Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

Junio 2021

RESUMEN EJECUTIVO

El presente documento es una guía para la gestión de riesgos para los derechos y libertades de los interesados aplicable a cualquier tratamiento, independientemente de su nivel de riesgo. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la Evaluación de Impacto para la Protección de Datos (EIPD) y, en su caso, la consulta previa a la que se refiere el artículo 36 del RGPD.

Esta guía actualiza y unifica las presentadas hace más de tres años por la AEPD: la "Guía práctica de análisis de riesgo para el tratamiento de datos personales" y la "Guía práctica para la evaluación de impacto en la protección de datos personales". El objetivo de la guía es incorporar las lecciones aprendidas en la aplicación de la gestión del riesgo en el ámbito de la protección de datos, y los nuevos criterios e interpretaciones, tanto de la AEPD como del Comité Europeo de Protección de Datos (CEPD) y del Supervisor Europeo de Protección de Datos (SEPD). Además de recoger la experiencia acumulada, pretende mejorar los materiales dirigidos a ayudar al cumplimiento por parte de los responsables, dando una visión unificada de la gestión de riesgos y de la EIPD. Finalmente, este documento facilitará la necesaria integración de la gestión de riesgos para los derechos y libertades, y en general el cumplimiento del RGPD, en los procesos de gestión y gobernanza de las entidades.

La guía consta de tres grandes apartados divididos en capítulos: un primer apartado con una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades, un segundo apartado que incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo para los derechos y libertades, y un apartado final, enfocado a los casos en los sea preciso realizar una Evaluación de Impacto para la Protección de Datos, con unas orientaciones metodológicas específicas al respecto.

Este documento está dirigido, preferentemente, a responsables, encargados de tratamientos y delegados de protección de datos (DPD).

Palabras clave: protección de datos, responsabilidad proactiva, riesgo, evaluación de impacto, EIPD, gestión, gobernanza, políticas, impacto, medidas, garantías, protección de datos desde el diseño, protección de datos por defecto, consulta previa, DPD, derechos, seguridad.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

I. INTRODUCCIÓN

En toda nueva actividad, el realizar una reflexión previa con el objeto identificar posibles problemas y anticiparse a las futuras dificultades permite tomar decisiones racionales y actuar con garantías de éxito. El esfuerzo que se dedique a sopesar las posibles consecuencias[1] de las futuras acciones ha de ser proporcional al posible perjuicio o impacto que podrían derivar de ellas. Cuando esta forma de proceder se aplica al gobierno de una organización se le denomina "gestión del riesgo". El grado de eficacia y eficiencia de dicha gestión determina el nivel de madurez de la entidad.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (Reglamento General de Protección de Datos, en adelante RGPD) tiene como objetivo alinear la protección de los datos personales con la evolución de actividades de tratamiento, que son cada vez más complejas[2,3]. Esto supone implementar un modelo de cumplimiento denominado "accountability" o "responsabilidad proactiva". Este modelo está orientado a tratamientos y su gestión está basada en el enfoque al riesgo. Por lo tanto, el RGPD es un modelo compatible, e integrable, con la gestión moderna de cualquier organización.

Con anterioridad a la plena aplicación del RGPD, hace tres años, la AEPD presentó las guías tituladas "Guía práctica de análisis de riesgo para el tratamiento de datos personales" y "Guía práctica para la evaluación de impacto en la protección de datos personales". Desde entonces, y en el marco de las lecciones aprendidas de la aplicación de la gestión del riesgo, se han desarrollado nuevos criterios e interpretaciones, tanto por parte de la AEPD como por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD). La presente guía unifica las dos guías anteriores con varios propósitos: recoger la experiencia acumulada, mejorar los materiales que ayuden al cumplimiento de los responsables, dar una visión unificada de la gestión de riesgos y la EIPD, y facilitar la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

El presente documento es una guía para la gestión de riesgos para los derechos y libertades de los interesados aplicable a cualquier tratamiento, independientemente de su nivel de riesgo. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la Evaluación de Impacto para la Protección de Datos (EIPD).

La guía se estructura en tres grandes secciones:

- Una primera sección que contiene los fundamentos de la gestión de riesgos para los derechos y libertades, y que se organiza en los siguientes capítulos.

