los datos con diferentes fuentes pueden ser una importante amenaza a la privacidad de las personas y el derecho a la determinación informativa.

- **La seguridad de los datos,** que no siempre responde a los riesgos de la información que es tratada, configurándose niveles de protección muy a la zaga de la expansión en el volumen; facilitando potenciales situaciones de gran impacto sobre los ciudadanos como, por ejemplo, en el caso accesos no autorizados por atacantes cibernéticos.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **La transparencia,** la posible desprotección del ciudadano frente a usos sobre los que no se le proporciona suficiente información para poder ejercitar de manera adecuada sus derechos, el sometimiento de los ciudadanos a decisiones que no entienden y sobre las que no tienen ningún control.

- **La inexactitud, la discriminación, la exclusión y el desequilibrio económico** entre las grandes corporaciones y el ciudadano, que limitan las capacidades de este en la defensa de sus intereses.

- El **dramático aumento de las posibilidades de vigilancia del gobierno** . Que facilita una capacidad de supervisión y acceso a información sobre el comportamiento de los individuos, con la capacidad de generar inferencias sobre aspectos políticos, filosóficos y religiosos, nos disponibles hasta ahora.

En el texto se considera, además, que el tipo de técnicas de análisis empleado puede llevar a resultados que son inexactos, discriminatorios o ilegítimos. Por ejemplo: un algoritmo podría detectar una correlación errónea y, a continuación, dibujar una inferencia estadística, de manera que, cuando se aplique para informar en acciones comerciales o en la toma de decisiones, estas podrían ser injustas y discriminatorias. Esto puede perpetuar los prejuicios y los estereotipos existentes y agravar los problemas de la exclusión social y la estratificación de clases.

© Universidad Internacional de La Rioja (UNIR)

Además, y en términos más generales, la disponibilidad de grandes conjuntos de datos y las herramientas de análisis sofisticadas utilizadas para examinarlos no están al alcance de todos y puede potenciar el desequilibrio económico entre las grandes empresas, por un lado, y los consumidores, por el otro. Este desequilibrio económico puede dar lugar, por ejemplo, a una discriminación de precios injusta con respecto a los productos y servicios que se ofrecen, así como a anuncios y ofertas dirigidas altamente intrusivas, perturbadoras y personalizadas.

También podría dar lugar a otros efectos significativos adversos en las personas, por ejemplo, con respecto a las oportunidades de empleo, prestamos bancarios u opciones de seguro de salud.

© Universidad Internacional de La Rioja (UNIR)

9.3. Cómo cumplir con la protección de datos en el big data

Todo tratamiento de datos personales ha de cumplir con los principios de la protección de datos establecidos en la legislación en protección de datos personales vigentes y *big data analytics.* Si trata datos de carácter personal, no es una excepción.

Concepto de dato personal identificado o identificable

Revisemos rápidamente el concepto de dato de carácter personal. En el Reglamento General de Protección de Datos, se definen los datos personales como «toda información sobre una persona física identificada o identificable ("el interesado")» (art. 4.1, RGPD).

Y se considerará persona física identificable: «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4.1, RGPD).

No es una definición que esté lejos de la que nos facilitaba la Directiva 95/46/CE, pero sí es actualizada, debido a la relevancia de los avances en los últimos años, como es la consideración de la identidad genética en el concepto de **identificable.**

Dato personal: cualquier información concerniente a las personas físicas identificadas y/o identificables, tanto relativo a su identidad (nombre y apellidos, domicilio, filiación, NIF…), así como relativo a su existencia y ocupaciones (trabajo, estudios, enfermedades, actividades de ocio, etc.)

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Es fácil encontrar un consenso a la hora de determinar qué información hace que las personas físicas sean identificadas en el marco de las legislaciones de la UE. Ahora bien, la cuestión no resulta tan trivial si nos preguntamos: ¿qué información concreta hace a una persona identificable? Pregunta cuya respuesta no siempre se resuelve de manera uniforme.

Ejemplos de este carácter interpretativo amplio lo tenemos en la consideración de la dirección IP como dato personal. La Agencia Española de Protección de Datos lo considera como dato de carácter personal al hacer identificables a las personas, mientras que en Francia ya son dos las sentencias que restarían ese carácter de identificable a la IP. Lejos de pretender abundar en los argumentos de un caso concreto, que no pretende más que mostrarse como ejemplo, sí debemos resaltar aquello en lo que existe cierta unanimidad: **la particularidad de cada caso.**

No obstante, el devenir interpretativo viene marcado claramente por la jurisprudencia europea, y tras más de veinte años de directiva europea, han existido adaptaciones o correcciones interpretativas al hilo de las sentencias de los tribunales y, en especial, del Tribunal de Justicia Europeo.

Hoy estaríamos considerando la IP como dato de carácter personal, incluso las IP dinámicas.

El considerando 26 del RGPD establece que, **para determinar si una persona es identificable,** deberán tenerse en cuenta todos los medios que puedan ser utilizados por el responsable de tratamiento o cualquier otra persona para identificar directa o indirectamente a un individuo y estos medios deben estar objetivamente al alcance. Para ello se deberían tener en consideración los costes asociados, la cantidad de tiempo necesaria, la tecnología disponible y el desarrollo tecnológico. Es decir, no tendrá dicha consideración si son requeridos medios desproporcionados para proceder a la identificación de los individuos.

© Universidad Internacional de La Rioja (UNIR)

Además, el considerando clarifica dos aspectos (considerando 26, RGPD):

- La pseudonimización, como técnica primaria para reducir el riesgo de identificación, y la consideración de los datos pseudonimizados como datos de carácter personal.
- La anonimización de los datos como mecanismo de obtención de conjuntos de datos a los que no les son aplicables la normativa en protección de datos personales RGPD.

Ahora bien, del propio considerando se puede concluir que los datos que **no** tengan la consideración de datos identificables —y, por tanto, no están sujetos a la normativa en protección de datos— más adelante —con los avances tecnológicos y la facilidad de acceso a los mismos, la reducción de costes e incluso la facilidad de uso de otras fuentes alternativas de información— pueden elevar su consideración a dato identificable y, por tanto, estar sometidos a la normativa de protección de datos.

En cualquier caso, siempre que tratemos **datos de carácter personal** en el ámbito de *big data* deberemos aplicar desde el inicio la normativa en protección de datos personales. Esto implicará cumplir con los principios de la protección de datos y evaluar y aplicar técnicas que permitan sustraer los datos de las obligaciones legales, como la anonimización.

Por tanto, de inicio, el tratamiento de datos debe alinearse con los principios de la protección de datos personales, tal y como son entendidos en el RGPD (art. 5) los principios relativos al tratamiento. Recordémoslos brevemente:

© Universidad Internacional de La Rioja (UNIR)

Figura 6. Principios de la protección de datos personales RGPD. Fuente: elaboración propia.

- **Licitud, lealtad y transparencia:** con el consentimiento informado como base de la legitimación del tratamiento, a falta de la aplicabilidad de otras vías legales de legitimación (art 6., RGPD).
- **Limitación de la finalidad:** para la que se van a tratar los datos establecida de forma concreta.
- **Minimización de datos:** la reducción de los datos tratados a los estrictamente necesarios para el fin perseguido por el tratamiento.
- **Exactitud de los datos:** como obligación requerida para el mantenimiento de los datos y, en su defecto, proceder a su supresión.

© Universidad Internacional de La Rioja (UNIR)

- **Limitación del plazo de conservación:** durante el tiempo estrictamente necesario para cumplir con la finalidad del tratamiento.
- **Confidencialidad e integridad (seguridad):** garantizando la seguridad de los datos personales durante todo el ciclo de vida de los datos.
- **Responsabilidad proactiva:** el conjunto de obligaciones establecidas al responsable de tratamiento o encargado de tratamiento, que obliga a que los tratamientos sean conformes al resto de principios y a garantizar la transparencia y al ejercicio de derechos de los ciudadanos.

Retos de aplicación de la protección de datos en *big data*

Consentimiento del afectado: el principio de responsabilidad proactiva exige al responsable de tratamiento la prueba de la legalidad de este, y uno de los mecanismos establecidos para la legitimación (art 6., RGPD) es el consentimiento por parte del afectado, siendo el responsable el que debe probar que efectivamente dispone del consentimiento del afectado y que este otorgó respetando los términos establecidos en el reglamento (art. 7, RGPD).

El consentimiento debe ser concreto, para una finalidad específicamente informada, conforme al principio de finalidad, no pudiéndose tratar los datos para otros fines.

Los usos potenciales para los que se van a utilizar los datos a menudo no pueden ser totalmente identificados en la fase de captación de datos de usuarios, por ejemplo. Esto podría implicar que los usuarios no hayan sido informados de dichas finalidades y abriría la necesidad de obtener el correspondiente consentimiento para el tratamiento de datos para otras finalidades o que estas tuvieran la consideración de compatibles (art 89., RGPD) con la finalidad informada al afectado en el proceso de captación de la información (habría que tener la capacidad de prueba) o esté amparado por ley.

© Universidad Internacional de La Rioja (UNIR)

Además, en los procesos de *analytics* pueden aparecer nuevos datos que tengan la consideración de dato personal, mediante el enriquecimiento con fuentes externas, que faciliten los procesos de reidentificación de las personas, luego su tratamiento implicaría la legitimación del mismo.

Habrá que prestar especial atención a los tratamientos de datos personales de categorías especiales y a los datos de los menores.

Interés legítimo como base legal del tratamiento en lugar del consentimiento

Es de resaltar que **confiar en la legitimación con base en intereses legítimos no es una opción flexible,** que no permite cualquier cosa. Las organizaciones de *big data* siempre deben equilibrar sus propios intereses con los de las personas involucradas.

Hay que resaltar que no es posible recurrir al interés legítimo cuando dichos intereses sean anulados por los intereses o derechos y libertades fundamentales del interesado que requieren protección de datos personales, en particular, cuando el sujeto de datos es un niño. Esto lleva a la necesidad de:

- **Ponderación de intereses:** evaluar, previamente a su aplicación, los intereses de la organización frente a los intereses de los individuos.
- **Asunción de responsabilidad:** poder justificar que efectivamente existe un verdadero interés legítimo que, adecuadamente ponderado, no menoscaba los intereses de los afectados.
- **Informar:** la base del tratamiento en el interés legítimo no exime de informar al afectado.

