AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUIA PRÁCTICA DE ANÁLISIS DE RIESGOS EN LOS TRATAMIENTOS DE DATOS PERSONALES SUJETOS AL RGPD

Índice

1. Introducción

El **25 de mayo de 2018** se cumplen dos años desde la entrada en vigor del **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. Desde ese momento, será aplicable el RGPD y será obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la **necesidad de llevar a cabo un análisis de riesgos** con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, 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 personales hacia un nuevo modelo más dinámico, enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño.

El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo. De igual modo, es el momento idóneo para definir las **medidas de control y seguridad** para garantizar los derechos y libertades de los interesados con el objetivo de que un tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo a la que está expuesto.

La Agencia Española de Protección de Datos (AEPD) ha elaborado la presente guía para la realización de análisis de riesgos de las actividades de tratamiento con el objetivo de establecer una hoja de ruta para afrontar un enfoque orientado a riesgos.

La guía persigue ofrecer directrices y orientaciones para establecer una hoja de ruta que permita contemplar la privacidad desde el inicio, mediante un enfoque de análisis de riesgos, facilitando el cumplimiento del RGPD.

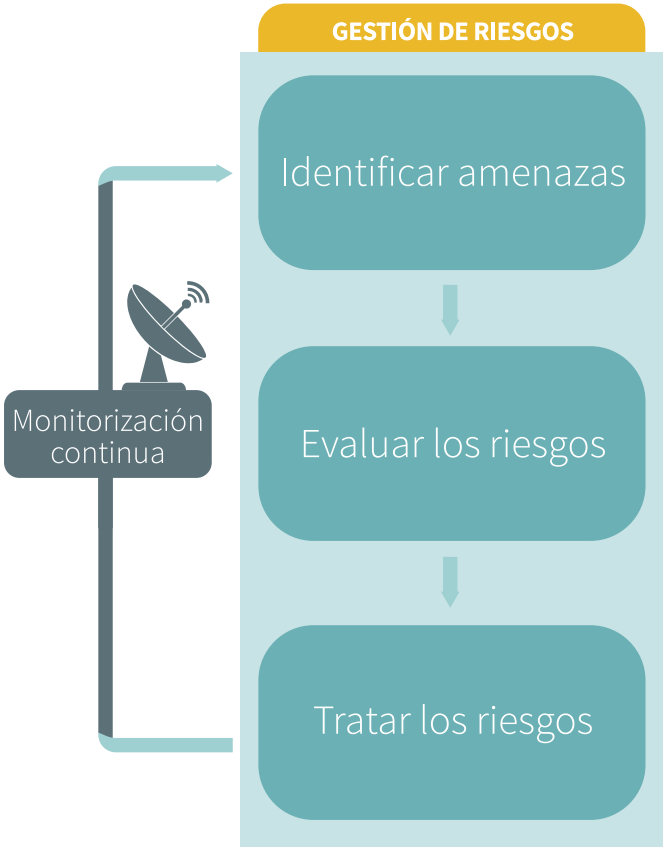
> "Esta guía se ha creado con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades"

2. Consideraciones generales

Conceptos generales sobre gestión de riesgos

Gestión de riesgos es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.

La gestión de riesgos se puede dividir en **tres etapas** diferenciadas: La identificación, la evaluación y el tratamiento de los riesgos.



Identificar amenazas y riesgos

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

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. Si ponemos el foco en la protección de los datos, las amenazas se pueden categorizar principalmente en tres tipos:

Acceso ilegítimo a los datos: ¿qué daño causaría que lo conociera quien no debe? ➡ confidencialidad

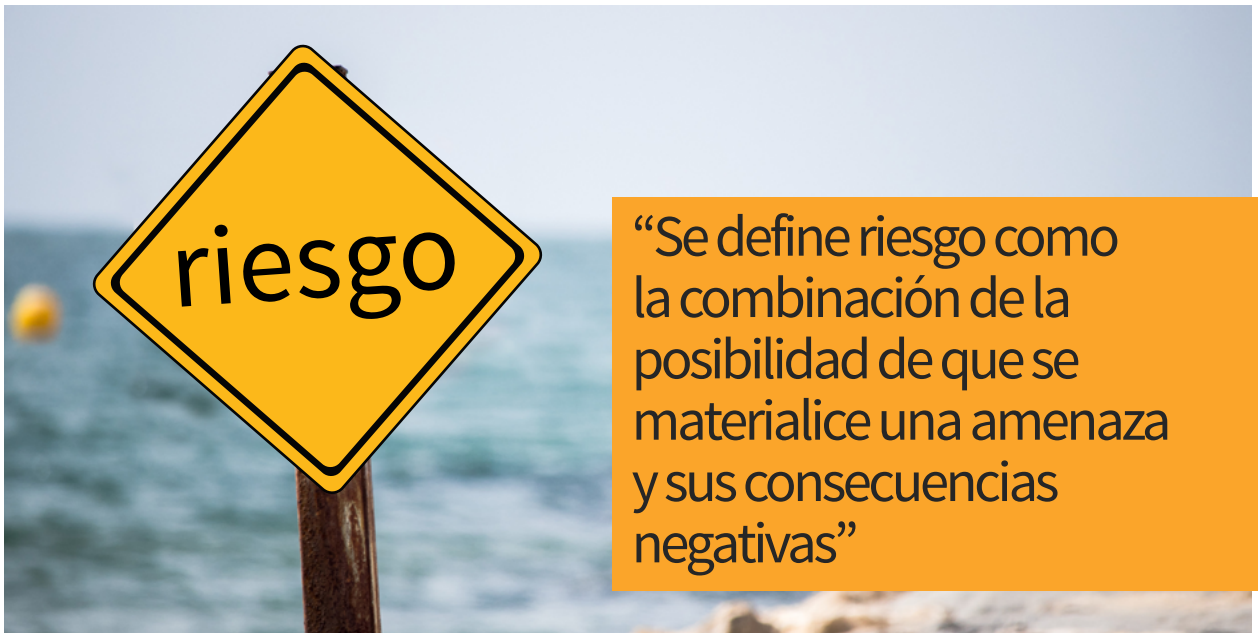
Modificación no autorizada de los datos: ¿qué perjuicio causaría que estuviera dañado o corrupto? ➡ integridad

Eliminación de los datos: ¿qué perjuicio causaría no tener un dato o no poder utilizarlo? ➡ disponibilidad.

Un **riesgo** se puede definir como la combinación de la **posibilidad de que se materialice una amenaza y sus consecuencias negativas**. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar.

Evaluar los riesgos

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en **valorar el impacto de la exposición a la amenaza**, junto a la **probabilidad de que esta se materialice. El impacto**, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre el interesado o, por el contrario, un impacto sería significativo si el daño ocasionado sobre los derechos y liberta-



"Se define riesgo como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas"

des del interesado fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente.

Tratar los riesgos

La última fase 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 reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.

Gestión de riesgos, ¿qué implicaciones tiene en la protección de los datos?

La gestión de riesgos es una actividad común hoy en día en las compañías, utilizada en múltiples ámbitos y con un enfoque dirigido a los potenciales daños o riesgos a los que está expuesta la compañía con respecto a una tipología concreta de amenazas.

El RGPD busca aprovechar las ventajas que ofrece la gestión de riesgos, pero introduce una nueva visión, donde el foco de atención no se centra en las amenazas que se ciernen sobre la compañía, centrando su atención en las amenazas sobre los derechos y libertades de los interesados. La evaluación de los riesgos debe ser el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen sobre los interesados. Se trata de establecer hasta qué punto una actividad de tratamiento, por sus características, el tipo de datos a los que se refiere o el tipo de operaciones puede causar un daño a los interesados. Este enfoque implica estimar el daño y la tipología de daño que se puede producir sobre los interesados, por ejemplo, un daño material derivado de la vulneración de sus derechos y libertades.

3. Protección de datos desde el diseño y la gestión de riesgos: ¿cuál debe ser la hoja de ruta a seguir?

La exposición a los riesgos con impacto en la protección de datos se produce desde el inicio o puesta en marcha de los tratamientos, evolucionando en función de las variaciones del contexto y de factores o elementos que intervienen en las mismas.