    II. Conceptos asociados a la gestión del riesgo

[1] Consecuencias a corto y a largo plazo.

[2] Considerando 6: *"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales."*

[3] Considerando 7: *"Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas."*

III. El proceso de gestión del riesgo para los derechos y libertades
IV. La gobernanza de los riesgos

- Una sección con el desarrollo metodológico básico para la aplicación práctica de la gestión del riesgo para los derechos y libertades, organizada en los siguientes capítulos:
  V. La descripción y contextualización del tratamiento
  VI. La identificación y el análisis de las fuentes de riesgo para los derechos y libertades
  VII. La evaluación del nivel de riesgo del tratamiento
  VIII. Controles para disminuir el riesgo
  IX. Valoración del riesgo residual y revisión
- Para cuando se precise una Evaluación de Impacto para la Protección de Datos (EIPD), una sección dedicada a las orientaciones metodológicas con los capítulos:
  X. La evaluación de impacto relativa a la protección de datos.
  XI. Análisis de la obligación de llevar a cabo la EIPD
  XII. Análisis de la necesidad de realizar una EIPD
  XIII. Evaluación de la necesidad y proporcionalidad del tratamiento
  XIV. Obligación de documentación
  XV. Recabar la opinión de los interesados.
  XVI. Consulta previa a la Autoridad de Control

Este documento está orientado, preferentemente, a responsables, encargados de tratamientos y delegados de protección de datos (DPD). Tal como establece el artículo 24 del RGPD, el responsable es quien tiene la obligación de garantizar la adopción de medidas para gestionar el riesgo para los derechos y libertades de los interesados. En caso de tratamientos de alto riesgo, el RGPD establece que corresponde al responsable del tratamiento, la obligación de llevar a cabo la EIPD con el asesoramiento, en su caso, del DPD (artículos 35 y 39 RGPD).

Por otro lado, el artículo 28, en sus apartados 3.c, f y h, establece la obligación del encargado de ayudar al responsable y poner a su disposición las herramientas y la información para demostrar el cumplimiento. En consecuencia, este documento también está orientado a encargados de tratamiento en el marco del desarrollo de estas obligaciones.

Finalmente, con el fin de poder cumplir con las funciones establecidas en el artículo 39 del RGPD, esta guía es prácticamente de obligada lectura para los delegados de protección de datos.

Como cierre de esta introducción, y más allá de la obligación de cumplimiento del principio de responsabilidad proactiva en el RGPD, es importante subrayar una cuestión capital: eludir las actividades de identificación y gestión de riesgos en un tratamiento, ignorarlos, o procrastinar ante los deberes y obligaciones del responsable, es una gran fuente de futuros problemas para los interesados, ciudadanos, usuarios, empleados y para el propio responsable. Los mayores perjuicios no se originarán de tratamientos de alto riesgo cuando éstos se encuentren bien gestionados. Los impactos negativos, a medio y largo plazo, se producirán en aquellos tratamientos mal gestionados, en los que se ignoran las amenazas y la gravedad de sus consecuencias.

SECCIÓN 1: FUNDAMENTOS DE LA GESTIÓN DE RIESGOS PARA LOS DERECHOS Y LIBERTADES

II. CONCEPTOS ASOCIADOS A LA GESTIÓN DEL RIESGO

La gestión del riesgo es un elemento capital en los procesos de cualquier organización y es una parte inherente de la gestión de toda entidad, proyecto o actividad humana.

La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que han de ser protegidos. La gestión del riesgo precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere tomar decisiones que se han de plasmar en hechos concretos (controles) que minimicen el impacto sobre los activos hasta unos niveles tolerables.

El RGPD demanda la identificación, evaluación y mitigación[4], realizadas de una forma objetiva[5], del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos[6]. Estás deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento[7]. Además, dichas medidas se revisarán y actualizarán cuando sea necesario[8]. En definitiva, el RGPD exige un proceso de gestión del riesgo[9] para los derechos y libertades de los interesados.

