

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



GUÍA PRÁCTICA PARA LAS EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE LOS DATOS SUJETAS AL RGPD



Índice

1. Introducción	2
2. Aspectos previos.....	4
2.1 ¿Qué es una Evaluación de Impacto en Protección de Datos?	4
2.2 ¿Qué debe incluir una EIPD?	5
2.3 ¿Quién debe realizar una EIPD y a quién se debe involucrar?	7
3. Metodología para la realización de una EIPD	10
3.1 Ejemplo metodología	11
3.2 Contexto del tratamiento	12
3.3 Gestión de riesgos: Identificar, evaluar y tratar	21
3.4 Conclusión	33
3.5 Comunicación y consulta a la autoridad de control	35
3.6 Supervisión y revisión de la implantación	36
4. Cuestiones clave.....	37
4.1 Si una operación de tratamiento presenta una EIPD con un riesgo elevado, ¿puedo proceder a llevar a cabo la actividad de tratamiento?.....	37
4.2 ¿Cómo realizar una EIPD cuando se presta un servicio como encargado de tratamiento?.....	37
4.3 ¿Cuándo se debe revisar una EIPD?	38
4.4 ¿Qué ocurre cuando se está adherido a un código de conducta?	38
5. Anexos	39
5.1 Anexo I: Plantilla de análisis de documentación del ciclo de vida de los datos asociados a las actividades de tratamiento	39
5.2 Anexo II: Plantilla de análisis de la necesidad y proporcionalidad del tratamiento	40
5.3 Anexo III: Plantilla de gestión de riesgos	41
5.4 Anexo IV: Plantilla de plan de acción y conclusión.....	43
5.5 Anexo V: Catálogo de amenazas.....	44
5.6 Anexo VI: Catálogo de amenazas y posibles soluciones	49
6. Referencias.....	64

1. Introducción

El próximo **25 de mayo de 2018** será directamente aplicable el **Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016**, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, **RGPD**. Por tanto, a partir del 25 de mayo de 2018 será **obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable del tratamiento** que este incluye, entre las que destaca, la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de los datos personales siempre y cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

La aplicación del RGPD no debe entenderse como la necesaria obligación de realizar la **evaluación de impacto** de todos los tratamientos que hasta la fecha se vinieran realizando sino que será necesario atender a las especificidades concretas de cada tratamiento.

La reforma de la regulación de protección de datos supone un **cambio del modelo tradicional** para afrontar las medidas que garantizan la protección de los datos hacia un modelo más dinámico, adaptado a la profunda transformación tecnológica que se está produciendo en el ámbito del tratamiento de la información personal y enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento. Adicionalmente, el RGPD refuerza el principio de responsabilidad proactiva (“*accountability*”) de quienes tratan datos personales, lo que requiere que estos analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de tratamientos llevan a cabo con el objetivo de determinar qué medidas son adecuadas para cumplir con lo dispuesto en el RGPD.

La **Evaluación de Impacto en la Protección de Datos Personales** (en adelante, la **EIPD**) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo “antes del tratamiento” en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

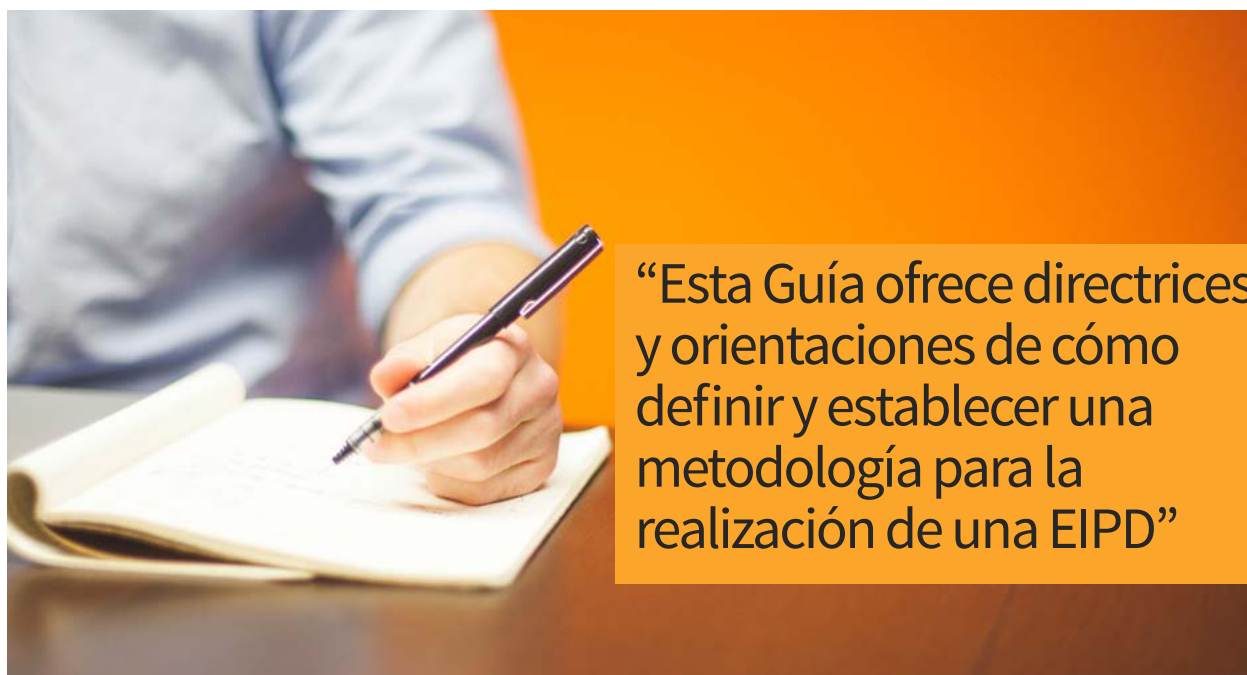
Sin embargo, sí debiera realizarse una Evaluación cuando en una operación iniciada con anterioridad a la aplicación del Reglamento se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se puso en marcha.

Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo más datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento.

La Evaluación de Impacto es un proceso que no se agota cuando se ha finalizado. Los responsables, y así lo señala el propio RGPD, deberían revisar si los tratamientos siguen siendo conformes con la Evaluación a la que hubieran sido sometidos y, en todo caso, hacerlo cuando exista un cambio del riesgo del tratamiento.

La AEPD ha elaborado la presente **Guía para la Evaluación de Impacto en la Protección de los Datos Personales** con el objetivo de **promover una cultura proactiva de la privacidad**, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas.

Esta Guía ofrece directrices y orientaciones de cómo definir y establecer una metodología para la realización de una EIPD, sin embargo, no pretende ser la única manera en que puede llevarse a efecto una EIPD. Las organizaciones que tengan ya implantados procesos y herramientas de análisis de riesgos pueden utilizarlas para evaluar los relativos a la privacidad y la protección de datos siempre que cubran los aspectos esenciales que toda Evaluación de Impacto en la Protección de Datos debe tener, respetando los requerimientos del RGPD.



“Esta Guía ofrece directrices y orientaciones de cómo definir y establecer una metodología para la realización de una EIPD”

2. Aspectos previos

2.1 ¿Qué es una Evaluación de Impacto en Protección de Datos?

El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen **medidas de control**¹ adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los “riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas” (artículo 24.1) y aplicando las medidas oportunas. Para ello, el responsable del tratamiento debe considerar desde el inicio, en la fase de diseño, las acciones preventivas suficientes para poder **identificar, evaluar y tratar los riesgos** asociados al tratamiento de datos personales, y así, poder asegurar los principios de protección de los datos garantizando los derechos y libertades de los interesados.

El GT29 define en su guía (WP248 ‘Guías sobre las Evaluaciones de Impacto en Protección de Datos (EIPD)’ un riesgo como “*un escenario que describe un evento y sus consecuencias, estimado en términos de impacto y probabilidad*”. Por tanto, la gestión de riesgos es el conjunto de aquellas actividades y tareas realizadas en una organización para monitorizar y controlar su exposición ante los riesgos.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.



Artículo 35 **del RGPD**

Establece que ante la probabilidad de que un tratamiento “*entrañe un alto riesgo para los derechos y libertades de las personas físicas*” será necesario llevar a cabo una EIPD antes de la puesta en marcha del tratamiento. Esta obligación está alineada con el principio de privacidad que tiene como objetivo analizar un tratamiento desde su fase de diseño y garantizar una adecuada gestión de los riesgos, además de cumplir con los principios de necesidad y proporcionalidad.

El resultado de la EIPD se debe tener en cuenta, necesariamente, a la hora de tomar las decisiones relacionadas con el cumplimiento de lo previsto en el RGPD y la toma de decisión de la viabilidad o no de llevar a cabo el tratamiento de los datos.

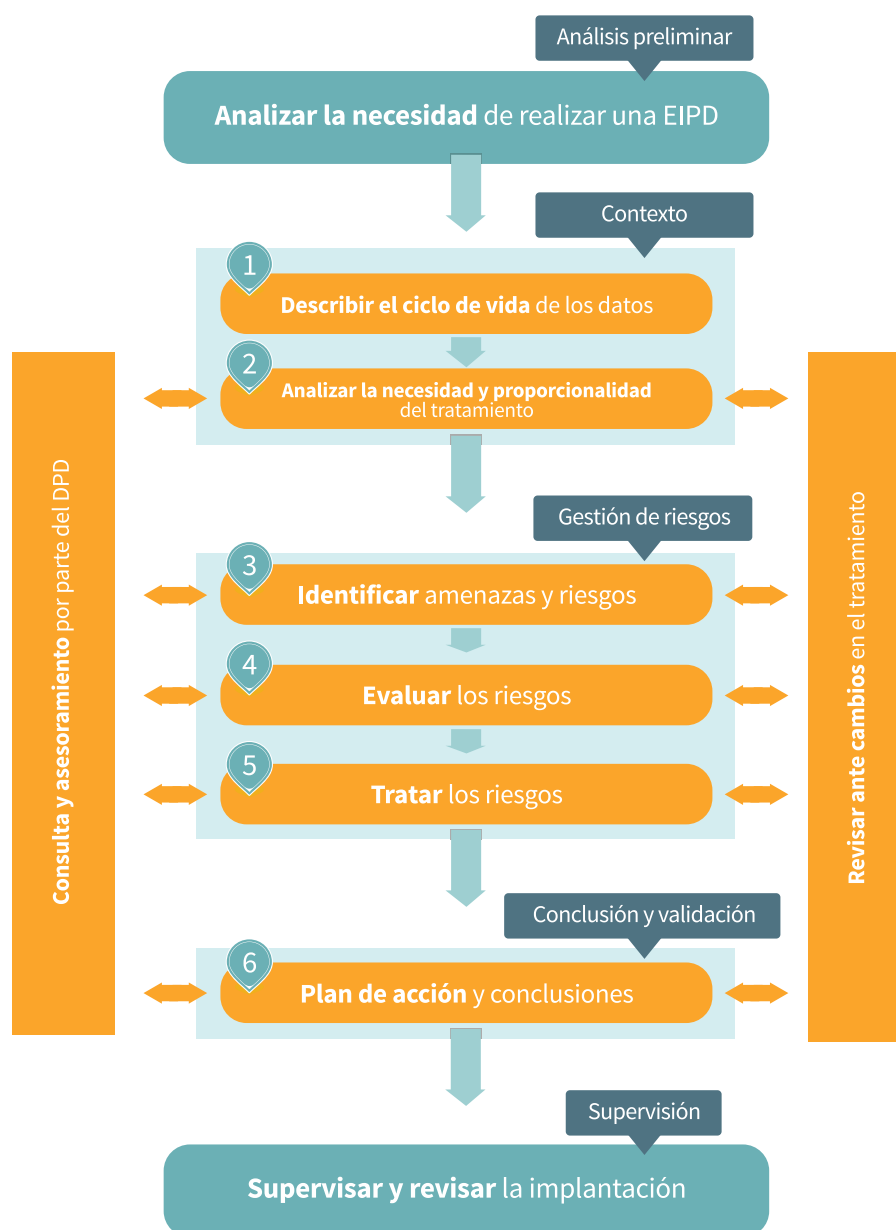
¹ En el contexto de este documento se entiende por controles o medidas de control los medios técnicos y procedimentales implantados para mitigar los riesgos que las actividades de tratamiento puedan suponer a los derechos y libertades de los interesados.

2.2 ¿Qué debe incluir una EIPD?

A la hora de realizar una EIPD, se debe disponer de una metodología que considere los requerimientos exigidos por el RGPD en su artículo 35.7, donde se establece que la EIPD deberá incluir como mínimo:

- Una **descripción sistemática** de la actividad de tratamiento previstas
- Una **evaluación de la necesidad** y proporcionalidad del tratamiento respecto a su finalidad
- Una **evaluación de los riesgos**
- Las **medidas previstas para afrontar los riesgos**, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Estructura con las diferentes etapas de una EIPD y el flujo a seguir en la ejecución de una EIPD:



■ **Contexto:**

1 Describir el ciclo de vida de los datos: Descripción detallada del ciclo de vida y del flujo de datos en el tratamiento. Identificación de los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.

2 Analizar la necesidad y proporcionalidad del tratamiento: Análisis de la base de legitimación, la finalidad y la necesidad y proporcionalidad del tratamiento que se pretenden llevar a cabo.