El RGPD, consciente de que un tratamiento nace expuesto a riesgos con impacto en la protección de los datos, introduce los conceptos de *"protección de datos desde el diseño y por defecto"*.

Apartado 1 ***del artículo 25 del RGPD:***

"Teniendo en cuenta el ***estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas,*** *el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento,* ***medidas técnicas y organizativas apropiadas,*** *como la seudonimización, concebidas* ***para aplicar de forma efectiva los principios de protección de datos,*** *como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".*

Apartado 2 ***del artículo 25***

"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".

Ambos conceptos, tienen como premisa, garantizar los derechos y libertades de los interesados desde la definición de una actividad de tratamiento.

El responsable del tratamiento que realiza o desea realizar actividades de tratamiento con datos personales, debe establecer procedimientos de control que garanticen cumplir los principios de protección desde el diseño y por defecto.

Definir y establecer medidas de control y seguridad es una tarea fundamental que se debe realizar de acuerdo a las particularidades de las actividades de tratamiento.

Artículo 32 ***Seguridad del tratamiento:***

1 *Teniendo en cuenta el* ***estado de la técnica,*** *los* ***costes de aplicación,*** *y la* ***naturaleza,*** *el* ***alcance,*** *el* ***contexto*** *y los* ***fines del tratamiento,*** *así como* ***riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas,*** *el responsable y el encargado del tratamiento* ***aplicarán medidas técnicas y organizativas apropiadas*** *para* ***garantizar un nivel de seguridad adecuado al riesgo,*** *que en su caso incluya, entre otros:*

a *la seudonimización y el cifrado de datos personales;*

b *la capacidad de* ***garantizar*** la ***confidencialidad, integridad, disponibilidad*** y ***resiliencia permanentes*** *de los* ***sistemas y servicios de tratamiento;***

c la ***capacidad de restaurar la disponibilidad*** *y el acceso a los datos personales de forma rápida* ***en caso de incidente físico o técnico;***

d *un* ***proceso de verificación, evaluación y valoración regulares de la eficacia*** *de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2 *Al* ***evaluar la adecuación del nivel de seguridad*** *se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*

"El responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas"

Con el objetivo de establecer la relación entre los conceptos de "privacidad desde el diseño y por defecto" y las medidas de control y seguridad que se deben definir e implantar para garantizar los derechos y libertades de los interesados en las actividades de tratamiento, a continuación, se describe un posible flujo de trabajo con la hoja de ruta a seguir por parte de un responsable de tratamiento que quiera llevar a cabo una actividad de tratamiento:

Definición y diseño de las actividades de tratamiento

La definición de una actividad de tratamiento es un paso fundamental que requiere tener claro cuáles son las finalidades del tratamiento de datos personales.

Corresponde a cada organización, de acuerdo al principio de responsabilidad proactiva (*accountability*), decidir el **nivel de agregación o segregación** para elaborar el registro de actividades de tratamiento y deberá valorar hasta qué punto esa agregación o segregación corresponde con finalidades, bases jurídicas y grupos de individuos distintos.

Asimismo corresponde ponderar, como se hizo con anterioridad a la hora de definir ficheros, la **optimización de la gestión de la protección de datos** dentro de su organización para que esta resulte **útil, ágil, efectiva** y permita alcanzar los objetivos que la legislación busca: que los individuos cuyos datos son objeto de tratamiento puedan tener, en su caso, un conocimiento efectivo de los tratamientos que la organización realiza sobre ellos.

Puede resultar útil al responsable y al encargado del tratamiento, a la hora de elaborar el registro de actividades de tratamiento, **volver la vista a los ficheros** que la organización hubiera descrito con anterioridad para comprobar, si todos los tratamientos sobre datos de carácter personal que la entidad realiza están recogidos en ellos, si el nivel separación o división sigue siendo el adecuado o no y corresponde segregar o, por el contrario, aproximar finalidades en una única actividad de tratamiento puesto que la finalidad es la misma, corresponde a una base jurídica única y el colectivo de afectados es el mismo.

> "La AEPD incluye la posibilidad de obtener una copia del contenido completo de la declaración de sus ficheros"

Una vez incorporadas al registro de tratamientos de la entidad todas aquellas actividades que corresponden al trabajo o funciones que esta realiza sobre los datos de carácter personal de los colectivos de personas que maneja, deberá fijarse en las nuevas obligaciones que el RGPD describe sobre el responsable del tratamiento y el encargado de tratamiento. **¿Suponen estas nuevas obligaciones la generación de nuevas actividades de tratamiento que deban ser descritas e incorporadas al registro de actividades?**

El RGPD establece en el **artículo 5** los siguientes principios relativos al tratamiento de datos personales que es necesario considerar en la definición de un tratamiento:

- **Licitud, lealtad y transparencia:** Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

- **Limitación de la finalidad:** Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

- **Minimización de datos:** Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

- **Exactitud:** Los datos deben ser exactos, y si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.

- **Limitación del plazo de conservación:** Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

- **Integridad y confidencialidad:** Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

Adicionalmente, el **artículo 5** del RPGD establece que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al tratamiento, así como, la figura responsable de demostrarlo. Por tanto, es fundamental **definir adecuadamente las actividades de tratamiento** y documentar los análisis realizados, así como, dejar trazabilidad de los mismos y de las conclusiones que los soportan para poder garantizar la responsabilidad proactiva.

A continuación, se describen diferentes métodos de análisis que permiten determinar el tipo de riesgo asociado a los tratamientos y seguir la hoja de ruta más adecuada para establecer medidas de control considerando los riesgos a los que están expuestas las actividades de tratamiento.

FACILITA: Herramienta para tratamientos de escaso riesgo

Las actividades de tratamiento deben ser evaluadas con el objetivo de determinar el potencial riesgo al que están expuestas. Con el fin de determinar si un tratamiento entraña **escaso riesgo,** la Agencia Española de Protección de Datos ha puesto a disposición de los responsables de tratamiento de datos personales la herramienta **Facilita_RGPD**, destinada a aquellas

personas y empresas que realizan tratamientos de datos personales que, a priori, implicarían un escaso nivel de riesgo para los derechos y libertades de los interesados cuyos datos tratan, teniendo en cuenta que todo tratamiento conlleva un cierto nivel de riesgo.

Para las personas y entidades que no encuentren cubiertas sus necesidades por la herramienta **Facilita_RGPD**, se debe evaluar si las actividades de tratamiento entrañan un **alto riesgo** para los derechos y libertades del interesado. El siguiente paso en la hoja de ruta, será analizar, para cada actividad de tratamiento, si entraña un riesgo alto con el objetivo de determinar si se requiere una evaluación de impacto relativa a la protección de datos (EIPD).