© Universidad Internacional de La Rioja (UNIR)

Algunos ejemplos de intereses legítimos:

- El ejercicio del derecho de libertad de expresión o información, incluidas las situaciones en las que se ejerza dicho derecho en los medios de comunicación y en las artes.
- La prospección convencional y otras formas de comercialización o publicidad.
- La ejecución de derechos reconocidos en procedimientos judiciales, incluido el cobro de deudas mediante procedimientos extrajudiciales.
- La prevención del fraude, el uso indebido de servicios o el blanqueo de dinero.
- La supervisión de los empleados con fines de seguridad o de gestión.
- Los regímenes internos de denuncia de irregularidades.
- La seguridad física, la tecnología de la información y la seguridad en la red.
- El tratamiento con fines históricos, científicos o estadísticos.
- El tratamiento con fines de investigación.

Comunicación de datos

La analítica *big data* a menudo dibuja conjuntos de datos de múltiples fuentes para la obtención de relaciones o correlaciones que puedan generar conocimientos útiles. Este acceso a diferentes fuentes de datos para recopilar datos de carácter personal para ser objeto de tratamiento debe ser legitimado en el marco del RGPD.

Para estas dos hipotéticas situaciones no es difícil pensar en el esfuerzo que puede suponer recabar el consentimiento poscaptación para el caso de grandes masas de datos. Además, en muchas ocasiones no sería posible realizarla ante la dificultad de contactar con el afectado, pues no se cuenta con la información de contacto o esta no está actualizada.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

El artículo 14 del RGPD («Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado») reconoce las situaciones en las que la comunicación de dicha información no es posible o suponga un esfuerzo desproporcionado, y articula una salida para el caso de los tratamientos con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de manera que no se exija la comunicación siempre y cuando el hecho de tratar de cumplir con la obligación de información pueda obstaculizar gravemente los objetivos del tratamiento.

Para ello se debe cumplir con las garantías del artículo 89 del RGPD («Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos»). Estas garantís exigen, por ejemplo, procesos específicos para garantizar el respeto al principio de minimización de los datos personales.

Ejercicio de derechos

El acceso a fuentes dispares de datos en un mundo tan interconectado sometido a diferentes regulaciones puede imposibilitar el ejercicio eficaz de los derechos de acceso, rectificación, supresión y oposición.

Además, el fortalecimiento a los derechos que supone el RGPD (en virtud del cual se obliga a los responsables de tratamiento a comunicar el derecho ejercido a aquellas entidades a las que hubiera comunicados los datos, para que se actúe en consecuencia) añade una complejidad adicional: «obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento» (art. 19, RGPD). Cabe recordar que esta obligación es la base del llamado **derecho al olvido.**

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Acceso a datos por cuenta de terceros

Los servicios en la nube y transfronterizos pueden imposibilitar la regularización de la relación responsable del tratamiento y encargado de tratamiento en los términos establecidos en el artículo 28 del RGPD («Encargado del tratamiento»), máxime en un ecosistema de servicios en la nube en los que la superposición de diferentes capas de servicio y prestadores haga prácticamente imposible conocer los agentes implicados o sus ubicaciones.

Transferencias internacionales

La deslocalización de servicios y servicios en la nube pueden llevar asociados encargos de datos transfronterizos que, dadas las sustanciales y diferentes regulaciones en materia de protección de datos, no fueran legítimos conforme a la ley al ser realizados en espacios donde los marcos de protección no son equivalentes a los de la UE (capítulo V, RGPD: «Transferencias de datos personales a terceros países u organizaciones internacionales»).

Sobre este tema, cabe resaltar que las diferencias normativas de la UE y EE. UU. implican que las transferencias solo sean legítimas si están amparadas por alguna de las excepciones del RGPD o si están autorizadas por la Agencia Española de Protección de Datos Personales. Obtener el consentimiento del afectado también sería una opción, pero ya hemos comentado sus dificultades.

© Universidad Internacional de La Rioja (UNIR)

Derecho de oposición y decisiones automatizadas de datos

El RGPD reconoce a los ciudadanos el derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles. Además, reconoce el derecho del afectado a obtener información sobre los criterios de valoración y el programa utilizado en el tratamiento para adoptar la decisión (arts. 13 y 14, RGPD). Esto tiene implicaciones sobre las finalidades de los tratamientos en *big data* y la obligación de transparencia frente a las impugnaciones, algo complejo por la propia naturaleza de los procesos empleados.

Principios de la protección de datos, por ejemplo:

- **Principio de limitación del plazo de conservación (art. 5, RGPD):** implica que los datos solo serán retenidos por el tiempo razonablemente necesario conforme a la finalidad de los mismos, lo que parece estar en la antítesis del *big data,* donde la acumulación y el enriquecimiento mediante la adición de otros conjuntos de datos para uso prospectivo y una posible utilización futura desconocida pueden ser considerados una necesidad.

- **Principio de minimización de datos:** los datos recabados deben ser adecuados y pertinentes para la finalidad específica; ahora bien, la tendencia del *big data* al *overcollecting* puede atentar contra este principio que exige tratar los datos estrictamente necesarios.

- **Principio de limitación de la finalidad:** referido a la utilización de datos personales recabados para una finalidad con otros fines no siempre compatibles o no amparados por la ley. Esta tendencia a utilizar los datos que se tienen para otros fines sin considerar la finalidad concreta para la que se recabaron y sin analizar si la nueva finalidad es compatible o es admitida por la ley no es conforme a la normativa.

© Universidad Internacional de La Rioja (UNIR)

Limitación de la finalidad

Pretender recurrir a expresiones de finalidades ambiguas o excesivamente genéricas sobre las que recabar el consentimiento pondría en cuestión el principio de calidad e información y atentaría contra el principio de autodeterminación informativa de los afectados, ya que debemos recordar que, para que un usuario pueda ejercer su derecho al control sobre sus datos, el consentimiento debe estar basado en la transparencia y claridad en la finalidad.

Como norma debemos considerar que los datos de carácter personal objeto de tratamiento **no podrán usarse para finalidades diferentes de aquellas para las que los datos se hubieran recogido,** a menos que:

- Exista alguna habilitación legal aplicable.
- Esta nueva finalidad sea compatible con la finalidad con la que fueron recabados los datos.

El principio de limitación de la finalidad no necesariamente crea una barrera para el análisis de *big data,* pero significa que se debe hacer una evaluación de la compatibilidad de los propósitos de procesamiento para poder usar los datos con otros fines.

Los datos pueden usarse para otros fines si la finalidad es compatible, tras un análisis de compatibilidad de finalidades.

El WP29 (Art. 29 WP, 2013) identifica los aspectos que se deberían considerar a la hora de evaluar la compatibilidad de finalidades, entre ellos establece:

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- La relación entre los fines para los cuales fueron recabados los datos y los fines de su posterior procesamiento.
- El contexto en el que los datos han sido recogidos y las expectativas razonables de los titulares de los datos en cuanto a su uso posterior.
- la naturaleza de los datos y el impacto que el nuevo tratamiento puede tener sobre los titulares de los datos.
- las medidas aplicadas por el responsable de tratamiento para garantizar que el tratamiento es leal y para evitar cualquier impacto indebido sobre los titulares de los datos.

La información que las personas han puesto en las redes sociales se va a utilizar para evaluar sus riesgos para la salud o su solvencia, o para comercializar ciertos productos para ellos; a menos que se les informe de esto y se les pida que den su consentimiento, es poco probable que sea justo o compatible. Con el fin de identificar las medidas necesarias, el documento propone diferenciar dos escenarios de ejemplo:

1. Las organizaciones de procesamiento de los datos quieren detectar tendencias y correlaciones en la información.
2. Las organizaciones están interesadas en las personas: perfiles.

A continuación, veremos estos escenarios con más detalle.

© Universidad Internacional de La Rioja (UNIR)

Tratamiento de datos personales para el análisis de tendencias y correlaciones en la información

Aquí el concepto de separación funcional desempeña un papel clave. La separación funcional supone que cada función o departamento que participa en el tratamiento de datos personales solo tiene acceso a aquellos atributos estrictamente necesarios para su función.

Por ejemplo, el área de *telemarketing* accede a los datos de contacto telefónico de los clientes, pero no al resto de información de estos, aunque su finalidad se circunscriba dentro de un habitual tratamiento de datos para fines comerciales (legítimo para las empresas con respecto a sus clientes).

La separación funcional no supone una disociación, técnicamente hablando, pues de la aplicación de esta no se obtiene necesariamente un conjunto de datos que no permite la identificación de las personas, sino más bien un conjunto de datos limitado en cuanto a los atributos que contiene.

Pues bien, en la medida en que esta separación funcional sea posible, podría ser un factor importante para decidir si el uso adicional de los datos para análisis de *marketing* y otros pueden ser considerados compatibles.

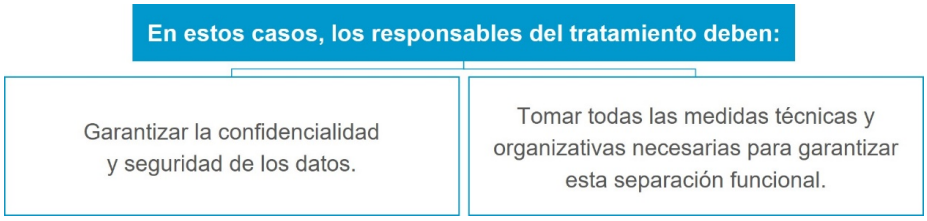


Figura 7. Deberes responsables del tratamiento. Fuente: elaboración propia.

© Universidad Internacional de La Rioja (UNIR)

De manera que no exista duda de que los datos utilizados para fines estadísticos u otros fines de investigación no estarán a disposición de tratamientos que tomen decisiones en relación con los titulares de los datos de que se trate (salvo autorización expresa de las personas interesadas). La organización deberá aplicar las medidas técnicas y organizativas adecuadas para ello.

Como es lógico en este punto, la disociación de datos puede ser una buena herramienta para facilitar el análisis y, al mismo tiempo, para garantizar que no se toman decisiones sobre individuos concretos con base en el análisis específico de sus datos o comportamientos.

Para estos casos, la anonimización total o parcial puede ser de gran ayuda.

Tratamiento de datos personales para análisis de comportamiento de las personas

Este es un posible escenario en el que una organización quiere específicamente analizar o predecir las preferencias personales, el comportamiento y las actitudes de los clientes individuales y, con base en dicho análisis, posteriormente tomar medidas o decisiones.