En cumplimiento del principio de responsabilidad proactiva o "accountability", la gestión del riesgo ha de estar documentada. Sin embargo, es importante saber diferenciar los informes que documentan las acciones de gestión del riesgo con la gestión del riesgo en sí misma. La gestión del riesgo no es un documento sino un proceso que se traduce en hechos y que se acredita documentalmente.

A. LA GESTIÓN DEL RIESGO

La gestión del riesgo es uno de los pilares de la dirección de cualquier organización. Toda entidad, cuando pretende iniciar con garantías un nuevo producto o servicio, debe gestionar los elementos de incertidumbre que se derivan de su naturaleza, ámbito, contexto y fines. Las normas ISO[10] definen esta actividad como la "aproximación basada en el riesgo" (RBT de "risk based thinking"). El RBT es, con la orientación a procesos

[4] Considerando 77 "…la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo…"
[5] Considerando 76 "…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" y otros.
[6] Artículo 24 "Teniendo en cuenta … los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar…"
[7] 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."
[8] Artículo 24 "Dichas medidas se revisarán y actualizarán cuando sea necesario."
[9] En la nota 6 de las Directrices WP248 se interpreta: Cabe señalar que, a fin de gestionar los riesgos para los derechos y libertades de las personas físicas, dichos riesgos deben identificarse, analizarse, estimarse, evaluarse, tratarse (p. ej., mitigarse) y revisarse con regularidad.
[10] Familia de normas ISO 9000

(tratamientos[11]), uno de los dos pilares para la gestión de la calidad en cualquier entidad o, dicho de otra forma, es el "idioma" que hablan los modernos sistemas de administración de las organizaciones.

Esta aproximación se encuentra así establecida en los estándares de calidad, como la familia ISO 9001, forma parte del plan de estudios de las escuelas de negocio, se encuentra en las metodologías de análisis y gestión de riesgos de los sistemas de información en las Administraciones Públicas[12] y hasta se recoge en el propio Código Penal[13]. La gestión de riesgo es una garantía para el crecimiento sostenible de cualquier entidad[14].

Las normas ISO[15] definen el concepto de "riesgo" como el *"efecto de la incertidumbre sobre la consecución de objetivos"* entendiendo como tal efecto cualquier desviación positiva o negativa sobre lo previsto inicialmente, teniendo en cuenta que los objetivos pueden ser de distinto tipo según el ámbito de actividad de una organización.

Cuando una organización se enfrenta al desarrollo de una nueva actividad, que se hará efectiva en la forma de un tratamiento, surgen elementos de incertidumbre. Las incertidumbres se manifiestan desde diferentes perspectivas. Por ejemplo, toda entidad ha de ser capaz de garantizar que dispondrá del capital necesario para realizar la nueva iniciativa, es decir, ha de gestionar el riesgo financiero. Para poner en marcha un proyecto no solo es necesario el capital, sino disponer de los recursos necesarios, humanos y materiales, en tiempo, lugar y forma, que están sujetos a problemas de disponibilidad, adecuación, etc., lo que implica gestionar el riesgo de ejecución del mismo proyecto. En la implementación de este se utilizarán técnicas y tecnologías novedosas que generan incertidumbres en su desempeño, lo que implica una gestión del riesgo de la fiabilidad técnica.

Otros riesgos que es necesario gestionar son: el riesgo de seguridad para las personas; el riesgo de seguridad con relación a la continuidad del negocio; los riesgos de fraude; determinar si la actividad generará suficientes beneficios, materiales o inmateriales, que compensen la inversión, es decir, realizar el análisis coste/beneficio, etc.

Además, la nueva actividad no está aislada del resto de la entidad. El tratamiento se desenvuelve en el contexto interno de la organización, por lo que hay que analizar el impacto que tendrá en otras actividades de esta (p.ej. en la utilización de personal, espacios, etc.), así como el riesgo de coste de oportunidad que supone relegar otras posibles iniciativas por limitación de recursos.