■ **Gestión de riesgos:**

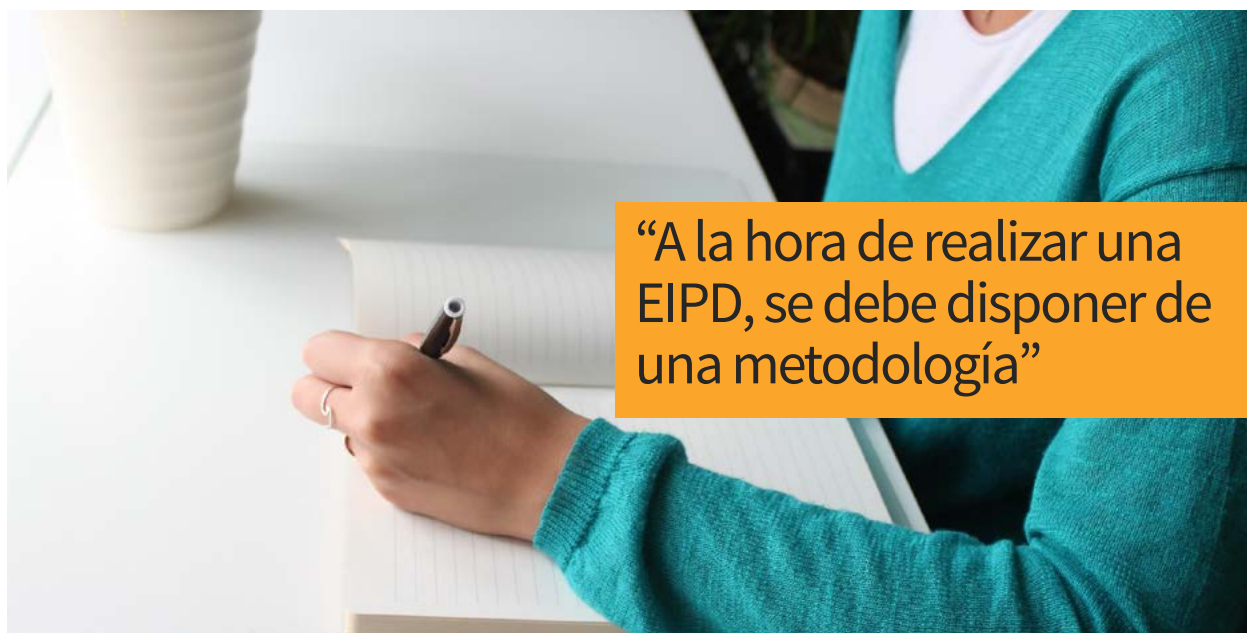
3 Identificar amenazas y riesgos: Identificación de las amenazas y riesgos potenciales a los que están expuestos las actividades de tratamiento.

4 Evaluar los riesgos: Evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización.

5 Tratar los riesgos: Respuesta ante los riesgos identificados con el objetivo de minimizar la probabilidad y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable que permita garantizar los derechos y libertades de las personas físicas.

■ **Conclusión y validación:**

6 Plan de acción y conclusiones: Informe de conclusiones de la EIPD donde se documente el resultado obtenido junto con el plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas y, si procede, el resultado de la consulta previa a la autoridad de control a la que se refiere el **artículo 36 del RGPD**.



“A la hora de realizar una EIPD, se debe disponer de una metodología”

Adicionalmente a las fases que componen una EIPD, es recomendable que exista un **proceso de supervisión y revisión** de la implantación o puesta en marcha del nuevo tratamiento con el objetivo de garantizar la implantación de las medidas de control descritas en el Plan de acción.

La EIPD debe entenderse como un **proceso de mejora continua**, de forma que esta se revise siempre que se modifique o actualice cualquier aspecto relevante de las actividades de tratamiento. Ante cambios en la descripción del tratamiento o en la experiencia que muestre amenazas o riesgos desconocidos hasta entonces (los fines y medios), se debe realizar una **nueva evaluación de impacto**, generar un **nuevo informe** y un **plan de acción** con las nuevas medidas de control. En caso de que los cambios sobre el tratamiento no sean significativos, y no generen por tanto nuevas amenazas y riesgos sobre los derechos y libertades de los interesados, igualmente se debe realizar una valoración de los cambios producidos y documentar claramente la no necesidad de implantar nuevas medidas de control adicionales.

2.3 ¿Quién debe realizar una EIPD y a quién se debe involucrar?

Corresponde al **responsable del tratamiento** la obligación de realizar la EIPD y no al DPD.



Apartado 2 del **artículo 35**

“El responsable del tratamiento recabará el asesoramiento del Delegado de Protección de Datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos”.

Por tanto, el **Delegado de Protección de Datos** (en adelante DPD) proporciona el asesoramiento necesario al responsable del tratamiento para el adecuado desarrollo de la ejecución de una EIPD.

Es importante destacar que **el DPD no es una figura de obligado nombramiento**. El RGPD establece los supuestos en los cuales se considera obligatorio disponer de DPD. Sin embargo, las organizaciones que llevan a cabo tratamientos que, por su número o por sus características, impliquen un cierto grado de complejidad, deberían contar con el asesoramiento técnico adecuado para estar en condiciones de cumplir con el RGPD y poder demostrarlo. Por ello, resultaría recomendable que estas organizaciones designen un **responsable de protección de datos** que pueda proporcionar este asesoramiento. Si esta figura reúne las condiciones que el RGPD establece para los DPD, **las organizaciones podrán beneficiarse de los incentivos previstos en el RGPD y en la legislación española**.

Desde un punto de vista práctico, existen varias figuras, con diferentes roles y responsabilidades, que pueden participar en la realización de una EIPD, entre estas figuras, la figura del DPD supone un valor añadido en el desarrollo de una EIPD aportando garantías para los derechos y libertades de los interesados.

La matriz de la asignación de responsabilidades o RACI, acrónimo formado por las iniciales de

los tipos de responsabilidad (**Responsible, Accountable, Consulted, Informed**), es un método utilizado en la gestión de proyectos para relacionar actividades con individuos o equipos de trabajo. RACI establece las siguientes figuras de responsabilidad:

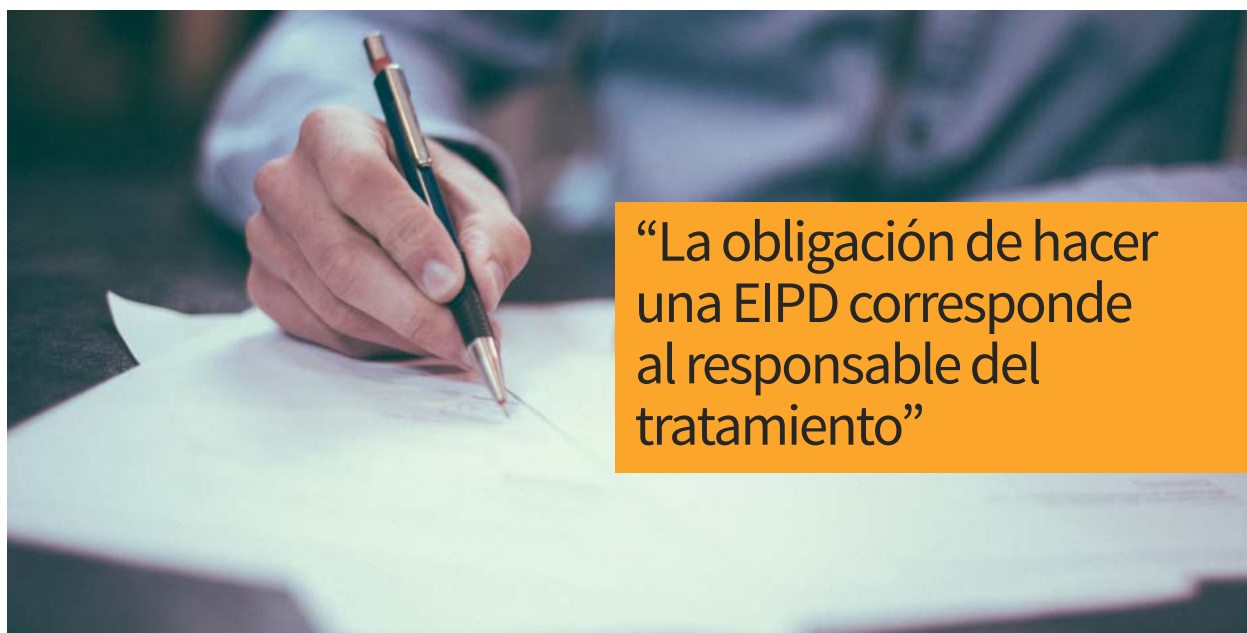
- **Responsible (R)**: Responsable de realizar la tarea.
- **Accountable (A)**: Responsable de que la tarea se realice, sin necesidad de ser el que la ejecute y responsable de rendir cuentas sobre su ejecución.
- **Consulted (C)**: Figura que debe ser consultada para la realización de la tarea.
- **Informed (I)**: Figura que debe ser informada sobre la realización de la tarea.

En base a la metodología RACI, a continuación, se proporcionan orientaciones y un ejemplo de cómo se podrían establecer las responsabilidades en el proceso de realización de una EIPD.

Es importante destacar que la responsabilidad “Responsible” no implica que el área indicada para cada fase de la EIPD sea obligatoriamente quien deba ejecutar las tareas asociadas, pudiendo, por tanto, apoyarse en otras áreas, expertos, recursos externos, etc. Un aspecto relevante en el desarrollo de una EIPD es la adecuada involucración de aquellas figuras que tienen un conocimiento profundo del tratamiento.

La obligación de hacer una EIPD corresponde al responsable del tratamiento, con el apoyo y la colaboración del encargado del tratamiento, si lo hubiese, y en su caso, con el Delegado de Protección de Datos.

Adicionalmente, el personal encargado de la seguridad, el área de tecnología, asesoría jurídica o incluso diferentes responsables de distintas áreas implicadas en el tratamiento pueden ser requeridas durante el proceso de evaluación.



En lo que respecta a la ejecución de la EIPD, puede realizarse por personal interno o externo de la organización, sin que esto exima del cumplimiento de sus obligaciones al responsable del tratamiento, que debe asegurar que esta se haga de forma adecuada y se implanten los controles y medidas de control resultantes de la evaluación.

La participación del Delegado de Protección de Datos en la elaboración debe entenderse como una función de asesoramiento, considerando que el DPD, entre sus funciones, debe responder a las consultas que surjan y monitorizar el proceso.

Finalmente, el RGPD prevé que cuando resulte procedente se deberá recabar la opinión de los interesados o de sus representantes, sin perjuicio de que se adopten las medidas necesarias para proteger intereses comerciales o de negocio.

Es fundamental que, a nivel interno de la Organización, exista una comunicación fluida con las áreas involucradas en las operaciones del tratamiento con el objetivo de obtener informaciones relevantes sobre el ciclo de vida de los datos asociados al tratamiento. Será vital poder describirlo de forma clara y fidedigna, identificar sus vínculos con otros tratamientos y llevar a cabo la evaluación de riesgos disponiendo de toda la información necesaria sobre lo que este realiza. Adicionalmente, la consulta con terceras partes encargadas de las actividades de tratamiento proporciona a la Organización la oportunidad de obtener una visión completa de cómo se verán afectados los datos por las actividades de tratamiento delegadas en terceros. Entre las posibles garantías para los derechos y libertades de los interesados deberá estimarse la posibilidad que el RGPD recoge también en su artículo 35.9 de pedir, cuando proceda, las opiniones de los interesados o sus representantes, como por ejemplo asociaciones, en relación con el tratamiento.

 FASE	Responsable del tratamiento DPD Encargado del tratamiento Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica, ...)			
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C

3. Metodología para la realización de una EIPD

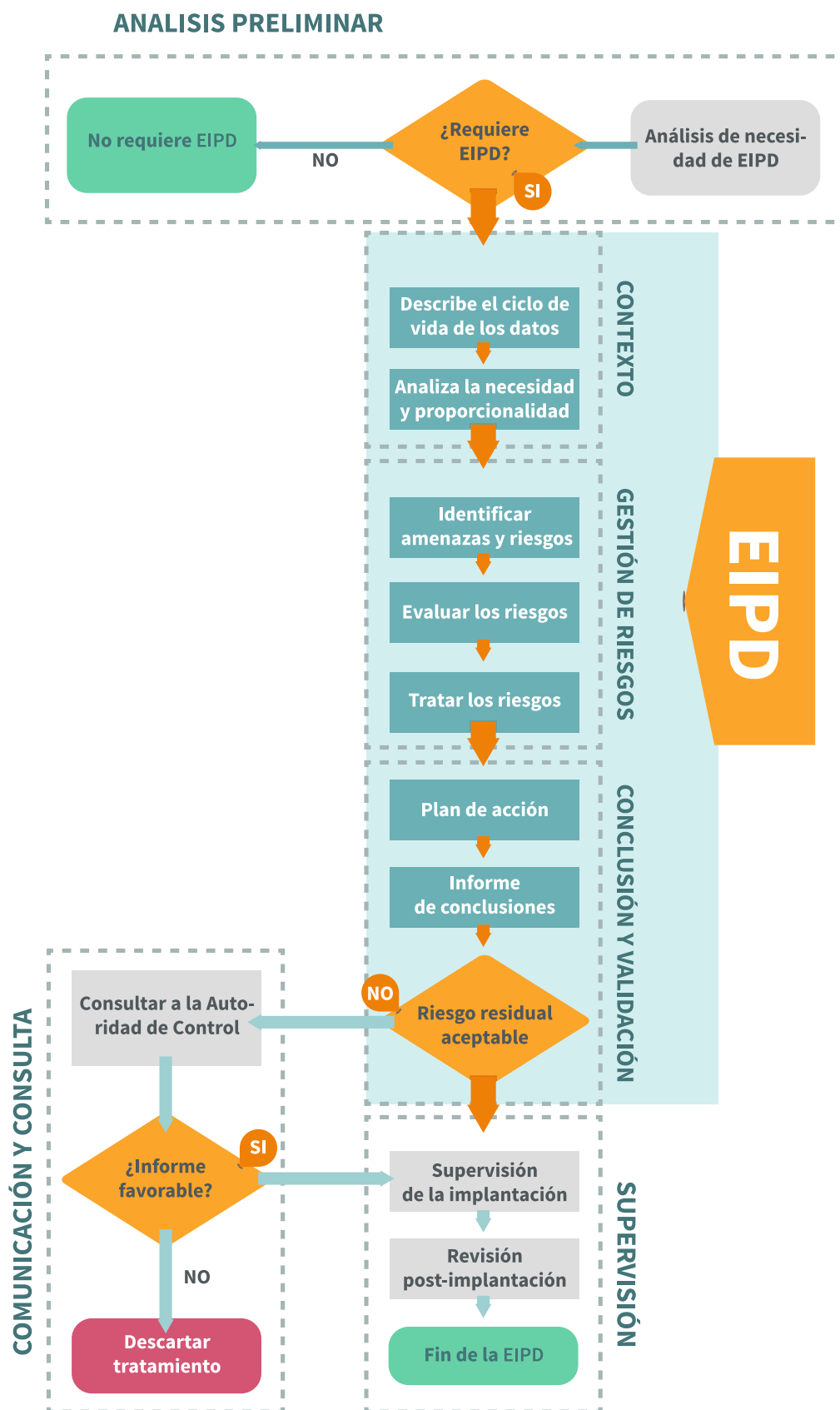
Una EIPD se compone de una serie de fases que convergen hacia un único objetivo, proporcionar una visión detallada de la gestión de los riesgos relativos a la protección de datos que se realiza durante el ciclo de vida de los datos asociados a las actividades de tratamiento para poder garantizar los derechos y libertades de las personas físicas.