© Universidad Internacional de La Rioja (UNIR)

En estos casos casi siempre se requiere el consentimiento libre, específico, informado e inequívoco del afectado. De lo contrario, su uso posterior no puede ser considerado compatible con la finalidad que motivó la recogida de datos. Veamos un ejemplo:

> Un supermercado se plantea mejorar el conocimiento que tiene de sus clientes con objeto de mejorar su experiencia y personalizar la oferta de productos. En su momento, facilitó a sus clientes una tarjeta de descuento, de manera que aquellos que la poseían accedían a un descuento sobre sus compras que no dependía de hábitos ni volúmenes de compra, por lo que no se asociaban a los clientes las compras realizadas. Es decir, la empresa no conocía qué compraba cada uno de sus clientes.
>
> Ahora han pensado en registrar todas las compras que realiza un cliente, para lo que se servirán de la tarjeta de fidelización a la que asociará cada compra. Esto permitirá saber qué compró y cuándo cada uno de los clientes que poseen la tarjeta. Analizar esta información facilitará un mejor conocimiento de gustos y hábitos de consumos, por lo que se le podrán dirigir ofertas específicas atendiendo a su histórico de compra.
>
> Por ejemplo, si compra pañales, se le comunicarán ofertas personalizadas de productos infantiles o, atendiendo a la frecuencia de compra de pañales, se le ofrecerá una oferta exclusiva para que se acerque al supermercado.

Este sería uno de los casos en los que el nuevo tratamiento de datos no podría considerarse compatible con el tratamiento que se realizaba anteriormente sobre las tarjetas de fidelización. Antes de activar este sistema, deberán previamente recabar el consentimiento de los afectados.

© Universidad Internacional de La Rioja (UNIR)

En opinión del WP29, es importante destacar que, en caso de ser necesario tal consentimiento —por ejemplo, para el seguimiento y elaboración de perfiles para fines de venta directa, de anuncios basados en comportamientos, intermediación de datos, publicidad basada en la localización o investigación de mercados basada en seguimiento—, se debe garantizar la transparencia y el consentimiento informado de los interesados o consumidores. Para ello, los interesados deberían tener acceso a sus perfiles, así como a la lógica de la toma de decisiones (algoritmo) que llevó a la elaboración del perfil.

En otras palabras, las organizaciones deberían revelar sus criterios de toma de decisiones. Esta es una medida fundamental y de gran calado en el mundo del *big data*.

Para ahondar más en la cuestión se puede consultar la Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, disponible en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd2a#_ftn1

También hay que considerar que la mayoría de las veces no será la información recabada en sí la que es sensible, sino más bien —y lo que es motivo de consideración— son las inferencias que se extraen de la información y la forma en que se dibujan esas inferencias.

El WP29 considera, además, que el potencial riesgo de inferencias erróneas se podría reducir con la transparencia. De hecho, si los titulares de los datos pueden acceder y corregir o actualizar sus perfiles y deciden hacerlo, facilitaría que la información sobre la que se base el tratamiento sea más precisa.

© Universidad Internacional de La Rioja (UNIR)

De hecho, en muchas situaciones, medidas como permitir el acceso directo a los datos de los interesados en un formato fácil de usar y legible ayudaría a mejorar los mismos datos, además de corregir el desequilibrio económico entre las grandes empresas, por un lado, y los interesados, por otro.

También se podrían compartir los beneficios con los individuos, por ejemplo, el acceso a la información sobre el consumo de energía en un formato fácil de usar podría hacer más fácil a las familias obtener las mejores tarifas de gas y electricidad, así como controlar su consumo de energía y modificar su estilo de vida para reducir sus facturas y, en consecuencia, su impacto ambiental. Un detalle que parece haber pasado desapercibido en España en la incorporación de lectores inteligentes de electricidad y el despliegue previsto de los mismos.

Por otro lado, permitir la portabilidad de datos (que se regula en la propuesta del RGPD) podría facilitar a las empresas y consumidores maximizar los beneficios del *big data* de una manera más equilibrada y transparente. También puede ayudar a minimizar las prácticas injustas o discriminatorias y reducir los riesgos del uso de los datos inexactos para la toma de decisiones, lo cual beneficiaría tanto a empresas como a personas o consumidores.

Sin duda, el WP29 considera la transparencia como un elemento clave, no solo a la hora de garantizar los derechos de los ciudadanos, sino también como vehículo enriquecedor de los datos y, por consiguiente, de los resultados.

Consecuencias de la incompatibilidad de finalidades

El WP29 también considera que el procesamiento incompatible no se puede

© Universidad Internacional de La Rioja (UNIR)

remediar con solo adoptar un nuevo fundamento jurídico.

No cumplir con el requisito de compatibilidad tiene graves consecuencias: **el tratamiento de los datos personales de manera incompatible con los fines especificados en la captación de datos es ilegal** y, por lo tanto, no está permitido. El RGPD lo considera una infracción.

La legalización del tratamiento de datos personales para **finalidades incompatibles no basta con solo cambiar los términos de un contrato con el interesado** o mediante la identificación de un interés legítimo adicional del responsable del tratamiento. Esto va en contra del espíritu del principio de limitación de finalidades y elimina su fundamento (Art. 29 WP, 2013).

En otras palabras, el responsable del tratamiento no puede limitarse a considerar el tratamiento posterior como una nueva actividad de procesamiento desconectado de la anterior y eludir esa prohibición.

Uso de los datos personales con motivo de la investigación histórica, estadística o científica

El artículo 6.1.b de la Directiva 95/46/C contenía una disposición específica sobre el tratamiento posterior de los datos de carácter personal con fines históricos, estadísticos o científicos. Esta disposición, en relación con los considerandos pertinentes, permite el tratamiento posterior de los datos con fines históricos, estadísticos y científicos, siempre y cuando el responsable del tratamiento aplique garantías apropiadas y, en particular, cuando garantice que los datos no se utilizarán para apoyar las medidas o decisiones relativas a personas concretas.

En este sentido, el artículo 5.2 del RGPD establece que la legitimidad del tratamiento de datos personales para los fines de la investigación histórica, estadística o científica (y según las condiciones establecidas en el artículo 86) **solo es posible mediante un tratamiento de datos que no permita la identificación de los sujetos.**

© Universidad Internacional de La Rioja (UNIR)

Es decir, **se recomienda siempre que sea posible** el tratamiento de datos que no permitan la identificación de los sujetos (disociados); **en este caso será necesario separar la información que permite la identificación de los sujetos del resto de información (separación funcional).** La aplicación de pseudonimización o, si es posible, el trabajo sobre datos anonimizados.

El WP29 recomienda que las publicaciones con motivo de investigaciones históricas, estadísticas o científicas **solo podrán incorporar datos de carácter personal si hay consentimiento por parte del interesado,** el interesado ha hecho públicos los datos o la publicación de los datos personales es necesaria para presentar los resultados de una investigación, siempre que los intereses o los derechos o libertades fundamentales del afectado no prevalezcan sobre tales objetivos. También abre la puerta a que la comisión pueda adoptar decisiones a fin de especificar los criterios y requisitos del tratamiento de los datos personales implicados, así como las limitaciones a los derechos de información y acceso por parte de los interesados.

Al respecto, el WP29 considera necesaria la incorporación de garantías adicionales, como las medidas técnicas u organizativas para garantizar la separación funcional u otras garantías que contribuyan a la transparencia o elección. Además, esta disposición no se implica ni deja claro que su uso ulterior con fines de investigación históricos, estadísticos o científicos esté sujeto a la misma evaluación de la compatibilidad de las finalidades de los tratamientos de datos de carácter personal.

En España, la LOPD contemplaba este tipo de tratamientos en línea con lo establecido en la Directiva 95/46/C. Además, desarrollos específicos legislativos posteriores tratan de dar cumplida respuesta en ámbitos de investigación específica, como es el caso de la investigación biomédica: Ley 14/2007, de 3 de julio, de Investigación biomédica.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En resumen, no se deberán tratar datos de carácter personal en estas áreas, a menos que sea estrictamente necesario para los fines de la investigación y no sea posible aplicar procesos de disociación o separación funcional entre datos identificativos y el resto de los datos, aplicando en este caso las medidas de seguridad adecuadas y organizativas destinadas a limitar la posible identificación de las personas.

Para terminar con este asunto, hagamos una breve pausa en la *Resolución big data* (de la 36a edición de la International Conference of Data Protection and Privacy Commissoner), pues seguir sus recomendaciones seguramente nos facilite obtener los beneficios derivados del *big data* sin hipotecar los principios de la protección de datos:

«- Respetar el principio de especificación de finalidad.

- Limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende.
- Obtener, cuando sea apropiado, el consentimiento válido del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles.
- Ser transparentes acerca de qué información se recolecta, cómo se procesa, con qué propósito serán utilizados y si será transferida a terceros.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- Dar a las personas acceso apropiado a los datos que han sido recolectados sobre ellas y a la información y decisiones que se han tomado con esos datos. Las personas deben ser avisadas de la fuente de sus datos personales y, cuando sea apropiado, de su derecho a corregir su información, así como de las herramientas para controlar esta información.

- Ofrecer a las personas cuando sea apropiado acceso a la información sobre los insumos principales y los criterios para la toma de decisiones (algoritmos) que se han utilizado como base para el desarrollo del perfil. La información debe presentarse en un formato claro y comprensible.

- Llevar a cabo una evaluación de impacto en la privacidad, especialmente cuando el análisis del *big data* implica usos novedosos o inesperados de los datos personales.

- Desarrollar y utilizar tecnologías del *big data* de acuerdo con los principios de la Privacidad por Diseño.

- Considerar cuándo los datos anónimos mejorarán la protección de la privacidad. La anonimización puede ayudar a mitigar los riesgos para la privacidad asociados con el análisis del *big data,* pero solo si la anonimización está diseñada y gestionada apropiadamente. La solución óptima para anonimizar los datos debe decidirse caso por caso, posiblemente utilizando una combinación de técnicas.

- Tener mucho cuidado y actuar cumpliendo la legislación aplicable en materia de protección de datos, cuando se comparten o se publican conjuntos de datos con seudónimos o que pueden ser identificables indirectamente. El acceso debe ser limitado y controlado cuidadosamente si los datos contienen suficientes detalles, es decir, que pueden vincularse con otros conjuntos de datos o contienen datos personales.