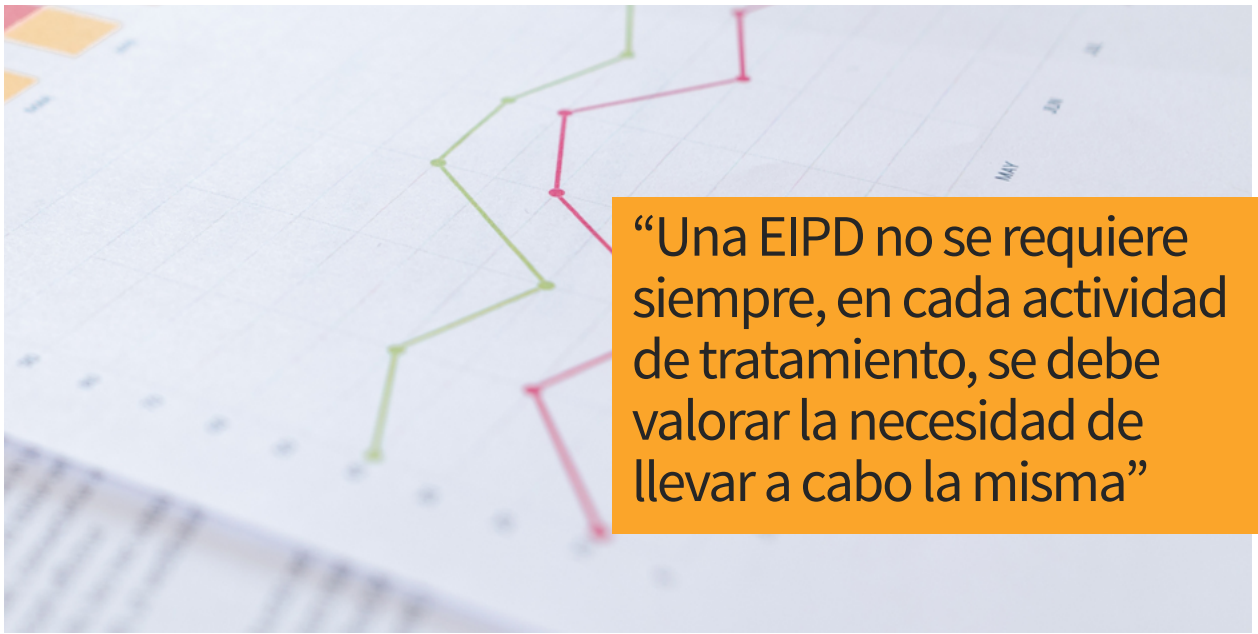
Análisis de la necesidad de realizar una Evaluación de Impacto sobre la Protección de los Datos: ¿Cuándo se debe realizar una EIPD?

Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar un **análisis previo** para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.

Del resultado del análisis sobre la necesidad de realizar una EIPD se puede concluir que:

- **Sí es necesario realizar una EIPD:** Se realizará y documentará una EIPD con todas sus fases (Ver Guía de Evaluación de Impacto en la Protección de Datos).

- **No es necesario realizar una EIPD:** Se entiende que las actividades de tratamiento no están expuestas a riesgos relevantes que motiven la necesidad de realizar una EIPD en profundidad. Si como resultado del análisis previo se considera que no es necesario llevar a cabo una EIPD, se debe documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis (responsabilidad proactiva).



> “Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma”

¿Qué criterios se deben seguir para analizar la necesidad de llevar a cabo o no una EIPD?
Para determinar si es necesario llevar a cabo la EIPD o no, se puede seguir una breve metodología de análisis constituida por dos fases:

- Análisis de las listas de tratamientos previstos en la regulación (art 35.3, 35.4, y 35.5)
- Análisis de la naturaleza, alcance, contexto y fines de tratamiento (art 35.1)

Fase I: Análisis de las listas de tratamientos previstos en la regulación (art 35.3, 35.4, y 35.5)

La regulación establece supuestos en los cuales es obligatorio realizar la EIPD sin necesidad de realizar un análisis de riesgos, por tanto, la comprobación de las listas y supuestos incluidos en la regulación, debe ser el primer paso para determinar la necesidad de llevar a cabo una EIPD.

El artículo 35.3, tal y como se ha indicado en la anterior sección, recoge **tres casos en los que es obligatorio hacer la EIPD**. Adicionalmente, el RGPD en los artículos 35.4 y 35.5 prevé la existencia de listas elaboradas por las autoridades de control que determinen en que casuísticas es obligatoria la realización de una EIPD, así como, en que casuísticas estaría excluida la necesidad de realizar una EIPD.

Si el tratamiento aparece en la lista de tratamientos que requieren la EIPD (art 35.4), que debe elaborar cada autoridad de control y validar el Comité Europeo de Protección de datos, se deberá documentar la casuística concreta en el informe de análisis de la necesidad de realizar la EIPD y proceder a iniciar la misma.

Si se considera que el tratamiento se incluye en la lista de tratamientos excluidos (art 35.5), es necesario garantizar que efectivamente el tratamiento encaja en esa casuística sin lugar a dudas y, si ese fuese el caso, se debe documentar y concluir que no es necesario llevar a cabo una EIPD.

Es importante destacar que, si el tratamiento no está incluido en los supuestos comentados y en ninguna de las listas, no implica que no sea necesario llevar a cabo la EIPD, y en todo caso, será necesario pasar a la segunda fase de análisis.

Fase II: Análisis de la naturaleza, alcance, contexto y fines de tratamiento (art 35.1)

La segunda fase de análisis se centra en evaluar las características de las actividades de tratamiento a realizar según los aspectos previstos en el artículo 35.1 del RGPD (naturaleza, alcance, contexto y finalidades del tratamiento).

Sobre cada uno de los aspectos, se deben tener en cuenta las siguientes consideraciones:

- **Naturaleza del tratamiento:** Se deben valorar las características más básicas del tratamiento y ver si estas pueden implicar un alto riesgo. Por ejemplo:

  - ¿Se tratan categorías especiales de datos?
  - ¿Se tratan datos a gran escala?

- ¿Se hace un seguimiento exhaustivo de las personas?
- ¿Se combinan diferentes conjuntos de datos? (fuentes de información diferentes)
- ¿Los datos se refieren a personas en situación de vulnerabilidad?

- **Alcance del tratamiento:** Se deben valorar los efectos o consecuencias del tratamiento, identificando hasta qué punto puede llegar y si éste puede suponer un alto riesgo. Por ejemplo:

  - ¿Se realiza un proceso de toma de decisiones con efectos jurídicos?
  - ¿Se realiza una valoración de riesgo crediticio?
  - ¿Se valora la exclusión de beneficios sociales o fiscales?

- **Contexto del tratamiento:** Se debe valorar el conjunto de circunstancias bajo las cuales se realizarán las actividades de tratamiento, con el objetivo de verificar si pueden suponer un alto riesgo. Por ejemplo:

  - ¿Se realiza un uso de nuevas tecnológicas? ¿son especialmente invasivas para la privacidad?
  - ¿Existen varios responsables del tratamiento?
  - ¿Existen cadenas complejas de encargados de tratamiento?
  - ¿Se producen transferencias internacionales?
  - ¿Existen cesiones de datos?

- **Finalidades del tratamiento:** Se deben identificar cada una de las finalidades del tratamiento y analizar si estas derivan en un alto riesgo. Por ejemplo, si la finalidad incluye:

  - Toma de decisiones
  - Elaboración de perfiles
  - Análisis predictivo
  - Prestación de servicios relacionados con la salud
  - Seguimiento, control y observación de personas (monitorización)

> “Se debe valorar el conjunto de circunstancias bajo las cuales se realizarán las actividades de tratamiento”

¿Qué dice la regulación?

Con carácter general, hay que realizar una EIPD cuando un tratamiento **puede suponer un alto riesgo para los derechos y las libertades de las personas físicas**, especialmente (pero no exclusivamente), si se utilizan nuevas tecnologías y teniendo en cuenta la **naturaleza, alcance, contexto o finalidades** del tratamiento (considerando 76 y artículo 35.1 del RGPD).

Derechos y libertades son todos aquellos reconocidos como fundamentales para el ordenamiento jurídico, incluidos los recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, donde se incluye el derecho a la protección de los datos de carácter personal.

El **artículo 35.3** del RGPD describe los siguientes casos en los cuales se ha considerado que un tratamiento puede derivar en riesgos elevados:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado como la elaboración de perfiles y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten de modo similar.

- Tratamiento a gran escala de las categorías especiales de datos personales, o datos sobre condenas e infracciones penales o medidas de seguridad conexas.

- Observación sistemática a gran escala de una zona de acceso público.

Adicionalmente, con el objetivo de poder determinar qué tipo de tratamientos pueden considerarse de alto riesgo, el GT29 en el documento ***WP248 Directrices sobre las Evaluaciones de Impacto en la Protección de Datos*** introduce criterios que pueden evidenciar un elevado riesgo inherente a las actividades de tratamiento y que, se deben evaluar y pueden determinar la necesidad de realizar un EIPD:

Tipo de tratamiento	DESCRIPCIÓN
Evaluación o scoring	Valoraciones y análisis, incluidos la elaboración de perfiles y predicciones, especialmente de “aspectos relacionados con el desempeño del interesado en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos”.
Toma de decisiones automatizada con efecto legal o similar	Procesamiento que tiene como objetivo la toma de decisiones sobre sujetos que producen “efectos legales sobre la persona física” o que “de manera similar afecta significativamente a la persona física”. Por ejemplo, si el procesamiento puede conducir a la exclusión o discriminación de las personas.