La ejecución de una EIPD implica la consideración de varios factores que permitan establecer una ruta de trabajo, las fases y pasos a seguir para poder realizarla de una forma adecuada. Antes del inicio de la EIPD, debemos considerar los siguientes factores:

- **¿Quién debe estar involucrado?** (Recursos necesarios y el equipo de trabajo involucrado en la ejecución).
 - Es necesario definir **quién va a realizar la EIPD** y que figuras o personas se van a involucrar en la ejecución de la misma (por ejemplo, el área responsable del tratamiento realizará la EIPD con el asesoramiento del DPD y del área de seguridad de la información).
- **¿Qué tareas se deben realizar y cómo?** (Metodología, actividades a desarrollar e hitos temporales asociados)
 - Una EIPD puede constar de varias fases, por tanto, es importante tener claro cuáles son cada una de las fases y los objetivos y tareas que se deben conseguir en cada una de ellas.
- **¿Qué y cómo documentar el proceso llevado a cabo?** (Documentación de análisis, conclusiones y plan de acción)
 - La documentación de las tareas, análisis y evaluaciones realizadas, así como las conclusiones obtenidas, deben ser documentadas. Es importante mantener trazabilidad de las acciones realizadas y disponer de una base que justifique las conclusiones o decisiones tomadas.

La **búsqueda de objetividad** es un principio fundamental en una EIPD. Es fundamental disponer de un proceso sistemático a través de una metodología o procedimiento estandarizado de trabajo que permita establecer criterios comunes para garantizar la **homogeneidad, repetitividad y comparabilidad** en la ejecución de una EIPD.

3.1 Ejemplo metodología



Este ejemplo de metodología se compone de 3 secciones diferenciadas que, a su vez, se desglosan en diferentes tareas:



EIPD

1 Contexto

- a Describir el ciclo de vida de los datos (asociados al tratamiento y a las entidades participantes)
- b Analizar la necesidad y proporcionalidad del tratamiento

2 Gestión de riesgos

- a Identificar amenazas y riesgos
- b Evaluar los riesgos
- c Tratar los riesgos

3 Conclusión

- a Plan de acción
- b Informe de conclusiones

Adicionalmente a las fases que componen una EIPD, se ha incluido una **sección de comunicación y consulta** que será de aplicación en exclusiva en aquellos casos donde el resultado de la EIPD conlleve un riesgo elevado para los derechos y libertades de los interesados y sea necesario activar el procedimiento de **Consulta Previa** ante la autoridad de control.

En los siguientes apartados se describen los aspectos a considerar en cada una de las fases de ejecución de una EIPD, así como una serie de orientaciones de cómo llevarlo a cabo.

3.2 Contexto del tratamiento

Describir el ciclo de vida de los datos

El análisis de riesgos conlleva tener un conocimiento muy claro del contexto y de los procesos a analizar. Como punto de partida, es necesario **conocer en detalle todo el ciclo de vida y el flujo de los datos personales** a través del mismo y todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin.

El apartado a) del **artículo 35.7 del RGPD** establece la obligación de que la EIPD incluya, al menos, una **descripción sistemática y detallada del tratamiento**. Como resultado de esta etapa, se debe obtener una visión en detalle que permita facilitar la identificación de las **amenazas y los riesgos** a los que están expuestos los datos de carácter personal asociados al mismo.

Adicionalmente a la descripción del tratamiento, se debe obtener una descripción clara de los elementos que intervienen en cada una de las fases del ciclo de vida de los datos del tratamiento.

El ciclo de vida de los datos se puede dividir en las siguientes etapas:



1 Captura de datos: Proceso de obtención de datos para su almacenamiento y posterior procesamiento. Dentro de la captura de datos se pueden encontrar diversas técnicas, como por ejemplo: formularios web, formularios en papel, la toma de muestras y realización de encuestas, grabaciones de audio y video, fuentes externas o públicas como redes sociales, captación mediante sensores, etc.

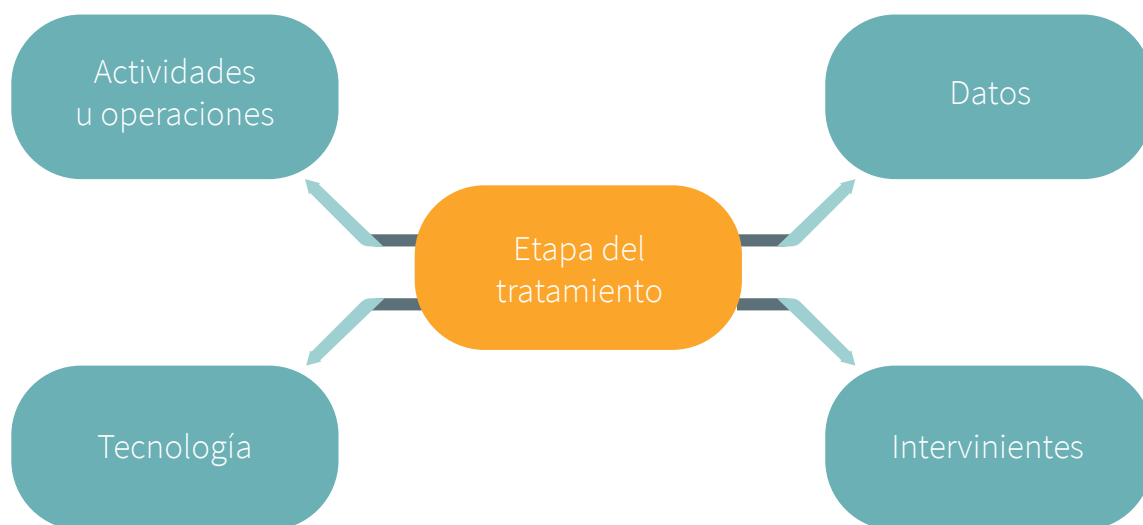
2 Clasificación / Almacenamiento: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.

3 Uso / Tratamiento: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.

4 Cesión de los datos a un tercero para su tratamiento: Traspaso o comunicación de datos realizada a un tercero (toda persona física o jurídica, pública o privada u órgano administrativo). El concepto de cesión o comunicación es muy amplio, puesto que la revelación recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma que facilite el acceso a los datos.

5 Destrucción: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes.

Adicionalmente, para cada una de las etapas del ciclo de vida de los datos en las actividades de tratamiento, se deben identificar todos los elementos involucrados en cada una de las etapas. Podríamos clasificar los elementos involucrados en las siguientes categorías:



Actividades de tratamiento sobre los datos de carácter personal

En cada etapa o en el conjunto de etapas del ciclo de vida se llevan a cabo actividades para alcanzar la finalidad del tratamiento. Es importante **describir en detalle todas las actividades u operaciones** que se llevan a cabo sobre los datos de carácter personal con el objetivo de entender los posibles riesgos a los que se pueden ver expuestos los datos.

En la práctica, puede identificarse un **tratamiento** como el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, por ejemplo, la recogida, registro, organización, estructuración, consulta o utilización de los datos. Una actividad de tratamiento se debe incluir en el registro de actividades en el momento previo antes de su puesta en marcha. Para facilitar la documentación del registro se puede utilizar la información previa documentada en los análisis iniciales realizados durante la fase de definición del tratamiento.

Una actividad u operación puede considerarse, por ejemplo, la captura de datos mediante un formulario web, el filtrado de información mediante un proceso de perfilado, un proceso de cifrado, el borrado o cualquier tarea que requiera el tratamiento o manipulación de los datos.

Datos

El ciclo de vida está directamente relacionado con los datos de carácter personal que se tratan. Se deben identificar los datos de carácter personal tratados o manipulados durante el tratamiento vigilando siempre que los mismos correspondan a los principios que el **artículo 5 del RGPD** dicta.

Para cada tipología de datos, se debe establecer su categoría y su grado de importancia dentro de las actividades de tratamiento, determinando si es imprescindible o no su inclusión.



Es necesario considerar el **principio de minimización de los datos** y asegurar que no existen datos que no se prevén utilizar o recopilar sin utilidad para la finalidad de las actividades de tratamiento.

Intervinientes

Durante todo el ciclo de vida de los datos pueden existir numerosos intervinientes que participan en las actividades de tratamiento. Se deben identificar a las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en el desarrollo de las actividades del tratamiento de los datos de carácter personal. A la hora de identificar a los diferentes intervinientes, es necesario tener en cuenta todos los flujos de información de los datos previstos en el tratamiento. **Los intervinientes en el tratamiento deben estar identificados** y tener delimitadas sus funciones y responsabilidades.

Dentro del grupo de los intervinientes se puede incluir el responsable del tratamiento, áreas o empleados de las organizaciones que participan activamente del procesado de los datos, encargados de tratamiento, etc.

La participación de cada uno de los intervinientes puede suponer una amenaza sobre los datos de carácter personal, como se ha descrito en el documento sobre análisis de riesgos, circunstancia que debe tenerse en cuenta en el análisis y evaluación de los riesgos incluido en la evaluación de impacto.

Tecnología

Asimismo, **la tecnología y los sistemas** son una capa clave que da soporte a las actividades de tratamiento de los datos de carácter personal. Se deben identificar aquellos elementos tecnológicos que intervienen en las actividades de tratamiento de los datos de carácter personal a un alto nivel, sin llegar entrar en un análisis tecnológico pormenorizado.



“La participación de cada uno de los intervinientes puede suponer una amenaza sobre los datos de carácter personal”

Dentro de cada etapa se debe **identificar el hardware y el software** que sea relevante desde la perspectiva del tratamiento de los datos de carácter personal. Las tecnologías están expuestas a diferentes riesgos, por ello, es fundamental realizar una adecuada identificación de todos los elementos tecnológicos que intervienen a lo largo del ciclo de vida de los datos asociados al tratamiento. Se debe identificar la tecnología (cloud, BBDD, servidores), aplicaciones, dispositivos y técnicas empleadas en el procesamiento de los datos.

Por último, no hay que olvidar que, si alguna actividad del proceso implica el tratamiento no automatizado de los datos, lo hemos de identificar como una técnica más de tratamiento y se debe inventariar como un activo más.

Ejemplo de tabla donde se podría documentar el ciclo de vida de los datos asociados a las actividades de tratamiento y cada uno de los elementos que intervienen a lo largo del mismo:

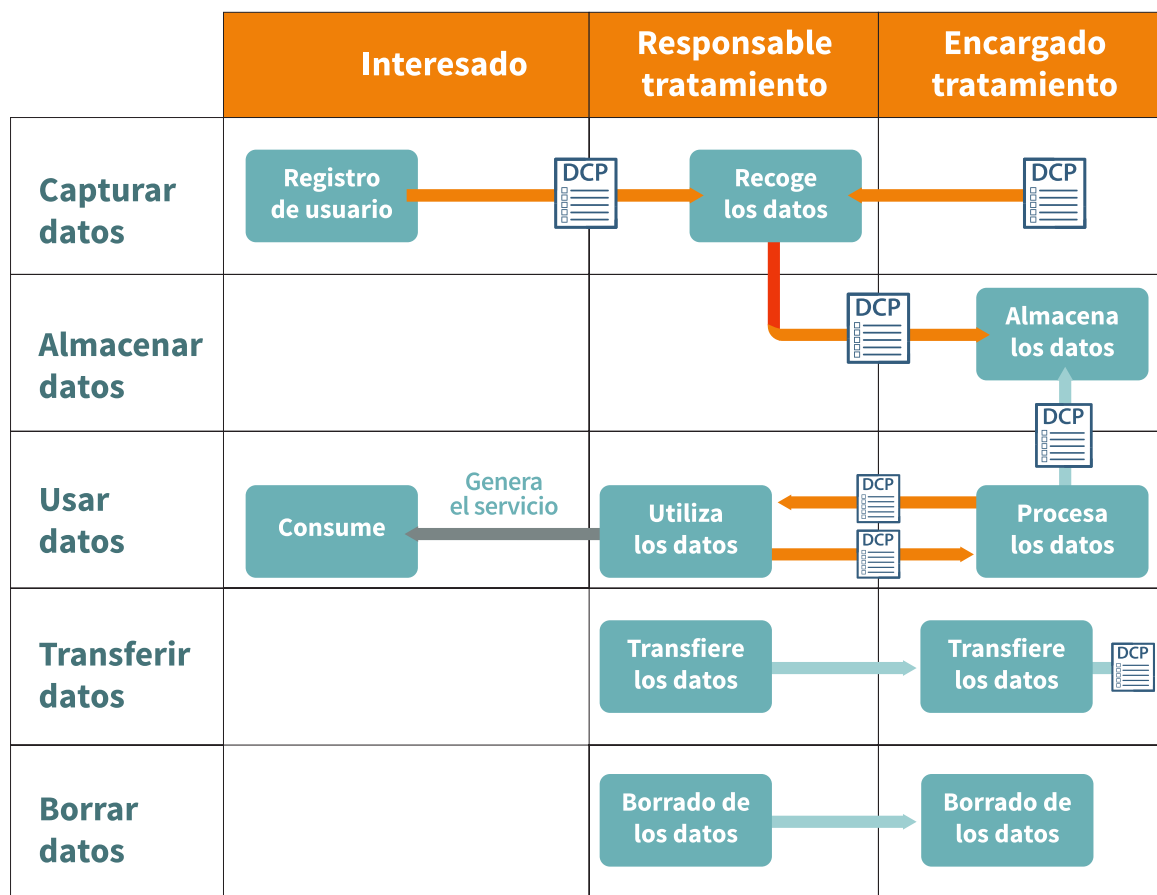
		ETAPAS				
		<i>Captura de datos</i>	<i>Clasificación / Almacenamiento</i>	<i>Uso / Tratamiento</i>	<i>Cesión o transferencia de los datos a un tercero</i>	<i>Destrucción</i>
ELEMENTOS	<i>Actividades del proceso</i>					
	<i>Datos tratados</i>					
	<i>Intervinientes involucrados</i>					
	<i>Tecnologías intervinientes</i>					

La claridad con la que se exponga la información es fundamental y para ello, además de utilizar un **lenguaje claro, directo y comprensible**, es recomendable apoyarse en **material gráfico** que permita, de forma visual y resumida, identificar los principales elementos que conforman el tratamiento y los flujos de información:

- Quiénes llevan a cabo los siguientes roles para cada paso del ciclo de vida de los datos y de las actividades de tratamiento: interesados, responsable del dato, encargado del tratamiento y terceras partes.
- Sistemas de información involucrados.
- Flujos de datos entre sistemas / roles.
- Quién tiene acceso a los datos durante todo el ciclo de vida de los datos y con qué finalidad.
- Cuál es la base legitimadora de las actividades de tratamiento (Consentimiento expreso, relación contractual, interés legítimo, etc.).