© Universidad Internacional de La Rioja (UNIR)

- Demostrar que las decisiones respecto al uso del *big data* son justas, transparentes y responsables. Relacionado con el uso de datos para fines de creación de perfiles. Tanto estos como los algoritmos en que están basados requieren una valoración continua. Este necesita revisiones regulares para verificar si los resultados de la creación de perfiles son responsables, justos y éticos y si son compatibles y proporcionados con el propósito para el cual los perfiles son usados. Debe evitarse la injusticia con las personas debido a resultados completamente automatizados que arrojen un falso positivo o un falso negativo. Siempre debe estar disponible una valoración manual de resultados, con efectos significativos para los individuos» (Norwegian Data Protection Authority, 2014).

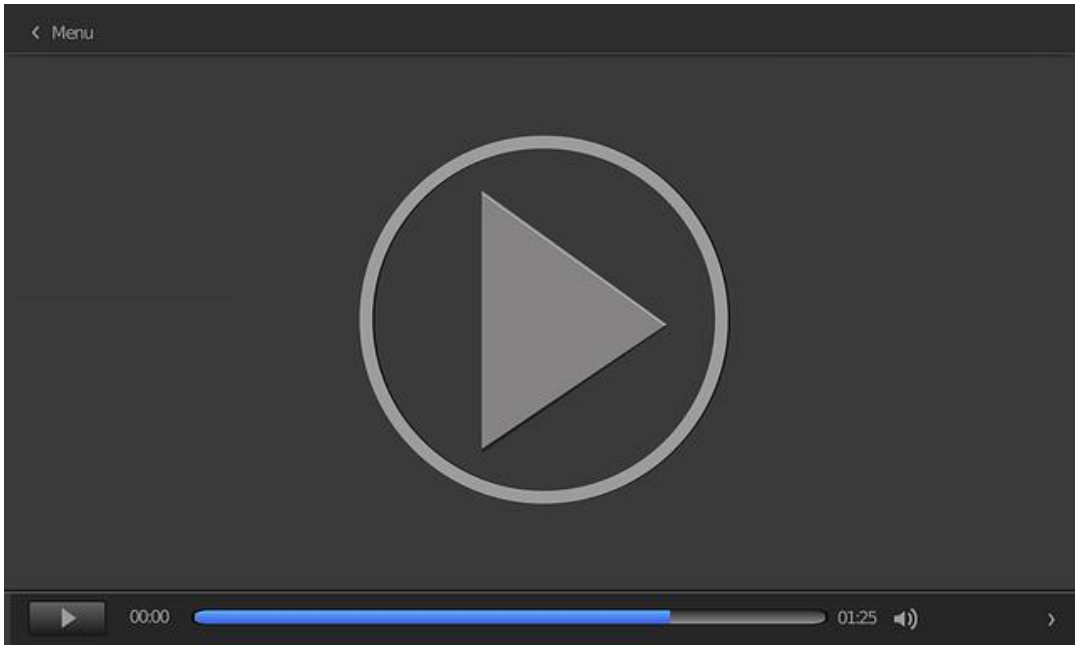
Usar fuentes de datos externas

También deberemos prestar atención al uso de datos de fuentes externas, facilitados por terceros. Debemos conocer si el tratamiento de datos que se va a realizar tiene una finalidad compatible o cuenta con la base legal adecuada como, por ejemplo, el consentimiento del afectado. Para evaluar estas cuestiones, es necesario plantear un proceso análisis específicos.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Para terminar este apartado, accede al vídeo *RGPD y el cloud computing.*



Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=4108f7ec-71e6-4f80-93ff-abd800c247a2

© Universidad Internacional de La Rioja (UNIR)

9.4. Privacidad por diseño

La privacidad por diseño (PbD) es un concepto desarrollado por Ann Cavoukian, Ph, Comisionada de Información y Privacidad de Ontario, Canadá, en los años 90. Concepto con el objeto de responder a los retos de los sistemas de datos en red y a gran escala.

Figura 8. Privacidad por diseño. Fuente: elaboración propia.

Nace como evolución al concepto de **tecnologías de mejora de la privacidad** y promueve garantizar la privacidad en todo el ciclo de vida de los datos, no solo desde el desarrollo de marcos regulatorios, sino también integrándola en el centro de las actividades de las organizaciones y englobando:

- Sistemas de tecnologías de la información.
- Prácticas de negocio responsables.
- Diseño físico e infraestructura en red.

© Universidad Internacional de La Rioja (UNIR)

Y de este modo poder asegurar la privacidad y obtener control de las personas de su propia información, facilitando el principio de autodeterminación informativa de los afectados y ofreciendo, además, a las organizaciones una ventaja competitiva sostenible.

La privacidad por diseño (PbD) desarrolla siete principios que pueden ser aplicados a todo tipo de información personal y, con especial atención, a datos de significada sensibilidad como es la información médica y datos financieros.

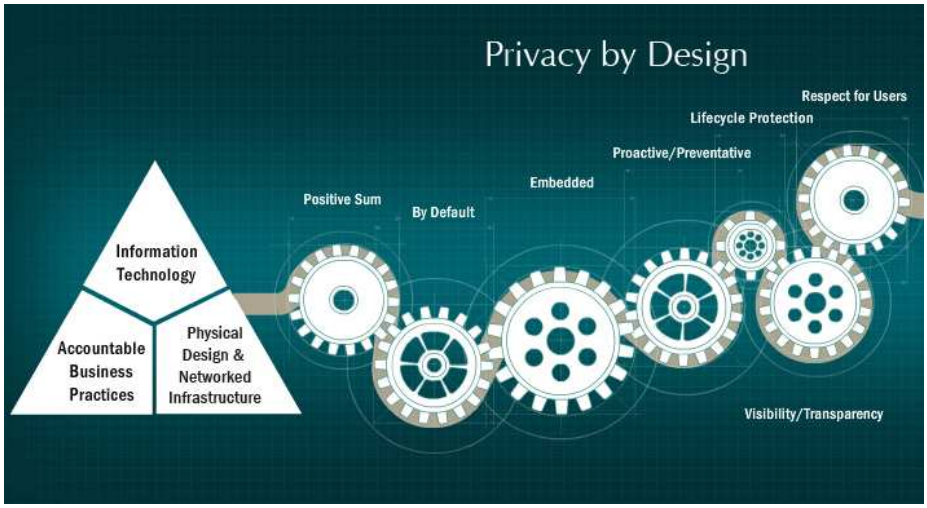


Figura 9. Los siete principios fundamentales de la privacidad por diseño. Fuente: MediaBUZZ, 2013.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Estos siete principios fundamentales, son:

- **Proactivo, no reactivo; preventivo, no correctivo**. El enfoque basado en medidas proactivas, en lugar de reactivas. Anticipar y prevenir eventos de invasión de la privacidad antes de que estos ocurran.

- **Privacidad como la configuración predeterminada (privacidad por defecto).** Asegurándose de que los datos personales estén protegidos automáticamente y por defecto en cualquier sistema de TI o en cualquier práctica de negocios, actuando como una configuración predeterminada de alta privacidad que requeriría la acción de la persona o el usuario para reducir esa configuración de garantía y facilitar acceso a su información. Dentro de esta configuración determinada y como buenas prácticas se incluiría:

  - Finalidad: la información recolectada debe ser una finalidad concreta.
  - Información: el usuario debe ser informado de la finalidad de la recolección.
  - Limitar los datos a la finalidad especificada.
  - Anonimizar los datos, limitar el uso de los datos, su retención, divulgación a la finalidad con la que fueron recabados y a las regulaciones legales.

- **Privacidad incrustada en el diseño**. La privacidad por diseño se incrusta en el diseño y la arquitectura de los sistemas de información y en las prácticas de negocios. Se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

- **Funcionalidad total «todos ganan», no «si alguien gana, otro pierde».** La privacidad por diseño busca acomodar todos los intereses y objetivos legítimos de una forma **ganar-ganar** y evita las falsas dualidades, tales como privacidad versus seguridad, partiendo de la idea de que sí es posible tener ambas al mismo tiempo.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **Seguridad de extremo a extremo. Protección de ciclo de vida completo.** Protección de dato en todo el ciclo de vida, desde la recolección del dato pasando por su almacenamiento y retención y, la fase final, su destrucción adecuada. Para ello se recurriría a la aplicación de medidas de seguridad eficaces.

- **Visibilidad y transparencia. Mantenerlo abierto.** Que las partes involucradas, negocio y tecnologías operen de conformidad a objetivos claros y declarados de forma transparente y bajo el principio de que todas las operaciones van a ser realizadas de conformidad con las premisas y objetivos fijados y van a estar sujetos a esquemas de verificación independientes.

- **Respeto por la privacidad de los usuarios. Mantener un enfoque centrado en el usuario.** Por encima de todo, requiere que los arquitectos y operadores prioricen el interés de las personas ofreciendo servicios robustos de privacidad por defecto, información adecuada y opciones amigables para el usuario, facilitándonos el control sobre sus datos.

© Universidad Internacional de La Rioja (UNIR)

9.5. Evaluaciones de impacto (PIA/EIPD)

Una evaluación de impacto es un análisis de los riesgos que sobre el derecho fundamental a la protección de datos personales de los afectados puede tener un tratamiento de datos determinado, ya sea como producto o como servicio.

Las evaluaciones de impacto forman parte de la respuesta que desde la perspectiva de la **privacidad por diseño** se está articulando desde las autoridades de protección de datos de la UE y que se incorporan en el articulado del reglamento de protección de datos de la UE.

En este epígrafe nos centramos en la guía desarrollada por la AEPD al entender que se adapta mejor a la legislación española, si bien es recomendable consultar otras como la elaborada por la Information Commissioner's Office *(Conducting privacy impact assessment code of practice).*

Antecedentes de la evaluación de impacto

Encontramos el origen de estas evaluaciones en el ámbito anglosajón, de ahí que sean ampliamente conocidas como PIA *(privacy impact assesments)* y no es difícil encontrar metodologías para desarrollar de forma completa dicha evaluación. En concreto, la Agencia Española de Protección de Datos nos ofrece una guía de cómo realizar una EIPD.