Monitorización sistemática	Procesamiento utilizado para observar o controlar a los interesados, incluidos los datos recopilados a través de redes o un sistema de control de un área de acceso público[2] .
Datos confidenciales o de naturaleza altamente personal	Actividades de tratamiento con categorías especiales de datos personales, por ejemplo, información sobre las opiniones políticas de los individuos o registros médicos, así como datos personales relacionados con condenas penales o delitos.
Coincidencia o combinación de conjuntos de datos	Actividades de tratamiento que implican la combinación de conjuntos de datos. Por ejemplo, procedentes de dos o más actividades de tratamiento de datos realizadas para diferentes propósitos y/o por diferentes responsables del tratamiento de una manera que exceda las expectativas razonables del sujeto de datos.
Datos relativos a las personas vulnerables	Los sujetos de datos vulnerables pueden incluir menores, segmentos más vulnerables de la población que requieren protección especial (personas con enfermedades mentales, solicitantes de asilo o ancianos, pacientes, etc.).
Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas	Actividades de tratamiento realizadas mediante el uso de tecnología innovadora que pueda implicar nuevas formas de recopilación y uso de datos, posiblemente con un alto riesgo para los derechos y las libertades de las personas. Por ejemplo, la combinación del uso de la huella dactilar y el reconocimiento facial para mejorar el control del acceso físico, etc.
Cuando el procesamiento en sí mismo "impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato"	Operaciones de procesamiento que tienen como objetivo permitir, modificar o rechazar el acceso de los interesados a un servicio o la entrada en un contrato.
Tratamientos sujetos a un código de conducta que lo requiere	Si a los tratamientos evaluados se les aplica un código de conducta que exige su cumplimiento también debe ser objeto de la evaluación.

El GT29 considera que cuantos más de los criterios mencionados cumplan un tratamiento, u operaciones concretas del tratamiento, más probable es que suponga un alto riesgo para los derechos y las libertades de los interesados. Sin embargo, el responsable del tratamiento puede considerar que, por la naturaleza del tratamiento, aunque los tratamientos cumplen varios de los criterios mencionados, realmente no hay un probable alto riesgo. En este caso, hay que documentar y argumentar de forma clara las razones por las que no se lleva a cabo la EIPD.

En el otro extremo, para aquellos tratamientos para los cuales no es necesario realizar una EIPD, el GT 29 establece también ciertos supuestos. Así lo considera, por ejemplo, cuando la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a las de un tratamiento para el que ya se ha hecho una evaluación, o cuando el tratamiento tiene como base jurídica el derecho del Espacio Económico Europeo o del Estado miembro y la EIPD ya se

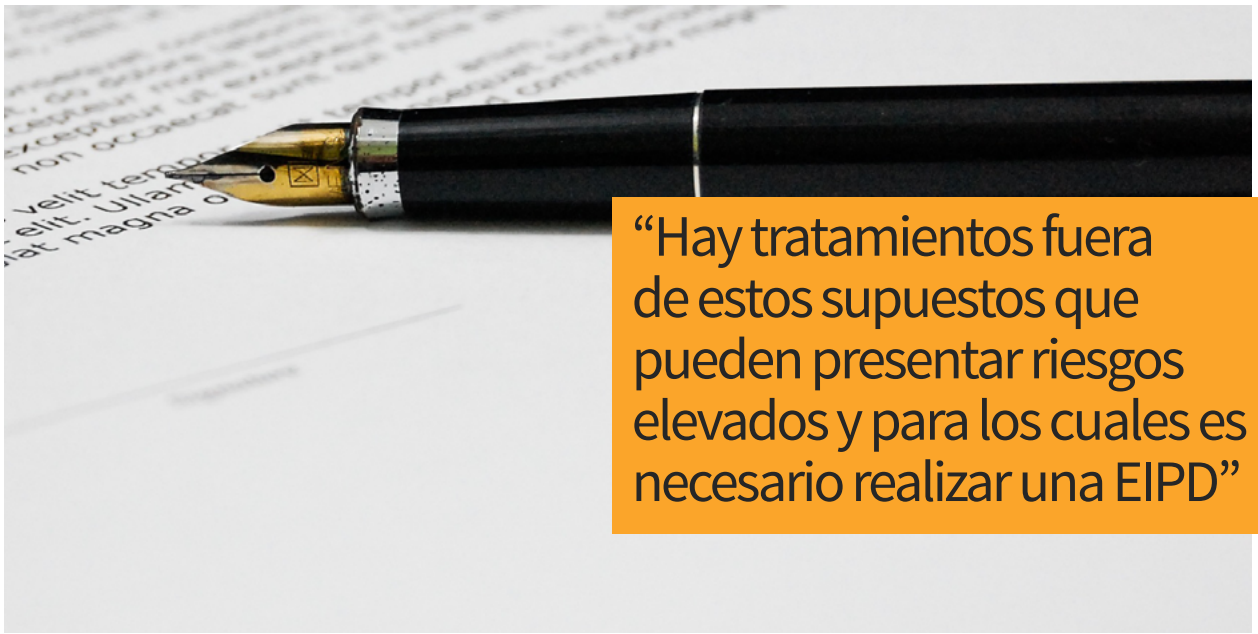
2 Se deberá distinguir siempre lo que corresponde lo que corresponde a un sistema de Videovigilancia para la seguridad de un proceso de observación sistemática con otros fines como el estudio de rutas de clientes sobre un espacio físico con objeto de optimizar la distribución de mercancía en una tienda.

ha hecho en este contexto. En ambos casos se debe argumentar que efectivamente, nos encontramos ante un tratamiento que encaja claramente en estas circunstancias y por tanto no es necesario llevar a cabo la evaluación.

Sin embargo, la regulación no se cierne exclusivamente a las casuísticas mencionadas, no se establece o enumera una lista de tratamientos concreta a la que se limite la necesidad de realizar una EIPD, por tanto, hay tratamientos fuera de estos supuestos que pueden presentar riesgos elevados y para los cuales es necesario realizar una EIPD. En aquellos casos en los que no esté claro la necesidad o no de llevar a cabo una EIPD, es recomendable la realización de la misma.

Tomando en consideración cada uno de los aspectos descritos y realizando una breve evaluación de los mismos, se puede determinar si hay necesidad o no de llevar a cabo la EIPD. Es imprescindible elaborar un informe donde se describan los criterios seguidos y los argumentos en los que se basa la conclusión para determinar si es necesario, o no, realizar la EIPD.

Como herramienta soporte para el análisis inicial que permita determinar la necesidad de realizar una EIPD, y a su vez para poder acreditar su realización, se adjunta en el Anexo I un ejemplo de plantilla con posibles cuestiones a tener en cuenta para analizar la necesidad de realizar una EIPD.



> “Hay tratamientos fuera de estos supuestos que pueden presentar riesgos elevados y para los cuales es necesario realizar una EIPD”

4. Registro de actividades de tratamiento

Descripción: ¿Qué es un registro de actividades de tratamiento?

Apartado 1 del ***artículo 30 del RGPD***

"Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad". Adicionalmente indica que "cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable".

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 de la operación de tratamiento, sin olvidar que la estructura del mismo deberá corresponder a lo que el punto 1 del artículo 30 del RGPD detalla.

La identificación y descripción de las actividades del tratamiento, no solo es una obligación, sino una necesidad en las fases iniciales para facilitar el análisis de riesgos.

Como se ha comentado en el apartado "Definición y diseño de las actividades de tratamiento", cada responsable de tratamiento deberá valorar el grado de segregación o agregación al que somete sus tratamientos generando elementos diferentes que se corresponden con finalidades, bases jurídicas y grupos de individuos distintos.