Para la realización de este ejercicio, el responsable de la realización de la EIPD puede apoyarse en varias áreas de la propia organización, incluyendo terceras partes en caso de existir.

A modo ilustrativo, y como herramienta de apoyo, se podrían utilizar **diagramas** para la identificación de los elementos mencionados, aunque no es estrictamente necesario.



Sin embargo, en tratamientos complejos, esta representación gráfica puede ser complicada y, por tanto, sólo es conveniente introducirla si sirve para aportar más claridad y comprensión del conjunto del tratamiento o de actividades de tratamiento específicas.

En el [Anexo I](#), se incluye un ejemplo de plantilla donde poder describir en detalle el ciclo de vida de los datos asociados a un tratamiento.

Analizar la necesidad y proporcionalidad del tratamiento

Analizar la necesidad y proporcionalidad de las actividades de tratamiento, como punto de partida, requiere plantearse las siguientes cuestiones:

■ **¿Qué se va a hacer con los datos y con qué finalidad?** Se debe analizar qué se prevé realizar con los datos y los medios mediante los cuales se realizará el tratamiento, así como identificar las diferentes finalidades para las cuales se quieren tratar los datos.

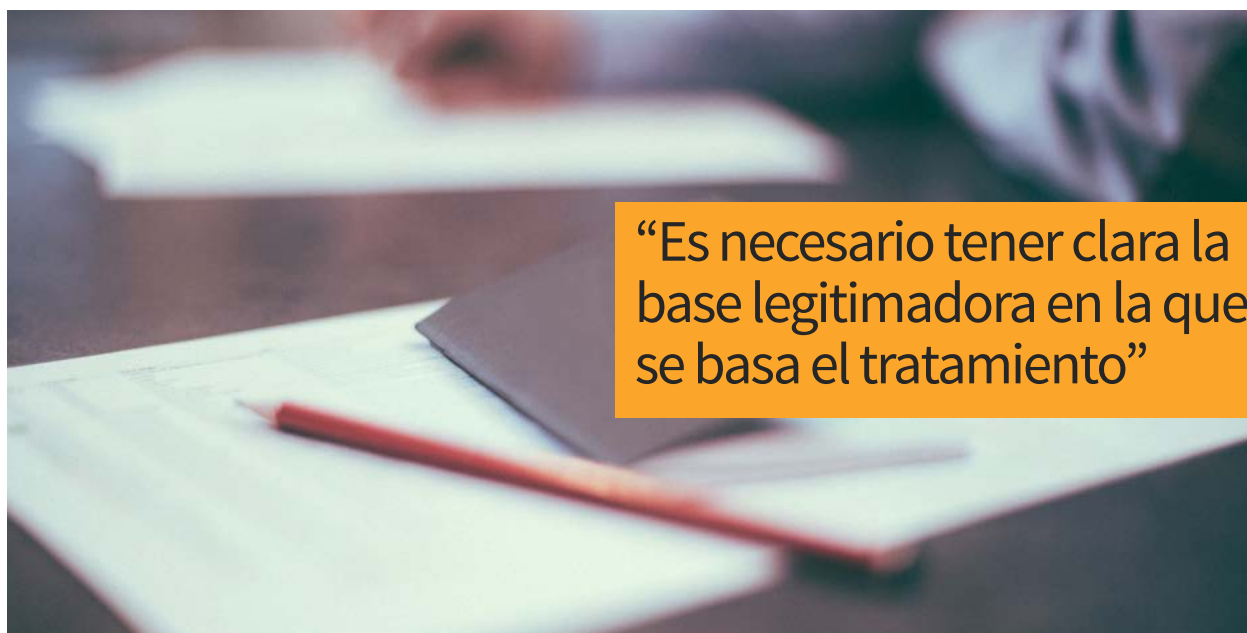
■ **¿Qué datos se van a tratar? ¿Son necesarios todos ellos? ¿De quién son los datos a tratar?** Se deben identificar todos los datos que puedan ser objeto de tratamiento (nombre, apellidos, dirección, datos de salud, correo electrónico o imágenes), su necesidad para la finalidad con la que se recogen y el origen o la fuente de los mismos (clientes, potenciales clientes, empleados, pacientes, redes sociales, fuentes externas, etc.)

Una vez se tiene una visión clara de los datos personales a tratar, cómo se van a tratar y con qué finalidades, es necesario tener clara la **base legitimadora en la que se basa el tratamiento**, así como la necesidad y la proporcionalidad de los datos para esas finalidades. Esta evaluación inicial, se puede haber realizado en la definición del tratamiento, en cuyo caso, sólo sería necesario recuperar la misma y documentarla en la EIPD.

Licitud del tratamiento

El tratamiento de los datos personales debe ser lícito y, por tanto, es necesario que los datos se traten de acuerdo con las condiciones recogidas en el RGPD. En este sentido, el **artículo 6 del RGPD**, recoge los supuestos en los que se considera que el tratamiento de datos personales es lícito:

- Que se cuente con el **consentimiento del interesado** para los fines específicos del tratamiento.
- Que el tratamiento sea **necesario para la ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
- Que el tratamiento sea necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento.

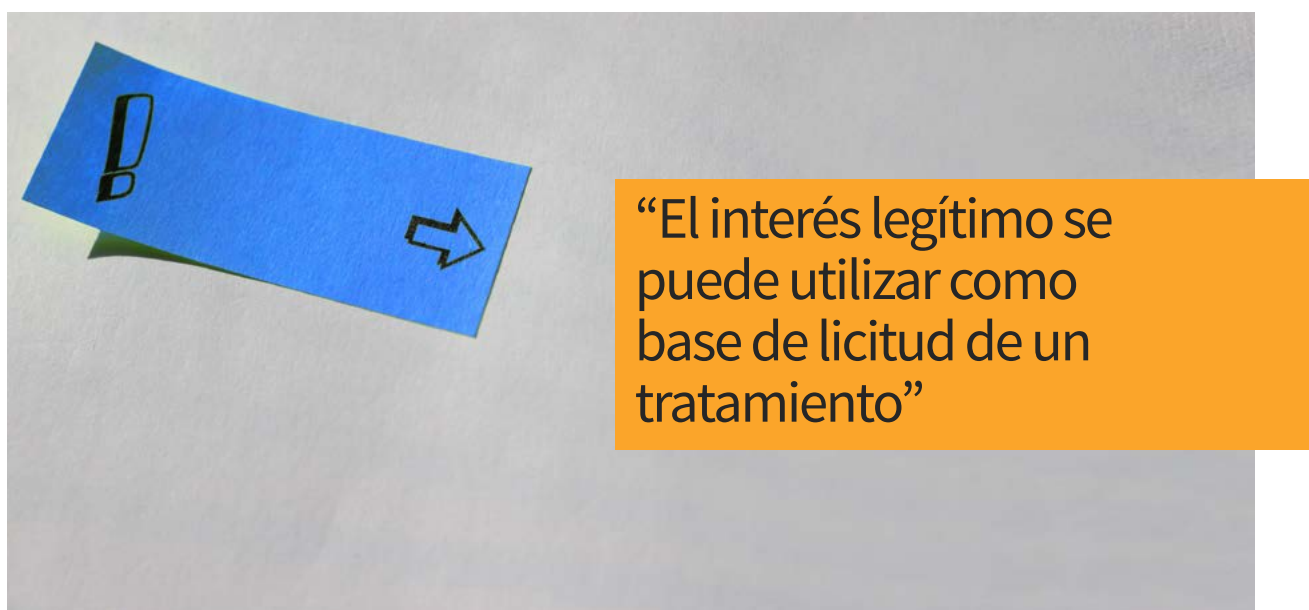


- Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.
- Que el tratamiento sea necesario para el **cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento.
- Que el tratamiento sea necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

El **artículo 35.7 apartado a) del RGPD**, hace mención a que las Evaluaciones de Impacto en Protección de Datos deben incluir, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento. Por tanto, es recomendable **considerar el análisis y justificación** (“examen de ponderación” que recoge el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE) que justifique la licitud de tratamiento basado en el interés legítimo del responsable del tratamiento.

El interés legítimo se puede utilizar como base de licitud de un tratamiento «siempre que no prevalezcan los intereses o los derechos y libertades de la persona interesada» y teniendo en cuenta las expectativas razonables de las personas afectadas por el tratamiento, basadas en la relación que tienen con el responsable del tratamiento. El uso del interés legítimo como base de licitud del tratamiento debe ser evaluado adecuadamente, tomando en consideración que cuando la licitud del tratamiento se basa en el interés legítimo del responsable del tratamiento (o de un tercero), hay que sopesar estos intereses y los de las personas que se verán afectadas.

Cuando la base de licitud del tratamiento es el consentimiento del interesado, el responsable del tratamiento debe poder garantizar y demostrar que ha obtenido el consentimiento inequívoco y libre según las directrices del Grupo de trabajo del art. 29 otorgadas en el documento ‘WP259 Directrices sobre el consentimiento’ en virtud del Reglamento General de Protección de Datos.



Necesidad y proporcionalidad del tratamiento

El principio de “**minimización de datos**” establece que los datos personales serán “*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que serán tratados*”. Durante la definición del mismo, se debe considerar **qué datos son estrictamente necesarios** para realizar las actividades de tratamiento en función de las finalidades previstas.

Del mismo modo, todas las acciones que el tratamiento incluya deben ser necesarias y proporcionales a las finalidades previstas. Para determinar la necesidad de llevar a cabo un tratamiento, se debe seguir un planteamiento pragmático. Si se toma como base el **artículo 39 del RGPD**, se deben tener en cuenta los siguientes aspectos para evaluar la necesidad del tratamiento:



- 1 “Los datos personales sólo se deben tratar si la finalidad del tratamiento no se puede hacer razonablemente por otros medios”, es decir, sin tratar datos personales.
- 2 “Las finalidades tienen que estar definidas de manera determinada, explícita y legítima”.
- 3 “Cualquier tratamiento de datos personales tiene que ser lícito y leal”. Este punto está unido al análisis de las finalidades establecidas en el tratamiento y su supuesto legitimador.
- 4 “Los datos personales tienen que ser adecuados, pertinentes y limitados a lo necesario para los fines para los cuales se tratan”.
- 5 “El plazo de conservación se limite a un mínimo estricto”.

La **proporcionalidad** tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: utilizando otros datos, reduciendo el universo de personas afectadas (de manera cuantitativa o cualitativa), haciendo uso de otras tecnologías menos invasivas o bien aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.

Las autoridades de protección de datos a menudo señalan que para comprobar si un tratamiento supone una medida restrictiva de un derecho fundamental, este debe superar los tres puntos del llamado **juicio de proporcionalidad**:

- **Juicio de idoneidad:** si la medida puede conseguir el objetivo propuesto.
- **Juicio de necesidad:** si, además, es necesario, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia.
- **Juicio de proporcionalidad en sentido estricto:** si la medida es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto.

En definitiva, a nivel práctico, se debe responder de manera argumentada a dos preguntas:

- ¿El tratamiento, tal y como está definido, es necesario para la finalidad prevista?
- ¿Las actividades de tratamiento son proporcionales a las finalidades previstas?

Si al evaluar estos aspectos, se concluye que el diseño del tratamiento no cumple con alguno de estos dos principios, tal y como recoge el **artículo 39 del RGPD**, «*Los datos personales sólo se tratarán si la finalidad del tratamiento no se puede hacer razonablemente por otros medios*», este tratamiento no se debe llevar a cabo y será necesario reformular o rediseñar dicho tratamiento.

En el **Anexo II**, se incluye un ejemplo de plantilla con consideraciones que faciliten en análisis de la necesidad y proporcionalidad del tratamiento de datos personales.

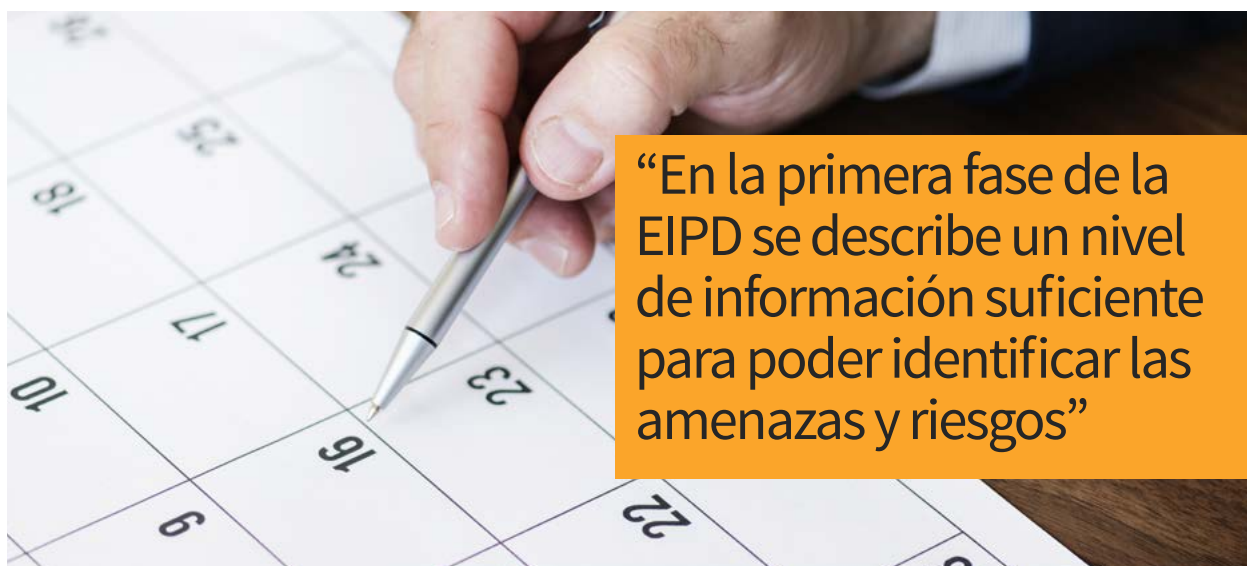
3.3 Gestión de riesgos: Identificar, evaluar y tratar

La gestión de riesgos es el proceso de **identificar, analizar y valorar** la probabilidad e impacto derivados de la posibilidad de que se materialice un riesgo con el objetivo de establecer las acciones preventivas, correctivas y reductivas que permitan minimizar el nivel de exposición al riesgo.