Las evaluaciones de impacto de protección de datos no eran obligatorias en la Directiva 96/45/CE, ni tampoco existe una metodología única o exigida, pero son incorporadas en el marco del reglamento de protección de datos de la UE y actualmente son ampliamente recomendados para los entornos *big data.*

En otros países sí se anticipó obligatoriedad, como el caso de Reino Unido, donde desde julio de 2008 es obligatorio realizar estas evaluaciones en el entorno de la administración de Estado y sus agencias.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En este tema desarrollaremos el concepto de un PIA/EIPD para facilitar su entendimiento e incorporaremos una aproximación metodológica desde una perspectiva didáctica. Como comentábamos, a la hora de meternos en harina existen múltiples metodologías a las que recurrir, aunque no todas tienen el mismo alcance, por ejemplo:

- Guía de evaluación de impacto de la AEPD (Agencia Española de Protección de Datos).
- *Conducting privacy impact assessments code of practice,* ICO (Information Commissioner's Office).
- ISO 22307:2008. Financial services. Privacy impact assessment (última revision: 2012).
- ISO/IEC WD 29134:2017. Information Technology. Security Techniques. Guidelines for privacy impact assessment.

Uno de los primeros países en el que se dio forma a las EIPD ha sido el Reino Unido, que publicó la primera guía en 2007 *(PIA Handbook),* revisada posteriormente en 2009.

La metodología intenta facilitar la integración de la evaluación de impacto dentro de los proyectos y las herramientas de gestión de riesgos y define el PIA como una herramienta más de gestión de riesgos con un foco que va más allá de asegurar a las organizaciones el mero cumplimiento normativo en protección de datos personales.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Las metodologías PIA en muchas ocasiones han tomado como inspiración metodológica las metodologías de evaluación de riesgos más conocidas, como:

- Gestión de riesgos:
  - ISO 31000:2009. Risk management. Principles and guidelines.
  - Combined Code and Turnbull Guidance.
  - UK Treasury's The Orange Book: Management of Risk.
  - ENISA's approach to risk management.
- Seguridad de la información:
  - ISO/IEC 27005:2011. Information security risk management.
  - IT-Grundschutz.
  - NIST SP 800-39. Managing Information Security Risk.
  - ISACA and COBIT.
- Metodologías de análisis de riesgos:
  - CRAMM.
  - EBIOS.
  - OCTAVE.
  - NIST SP 800-30. Guide for Conducting Risk Assessments.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En qué situaciones se debe realizar una evaluación de impacto

El RGPD recoge la obligación de la realización de evaluaciones de impacto en los siguientes casos (art. 35, RGPD):

- **Evaluación sistemática y exhaustiva de aspectos personales** de personas físicas que se base en un tratamiento automatizado.
- **Elaboración de perfiles** sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente.
- **Tratamiento a gran escala de categorías especiales de datos** o datos penales.
- Observación sistemática a gran escala de una zona de acceso público (por ejemplo, videovigilancia).

El RGPD recoge la capacidad de la autoridad de control de concretar una lista con los tratamientos que serán objeto de PIA, además de los ya contemplados en el RGPD.

La evaluación de impacto, por tanto, será obligatoria en general cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados debido a su tecnología, naturaleza, alcance, contexto o fines.

Una evaluación de impacto no siempre es necesaria y dependerá tanto del volumen de datos tratados, finalidades, naturaleza de los datos y tecnologías utilizadas.

© Universidad Internacional de La Rioja (UNIR)

Como ejemplo, veamos dos posibles casos:

- Caso 1. Diferencias en el volumen de afectados:
  - Fichero de clientes de un autónomo que alcanza, por ejemplo, a unos pocos cientos de ciudadanos.
  - Fichero de clientes de una operadora de comunicaciones que alcanza millones.
- Caso 2. Naturaleza de los datos tratados:
  - Los datos tratados por un pequeño servicio de reparaciones.
  - Los datos tratados por un consultorio médico.

En ambos escenarios es fácil prever un mayor perjuicio sobre los ciudadanos en el caso de, por ejemplo, un evento de brecha de seguridad que facilite el acceso a los datos personales a personal no autorizado para las situaciones *b* de los casos propuestos que para las situaciones *a*.

El alcance del PIA/EIPD como la formalidad de este se entiende que es poco generalizable y requiere significativos esfuerzos. Por ello, la **AEPD ha emitido una lista.**

Accede a la lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4) desde el siguiente enlace: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

---

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En esta lista se recogen características de tratamientos que deben ser objeto de una EIPD. Para ello bastara con reunir **dos o más características** de entre las incluidas. A modo de resumen, las características son:

- Uso de datos a gran escala.
- Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.
- Perfilado o valoración de sujetos:
  - Toma de decisiones automatizadas.
  - Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva.
  - El uso de categorías especiales, datos relativos a condenas o infracciones penales o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
  - Uso de datos biométricos con el propósito de identificar de manera única a una persona física.
  - Datos genéticos.
  - Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social.
  - Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas.
  - Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

También la AEPD ha emitido un listado de tratamientos que no tienen que ser objeto de una evaluación de impacto, aunque en algún caso puedan reunir dos o más características de las comentadas en el documento anterior.

Accede a la lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD desde el siguiente enlace: https://www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf

---

En este listado, a modo de resumen, se incluyen:

1. Realizados bajo las directrices de las autoridades de control.
2. Realizados estrictamente bajo las directrices de códigos de conducta aprobados.
3. Necesarios para el cumplimiento de una obligación legal.
4. Realizados por autónomos que ejerzan de forma individual.
5. Realizados por pymes para la gestión interna con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, requeridos por ley.
6. Realizados por comunidades.
7. Realizados por colegios profesionales y asociaciones sin ánimo de lucro.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

A la hora de proceder a realizar el EIPD, es importante resaltar que es mejor cuando más temprano tenga lugar. Se recomienda su incorporación en la fase de definición del servicio o producto. Cuanto antes se realice antes se podrán:

- Evaluar los posibles riesgos y establecer medidas o controles compensatorios que mitiguen los mismos.
- Una mayor eficacia en la aplicación de los controles e incluso a un menor coste.
- La implantación de controles antes de que se genere un perjuicio sobre los derechos de los ciudadanos.

En qué consiste EIPD o PIA

La EIPD, tal y como es entendida por parte de la AEPD, es una evaluación de riesgos que se caracteriza por:

- Ser un **proceso más amplio que la simple comprobación del cumplimiento de la normativa** en protección de datos personales (la expectativa es que vaya más lejos que una evaluación y que, con base en los riesgos identificados, formule controles con independencia de que sean o no explícitamente requeridos por la norma, por ejemplo, medidas de seguridad).
- Se debe realizar **antes de implantar un nuevo producto, servicio, sistema de información** o cuando uno existente sufra significativos cambios. Totalmente alineado con los principios de privacidad por diseño.
- Es un **proceso sistemático y reproducible.** Debe sustentarse en una aproximación metodológica.
- Ha de orientarse en **revisar procesos.** La revisión de procesos mejora el entendimiento de los flujos de datos y de sus finalidades.
- Debe permitir una identificación clara de los responsables de cada una de las fases del EIPD.

© Universidad Internacional de La Rioja (UNIR)

- Debe tener una **aproximación abierta** que invite a participar constructivamente a todos los afectados: departamentos, grupos de interés, entidades externas, agentes sociales; el enriquecimiento de la evaluación desde la participación de todos los afectados se considera clave a la hora alcanzar unos buenos resultados.
- El resultado del EIPD debe formalizarse en un documento.
- Debe ser un **proceso transparente** cuyo resultado sea conocido por miembros y grupos de interés de la organización.
- Debe ser un **proceso periódico** que evalúe la eficacia de la aplicación de las medidas previamente definidas y aplicadas y proponga correcciones o la aplicación de medidas adicionales en pro del objetivo de la reducción del riesgo. La orientación como un proceso de mejora continua que permita responder adecuadamente a los riesgos identificados y mejorar la eficacia de las medidas. Una aproximación basada en un modelo PDCA *(plan-do-check-act).*

Fases del EIPD

La metodología para desarrollar la EIPD que define la guía desarrollada por la AEPD contempla las siguientes fases:

© Universidad Internacional de La Rioja (UNIR)

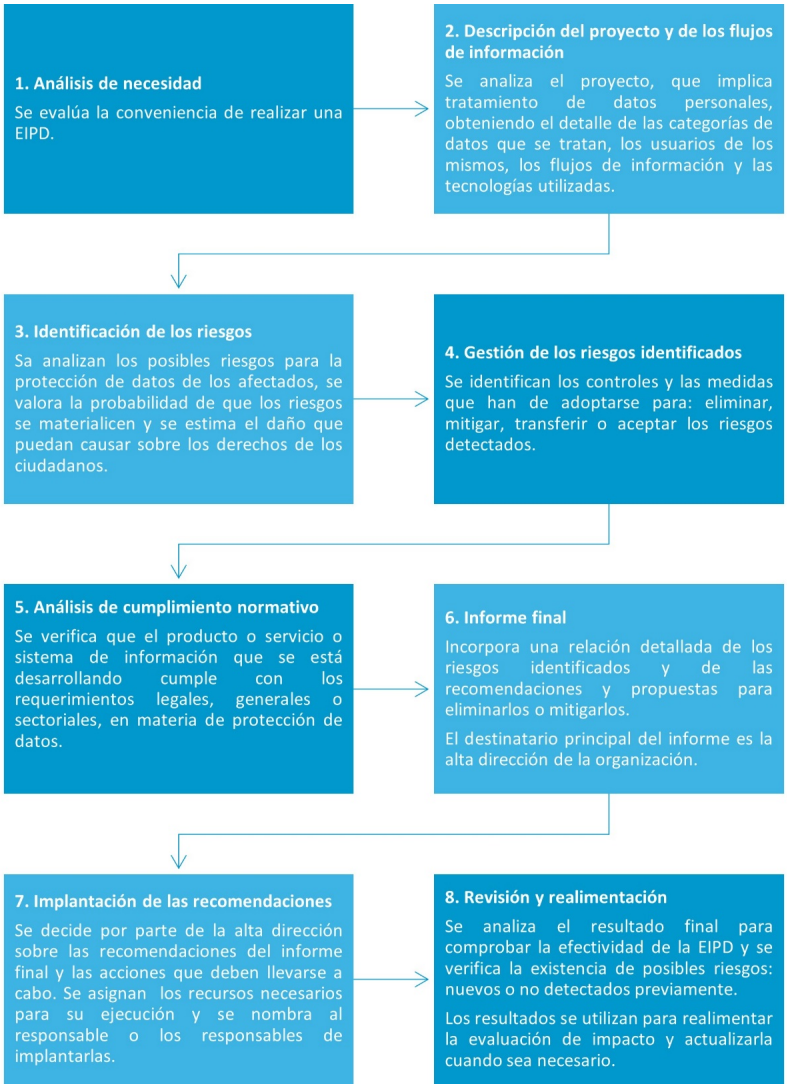


Figura 10. Metodología para desarrollar la EIPD. Fuente: elaboración propia.