"Cada tratamiento incluirá la recogida, registro, organización, estructuración, consulta o utilización de los datos"

Artículo 30 ***del RGPD***

"El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite".

Por tanto, es fundamental que el registro de actividades esté permanentemente actualizado y en un formato claro y legible que facilite su comprensión por parte de terceros. El registro de actividades de tratamiento se debe entender, necesariamente, como un documento vivo, que **requiere revisión continua** y actualización cada vez que se produzca un cambio relevante en alguna actividad de tratamiento registrada.

Estructura: ¿qué debe incluir un registro de actividades de tratamiento?

Artículo 30

"Dicho registro deberá contener toda la información indicada a continuación:

a *el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;*
b *los fines del tratamiento;*
c *una descripción de las categorías de interesados y de las categorías de datos personales;*
d *las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
e *en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*
f *cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;*
g *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1."*

De forma análoga, para la figura de encargado del tratamiento, el artículo 30 establece que

"Cada encargado y, en su caso, el representante del encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a *el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;*
b *las categorías de tratamientos efectuados por cuenta de cada responsable;*
c *en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*
d *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1".*

"Cada encargado y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad"

Considerando los requerimientos del RGPD, a continuación, se describen los distintos campos que deben componer el registro de actividades de tratamiento para la figura de responsable y encargado del tratamiento.

Responsable del tratamiento

Responsabilidad

Campo	Descripción
Responsable del tratamiento	Nombre y datos de contacto del responsable y, en su caso, del corresponsable o del representante del responsable
Delegado de Protección de Datos	Nombre y datos de contacto del Delegado de Protección de Datos

Descripción de la actividad de tratamiento y de los datos tratados

Campo	Descripción
Actividad de Tratamiento	Conjunto de operaciones, procesos o procedimientos, automatizados o manuales, que conlleve la recogida, consulta, grabación, modificación, cesión o destrucción de datos de carácter personal
Finalidad	Descripción de los fines explícitos y la base jurídica en virtud de los cuales el Responsable del tratamiento procede a la realización de las actividades de tratamiento sobre datos personales
Interesados	Categorías de personas físicas identificadas o identificables a quien corresponden los datos personales que son tratados: ■ Clientes ■ Empleados ■ Proveedores ■ Etc.
Categorías de datos personales	Detalle de los datos objeto del tratamiento en función de su clasificación: ■ Datos identificativos (nombre, DNI, dirección, …) ■ Datos financieros (cuenta bancaria, solvencia, …) ■ Datos profesionales (profesión, experiencia, …) ■ Datos de salud (enfermedades, alergias, …) ■ Datos ideológicos y políticos ■ Datos de menores (herencia, seguros, …) ■ Otros tipos de datos: especificar qué datos.

Transferencias y cesiones

Campo	Descripción
Cesiones	Categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
Transferencias de datos internacionales	Identificación de transferencias internacionales de los datos. Se debe identificar a dicho tercer país u organización internacional junto a la base jurídica que la hace posible en ausencia de una decisión de adecuación o de garantía adecuadas: ■ Consentimiento explícito del interesado a la transferencia ■ Transferencia necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento ■ Transferencia necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica ■ Transferencia necesaria por razones importantes de interés público ■ Transferencia necesaria para la formulación, el ejercicio o la defensa de reclamaciones ■ Transferencia necesaria para proteger los intereses vitales del interesado o de otras personas Si fuese de aplicación, medidas y garantías adecuadas adoptadas.
Periodo de conservación	Indicador de los plazos de conservación de la información establecidos en función del tratamiento, la finalidad, la categoría del dato y las leyes establecidas.

Medidas de seguridad

Campo	Descripción
Medidas de seguridad	Descripción general de las medidas técnicas y organizativas de seguridad

Encargado del tratamiento

Responsabilidad

Campo	Descripción
Encargado del tratamiento	Nombre y datos de contacto del encargado o encargados, y, en su caso, del representante del responsable o del encargado
Delegado de Protección de Datos	Nombre y datos de contacto del Delegado de Protección de Datos

Descripción del tratamiento y de los datos tratados

Campo	Descripción
Responsable del tratamiento	Nombre y datos de contacto del responsable por cuenta del cual actúe.
Categorías de Tratamiento	Operaciones, procesos o procedimientos, automatizados o manuales, que conlleve la recogida, consulta, grabación, modificación, cesión o destrucción de datos de carácter personal por cada uno de los responsables a los que se preste servicios.

"En la categoría de datos personales encontramos datos identificativos, financieros, profesionales, de salud, ideológicos, etc"

Transferencias y cesiones

Campo	Descripción
Transferencias de datos internacionales	Identificación de transferencias internacionales de los datos. Se debe identificar a dicho tercer país u organización internacional junto a la base jurídica que la hace posible en ausencia de una decisión de adecuación o de garantía adecuadas: ■ Consentimiento explícito del interesado a la transferencia ■ Transferencia necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento ■ Transferencia necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica ■ Transferencia necesaria por razones importantes de interés público ■ Transferencia necesaria para la formulación, el ejercicio o la defensa de reclamaciones ■ Transferencia necesaria para proteger los intereses vitales del interesado o de otras personas Si fuese de aplicación, medidas y garantías adecuadas adoptadas.

Medidas de seguridad

Campo	Descripción
Medidas de seguridad	Descripción general de las medidas técnicas y organizativas de seguridad

En los **Anexos IV y V,** se incluye un ejemplo de plantilla para documentar registro de actividades de tratamiento como responsable y encargado de tratamiento, respectivamente.

5. Análisis básico de riesgos

Considerando 74
"…el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas."

Considerando 76
"La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.".

El considerando 75
Enumera una serie de factores o supuestos asociados a riesgos para los derechos y libertades de los interesados.

Bajo el supuesto de que las actividades de tratamiento no requieren una EIPD, el análisis de riesgos para determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados se puede simplificar con un enfoque de mínimos considerando que el nivel de riesgo al que están expuestas las actividades de tratamiento no es elevado.

El **análisis básico de riesgos** es un análisis de mínimos que tiene como objetivo simplificar el proceso de análisis de riesgos en aquellas actividades de tratamiento con baja exposición al riesgo.

Como punto de partida, de igual modo que en una EIPD, se deben describir adecuadamente las actividades de tratamiento, proceso que facilitará la documentación del registro de actividades de tratamiento.

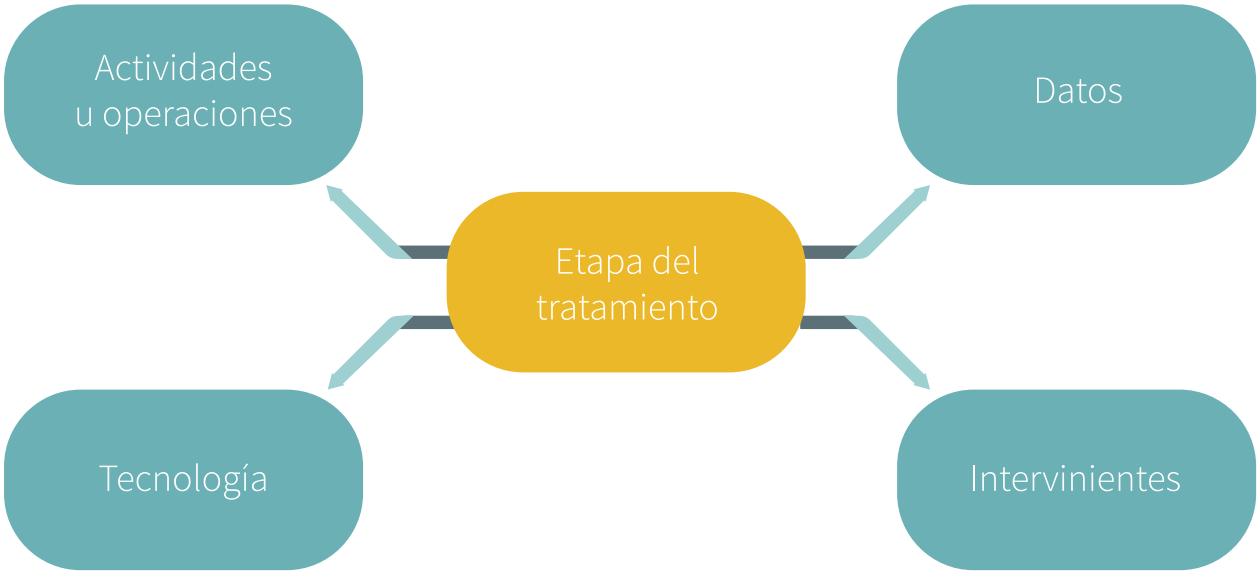
Descripción de las operaciones de actividades de tratamiento

La descripción de los tratamientos sujetos al análisis de riesgos, permite obtener un conocimiento del ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que interviene en las mismas.