En la primera fase de la EIPD se describe un nivel de información suficiente para poder identificar las amenazas y riesgos a las que está expuesto el tratamiento. Adicionalmente a la descripción de las actividades del tratamiento, el **artículo 35.7 del RGPD** prevé el siguiente contenido mínimo en las EIPD:

- Una **evaluación de los riesgos** para los derechos y las libertades de los interesados.
- Las **medidas previstas para afrontar los riesgos**, incluidas garantías, medidas de seguridad y mecanismos para garantizar la protección de datos personales y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Identificar y evaluar los riesgos son las tareas iniciales del proceso de gestión de riesgos. Asegurar la correcta identificación de los riesgos a los que están expuestas las actividades de tratamiento es una parte clave para poder realizar una evaluación completa. La no identificación de riesgos implica que estos no se evalúan y no se tratan, y el tratamiento podría estar más expuesto al potencial riesgo.



“En la primera fase de la EIPD se describe un nivel de información suficiente para poder identificar las amenazas y riesgos”

La AEPD pone a su disposición un documento que contiene un listado de riesgos asociados al cumplimiento normativo que se puede descargar desde la [sección de publicaciones](#) de la web de la AEPD.

Las siguientes actividades permiten establecer las bases para la identificación y evaluación de los riesgos:

- **Identificar el origen de los riesgos**, es decir, analizar los potenciales escenarios de riesgo a los que pueden estar expuestos los datos personales.



- **Por ejemplo**, un tratamiento que incluya un almacenamiento en la nube, es un escenario con exposición a riesgos que pueden implicar la pérdida de confidencialidad y disponibilidad, entre otros.

- **El análisis de las situaciones que generan riesgo**, teniendo en cuenta los factores y características que pueden entrar en juego a la hora de determinar el nivel de riesgo que implican.



- Continuando con el **anterior ejemplo**, en un tratamiento que incluya un almacenamiento basado en la nube, un potencial acceso no autorizado a los datos en caso de un ataque cibernético o la pérdida de los mismos ante ausencia de medios de respaldo ante un fallo en las bases de datos que soportan la nube, podrían ser situaciones que generan riesgo y que se deben considerar en el análisis.

- **La valoración de los riesgos**, teniendo en cuenta la probabilidad de que un evento no deseado se produzca y el impacto que puede tener (consecuencias).



- Ante el riesgo de acceso no autorizado a los datos, si no disponemos de medidas de control que limite el acceso a la nube, la probabilidad de que se materialice el riesgo será elevada y su impacto, en función de los datos almacenados, también podría ser elevado.

El último paso del proceso de gestión de riesgos es tratar los mismos. El objetivo de **tratar los riesgos** es disminuir su nivel de exposición con medidas de control que permitan disminuir la probabilidad y/o impacto de que estos se materialicen.

A continuación, se describen una serie de orientaciones sobre los pasos a seguir en el proceso de gestión de riesgos que incorpora las etapas de identificación, evaluación y respuesta o tratamiento.

Identificación de riesgos

En esta etapa inicial del proceso de gestión de riesgos se deben identificar los potenciales escenarios de riesgo que pueden afectar negativamente a los derechos y libertades de las personas derivados de un inadecuado tratamiento de sus datos.

El riesgo es la exposición a amenazas, por tanto, como punto de partida, es fundamental entender qué es una amenaza y cómo se puede identificar escenarios de riesgo a partir de la misma.

¿Qué es una amenaza?

Una amenaza es **cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados** sobre cuyos datos de carácter personal se realiza un tratamiento.

¿Qué tipos de amenazas hay?

De forma general, las amenazas pueden ser de diversas tipologías, por ejemplo:

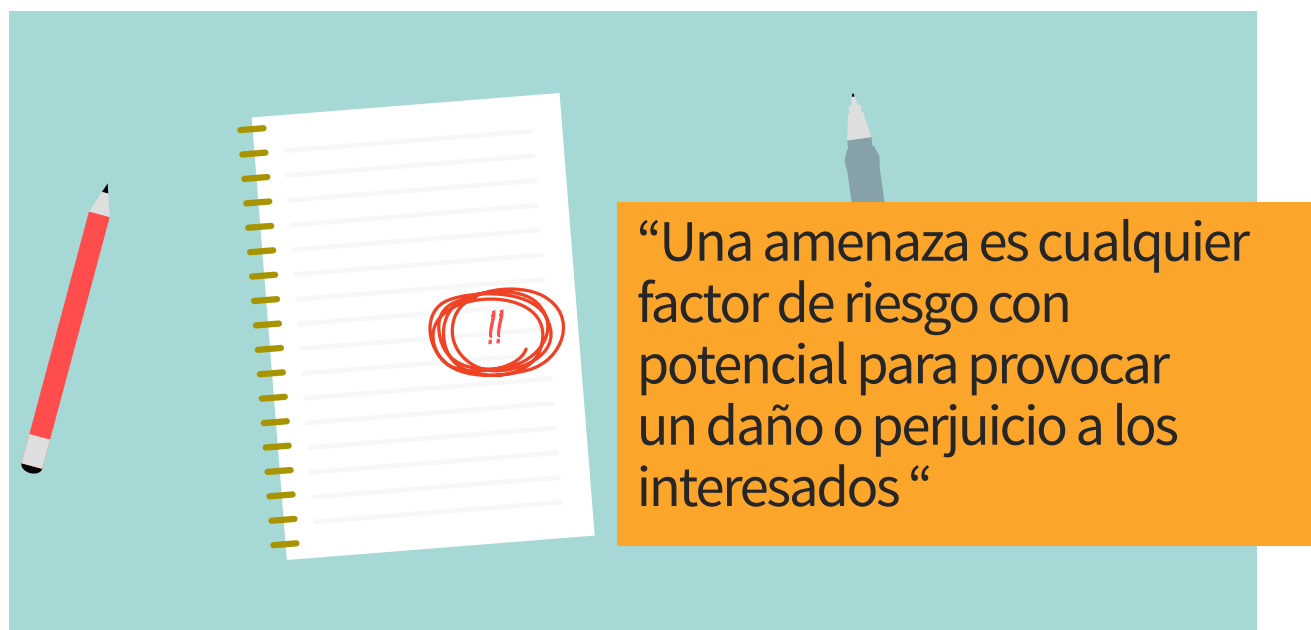
- **Desastres naturales:** Fuego, agua, desastres ambientales...
- **Errores y fallos:** Destrucción no intencionada, programación inadecuada de un proceso de perfilado, fuga de información...
- **Ataques intencionados:** Hacking, phishing, malware, robo...
- **Incumplimiento normativo:** Incumplimiento del periodo de retención, ausencia de base legitimadora del tratamiento...

Sin embargo, si ponemos foco en la protección de los datos, las amenazas se pueden categorizar principalmente en **3 tipos** en base a la tipología de daño que pueden producir en los datos:



- Acceso ilegítimo a los datos → **confidencialidad**
- Modificación no autorizada de los datos → **integridad**
- Eliminación de los datos → **disponibilidad**

Las amenazas se pueden clasificar en diversos grupos, cada entidad puede tener diferentes catálogos de amenazas internos.



“Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados”

¿Cómo identificar amenazas?

Para identificar de forma adecuada las amenazas asociadas a las actividades de tratamiento, se debe tener en cuenta todo el **ciclo de vida de los datos** en cada operación, desde su inicio hasta el momento en el que finaliza. Identificar una amenaza consiste en identificar la fuente de los escenarios en los que se puede producir un daño o una violación de los derechos y libertades de los interesados.

A continuación, se describen ejemplos de amenazas y de preguntas que permiten identificar las mismas. En este sentido, cada entidad puede disponer de catálogos estandarizados de amenazas que faciliten el proceso (catálogos internos de cada entidad para otro tipo de análisis de riesgos, buenas prácticas presentes y futuras, etc.).

Ejemplos de amenazas en función de su tipología:

 Tipo de amenaza	Amenaza	¿Qué preguntas se pueden formular para identificar la amenaza?
 Acceso ilegítimo a los datos	■ Pérdidas de dispositivos móviles ■ Fuga de información ■ Acceso intencionado por parte de personal no autorizado ■ Ataques intencionados (hacking, suplantación de identidad, etc.) ■ Uso ilegítimo de datos personales	• ¿Los dispositivos móviles y de almacenamiento están cifrados? • ¿Existen métodos para extraer la información durante la operación de tratamiento? • ¿Está expuesta la información al acceso por parte de terceros no autorizados? ¿Existe un mecanismo para dar acceso a los datos únicamente al personal autorizado? • ¿La operación de tratamiento es susceptible de ataques de hacking? ¿es susceptible de ataques de phishing o de otros métodos de suplantación de identidad? • ¿Existe una adecuada gestión de la configuración de los parámetros de seguridad de los elementos (elementos de red, SO y BBDD)? • ¿Existe una base legitimadora para la actividad de tratamiento? ¿las finalidades de las actividades de tratamiento son necesarias y proporcionales?
 Modificación no autorizada de los datos	■ Ataque para la suplantación de identidad ■ Errores en los procesos de recopilación y captura de información ■ Modificación no autorizada de datos intencionada ■ Uso ilegítimo de datos personales	• ¿Existen credenciales o mecanismos de control que limiten el acceso a personal no autorizado? ¿Se revisa periódicamente la actividad realizada por los usuarios cuando acceden a los sistemas? • ¿Existen controles sobre la integridad de la información durante el proceso de captura de datos? ¿se identifica adecuadamente al interesado que proporciona los datos? • ¿Los datos son modificables únicamente por el personal autorizado? • ¿La actividad de tratamiento sobre los datos son acordes a las finalidades para las cuales existe una base legitimadora? ¿se puede realizar un perfilado o una operación de tratamiento que no esté alineada con las finalidades de la operación de tratamiento?
 Eliminación de los datos	■ Corte de suministro eléctrico o fallos en servicios de comunicaciones ■ Error humano o ataque intencionado que provoca borrado o pérdida de datos ■ Desastres naturales	• ¿Un fallo de suministro eléctrico puede implicar la pérdida de datos? ¿Un fallo en los servicios de comunicaciones puede ocasionar una pérdida de datos? • ¿Los datos pueden ser eliminados únicamente por el personal autorizado? ¿Existen copias de seguridad? • ¿Están los sistemas que almacenan datos en ubicaciones expuestas a la posibilidad de que se produzca un desastre natural? ¿Existe réplica de los datos en diferentes ubicaciones?

¿Qué es un riesgo?

Un riesgo se puede definir como la combinación de la **posibilidad de que se materialice una amenaza y sus consecuencias negativas**. El nivel del riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo.

Para evaluar un riesgo es necesario considerar todos los posibles escenarios con los que el riesgo se haría efectivo, incluidos aquellos que impliquen un mal uso o abuso de los datos y las alteraciones técnicas o del entorno.

¿Cómo relacionar los riesgos con las amenazas?

Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar y evaluar los riesgos siempre implica considerar la amenaza que los puede originar.

Ejemplos prácticos de amenazas y su relación con el riesgo y su posible impacto:



Ejemplo nº1 (acceso ilegítimo a los datos): La pérdida de un dispositivo móvil o la fuga de información (**Amenaza**), podría derivar en un acceso por parte de personal no autorizado a los datos y, en consecuencia, se produciría una vulneración de los derechos y libertades de los interesados (**riesgo**), lo que podría derivar en un posible daño moral, físico o material sobre el interesado (**Impacto**).



Ejemplo nº2 (modificación no autorizada de los datos): La ausencia de mecanismos de control en un sistema es una vulnerabilidad que puede facilitar una suplantación de identidad derivada de un ataque cibernético (**amenaza**). El ataque puede provocar una modificación no autorizada de datos que altere la integridad y disponibilidad de los datos (**riesgo**), con la posibilidad de provocar daños y perjuicios, materiales a los interesados (**impacto**).



Ejemplo nº3 (eliminación de los datos): Un fallo en el suministro eléctrico o un desastre natural pueden provocar una pérdida de datos (**amenaza**), que podría derivar en la falta de disponibilidad de los datos para una determinada operación de tratamiento (**riesgo**), con la posibilidad de provocar daños y perjuicios, materiales a los interesados (**impacto**).

	Etapas del ciclo de vida de los datos	Amenaza identificada	Riesgo	Impacto
Ejemplo nº1	Almacenamiento de los datos	Pérdida de un dispositivo móvil o fuga de información	Vulneración de los derechos y libertades	Daño moral, físico o material
Ejemplo nº2	Uso / tratamiento de los datos	Ataque cibernético para la suplantación de identidad	Modificación no autorizada de datos	Daños materiales a los interesados
Ejemplo nº3	Uso / tratamiento de los datos	Fallo en el suministro eléctrico o desastre natural	Borrado o pérdida de datos	Daños materiales a los interesados

Evaluación de riesgos

La evaluación de riesgos consiste en **valorar y estimar la probabilidad y el impacto de que el riesgo se materialice**. Como punto de partida, es necesario haber definido el criterio que se seguirá a la hora de valorar los riesgos. Los criterios para cuantificar los riesgos, estimar el nivel de impacto y su probabilidad, se pueden basar en estándares o se pueden definir a criterio de la organización.

A la hora de definir los criterios para cuantificar los riesgos es importante destacar que, la diferencia principal entre la EIPD y los análisis de riesgos tradicionales que una entidad suele realizar, reside en que la EIPD se realiza desde “*el punto de vista del interés del sujeto*” mientras que los análisis de riesgos se realizan desde el punto de vista del “*riesgo para la entidad*”.

A continuación, se describen una serie de conceptos necesarios para poder evaluar los riesgos, así como, un método estandarizado para estimar y valorar el impacto y la probabilidad asociados a un riesgo.

¿Qué es el riesgo inherente y cómo se calcula?

El riesgo inherente es el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenaza asociada al riesgo se materialice.

El cálculo del riesgo inherente se realiza mediante la siguiente fórmula:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$



La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice.

A continuación, se presenta una posible metodología de valoración de la probabilidad e impacto basada en **cuatro niveles** (de acuerdo a la ISO 29134), aunque cada entidad podrá utilizar la metodología que mejor se ajuste a sus circunstancias (por ejemplo, el uso de alguna de las metodologías de riesgos internas).

Escala de posibles valores para el cálculo de la probabilidad:

- 1 Probabilidad despreciable:** La posibilidad de ocurrencia es muy baja (por ejemplo, un evento que puede pasar de forma fortuita).
- 2 Probabilidad limitada:** La posibilidad de ocurrencia es baja (por ejemplo, un evento que puede pasar de forma ocasional).
- 3 Probabilidad significativa:** La posibilidad de ocurrencia es alta (por ejemplo, un evento que puede pasar con bastante frecuencia).
- 4 Probabilidad máxima:** La posibilidad de ocurrencia es muy elevada (por ejemplo, un evento cuya ocurrencia se produce con mucha frecuencia).