Es una aproximación cíclica de mejoramiento que en sus correspondientes fases integra a las partes afectadas (internas o externas a la organización) para alcanzar una correcta identificación de los riesgos.

A continuación, profundizaremos en algunas de las fases identificadas (siguiendo la guía de evaluación de impacto de la Agencia Española de Protección de Datos).

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

El equipo de trabajo para desarrollar el EIPD

La guía no establece reglas sobre quién ha de participar en la evaluación, esto lógicamente variará de una organización a otra. Ahora bien, por la propia naturaleza del proceso parece lógico que en el equipo estén integrados:

- Delegado de protección de datos con conocimientos de obligaciones legales en el ámbito de la protección de datos.
- Representantes del departamento TIC.
- Responsables de seguridad.
- Representantes de las áreas de negocio o departamentos que patrocinen el proyecto o se vean afectados por el mismo.

El éxito del EIPD va a depender también de la implicación de la alta dirección, de su compromiso y apoyo para liderar y garantizar la disponibilidad de los recursos necesarios para su realización. Y también dependerá del alcance que se le pretenda dar de la capacidad de su concreción y de lo ambicioso del mismo. Cuanto más ambicioso sea, más riesgos tendrá de no responder a los objetivos definidos.

Análisis de necesidad

Ya hemos mencionado los ámbitos en los que la AEPD considera aplicable el EIPD. Por lo que en esta fase procederíamos a verificar si estamos en alguna de dichas circunstancias que nos indiquen la necesidad de realizar el EIPD.

Descripción del proyecto y los flujos de datos personales

Como mencionábamos, es conveniente realizar el EIPD al inicio del proyecto. Esto puede suponer que la descripción, como los flujos identificados, sea un tanto inmadura. El grado de definición en las fases iniciales siempre es más difuso, por lo que será conveniente, si se da el caso, proceder a una revisión posterior de estos aspectos.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

En esta fase de descripción debemos incorporar en **la documentación del EIPD:**

- Un **resumen del proyecto y características** incluyendo descripción de necesidad u oportunidad de este.
- Explicitar **los aspectos que resulten ser más relevantes,** que desde la perspectiva de la protección de datos personales tendrá el proyecto y que *a priori* sean susceptibles de presentar un mayor riesgo o que presentan una mayor dificultad a la hora de cumplir con la normativa.
- Además, es aconsejable incorporar una descripción detallada de:
  - Medios de tratamiento y tecnologías que se utilizan.
  - Categorías de datos personales que se tratan (datos de identificación…), las finalidades de su tratamiento, los colectivos afectados y justificación de la necesidad de la utilización de estos datos.
  - Criterios de acceso a cada categoría de datos personales, justificando convenientemente dicha necesidad. Es decir, quién accede.
  - Los flujos de información en el ciclo de vida de los datos:
  - Recogida de datos.
  - Circulación de los datos dentro de la organización.
  - Las comunicaciones de los datos.
  - Las posibles cesiones provenientes de terceros.
  - Las transferencias internacionales previstas.
  - Los encargos de tratamientos previstos.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

Identificación y evaluación de riesgos para la protección de datos

La utilización inadecuada o no lícita de datos personales es un riesgo inherente al tratamiento de datos personales, veamos algunos ejemplos:

- El uso de la información accesible. Por ejemplo, el uso de Internet, ubicaciones para fines comerciales (correo no deseado, publicidad dirigida…).
- La utilización de los hábitos o información de los empleados recogidos y utilizados por sus superiores para dirigir la búsqueda de evidencias que sustenten posibles despidos procedentes.
- Falseamiento de identidades para realizar actividades ilegales en nombre de los interesados, este último frente persecución penal.
- La toma de decisiones sobre información **alterada** de forma **no deseada** de los datos de salud de manera que los pacientes son inadecuadamente atendidos, con el empeoramiento de su condición e incluso generando efectos de discapacidad o la muerte.

El objetivo del PIA/EIPD es identificar los riesgos existentes y gestionar este riesgo: evitándolo o eliminándolo, mitigándolo, transferirlo o aceptarlo. Ello implica el establecimiento de medidas para actuar frente a los riesgos identificados, evaluar la eficacia de la implementación de dichas medidas e incorporar acciones correctoras o compensatorias, dentro de una visión cíclica de la gestión de riesgos.

© Universidad Internacional de La Rioja (UNIR)

Figura 11. Objetivo del PIA/EIPD. Fuente: elaboración propia.

Los riesgos sobre los que se orienta principalmente la evaluación son los riesgos que afectan a los derechos de los ciudadanos, y esto implica evaluar aspectos técnicos, organizativos y jurídicos. Pero, al mismo tiempo del modo en que a las organizaciones realizan los tratamientos de datos personales y de cómo estas respetan los derechos de los afectados, se derivan potenciales riesgos para las propias organizaciones que trascienden eventuales sanciones que convienen tener también en consideración en la evaluación, aunque habitualmente las metodologías no los contemplen:

- **Pérdida de ventas:** una respuesta negativa por parte de los consumidores hacia un producto o servicio si se identifica una falla referente a la protección de datos. La pérdida de confianza por el consumidor origina una baja de ventas o la retirada del producto o servicio.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **Incremento de costes:** la incorporación de costes adicionales para subsanar las deficiencias que sin los principios de la protección de datos hubieran sido incorporados en las fases de diseño y desarrollo. Incremento de los costes de puesta en el mercado de los productos o servicios o incluso de obligaciones indemnizatorias afectan a la viabilidad del proyecto.

- **Imagen corporativa:** impacto sobre la imagen de la organización y sobre la confianza de accionistas o terceras partes interesadas.

© Universidad Internacional de La Rioja (UNIR)

Por tanto, en el EIPD se **consideran dos tipos de riesgos:**

- Los que afectan a las personas:
  - La posible violación de los derechos de los ciudadanos directamente afectados por el tratamiento, por ejemplo:
  - La disponibilidad del consentimiento para el tratamiento de los datos personales.
  - El deber de secreto.
  - Bloqueo y cancelación de los datos efectiva tras el requerimiento por parte del afectado.
  - Procesos de rectificación de datos no eficaces. No comunicación a cesionarios.
  - La pérdida de información, por ejemplo:
  - Desastre que afecta a los entornos de tratamiento de datos.
  - Falta de eficacia en las copias de seguridad.
  - Procesos que atentan contra la integridad de la información.
  - La pérdida de información, por ejemplo:
  - Decisiones que afectan a los ciudadanos.
  - Revelación de información.

© Universidad Internacional de La Rioja (UNIR)

- Los que afectan a las organizaciones, entre otros:
  - La negativa percepción del producto o servicio puede originar una disminución en su uso.
  - Costes por el rediseño.
  - La posible retirada del mismo.
  - Reputación e imagen.
  - Sanciones.

Para el análisis de riesgos podemos recurrir a diferentes metodologías que nos pueden ayudar en este punto. Algunas en las que encontraremos especial acomodo para la realización del EIPD son:

- *Methodology for privacy risk management* de la Commission Nationale de l'Informatique et des Libertés (CNIL). Muy recomendable.
- MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), herramienta creada por el Consejo Superior de Administración Electrónica.
- Risk IT de ISACA.
- ISO/IEC 27005. Gestión de riesgos de la seguridad la información.
- ISO 31000:2009. Gestión de riesgos, principios y directrices que da nombre a una familia de normas sobre principios y directrices de gestión del riesgo.
- ISO/IEC 31010, Gestión de riesgos, técnicas de evaluación del riesgo, en la que se detallan diversos métodos que pueden ayudar a identificar y detectar los riesgos de un nuevo producto o servicio.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

De la misma manera que existen diferentes metodologías, también nos encontramos con diferentes formas de definir el riesgo, una de ellas es definir el concepto de riesgo con base en los componentes que los configuran:

- Amenazas a las que se está sometido (¿qué puede pasar?).
- Las vulnerabilidades existentes (¿qué facilita que si algo pasa afecte o genere un mayor perjuicio?).
- La probabilidad de que un evento tenga lugar, es decir, que una amenaza se materialice y explote una vulnerabilidad (¿con qué frecuencia se puede dar?).
- El impacto que dicho evento tendrá sobre los afectados en el caso de materializarse: que la amenaza aproveche una vulnerabilidad y que se puede establecer con base en la sensibilidad de la información divulgada (salud, orientación sexual, orientación política, etc.) y número de personas afectadas.

De manera que se define así:

El **riesgo** es la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad.

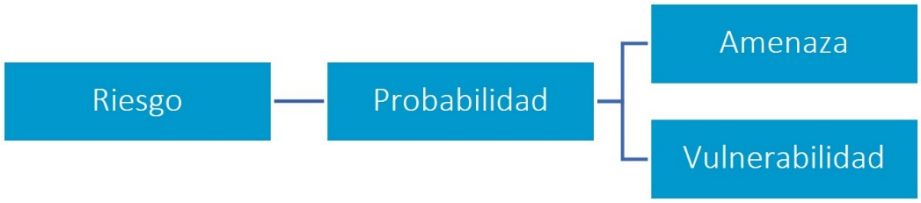


Figura 12. Concepto de riesgo. Fuente: elaboración propia.

La cuantificación del riesgo, en términos de cálculo (económico o cualitativo de daños), se puede obtener a partir del potencial impacto y con base en la probabilidad de que una amenaza explote una vulnerabilidad.

Riesgo = Probabilidad x Impacto.

© Universidad Internacional de La Rioja (UNIR)

Vemos un par de ejemplos para entenderlo:

- Ejemplo A:

  - **Amenaza:** en un centro sanitario conocido por la prestación asistencial a personas de gran proyección pública, podemos identificar como posible amenaza a la privacidad de los enfermos, la curiosidad de los profesionales del centro o de terceros interesados con motivaciones económicas.

  - **Vulnerabilidad:** el centro dispone de un sistema de información clínica, es decir, la historia clínica está informatizada. Por tanto, el acceso a la historia clínica de un paciente le facilita toda la información sobre su estado de salud. Este sistema está en una fase de mejoramiento, el sistema de control de acceso lógico al sistema informático dispone de un usuario/clave (ADMIN/ADMIN) que aún no ha sido eliminado y que permite el acceso global a toda la información.