A diferencia de la EIPD, donde el análisis se realiza para una actividad de tratamiento específica, en un análisis de riesgos global, las **actividades de tratamiento** se agrupan por procesos comunes expuestos a riesgos similares, lo que simplifica el análisis y permite establecer medidas de seguridad por defecto. Por ejemplo, todas las operaciones de almacenamiento de datos están asociados al riesgo de falta de disponibilidad, por lo que la medida mitigadora aplicable puede ser una política diaria de copias de seguridad definida para todas las bases de datos.
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 procesado. Dentro de esta categoría se pueden encontrar diversas técnicas: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y video, 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 o transferencia de los datos a un tercero para su tratamiento:** Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de 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 de almacenamiento.

Los elementos involucrados en cada una de las etapas del ciclo de vida de los datos en las actividades de tratamiento, se pueden clasificar en las siguientes categorías:



Este paso clave para facilitar la identificación de riesgos servirá como información requerida para su inclusión en el registro de tratamientos.

Actividades de tratamiento sobre los datos de carácter personal

Una actividad de tratamiento responde a la materialización de una finalidad sobre los datos personales de un determinado colectivo de personas. Así una actividad de tratamiento puede ser la gestión de personal, la gestión de historias clínicas, la gestión de alumnos, la gestión de becas, la gestión de una biblioteca, la gestión de la agenda institucional de una organización ...

Son las que se ejecutan en el ciclo de vida o en el conjunto de etapas del ciclo de vida o en el conjunto de etapas del ciclo de vida, y que dan lugar a alcanzar su finalidad definida. Una actividad u operación puede considerarse, por ejemplo, el almacenamiento de datos en una base de datos, la manipulación de la información para la obtención de decisiones, un proceso de borrado o cualquier tarea que requiera el tratamiento o manipulación de los datos y que formen parte de un tratamiento que tiene una finalidad concreta y que define uno de los objetivos o actuaciones que la organización debe realizar sobre los datos de carácter personal.

En este paso, se deben considerar todas las actividades u operaciones de tratamiento similares y que están expuestas a los mismos riesgos, con el objetivo de establecer medidas de control comunes que permitan reducir su nivel de exposición. El enfoque de análisis de riesgos global, busca la agrupación de procesos, actividad que simplifica el análisis sin reducir su nivel de efectividad. A modo de ejemplo, se presentan los procesos de perfilado que se soportan en sis-

temas similares o bases de datos con una tipología concreta. También puede ser criterio de la organización agrupar las actividades de tratamiento entre aquellas que atiendan a finalidades similares sobre grupos de individuos diferentes por ejemplo, supongamos que deba realizarse la historia clínica sobre los empleados de una organización y además sobre los aspirantes a formar parte de una organización.

Datos

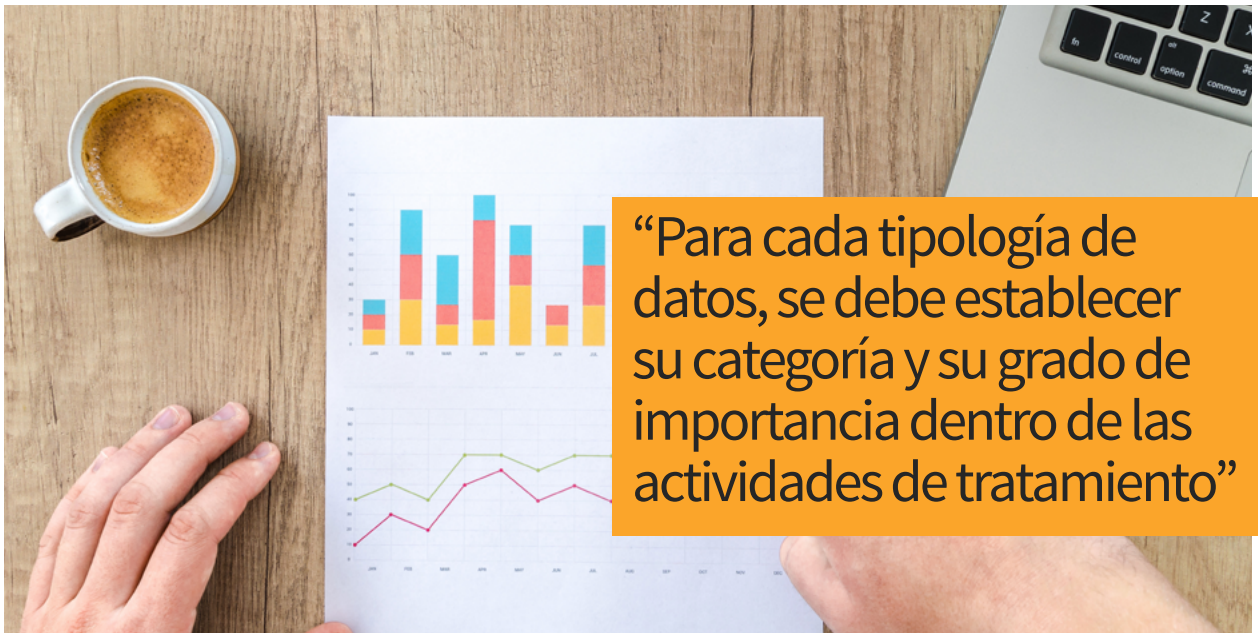
El ciclo de vida está directamente relacionado con los datos personales que se tratan. Por ello, su identificación en cada etapa es fundamental para poder establecer interrelaciones y dependencias entre las operaciones de tratamiento y conjuntos de datos identificados.

Para cada tipología de datos, se debe establecer su categoría (datos especiales) y su grado de importancia dentro de las actividades de tratamiento, determinando si es imprescindible o no su inclusión. En este punto, también 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 participen en cada una de las actividades de tratamiento. Esto se refiere a aquellas personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en las actividades del tratamiento de los datos de carácter personal, y cuyas funciones y responsabilidades están definidas y delimitadas claramente.

Dentro de este grupo 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.



> “Para cada tipología de datos, se debe establecer su categoría y su grado de importancia dentro de las actividades de tratamiento”

La participación de cada uno de los intervientes puede suponer una amenaza sobre los datos de carácter personal, como se ha descrito en el epígrafe “Conceptos generales sobre gestión de riesgos”, circunstancia esta que debe tenerse en cuenta en el análisis y evaluación de los riesgos.