El impacto se determina en base a los posibles daños que se pueden producir si la amenaza se materializa. De igual modo, el impacto también se evaluará con la misma escala de cuatro valores posibles:

- 1 Impacto despreciable:** El impacto es muy bajo (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
- 2 Impacto limitado:** El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
- 3 Impacto significativo:** El impacto es alto (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto sobre el interesado).
- 4 Impacto máximo:** El impacto es muy alto (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado un impacto crítico sobre el interesado).



El impacto asociado a un riesgo puede ser ocasionado por daños de diferente índole. Para evaluar el impacto asociado a un riesgo, se recomienda realizar la evaluación considerando tres dimensiones diferentes de posibles daños que se pueden producir sobre el interesado:

- a Daño físico:** Conjunto de acciones que pueden ocasionar un daño en la integridad física del interesado.
- b Daño material:** Conjunto de acciones que pueden ocasionar pérdidas económicas, de patrimonio, de empleo, etc.
- c Daño moral:** Conjunto de acciones que pueden ocasionar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.

La escala de impacto dependerá del tipo y cantidad de daño o perjuicio causado. El valor final de impacto deberá ser solo uno por riesgo, entre las cuatro posibilidades. A continuación, se pueden ver ejemplos prácticos de cada uno de los niveles de impacto en todas sus magnitudes:

 Ejemplos de posibles daños físico, material o moral	
 Despreciable: Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia	■ Molestias o irritación. ■ Se incumplen obligaciones materiales sin perjuicios relevantes. ■ No se priva de los derechos y libertades.
 Limitado: Los interesados podrán encontrar inconveniencias no significativas	■ Estrés o padecimientos físico menores. ■ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos. ■ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
 Significativo: Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.	■ Empeoramiento del estado de salud o agresiones físicas. ■ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes. ■ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
 Máximo: Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.	■ Agresiones físicas con consecuencias irreparables. ■ Asunción de una deuda inabarcable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables. ■ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.

Tomando como base las escalas de probabilidad e impacto, para poder determinar el riesgo inherente, es necesario **asignar valores a cada uno de los niveles** de las escalas de probabilidad e impacto. La escala de valores comprende desde el valor 1, en el caso de que la magnitud sea despreciable, hasta el valor 4 en el caso donde la magnitud es máxima:



Si se enfrentan la probabilidad y el impacto, se forma una matriz de riesgo, tal y como se puede ver a continuación:

Probabilidad	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4

IMPACTO

☐ Bajo ☐ Alto
☐ Medio ☐ Muy Alto

Si se establece un valor numérico a la probabilidad y otro valor al impacto, según la escala de valores definida, se obtiene una posición en la matriz de riesgos que se corresponde con el riesgo inherente resultado de aplicar la fórmula de estimación del riesgo. El resultado del riesgo inherente se puede considerar en los siguientes niveles en función del valor obtenido:

- ☐ **Bajo:** Si el valor resultante se sitúa entre los valores 1 y 2.
- ☐ **Medio:** Si el valor resultante es mayor de 2 y menor o igual que 6.
- ☐ **Alto:** Si el valor resultante es mayor que 6 y menor o igual que 9.
- ☐ **Muy Alto:** Si el valor resultante es mayor que 9.

Considerando los criterios establecidos, si se deseara valorar un riesgo, por ejemplo, al añadir valores numéricos a la probabilidad y al impacto, ante un riesgo con **probabilidad limitada (2) e impacto significativo (3), el nivel de riesgo inherente será medio (2 x 3 = 6).**

Durante la fase de evaluación de riesgos, se debe realizar este ejercicio para cada una de las amenazas identificadas, considerando los riesgos asociados, el impacto y la probabilidad de que se materialice y determinando su riesgo inherente.

Ejemplos de cálculo de riesgo inherente:

Para poder estimar y valorar el riesgo, es necesario tener contexto sobre la exposición a la que se somete el riesgo. Para dotar de contexto al ejemplo, supongamos una aplicación móvil con almacenamiento en la nube que captura datos a través de *weareables* (dispositivos como un reloj o pulsera), además de permitir la introducción manual de datos de salud por parte del usuario. La finalidad de la actividad de tratamiento es monitorizar la actividad del usuario y recomendar hábitos de vida saludables. La aplicación móvil no dispone de medidas de control de acceso, ni de detección de malware, además no se realizan copias de seguridad de los datos. Adicionalmente, durante la fase de registro del usuario no se solicita consentimiento expreso para ninguna finalidad adicional a la mencionada.

Ante este contexto, se puede identificar, entre otras, varias amenazas y riesgos asociados que se describen y evalúan a continuación:

Tipo amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	Fuga de información (derivada de la pérdida del dispositivo móvil)	Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad)	Significativa 3	Significativo 3	Alto 9
	Operación de tratamiento no autorizada (derivada del uso de los datos para una finalidad sin base legítima, por ejemplo, acciones de marketing indirecto sobre productos de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima 4	Limitado 2	Alto 8
Modificación no autorizada de los datos	Ataque cibernético (malware que modifica los datos almacenados en la nube)	Modificación de datos no autorizada por parte de terceros (violación de la integridad)	Significativa 3	Limitado 2	Medio 6
	Operación de tratamiento no autorizada (derivada de una decisión automatizada en base al perfilado de datos erróneo por una mala programación del software , por ejemplo, una categorización de personas saludables con acceso a determinadas coberturas de un seguro de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima 4	Significativo 3	Muy alto 12
Eliminación de los datos	Corte de suministro eléctrico o fallos en servicios de comunicaciones (como consecuencia del fallo se produce un periodo temporal en el cual los datos no han sido almacenados)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Limitada 2	Limitado 2	Medio 4
	Ataque intencionado que provoca la indisponibilidad de los datos (como consecuencia de un ataque de cifrado de las bases de datos que inhabilita las mismas)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Significativa 3	Significativo 3	Alto 9

Tratamiento o respuesta ante los riesgos

La última etapa del proceso de gestión de riesgos consiste en **definir la respuesta o las medidas necesarias para tratar el riesgo y reducir su nivel de exposición**. Tratar un riesgo es el resultado de definir y establecer medidas de control para disminuir la probabilidad y/o el impacto asociados al riesgo inherente de una operación de tratamiento.

¿Qué alternativas existen para reducir o mitigar un riesgo?

El nivel de riesgo se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte. Existen **cuatro medidas diferentes para tratar el riesgo**:

- a Reducción del riesgo:** Para reducir el nivel de riesgo, se deben establecer medidas de control que reduzcan los niveles de probabilidad y/o impacto asociados al riesgo inherente.
- b Retención del riesgo:** Si el nivel de riesgo inherente es inferior al nivel de riesgo considerado como aceptable, no existe necesidad de implementar controles adicionales.
- c Transferencia del riesgo:** Consiste en compartir un riesgo con una organización externa. Se puede transferir el riesgo a una aseguradora que afronte las posibles consecuencias materiales. Sin embargo, se ha de considerar que, en ocasiones, la transferencia de riesgos puede generar otros riesgos. Por ello, la transferencia puede generar la necesidad de análisis adicionales.
- d Anulación del riesgo:** Si el riesgo es muy elevado y no se quiere asumir el mismo, se puede decidir abandonar la actividad de tratamiento.

Las **medidas de control** tienen como objetivo mitigar o minimizar el riesgo asociado a una operación de tratamiento. Es importante destacar que el objetivo principal de una EIPD no es eliminar completamente el riesgo asociado a la actividades de tratamiento, lo que se pretende es **reducir el mismo hasta un nivel aceptable** para poder llevar a cabo las mismas garantizando los derechos y libertades de los interesados.



“Las medidas de control tienen como objetivo mitigar o minimizar el riesgo asociado a una operación de tratamiento”

Durante el proceso de definición de las medidas de control se debe considerar de forma independiente cada riesgo identificado y establecer tantas medidas de control como sean necesarias hasta lograr un nivel de riesgo aceptable.

Existen diversos tipos de medidas de control, por ejemplo:

- **Organizativas:** Medidas asociadas a procedimientos, a la organización y gobierno de la entidad. En esta tipología de medidas se pueden incluir los procedimientos para ejercer los derechos de los interesados, protocolos para gestionar vulnerabilidades e incidentes, etc.
- **Legales:** Medidas asociadas al cumplimiento normativo. Por ejemplo, cláusulas para recogida de consentimientos expresos, etc.
- **Técnicas:** Medidas que permiten velar por la seguridad física y lógica de los activos de información. Por ejemplo, controles de acceso, cifrado, etc.

¿Qué es el riesgo residual y cómo se calcula?

El riesgo residual es el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre la actividad de tratamiento para valorar la probabilidad y/o el impacto asociado al riesgo.

Para evaluar el riesgo residual, se debe estimar de nuevo la probabilidad y el impacto considerando las medidas de control definidas, mediante la siguiente fórmula:

$$\text{Riesgo residual} = \text{Probabilidad} \times \text{Impacto}$$

Por ejemplo, ante un riesgo de acceso no autorizado por parte de terceros en un proceso de autenticación, el hecho de establecer un **usuario y una contraseña** asignados al usuario (cumplimiento con políticas de control de acceso e identificación), reduce significativamente la probabilidad de que un tercero pueda realizar un acceso no autorizado. En este caso, la medida de control reduce la probabilidad de ocurrencia del riesgo y, por tanto, minimiza el riesgo residual asociado.

Ejemplo práctico de estimación del riesgo residual:

- **Ciclo de vida del dato (fase almacenamiento):** Almacenamiento de datos de clientes en dispositivos móviles.
- **Amenaza:** Pérdida del dispositivo móvil.
- **Riesgo:** Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad).

- **Impacto:** Violación de derechos fundamentales (Significativo 3) .
- **Probabilidad:** Se puede producir cada vez que el usuario no tiene en su poder el dispositivo móvil (Significativa 3).
- **Riesgo inherente:** Impacto x Probabilidad $\rightarrow 3 \times 3 = 9$ (Riesgo alto).
- **Medidas de control:** Método de autenticación mediante usuario, contraseña y huella biométrica. Cifrado del dispositivo móvil y pseudonimización de los datos.
- **Eficacia del control:** Reduce la probabilidad a despreciable 1, debido a que, aunque se pierda el dispositivo, no será posible el acceso sin credenciales. Adicionalmente, reduce el impacto a despreciable 1, debido a que, aunque se pierda el dispositivo, los datos nunca serán identificables evitando producir daños sobre los interesados.
- **Riesgo residual:** Impacto x Probabilidad $1 \times 1 = 1$ (Riesgo bajo)

Probabilidad	Máxima 4	4	8	12	16
	Significativa 3	3	6	9 Almacenamiento de datos	12
	Limitada 2	2	4	6	8
	Despreciable 1	1 Almacenamiento de datos	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4
IMPACTO					

Bajo
 Medio
 Alto
 Muy Alto

En el [Anexo III](#), se incluye un ejemplo de plantilla donde poder documentar el proceso de gestión de riesgos, considerando las etapas de identificación, evaluación y tratamiento de los riesgos.

3.4 Conclusión

Como último paso en la realización de una EIPD, se debe elaborar un **plan de acción** donde se describan todas las medidas de control definidas para tratar los riesgos identificados y concluir con respecto al resultado obtenido.

Un plan de acción es el **conjunto de iniciativas que se deben llevar a cabo para implantar los controles que ayudan a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable**. Se recomienda que el plan de acción incluya al menos los siguientes **campos de información**:

- Control
- Descripción del control
- Responsable de implantación
- Plazo de implantación

Para la ejecución del plan de acción, se deben considerar dos posibilidades:

- a) La EIPD se ha hecho sobre un nuevo tratamiento.
- b) La EIPD se ha hecho sobre un tratamiento ya existente.

En el primer caso, el plan de acción obtenido se deberá considerar durante la fase de definición de requerimientos de la actividad de tratamiento (privacidad desde el diseño).

Si la EIPD se ha realizado sobre un tratamiento ya existente, se debe lanzar un proyecto o iniciativa para implantar las medidas incluidas en el plan de acción sobre el tratamiento actual. El responsable del tratamiento debe establecer un plazo máximo en el cual se deben implantar las medidas de control incluidas en el plan de acción. En caso de superar el plazo establecido, considerando que el riesgo residual actual del tratamiento no es aceptable, el responsable del tratamiento puede exigir que se interrumpa el tratamiento hasta la implantación de las medidas correspondientes.

La conclusión de la EIPD debe realizarse basándose en el nivel de riesgo residual obtenido durante la fase de gestión de riesgos, valorando si este es elevado o se considera aceptable y dentro de unos límites razonables.

Si la conclusión de la EIPD, **no es favorable**, se debe analizar la posibilidad de incluir medidas de control adicionales que permitan reducir el nivel de exposición al riesgo, disminuyendo el mismo hasta un nivel aceptable. Si no fuese posible el tratamiento no se podría llevar a cabo y sería necesario activar el procedimiento de consulta previa a la Autoridad de Control.

Si la conclusión de la EIPD **es favorable**, la actividad de tratamiento se puede llevar a cabo, siempre y cuando, las medidas de control incluidas en el plan de acción hayan sido implantadas.



“Si la conclusión de la EIPD, no es favorable, se debe analizar la posibilidad de incluir medidas de control adicionales”

Se recomienda realizar un proceso de supervisión durante la fase de implantación con el objetivo de garantizar y validar que las medidas de control definidas en el plan de acción han sido implantadas correctamente.

En el [Anexo IV](#), se incluye un ejemplo de plantilla donde poder documentar el Plan de Acción y la conclusión de la EIPD.

3.5 Comunicación y consulta a la autoridad de control



Artículo 36 **del RGPD**

“El responsable consultará a la Autoridad de Control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo”.

Como criterio general, siempre y cuando el resultado de la EIPD suponga que el **riesgo residual del tratamiento es alto o muy alto**, el responsable del tratamiento debe realizar una consulta a la Autoridad de Control mediante los canales de comunicación establecidos. La consulta a la Autoridad de Control y en virtud de lo que se detalla en el **apartado 3 del artículo 36 del RGPD**, deberá incluir la siguiente información:

- Las **responsabilidades** respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento.