  - **Impacto:** se ha filtrado información sobre el estado de salud de la persona pública citada junto con un listado de cientos de pacientes, esto ha perjudicado tanto a los afectados como a la entidad que ha sido sancionada y ha perdido reputación.

En este mero ejemplo podemos considerar que la amenaza está ampliamente motivada (la motivación es un factor relevante a la hora de evaluar la amenaza que puede suponer la acción de un atacante o del adversario) y la vulnerabilidad existente es muy fácil de explotar, lo que nos llevaría a estimar la probabilidad de que dicho evento, amenaza-vulnerabilidad, tuviera lugar como alta-muy alta.

© Universidad Internacional de La Rioja (UNIR)

- Ejemplo B:

  - **Amenaza:** una trama de estafadores quiere verificar el número de cuenta de un anciano para proceder al giro fraudulento de recibos con cargo a la cuenta del anciano.

  - **Vulnerabilidad:** en la oficina bancaria, por baja del personal, se ha incorporado un nuevo profesional temporal el cual no ha recibido formación sobre confidencialidad ni protección de datos. Los estafadores suplantan la personalidad de un hijo y obtienen la cuenta del anciano y el saldo de la cuenta girando un recibo por falsos servicios prestados, que el anciano no devuelve.

  - **Impacto:** la revelación le ocasiona un quebranto económico al anciano, sin que exista repercusión mediata ni denuncia ante las instancias jurisdiccionales correspondientes.

Como decíamos, existen diferentes metodologías de evaluación de riesgos y para proceder a la misma de una forma sencilla y cualitativa podemos evaluar los diferentes riesgos atendiendo a una clasificación sencilla:

- Probabilidad de que suceda:

  - Muy alta (81 %-100 %): es casi seguro que suceda.

  - Alta (61 %-80 %): es muy probable.

  - Media (41 %-60 %): es probable.

  - Baja (21 %-40 %): es poco probable.

  - Muy baja (0 %-20 %): es muy poco probable.

© Universidad Internacional de La Rioja (UNIR)

- Impacto que tiene en caso de que suceda:
  - Muy alto (81 %-100 %): información sensible con un volumen alto de afectados.
  - Alto (61 %-80 %): información sensible con un volumen alto de afectados.
  - Medio (41 %-60 %): muchos afectados, informaciones no sensibles.
  - Bajo (21 %-40 %): muy pocos afectados, pero información sensible.
  - Muy bajo (0 %-20 %): pocos o muy pocos afectados, información no sensible.

Si estimamos un mapa de calor del impacto atendiendo a la sensibilidad de los datos y alcance en el número de afectados, tendremos:

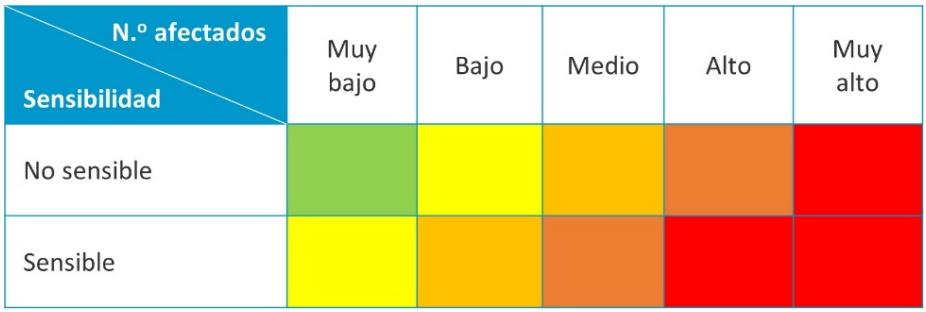


Figura 13. Mapa de calor sensibilidad/afectados. Fuente: elaboración propia.

© Universidad Internacional de La Rioja (UNIR)

De esta manera, si evaluamos el riesgo considerando la ecuación anterior (Riesgo = Probabilidad x Impacto), podemos establecer un mapa de riesgo cualitativo:

Impacto / Probabilidad	Muy bajo	Bajo	Medio	Alto	Muy alto
Muy baja					
Baja					
Media					
Alta					
Muy alta					

Figura 14. Mapa de calor probabilidad/impacto. Fuente: elaboración propia.

De este modo, eventos con muy alta probabilidad de ocurrencia pero que tienen un muy bajo efecto sobre los derechos a la protección de datos personales o la organización tendrán la misma consideración (valor) de aquellos eventos que, aun teniendo una baja probabilidad de ocurrencia, su impacto puede ser muy severo.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

De la propia definición de riesgo se entiende que es preciso extender el análisis a todo el mapa de amenazas por vulnerabilidades y, con base en su probabilidad, cualificar el riesgo derivado. Este valor de riesgo obtenido nos guía a la hora de identificar qué vulnerabilidades debemos corregir, empezando por:

- Corregir aquellas vulnerabilidades que implican un mayor riesgo, eliminando la vulnerabilidad o incorporando controles que reduzcan la probabilidad de que sea explotada por una amenaza. Veamos unos ejemplos:

- En el acceso lógico a la base de datos, exige la incorporación de un identificador y una clave. Incorporar procedimientos de distribución de usuarios/claves adecuados y robustez en las contraseñas no elimina el riesgo, pero lo reduce al disminuir la probabilidad de que un **agente motivado** acceda fácilmente mediante, por ejemplo, un ataque de diccionario.

- El establecimiento de procedimientos adecuados y la formación del personal de atención al cliente para identificar y actuar ante un intento de suplantación de identidad que pretenda acceder a información de un ciudadano. Tampoco elimina el riesgo, pero lo reduce al hacerlo también su probabilidad.

- Aplicar los controles más inmediatos en coste y esfuerzo que reducen el perfil de riesgo de manera más significativa. Por ejemplo: eliminar un dato sensible del tratamiento de datos por realizar, que por el mayor impacto en la protección de datos incorpora un riesgo mayor (por mayor impacto en los afectados).

El objetivo del análisis de riesgos es evaluar los riesgos existentes y orientar la adopción de controles para la disminución de este. Como los componentes del riesgo son dinámicos, las evaluaciones deben ser periódicas, dentro de un proceso de gestión del riesgo que permita evaluar la eficacia de las medidas aplicadas, su efecto sobre el perfil de riesgo y su mejora.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

La guía de EIPD de la AEPD ya incorpora una serie de riesgos que debemos evaluar en un producto o servicio que realice un tratamiento de datos personales, y en su Anexo II incluye un posible modelo para ayudar a sistematizar y gestionar las fases de identificación y gestión de riesgos. En la guía de EIPD los riesgos que se proponen que sean evaluados son, por ejemplo:

- **Riesgos de carácter general:**
  - Pérdidas económicas y daños reputacionales derivados de:
  - Incumplimiento de la legislación sobre protección de datos personales.
  - Incumplimiento de legislaciones sectoriales aplicables con incidencia en la protección de datos personales.
  - Falta de medidas de seguridad adecuadas que generen pérdida de datos.
  - Pérdida de competitividad del producto o servicio, por impacto en la reputación.
  - No disponer de conocimiento experto en protección de datos desde la fase de definición del servicio o producto.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **Legitimación de los tratamientos y cesiones de datos personales:**
  - Incurrir en tratamiento o cesiones de datos no adecuados para las finalidades del tratamiento.
  - No disponer de legitimidad.
  - Trabajar sobre consentimientos de dudosa legalidad.
  - No atender a las revocaciones de consentimiento.
  - Incorporar datos de categorías especialmente protegidas sin velar adecuadamente por la legitimidad de dicho tratamiento.
  - Incurrir en el enriquecimiento de los datos personales no previstos en las finalidades, no informando adecuadamente a los afectados.
  - Incorporar prácticas de reidentificación de personas incorporando fuentes adicionales de información.
  - Utilización de *cookies* de seguimiento de manera no legítima.
  - Impedir la utilización del producto o servicio de manera anónima cuando la identificación no es indispensable para el producto o servicio.
- **Transferencias internacionales:**
  - Acceso secreto de las autoridades de terceros países.
  - No asistir a los ciudadanos en el ejercicio de sus derechos ante los importadores de datos.
- **Notificación administrativa de los tratamientos:**
  - No disponer de procedimientos internos para mantener actualizadas las notificaciones a la AEPD.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **Transparencia de los tratamientos ante los afectados:**
  - No informar adecuadamente de los datos recabados (*cookies,* ubicación geográfica en dispositivos móviles, comportamiento en Internet y hábitos de navegación, etc.).
  - Dificultar el acceso a la política de protección de datos o la redacción de estas de forma confusa que no permite conocer a los afectados la finalidad y uso de sus datos personales.
- **Calidad de los datos. Cumplimiento de los principios**
  - Incorporar categorías de datos no necesarias.
  - Errores que facilitan la pérdida de integridad de la información.
  - Conculcar garantías en el uso de datos personales con fines históricos, científicos o estadísticos.
  - Utilizar los datos para otros fines, no informados y para los que no se tiene consentimiento. Por ejemplo, la toma de decisiones que puede ser adversa o discriminatoria, como la oferta de precios diferentes.
  - Riesgo de realizar inferencias erróneas usando, por ejemplo, técnicas de minería de datos, reconocimiento facial y datos biométricos.
  - No disponer de procedimientos internos que garanticen la cancelación de datos de oficio una vez que estos ya no son necesarios para la finalidad para la que se recabaron.

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

- **Datos especialmente protegidos, con especiales requerimientos:**
  - Fallas en el consentimiento.
  - Disociaciones deficientes en procesos de investigación que solo requieren información anonimizada y que facilitan la reidentificación de los individuos.
- **Deber de secreto al que están obligados los participantes en el tratamiento:**
  - Acceso no autorizado.
  - Violaciones de la confidencialidad por parte de los empleados.
- **Tratamiento por encargo a terceras partes:**
  - No existencia de contrato o no conformidad con la ley.
  - La ausencia de protocolos para garantizar la debida diligencia en la elección del encargado de tratamiento.
  - Ausencia de control sobre subcontrataciones.
  - No considerar la cadena de encargos dentro de los procesos de ejercicio de derechos de los afectados.
  - Ausencia de disposiciones concretas sobre los datos personales una vez finalizada la prestación del encargo de tratamiento: destrucción de los datos, devolución de estos y su portabilidad a otros sistemas.
- **Derechos de los usuarios:**
  - Ausencia de procedimientos para la respuesta eficaz al ejercicio de derechos.
  - Obstrucción del ejercicio para su dilación o limitación del derecho.