Tecnología

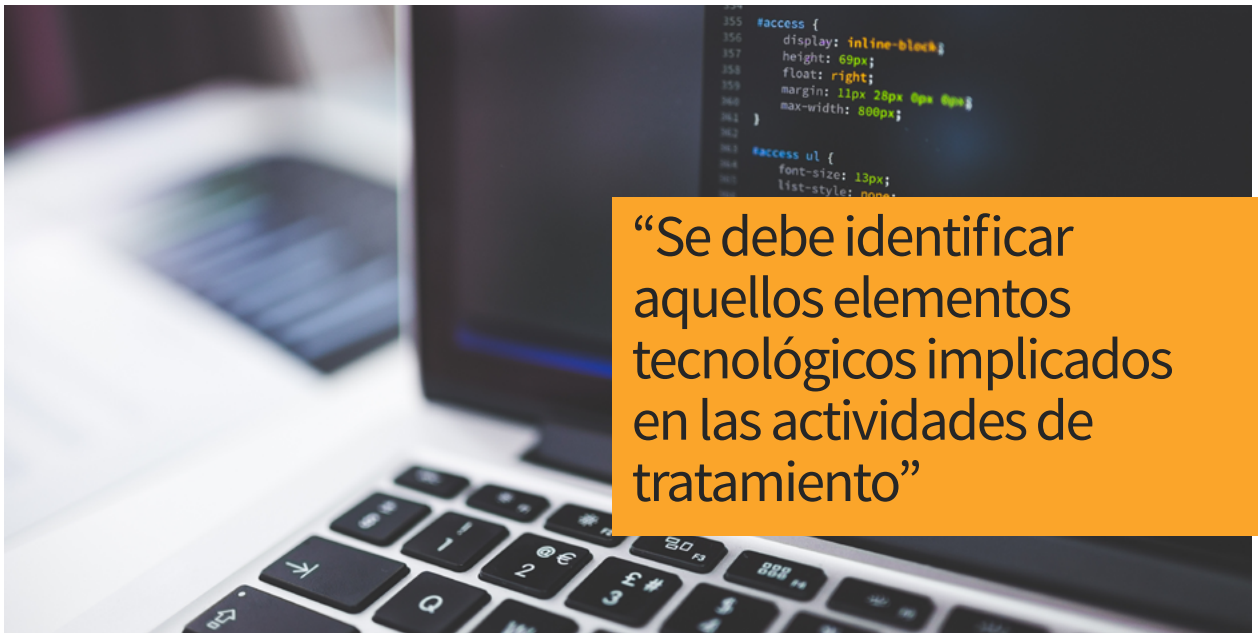
De igual forma, la tecnología y los sistemas son una capa clave que da soporte a las actividades de tratamiento de los datos de carácter personal. Se debe identificar aquellos elementos tecnológicos implicados (tanto hardware como software) en las actividades de tratamiento a un alto nivel, sin llegar entrar en un análisis tecnológico pormenorizado, como son las distintas tecnologías (cloud, BBDD, servidores), aplicaciones, dispositivos y/o técnicas empleadas de procesamiento de los datos.

Para actividades de tratamiento con soporte en la misma tecnología, la exposición a los riesgos derivados de su uso será similar y, por tanto, se podrá agrupar bajo este criterio las actividades de tratamiento a la hora de identificar, evaluar y tratar los mismos.

Por último, no hay que olvidar que, si alguna actividad de tratamiento implica el procesamiento no automatizado de los datos, se ha de identificar como una actividades más de tratamiento e inventariar como un activo más.

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

En el **Anexo II,** se incluye un ejemplo de plantilla donde poder documentar la descripción de las actividades de tratamiento.



“Se debe identificar aquellos elementos tecnológicos implicados en las actividades de tratamiento”

Gestión de riesgos por defecto

La adecuada gestión de riesgos requiere un profundo proceso de identificación, evaluación y tratamiento de los riesgos a los que está expuesto una actividad de tratamiento. La metodología para la realización de una EIPD descrita en la guía (Ver Guía de Evaluación de Impacto en la Protección de Datos) describe un proceso detallado de análisis y está enfocada a las actividades de tratamiento donde la exposición al riesgo es elevada. Sin embargo, ante niveles de riesgo no elevados, el proceso de análisis se puede simplificar poniendo foco en aquellos más relevantes que pueden impactar en las actividades de tratamiento.

Las actividades de tratamiento donde se puede aplicar el enfoque de gestión de riesgos por defecto, considerando que han sido analizadas previamente mediante el análisis de la necesidad de realizar una EIPD, se situarán siempre en un nivel de riesgo no elevado, tal y como se indica 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 · Medio · Alto · Muy Alto

Los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, se pueden diferenciar en 2 dimensiones:

- **Riesgos asociados a la protección de la información** con foco en la integridad, disponibilidad y confidencialidad de los datos. Por ejemplo, acceso ilegítimo a los datos o pérdida de datos.

- **Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.** Por ejemplo, uso ilegítimo de datos personales o la posibilidad de que el responsable no pueda atender el ejercicio de los derechos que el RGPD reconoce al titular de los datos porque la organización no tiene correctamente implementados y operativos los procedimientos correspondientes.

En las metodologías de riesgos tradicionales, el proceso de gestión de riesgos se estructura en **tres fases diferenciadas:**

- Identificación
- Evaluación
- Tratamiento

A partir de la **identificación** de un riesgo inherente a la actividad de tratamiento de partida, se aplican una serie de medidas de seguridad y se obtiene un riesgo residual. Sin embargo, en

el método simplificado propuesto, en base a las dos dimensiones descritas anteriormente, se deben identificar cuáles son los principales riesgos a los que están expuestas las actividades de tratamiento, sin llegar a valorar los riesgos, considerando siempre que el nivel inherente de los mismos será siempre medio o bajo. Para cada uno de los riesgos identificados, se deben establecer medidas de seguridad y control que reduzcan su nivel de exposición.

¿Cómo identificar y gestionar los riesgos potenciales asociados a una actividad de tratamiento?

Los riesgos son variables y dependen de las amenazas a las que está expuesta la actividad de tratamiento, por ello, es fundamental **disponer de una descripción detallada del tratamiento, de su contexto y de los elementos más relevantes que intervienen en la misma.**

El método descrito a continuación, es un método simple que tiene como objetivo **facilitar significativamente el proceso de gestión de riesgos** para aquellas actividades de tratamiento que están expuestas a un nivel de riesgo medio o bajo y en consecuencia el nivel de riesgo se moverá siempre por debajo del umbral de riesgo elevado y, por tanto, la valoración exacta del nivel de riesgo carece de relevancia.

En cada actividad de tratamiento, se debe analizar y determinar cuáles de los riesgos situados dentro de las dimensiones de protección de los datos personales y derechos y libertades de los interesados son de aplicación. A continuación, para cada uno de los riesgos identificados, se deberán establecer tantas medidas de seguridad como sean necesarias para garantizar un nivel de seguridad y control adecuado que reduzca la exposición al riesgo.

A continuación, se describe un ejemplo básico de los riesgos identificados y las medidas de control definidas para gestionar los riesgos de un tratamiento cuyo nivel de riesgo es bajo.

Actividad de tratamiento
Registro y almacenamiento de una lista de asistentes a un curso de formación en una aplicación sin elevado riesgo para los derechos y libertades de los interesados.

Principales riesgos potenciales identificados

- **Protección de de la información:**
  - Integridad de los datos personales:
    - Modificación o alteración de datos personales no intencionada
  - Disponibilidad de los datos personales:
    - Pérdida o borrado no intencionado de datos personales
  - Confidencialidad de los datos personales:
    - Acceso no autorizado a los datos personales

- **Riesgos asociados al cumplimiento:**
  - Garantizar el ejercicio de los derechos de los interesados:
    - Ausencia de procedimientos para el ejercicio de derechos
  - Garantizar los principios relativos al tratamiento:
    - Ausencia de legitimidad para el tratamiento de los datos personales
    - Tratamiento ilícito de datos personales

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.

Ejemplos de medidas de control que ayudan a reducir el nivel de exposición del riesgo potencial identificado

Tipología de riesgo	Riesgo	Medidas de control
Integridad de los datos personales	Modificación o alteración de datos personales no intencionada	■ Segregación de funciones mediante perfiles de acceso ■ Controles de monitorización de amenazas en red
Disponibilidad de los datos personales	Pérdida o borrado no intencionado de datos personales	■ Copias de seguridad ■ Almacenamiento en dos ubicaciones diferentes
Confidencialidad de los datos personales	Acceso no autorizado a los datos personales	■ Mecanismos de control de acceso ■ Segmentación de la red

Garantizar el ejercicio de los derechos de los interesados	Ausencia de procedimientos para el ejercicio de derechos	■ Procedimientos y canales para el ejercicio de derechos
Garantizar los principios relativos al tratamiento	Ausencia de legitimidad para el tratamiento de los datos personales	■ Cláusulas informativas y base legitimadora para el tratamiento de datos
	Tratamiento ilícito de datos personales	■ Monitorización del uso de datos personales

Los riesgos identificados y las medidas de control definidas deben documentarse, con el objetivo de evidenciar la evaluación de riesgos realizada y tener una base de trabajo ante futuras revisiones del análisis derivadas de cambios en las actividades de tratamiento.