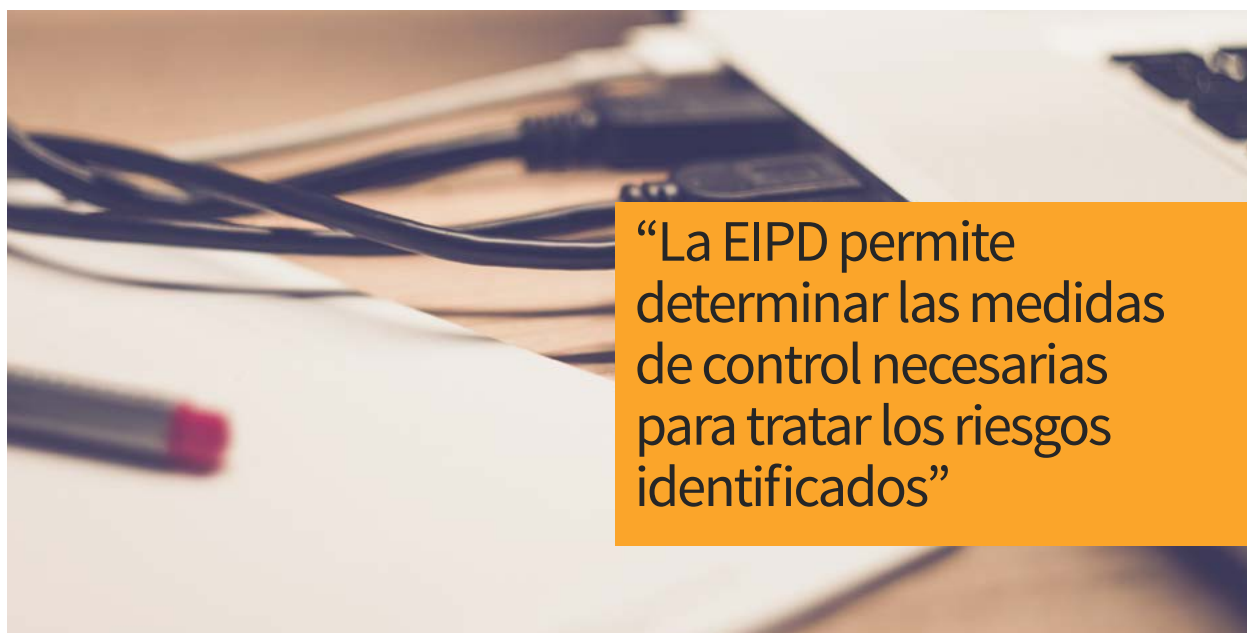
- Los **fines y medios** del tratamiento previsto.
- Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados.
- Los **datos de contacto** del DPD.
- La **EIPD**.
- Cualquier **otra información** que solicite la Autoridad de Control.

Por defecto, la EIPD debe contener toda la información requerida por el RGPD, por tanto, debe ser suficiente con entregar la EIPD, la metodología aplicada y una explicación de cómo se ha llevado a cabo.

3.6 Supervisión y revisión de la implantación

La EIPD permite determinar las medidas de control necesarias para tratar los riesgos identificados, sin embargo, no deja de ser un **ejercicio teórico que requiere su puesta en práctica** de forma íntegra para garantizar los derechos y las libertades de los interesados. Es fundamental que se realice una adecuada supervisión y una posterior revisión de la implantación de las medidas de control definidas en la EIPD para reducir el riesgo inherente hasta un riesgo residual que permita llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas.

A nivel práctico, es recomendable que una figura delegada supervise y garantice que las medidas de control definidas durante la EIPD se implantan adecuadamente antes de llevar a cabo las actividades de tratamiento de datos de carácter personal por parte del responsable del tratamiento.



4. Cuestiones clave

4.1 Si una operación de tratamiento presenta una EIPD con un riesgo elevado, ¿puedo proceder a llevar a cabo la actividad de tratamiento?

No, **en ningún caso se puede proceder a llevar a cabo el tratamiento si el riesgo es elevado**. En aquellos casos donde la EIPD se concluya con un riesgo residual elevado, el responsable del tratamiento deberá activar el **procedimiento de Consulta Previa a la Autoridad de Control local**. En función de la resolución a la que llegue la Autoridad de Control, se establecerán las condiciones y medidas que se deben aplicar para llevar a cabo el tratamiento o, si fuese de aplicación, se indicaría que en ningún caso se podrá llevar a cabo.

De igual modo, si la Autoridad de Control especifica una serie de medidas para poder realizar el tratamiento, será necesario realizar y planificar un plan de acción para implantarlas y evaluar su impacto en el cálculo del riesgo residual futuro.

4.2 ¿Cómo realizar una EIPD cuando se presta un servicio como encargado de tratamiento?

En aquellos casos donde se presta un servicio como encargado de tratamiento y no se tiene información suficiente sobre las actividades de tratamiento que se están realizando por cuenta del responsable del tratamiento, se recomienda realizar un **análisis de riesgos** sobre la tipología del servicio prestado.

En los casos donde la organización actúa como encargado de tratamiento en el marco de un contrato de prestación de servicios con un responsable del tratamiento, éste debe ser capaz de ofrecer las garantías suficientes, así como proporcionar a dicho responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones legales y las garantías que ofrece con respecto a los derechos y libertades de las personas físicas de las cuales se tratan datos.

En este sentido, el encargado de tratamiento no siempre dispone de todo el conocimiento necesario para poder determinar las medidas de control que permitan mantener un nivel de riesgo aceptable en las actividades de tratamiento que garantice los derechos y libertades de las personas físicas. Este punto es un factor clave a tener en cuenta, ya que, en función de la importancia o impacto de los tratamientos externalizados, el encargado de tratamiento deberá aplicar las medidas y controles más adecuados para **garantizar una correcta gestión de los riesgos** a los cuales se ven expuestos los datos de carácter personal.

A nivel práctico, el encargado de tratamiento debe apoyar al responsable del tratamiento en la elaboración de la EIPD. Sin embargo, como medida preventiva que facilite la interrelación con el responsable del tratamiento, un encargado de tratamiento puede realizar un análisis de los

servicios que provee e identificar los riesgos generales a los que se ve expuesto con respecto a los derechos y libertades de los interesados y establecer e inventariar las medidas de control que debe implantar para reducir el nivel de riesgo al que se ve expuesto y mantener el mismo en niveles aceptables. Por ejemplo, un servicio de *hosting*, está expuesto a riesgos que impliquen la pérdida de disponibilidad y para ello disponer de medidas de control que se basen en copias de seguridad para garantizar la seguridad de los datos de carácter personal.

4.3 ¿Cuándo se debe revisar una EIPD?

Siempre y cuando exista una **variación relevante en el contexto** de las actividades de tratamiento que pueda suponer un incremento del riesgo asociado al mismo, deberá realizarse una actualización de la EIPD.

Por ejemplo, la inclusión de un nuevo canal en un tratamiento, su automatización, externalización, etc. son ejemplos en los cuales se debería revisar la EIPD.

4.4 ¿Qué ocurre cuando se está adherido a un código de conducta?

En el caso de que el responsable del tratamiento esté adherido a algún código de conducta (art. 40 y siguientes del RGPD) donde se incluya una metodología propia, se puede **utilizar la misma para la realización de las EIPD sin eximir de la obligación de realizar la EIPD si fuese de aplicación.**



5. Anexos

5.1 Anexo I: Plantilla de análisis de documentación del ciclo de vida de los datos asociados a las actividades de tratamiento

Ciclo de vida



Información General

El siguiente formulario debe recoger toda información que permita una adecuada identificación de amenazas y valoración de los riesgos a los que están expuestos los datos de carácter personal afectados.

		CICLO DE VIDA DE LOS DATOS EN LAS OPERACIONES DEL TRATAMIENTO				
		Captura de datos	Clasificación / Almacenamiento	Uso / Tratamiento	Cesión o transferencia de los datos a un tercero para su tratamiento	Destrucción
ELEMENTOS QUE INTERVIENEN EN LAS ACTIVIDADES DE TRATAMIENTO	Actividades del proceso					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					

Roles	
Interesados	
Responsable del tratamiento	
Encargados de tratamiento	
Terceras partes involucradas	

Descripción sistemática de las operaciones y finalidades del tratamiento	
Cesiones de datos:	
Flujos de datos entre sistemas	
Productos o servicios generados por procesamiento de los datos	
Procedimiento para cumplir el deber de información, en caso de que se recojan los datos directamente del interesado	
Procedimiento para la solicitud de consentimiento, en caso de que se recojan los datos directamente del interesado	
Procedimiento para el ejercicio de los derechos por parte de los interesados (acceso, rectificación, cancelación/bloqueo, oposición y portabilidad)	
Se considera la identificación de las obligaciones y medidas de seguridad de los encargados de tratamiento en su contrato	
En caso de existir transferencias internacionales fuera del Espacio Económico Europeo, estas son adecuadamente protegidas	

5.2 Anexo II: Plantilla de análisis de la necesidad y proporcionalidad del tratamiento

Analizar la necesidad y proporcionalidad del tratamiento



1 Legitimación

Legitimación	
Justificación	

2 Evaluación de la necesidad y proporcionalidad del tratamiento

	(SI/NO)	Justificación
1 Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad)		
2 La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas/interesados afectados (principio de minimización de datos).		
3 Las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad.		
4 Los datos no se mantienen más tiempo del necesario para las finalidades del tratamiento (principio de limitación del plazo de conservación).		
Conclusión:		

5.3 Anexo III: Plantilla de gestión de riesgos

Gestión de riesgos



Información General

El siguiente formulario presenta la evaluación de riesgos realizada sobre las amenazas identificadas en las operaciones de tratamiento, hasta la determinación del riesgo residual existente, para lo cual se han de tener en cuenta las medidas de control que reducen el nivel de exposición del riesgo.

Identificación de amenazas				
Referencia de la actividad del tratamiento fuente del riesgo	Operación de tratamiento	Referencia de amenaza	Amenazas	Descripción amenaza

Valoración del riesgo inherente				
Referencia Amenaza	Riesgo	Evaluación probabilidad (1-4)*	Evaluación impacto (1-4)*	Evaluación riesgo inherente

Gráfico (Riesgo inherente)				
	1	2	3	4
5				
4				
3				
2				
1				
0				

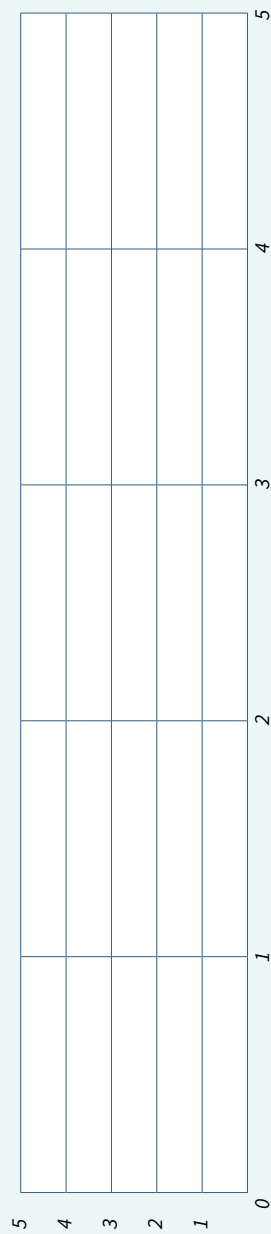
Gestión de riesgos (Continuación)



Identificación de medidas de control

[illegible]

Gráfico (Riesgo residual)



5.4 Anexo IV: Plantilla de plan de acción y conclusión

Plan de acción



Información General

Una vez se ha realizado la evaluación de riesgos sobre el tratamiento afectado por la EIPD, el presente formulario detalla el conjunto de medidas mitigantes adicionales que la entidad ha planeado implantar para reducir dichos riesgos a niveles más bajos. Las medidas de mitigación se establecen principalmente por 4 posibles causas:

- 1 Necesidad de reducir el riesgo residual asociado a alguna de las amenazas identificadas a niveles aceptables, por ser considerados actualmente “Altos” o “Muy altos”.
- 2 Criterio del responsable del tratamiento, como parte de los procesos de mejora continua o por considerarlo oportuno.
- 3 Necesidad de adoptar medidas mitigantes adicionales como fruto de cambios previstos en el ciclo de vida del tratamiento.
- 4 Aplicación de medidas adicionales como buenas prácticas que contribuyan a mejorar el nivel de protección general de los datos de carácter personal.

Identificación de medidas mitigantes planificadas

Referencia Amenaza/Riesgo	Referencia medida de control	Descripción de la medida de control	Responsable de la implantación	Fecha prevista	Estado Actual

5.5 Anexo V: Catálogo de amenazas



Información General

A continuación se recoge, a modo de ejemplo, un catálogo de amenazas pero no pretende ser ni completo ni exhaustivo por lo que se entiende que puede haber amenazas que afecten al tratamiento de los datos personales que no estén contenidas en este catálogo.

Generales

- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.
- Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento.
- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.
- Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad.
- Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.
- Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias.

Legitimación de los tratamientos y cesiones de datos personales

- Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida.
- Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.
- Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.
- Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.
- Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.
- Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardas necesarias.

Catálogo de amenazas (Continuación)



- Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada.
- Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.

Transferencias internacionales

- Acceso secreto a los datos personales por parte de autoridades de terceros países.
- Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.
- Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados.
- Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador.
- No obtención de las autorizaciones legales necesarias.

Notificación y registro de las actividades de tratamiento

- Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento.
- Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control.

Transparencia de los tratamientos.

- Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (ubicación geográfica, comportamiento, hábitos de navegación, etc.).
- En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que dificulten su acceso conjunto y detallado.
- Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.

Catálogo de amenazas (Continuación)



Calidad de los datos

- Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio.
- Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas.
- Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.
- Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas.

Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas.

Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras.

Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.

Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.

- Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo.
- Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron.

Categorías especiales de datos

- Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión.
- Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales.
- Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos.

Catálogo de amenazas (Continuación)



Deber de secreto

- Accesos no autorizados a datos personales.
- Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.

Tratamientos por encargo

- Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.
- Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento.
- Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
- No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento.
- Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.

Derechos de los interesados

- Dificultar o imposibilitar el ejercicio de los derechos de los interesados.
- Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados.
- Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.