© Universidad Internacional de La Rioja (UNIR)

- **Seguridad de la información:**
  - Deficiencias en la definición de funciones y obligaciones en el tratamiento de datos personales.
  - Inexistencia de política de seguridad.

Consulta a las partes afectadas

Estas fases siempre son las más delicadas en toda metodología por las posibles controversias que se pueden generar tras realizar la consulta, mayor si el tratamiento afecta a amplios sectores de la población, y no siempre es factible su realización. Pero en el caso de que sea posible realizarlo, nos permite:

- Obtener la opinión de grupos o personas que no están viciados por el proyecto (habrá que tener en consideración el interés de las partes).
- Dotar al proyecto de transparencia y conocer las incertidumbres o preocupaciones que puede generar entre los afectados con objeto de responder a las mismas de forma adecuada.

La consulta a agentes externos normalmente se realizará a asociaciones de usuarios, consumidores, ONG dedicadas a la defensa de la privacidad, organizaciones sectoriales, sindicales…, es decir, a agentes con cierto carácter de representación sobre los colectivos afectados o directamente sobre grupos de consumidores o posibles usuarios. Por ejemplo, si afecta a los trabajadores de una corporación, en esta fase se debería entablar la consulta con, entre otros, el comité de empresa.

También esta fase contempla la realización de consultas internas incorporando, según el tamaño de la organización, a la dirección, los departamentos implicados e incluso a proveedores que vayan a participar en el tratamiento de datos personales.

© Universidad Internacional de La Rioja (UNIR)

Se recomienda que esta fase se aborde cuanto antes, siempre y cuando se disponga de suficiente grado de definición sobre el tratamiento de datos por realizar, su finalidad y el proyecto de definición del producto o servicio, para que su exposición a los grupos de interés sea efectiva.

En general, **los principios que debe cubrir esta fase** son:

- **Planificar adecuadamente:** realizarla en el momento más adecuado y con tiempo suficiente para poder disponer de las respuestas dentro del proceso de evaluación que se está realizando. Es una fase que se suele demorar, esto hay que tenerlo muy en cuenta.

- **Concreción y claridad:** concreción en el alcance y claridad de las cuestiones planteadas son claves en el resultado adecuado de esta fase. Es importante obtener la mejor respuesta y para ello hay que prestar especial atención a que las cuestiones sean claras y concretas.

- **Extensión y diversidad:** la extensión de los consultados y su diversidad dotará en un mayor enriquecimiento en las opiniones obtenidas.

- **Transparencia:** es conveniente facilitar información sobre los resultados a las partes intervinientes. También suele ser un tema delicado al que habrá que prestar atención, a la mejor forma de abordar este aspecto.

El informe de la evaluación de impacto

El informe final deberá hacerse público de forma parcial o en su totalidad (dependerá de las posibles restricciones que sean aplicables: legales, comerciales o de seguridad) y para ello se podrá hacer uso del sitio web de la organización. Cabe recordar que uno de los aspectos que motivan la EIPD es la transparencia.

No existe un modelo único de informe, pero la guía establece los aspectos que dicho informe debe integrar:

© Universidad Internacional de La Rioja (UNIR)

Ideas clave

1. Identificación del proyecto, la persona o personas responsables de la EIPD, sus datos de contacto, la fecha de realización del informe y número de versión del mismo.
2. Resumen del informe con los resultados esenciales.
3. Introducción y descripción general del proceso de evaluación.
4. Resultado del análisis de necesidad de la evaluación y su justificación.
5. Descripción general del proyecto.
6. Descripción detallada de los flujos de datos personales.
7. Riesgos identificados.
8. Identificación de partes interesadas o a las que afecta el proyecto, tanto internas como externas a la organización y resultados de las consultas llevadas a cabo.

Figura 15. Guía informe evaluación impacto. Fuente: elaboración propia.

© Universidad Internacional de La Rioja (UNIR)

9.6. Referencias bibliográficas

Article 29 Working Party. (2013). Opinion 03/2013 on purpose limitation [Archivo PDF]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de las Comunidades Europeas L 281, 23 de noviembre de 1995, pp. 31-50.

Google. (s.f.). Términos del servicio de Google [Página web]. https://policies.google.com/terms?hl=es

ISACA. (2013). *Big data: impactos y beneficios.* ISACA.

MediaBuzz. (agosto de 2013). The 7 foundational principles of privacy by design [Página web]. https://www.mediabuzz.com.sg/best-practices-aug-13/the-7-foundational-principles-of-privacy-by-design

Norwegian Data Protection Authority. (13 de octubre de 2014). *Resolution Big Data.* 36th International Conference of Data Protection and Privacy Commissioners, Mauricio. http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf

Protiviti Chile [@ProtivitiChile]. (8 de febrero de 2018). En un mundo cada vez más digital, los auditores internos deben ser observadores entusiastas de todos los cambios tecnológicos que [Imagen adjunta] [Tuit]. Twitter.

© Universidad Internacional de La Rioja (UNIR)

https://twitter.com/ProtivitiChile/status/961606275443326977

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1-88.
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Zhenhua's Wiki. (s.f.). Big Data [Página web].
https://techlarry.github.io/Data%20Science/Big%20Data/

© Universidad Internacional de La Rioja (UNIR)

Opinion 03/2013 on purpose limitation

Article 29 Working Party. (2013). Opinion 03/2013 on purpose limitation [Archivo PDF].
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Documento del grupo de trabajo del artículo 29 (WP29) que analiza el principio de limitación de la finalidad en el tratamiento de datos personales y realiza aclaraciones sobre la consideración de finalidades compatibles.

© Universidad Internacional de La Rioja (UNIR)

Privacidad por defecto: los siete principios fundamentales

Cavoukian, A. (2011). *Privacy by design: the 7 foundational principles.* Information and Privacy Commissioner of Ontario [Archivo PDF].
https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Documento que describe los principios de la privacidad.

© Universidad Internacional de La Rioja (UNIR)

Guía de evaluación de impacto de la Agencia Española de Protección de Datos

AEPD. (s.f.). Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD [Archivo PDF].
https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Desarrollada por la AEPD, guía en el proceso de la evaluación de impacto.

© Universidad Internacional de La Rioja (UNIR)

Guía de evaluación de impacto de la autoridad en protección de datos de Reino Unido

ICO. (s.f.) Conducting privacy impact assessment code of practice [Archivo PDF]. https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

Incorpora *templates* útiles en el proceso de evaluación.

© Universidad Internacional de La Rioja (UNIR)

Test

1. Identifica cuáles de los siguientes son principios de la privacidad por diseño:

A. Privacidad por defecto.

B. Privacidad incrustada en el diseño.

C. Seguridad extremo a extremo.

D. Todos los anteriores son correctos.

2. ¿Qué países forman el Comité de Protección de Datos RGPD, antiguo Grupo de trabajo del artículo 29 (WP29)?

A. Los miembros de la UE.

B. Los miembros de la OCDE.

C. Los países miembros del G8.

D. Alemania, Francia, Italia, España y Reino Unido.

3. Identifica cuáles de los siguientes aspectos se corresponden con las amenazas del *big data* definidas por el WP29:

A. Magnitud de la recopilación.

B. Seguridad de los datos.

C. Aumento dramático de las posibilidades de vigilancia del gobierno.

D. Todas las anteriores son correctas.

4. ¿Qué afirmación de las siguientes respecto a las evaluaciones de impacto es falsa?

A. La ley vigente obliga a la realización de evaluaciones de impacto cada seis meses de manera obligatoria.

B. La evaluación de impacto es un proceso sistemático y reproducible.

C. El resultado de la evaluación se debe plasmar en un documento.

D. La evaluación de impacto debe ser un proceso periódico.

© Universidad Internacional de La Rioja (UNIR)

5. ¿En qué casos de los siguientes no se recomienda la realización de una evaluación de impacto?

A. Cuando el tratamiento afecta a un número elevado de personas.

B. Cuando se traten grandes volúmenes de datos personales.

C. Cuando existan transferencias internacionales.

D. Cuando el tratamiento sea esporádico, limitado y afecte a personas de interés público.

6. ¿Cuáles de los siguientes tratamientos no requieren la realización de una evaluación de impacto?

A. Los realizados bajo las directrices de las autoridades de control.

B. Los necesarios para el cumplimiento de una obligación legal.

C. Los realizados por autónomos que ejerzan de forma individual.

E. Ninguno de los anteriores requiere la realización de una evaluación de impacto.

7. De entre los siguientes, ¿cuál no es un principio de la privacidad por diseño?

A. Privacidad por defecto.

B. Privacidad por diseño (incrustada en el diseño).

C. Seguridad de extremo a extremo.

D. Privacidad global.

8. En *big data,* ¿qué principio de entre los siguientes se ve principalmente afectado por el *overcollecting*?

A. Principio de minimización de datos.

B. Principio de limitación de la finalidad.

C. Exactitud de los datos.

D. Confidencialidad e integridad.

© Universidad Internacional de La Rioja (UNIR)

9. El interés legítimo puede dar base legal al tratamiento de datos personales. De entre las siguientes, indica qué afirmación al respecto es incorrecta:

A. Si un tratamiento se basa en el interés legítimo, no requiere el consentimiento del afectado.

B. El interés legítimo se aplica bajo la responsabilidad del responsable de tratamiento, que en su caso deberá demostrar que dicho interés no es anulado por los intereses o derechos y libertades fundamentales del interesado.

C. El interés legítimo permite justificar cualquier tratamiento de datos de carácter personal.

D. El derecho de información se debe garantizar, aunque la base legal del tratamiento sea el interés legítimo.

10. Una universidad va a realizar un tratamiento de datos biométricos a gran escala que afectará a todos los miembros de la comunidad educativa. Es este contexto, ¿cuál de las siguientes afirmaciones no es correcta?

A. Es necesario realizar una EIPD, al ser datos biométricos destinados a la identificación unívoca de las personas a gran escala.

B. Los datos biométricos no son datos de carácter personal.

C. Los datos biométricos pertenecen a categorías especiales de datos.

D. No es necesario realizar una EIPD porque es una pyme.

© Universidad Internacional de La Rioja (UNIR)