Monitorización continua

Los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento. Garantizar una adecuada gestión de riesgos requiere la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo.

Se recomienda revisar el análisis de riesgos realizado ante cualquier cambio significativo en las actividades de tratamiento que pueda derivar en la aparición de nuevos riesgos.

En el **Anexo III**, se incluye un ejemplo de plantilla donde poder documentar el proceso básico de análisis de riesgos.

"Garantizar una adecuada gestión de riesgos requiere la monitorización continua de los riesgos"

6. Anexos

6.1. Anexo I: Plantilla de análisis de la necesidad de la realización de una EIPD

Análisis de Riesgos

Información General

El siguiente cuestionario pretende analizar si la iniciativa realizada por el área implica tratamiento de datos de carácter personal sujetos al marco jurídico que regula el derecho de protección de datos y valorar si en el tratamiento concurren circunstancias y situaciones que obliguen a realizar una Evaluación de Impacto en la Protección de Datos (EIPD).

Indicar la siguiente información general sobre el tratamiento:

Tipología de Datos	*SI/NO*
¿Se van a tratar (1) datos personales (2)? (SI/NO)	
(1) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción	
(2) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona	
Continuar sólo en caso de contestar afirmativamente a la pregunta anterior:	

Finalidades del tratamiento	*DETALLE*	*SI/NO*
Marque SI/NO (donde aplique) en función de si el tratamiento responde a las siguientes posibles finalidades:		
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:		
▪ *El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento)*	☐ *de 0 a 10.000* ☐ *de 10.000 a 100.000* ☐ *+ de 100.000*	
▪ *Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales ,Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro,Transacciones de bienes y servicios). Indicar cuántas de estas categorías aplicarían.*	☐ *1* ☐ *2* ☐ *3* ☐ *4* ☐ *5* ☐ *6* ☐ *7* ☐ *8* ☐ *9*	
▪ *La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M),...)*	☐ *instantaneo* ☐ *días* ☐ *semanas* ☐ *meses*	
▪ *La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))*	☐ *regional* ☐ *nacional* ☐ *internacional*	
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? *(tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?)*		
Por ejemplo, uso de registro de actividad sobre clientes para detectar patrones de usuarios susceptibles de contratar un producto, perfiles comerciales, scoring, etc.		

Análisis de Riesgos

Finalidades del tratamiento (Continuación)	DETALLE	SI/NO
¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos (4)?		
(4) Datos identificativos de personas identificadas o identificables asociadas a: ▪ *Ideología o opiniones políticas* ▪ *Afiliación sindical* ▪ *Religión o opiniones religiosas* ▪ *Creencias o creencias filosóficas* ▪ *Origen étnico o racial* ▪ *Datos relativos a salud* ▪ *Vida sexual u orientación sexual* ▪ *Datos de violencia de género y malos tratos* ▪ *Datos biométricos* ▪ *Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica* ▪ *Datos solicitados para fines policiales sin consentimiento de las personas afectadas* ▪ *Datos relativos a condenas y delitos penales"*		
¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevee el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?		
(5) A modo de ejemplo, las llamadas telefónicas podrían considerarse intrusivas		
(6) A modo de ejemplo, la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, Big Data o la utilización de etiquetas de radiofrecuencia o RFID10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro"		
¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad *(p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, …)?*		
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones (7)?		
(7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales		
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados (8)?		
(8) A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones		
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usen las exitentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?		
(9) A modo de ejemplo, el uso de la información contenida en ficheros externos como ASNEF o CIRBE		
¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? *Por ejemplo, un departamento que no participe en el tratamiento.*		
¿Se van a tratar datos relativos a la observación de zonas de acceso público? *(por favor, tenga en cuenta que las zonas de acceso público únicamente estarán situadas en la via publica, excluyendo los lugares de trabajo (p.e.: oficinas comerciales))*		
Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?		
(10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados		
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.?		

Análisis de Riesgos

Tecnologías empleadas para el tratamiento	DETALLE	SI/NO
Marque SI/NO en función de si dichas tecnologías se usan para soportar las finalidades del tratamiento:		
¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado (11)?		
(11) A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura		

Cesiones de datos y transferencias internacionales de datos	DETALLE	SI/NO
Marque SI/NO:		
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? *(en caso afirmativo detallar cuáles)*		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control (12)? (en caso afirmativo detallar cuáles)		
(12) A modo de referencia, el siguiente listado contiene los países considerados seguros para las transferencias de datos: ▪ *Andorra* ▪ *Argentina* ▪ *Canadá (Sector privado)* ▪ *Suiza* ▪ *Islas Feroe* ▪ *Guernsey* ▪ *Israel* ▪ *Isla de Man* ▪ *Jersey* ▪ *Nueva Zelanda* ▪ *Uruguay*		

Percepción de la existencia un riesgo elevado por parte del responsable de la actividad de tratamiento	JUSTIFICACIÓN	SI/NO
Marque SI/NO:		
¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD (13)?		
(13) En caso afirmativo, se pueden utilizar las conclusiones del EIPD ya realizado para dicho tratamiento		
¿Este tratamiento puede conllevar una pérdida o alteración de la información?		
¿Se utilizada documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:		
▪ *Se guarda bajo llave*		
▪ *Se destruye de forma confidencial*		
▪ *Se guarda con un registro de accesos*		
▪ *Otros*		

Terceros que intervengan en el tratamiento	JUSTIFICACIÓN	SI/NO
¿Interviene algún proveedor en el proceso?, en caso afirmativo, indicar su denomicación social:		

Sistemas utilizados en el tratamiento		
Por favor, en la medida de lo posible, identifique los sistemas que intervienen en el tratamiento:		
TIPOLOGÍA A	***TIPOLOGÍA B***	***TIPOLOGÍA C***
☐ *APP1* ☐ *APP1* ☐ *APP1* ☐ *APP1* ☐ *APP1* ☐ *APP1* ☐ *APP1*	☐ *APP8* ☐ *APP9* ☐ *APP10* ☐ *APP11* ☐ *APP12* ☐ *APP13*	☐ *APP14* ☐ *APP15* ☐ *APP16*

Resultado del Análisis:	

6.2. Anexo II: Plantilla de descripción de 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 OPERACIONES 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	
Principales transferencias / envíos 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	

6.3. Anexo III: Plantilla para documentar el análisis básico de riesgos

Gestión de riesgos por defecto

Operaciones de tratamiento			

Riesgos por defecto			
	Tipología de riesgo	*Riesgos*	*Medidas de control*
Protección de los datos personales			
Derechos y libertades de los interesados			

6.4. Anexo IV: Plantilla de registro de actividades de tratamiento (Responsable de tratamiento)

Datos comunes a todos los tratamientos

Responsable del tratamiento	*Nombre y datos de contacto*
Delegado de Protección de Datos	*Nombre y datos de contacto*

Medidas de seguridad																			
Periodo de conservación																			
Transferencias internacionales																			
Cesiones de datos																			
Categorías datos personales																			
Categorías de Interesados																			
Finalidad																			
Actividad de Tratamiento																			

6.5. Anexo V: Plantilla de registro de actividades de tratamiento (Encargado de tratamiento)

Datos comunes a todos los tratamientos

Encargado del tratamiento	*Nombre y datos de contacto*
Delegado de Protección de Datos	*Nombre y datos de contacto*

Responsable del tratamiento	*Categoría de Tratamiento*	*Transferencias de datos personales*	*Medidas de seguridad*

7. 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