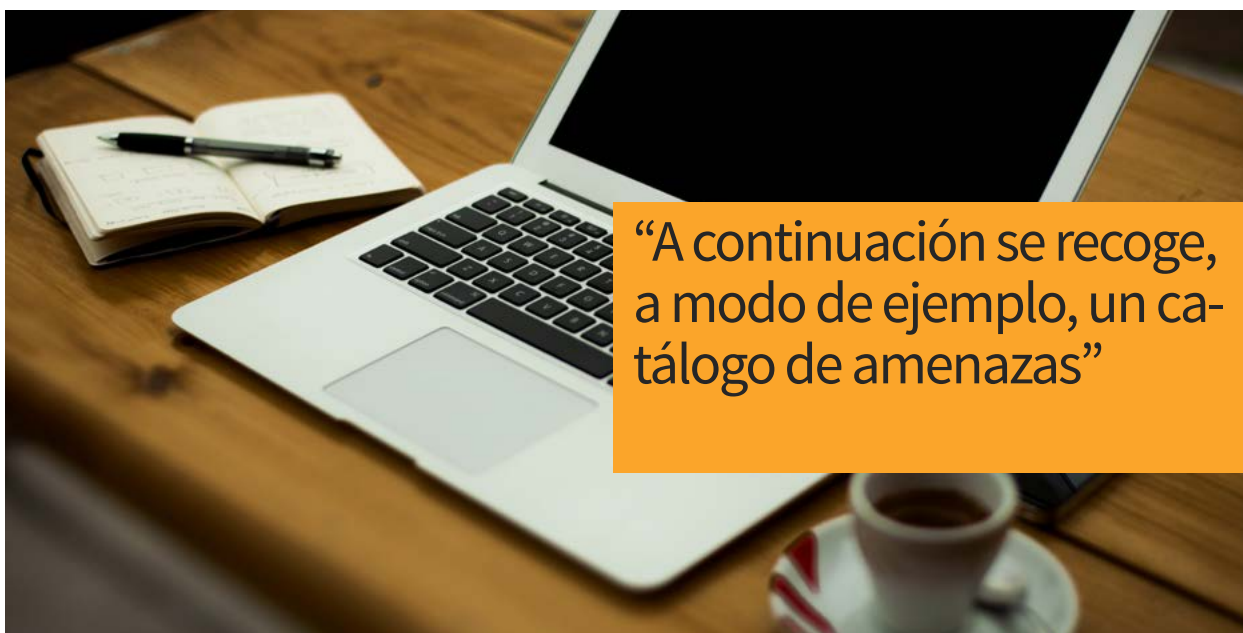
Seguridad

- Inexistencia de responsable de seguridad o deficiente definición de sus funciones y competencias.
- Inexistencia de política de seguridad.
- Deficiencias organizativas en la gestión del control de accesos.
- Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.

Catálogo de amenazas (Continuación)



- Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.
- Uso de identificadores que revelan información del afectado.
- Deficiencias en la protección de la confidencialidad de la información.
- Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.
- Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.



“A continuación se recoge, a modo de ejemplo, un catálogo de amenazas”

5.6 Anexo VI: Catálogo de amenazas y posibles soluciones



Información General

A continuación se recoge, a modo de ejemplo, un catálogo de amenazas y posibles soluciones pero no pretende ser ni completo ni exhaustivo por lo que se entiende que puede haber amenazas que afecten al tratamiento de los datos personales que no estén contenidas en este catálogo así como soluciones distintas de las propuestas.

Generales	
Amenazas	Soluciones
Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.	■ Formación apropiada del personal sobre protección de datos. ■ Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas.
Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento.	■ Formación apropiada del personal sobre protección de datos en el sector específico de que se trate. ■ Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización relativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas.
Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.	■ Formación apropiada del personal sobre seguridad y uso adecuado de las TIC. ■ Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas.
Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad de las personas.	■ Formación apropiada del personal sobre protección de datos, seguridad y uso adecuado de las TIC.

Catálogo de amenazas y posibles soluciones (Continuación)



Generales	
Amenazas	Soluciones
Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	■ Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella.
	■ Nombrar un Delegado de Protección de Datos o Data Protection Officer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados.
Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias.	■ Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPO en las fases iniciales de los mismos.
	■ Establecer desde la dirección las funciones, competencias y atribuciones del DPO en el desarrollo y gestión de los proyectos.

Catálogo de amenazas y posibles soluciones (Continuación)



Legitimación de los tratamientos y cesiones de datos personales	
Amenazas	Soluciones
Tratar datos personales cuando no es necesario para la finalidad perseguida.	■ Usar datos disociados siempre que sea posible y no implique un esfuerzo desproporcionado. ■ Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas. ■ Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. ■ Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificado.
Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.	■ Formación adecuada del personal sobre protección de datos, seguridad y uso adecuado de las TIC. ■ Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas. ■ Si es necesario, buscar asesoramiento experto. ■ Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones ulteriores así como las posibilidades de supervisión y control del cumplimiento del acuerdo.

Catálogo de amenazas y posibles soluciones (Continuación)



Legitimación de los tratamientos y cesiones de datos personales	
Amenazas	Soluciones
Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	■ Asegurarse de que no existen otras causas de legitimación más adecuadas.
	■ Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato.
	■ Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes.
	■ En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores.
Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.	■ Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas.
	■ Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas.
	■ Establecer los mecanismos necesarios para garantizar que se consultan los ficheros de exclusión de publicidad, tanto de la organización como externos, y que se tienen en cuenta los deseos de quienes se han inscrito en ellos.

Catálogo de amenazas y posibles soluciones (Continuación)



Legitimación de los tratamientos y cesiones de datos personales

Amenazas	Soluciones
Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.	■ Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido legal y lealmente. ■ En la realización de campañas publicitarias con datos provenientes de terceros en las que se segmenta el público objetivo en función de parámetros determinados, exigir garantías de que las personas cuyos datos van a ser utilizados han dado su consentimiento para ello.
Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.	■ Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas. ■ Verificar si el tratamiento está amparado o es requerido por una ley. ■ En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada.	■ Verificar la legitimidad de la interconexión de datos prevista. ■ Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado.
Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada.	■ Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.). ■ Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. ■ Respetar las preferencias establecidas por los afectados en sus navegadores sobre el rastreo de su navegación.

Catálogo de amenazas y posibles soluciones (Continuación)



Transferencias Internacionales

Amenazas	Soluciones
Acceso secreto a los datos personales por parte de autoridades de terceros países.	■ Incluir cláusulas de salvaguarda en las que se requiera información sobre el acceso a los datos personales transferidos por parte de autoridades de terceros países tan pronto como sea posible.
Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.	■ Si existen transferencias internacionales a países fuera del Espacio Económico Europeo, implantar los procedimientos de control necesarios (incluidos los contractuales) para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia. En este sentido, hay que prestar especial atención cuando se contraten servicios de cloudcomputing u hospedados en terceros.
Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados.	■ Asegurarse de la exigibilidad de mecanismos de control del importador tales como listas de encargados de tratamiento, países donde operan, posibilidad de revisar documentación y realizar auditorías, etc.
Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador.	■ Asegurarse de la definición y funcionamiento de un canal de comunicación entre exportador e importador para hacer llegar las solicitudes y reclamaciones de los afectados. ■ Poner en marcha procedimientos que garanticen la adecuada atención de las demandas de los afectados.
No obtención de las autorizaciones legales necesarias.	■ Solicitar la autorización del Director de la Agencia Española de Protección de Datos en aquellos casos que resulte necesario.

Catálogo de amenazas y posibles soluciones (Continuación)



Notificación y Registro de las Actividades de Tratamiento

Amenazas	Soluciones
Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento.	■ Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo.
Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control.	■ Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo.

Transparencia de los tratamientos

Amenazas	Soluciones
Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.).	■ Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. ■ Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada.
En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado.	■ Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. ■ Verificar que la información que se ofrece en todos los lugares y situaciones es coherente y sistemática. ■ Verificar que la información se ofrece en todos los formularios.

Catálogo de amenazas y posibles soluciones (Continuación)



Transparencia de los tratamientos

Amenazas	Soluciones
Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.	■ Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.

Calidad de los datos

Amenazas	Soluciones
Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio.	■ Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.
Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas.	■ Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlos.
Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.	■ Siempre que sea posible, utilizar datos anónimos o disociados. ■ Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. ■ Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados.

Catálogo de amenazas y posibles soluciones (Continuación)



Calidad de los datos	
Amenazas	Soluciones
Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas: • Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas. • Toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras.	■ Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible. ■ Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona. ■ Proporcionar información sobre las medidas que se han implantado para lograr el necesario equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los afectados.
• Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas. • Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas. Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo.	■ Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. ■ Establecer posibilidades de impugnación ágiles para ofrecer vías de recurso adecuadas a los afectados. ■ Establecer canales alternativos para tratar con los falsos negativos y falsos positivos en la identificación y autenticación de personas a través de datos biométricos.
Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron.	■ Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información. ■ Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información. ■ Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales.

Catálogo de amenazas y posibles soluciones (Continuación)



Categorías Especiales de Datos

Amenazas	Soluciones
Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión.	■ Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario. ■ Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales.	■ Nombrar un Delegado de Protección de Datos o Data Protection Officer (DPO) para contar con asesoramiento cualificado.
Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos.	■ Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación es mínimo.

Deber de secreto

Amenazas	Soluciones
Accesos no autorizados a datos personales.	■ Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. ■ Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización. ■ Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento. ■ Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales. ■ Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.

Catálogo de amenazas y posibles soluciones (Continuación)



Deber de secreto

Amenazas	Soluciones
Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.	■ Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. ■ Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas.

Tratamientos por Encargo

Amenazas	Soluciones
Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	■ Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.
Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento.	■ Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia. ■ Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros.
Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.	■ Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento. ■ Realizar auditorías periódicas al encargado de tratamiento para verificar que cumple las estipulaciones del contrato. ■ Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas.
No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento.	■ Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados. ■ Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente.

Catálogo de amenazas y posibles soluciones (Continuación)



Tratamientos por Encargo

Amenazas	Soluciones
Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.	■ Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. ■ Establecer medidas técnicas y organizativas que garanticen la portabilidad.

Derechos de los Interesados

Amenazas	Soluciones
Dificultar o imposibilitar el ejercicio de los derechos de los interesados.	■ Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos. ■ Evitar sistemas de ejercicio de los derechos de los interesados que impliquen solicitar una remuneración. ■ Evitar establecer procedimientos poco transparentes, complejos y laboriosos. ■ Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho de los interesados o ha de informar a los afectados sobre cómo ejercerla. ■ Definir qué personas o departamentos se ocuparán de gestionar los derechos de los interesados y formarlos adecuadamente.

Catálogo de amenazas y posibles soluciones (Continuación)



Derechos de los Interesados

Amenazas	Soluciones
Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados.	■ Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados. ■ Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados.
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.	■ Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate. ■ Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos. ■ Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados.

Seguridad

Amenazas	Soluciones
Carencia de medidas de seguridad o aplicación deficiente las mismas. Indefinición de funciones de seguridad y de establecimiento de competencias.	■ Nombramiento de un responsable de seguridad y establecimiento por parte de la dirección de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos. ■ Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del responsable de seguridad en las fases iniciales de los mismos.

Catálogo de amenazas y posibles soluciones (Continuación)



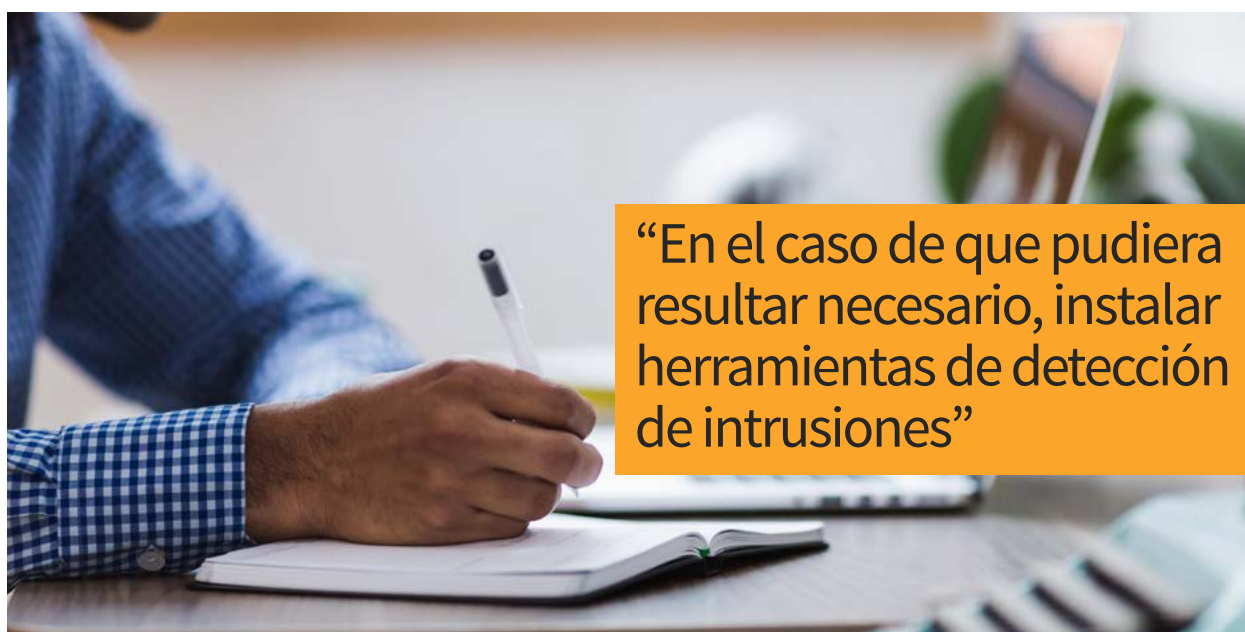
Seguridad	
Amenazas	Soluciones
Deficiencias organizativas en la gestión del control de accesos.	■ Políticas estrictas de acceso a la información por necesidad de conocer (need to know) para la concesión de accesos a la información y de escritorios limpios de documentación (cleandesks) para minimizar las posibilidades de acceso no autorizado a los datos personales. ■ Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.). ■ Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones.
Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	■ Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales. ■ En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (IDS o IntrusionDetectionSystems) y/o de prevención de intrusiones (IPS o IntrusionPreventionSystems) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad. ■ En la medida que pudiera resultar necesario, implantar sistemas de Prevención de Pérdida de Datos (DLP o Data LossPrevention) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.

Catálogo de amenazas y posibles soluciones (Continuación)



Seguridad

Amenazas	Soluciones
Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.	■ Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes.
Uso de identificadores que revelan información del afectado.	■ Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales como fecha de nacimiento, nombre y apellidos, etc. ■ Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o similares, ya que favorecen el fraude en la identificación e incluso la suplantación de identidad.



“En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones”

6. Referencias

- ISO/IEC 27005:2008 Tecnologías de la Información – Técnicas de Seguridad – Gestión de riesgos de seguridad de la Información.
- ISO 31010 de Gestión y Evaluación de Riesgos
- ISO 29134 Tecnologías de la información – Guías para las Evaluaciones de Impacto en la Protección de los Datos
- WP248 Guía sobre las Evaluaciones de Impacto en Protección de datos – Grupo Europeo Artículo 29

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



www.agpd.es