Más aún, la actividad y la organización se desenvuelven en un contexto social y económico cambiante y con el que es preciso interactuar. Por ejemplo, la actividad ha de adecuarse a la normativa (riesgo de cumplimiento) y tendrá que adaptarse a los cambios normativos futuros (riesgo legal). Hay que gestionar los riesgos de

[11] En la versión en inglés del RGPD se utiliza la palabra "proceso" (processing) para referirse a "tratamiento".
[12] MAGERIT https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
[13] Artículo 31 bis sobre la responsabilidad penal de las personas jurídicas. Apartado 2 sobre la exención de responsabilidad: "1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión"
[14] "Risk in review: decoding uncertainty, delivering value" PWC https://www.pwc.com/gx/en/audit-services/publications/assets/pwc-risk-in-review-2015.pdf
[15] ISO 31000:2018(ES) Gestión del riesgo e ISO 31010:2019 Gestión del riesgo. Técnicas de apreciación del riesgo

responsabilidad civil[16] o penal que se puedan derivar de efectos directos o colaterales del tratamiento. Además de los efectos del entorno hacia la organización, hay que analizar los efectos de tratamiento hacia el entorno mediante el análisis de riesgo medioambiental o de impacto social (responsabilidad social), etc.

Ejemplos de distintas perspectivas de la gestión del riesgo	
El tratamiento en sí mismo	Riesgo financiero
	Riesgo de proyecto
	Riesgo de fraude
	Riesgos de seguridad para las personas (laborales)
	Coste/beneficio
	Riesgo de fiabilidad técnica
	Riesgos de continuidad de negocio en S.I., etc.
El tratamiento en el contexto interno de la organización	Impacto en otros tratamientos de la misma organización de forma directa o indirecta
	Coste de oportunidad, etc.
El tratamiento en el contexto externo normativo, social y económico	Riesgo legal y de cumplimiento
	Riesgos de responsabilidad civil o penal
	Riesgo medioambiental
	Impacto social
	Riesgo para los derechos y libertades, etc.

Tabla 1 Ejemplos de distintas perspectivas de la gestión del riesgo

Por tanto, la gestión del riesgo debe de entenderse como una metodología general que integra distintos objetivos de gestión (riesgo financiero, legal, laboral, social, etc.)[17].

[16] Riesgo que en caso de producirse el siniestro asociado a este provoca un aumento en las obligaciones de aquellos que han sido responsables civiles de los daños o perjuicios causados a terceros.

[17] Prácticamente todas las personas están gestionando riesgos desde distintas perspectivas y de forma integrada. Por ejemplo, a la hora de adquirir un vehículo han analizado la capacidad y forma de pagarlo (riesgo financiero), han analizado el riesgo de adquirir el vehículo a terceros en vez de al concesionario (riesgo de fraude), la fiabilidad mecánica de una marca frente a otra (riesgo técnico), cuál se comporta mejor ante un accidente (riesgo de seguridad), si merece la pena la inversión con relación al uso que se le piensa dar (análisis coste/beneficio), si es ecológico (riesgo medioambiental), la protección jurídica y económica ante posibles daños a terceros (riesgo de responsabilidad civil), si sería mejor abordar la compra de una casa antes que un vehículo (análisis de coste de oportunidad), la posibilidad de que tipos de vehículos se ilegalicen en el futuro (riesgo legal), etc. Toda persona juiciosa realizará este análisis, balanceando pros y contras, de forma integral y tomando decisiones y medidas para minimizar el riesgo. La diferencia entre unas personas y otras a la hora de hacer este análisis se encontrará en la profundidad del mismo, y en la formalidad que haya empleado para su estudio. Ambas dependerán del impacto que pueda tener esta, o cualquier otra, actividad en sus vidas.

B. LA GESTIÓN DEL RIESGO EN EL RGPD

El RGPD hace referencia al término "riesgo" en setenta y tres ocasiones a lo largo del texto, y de forma específica, en los artículos 4.24, 23.2.g, 24.1, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 39.2, 49.1, entre otros. En particular, el artículo 24.1 establece:

> *Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario*

La "aproximación basada en el riesgo" se desarrolla en el "*Statement on the role of a risk-based approach in data protection legal frameworks WP218*" del Grupo de Trabajo del Artículo 29[18] (en adelante la Declaración WP218) y no es un concepto novedoso en el marco de la protección de datos[19].

El RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. El riesgo surge tanto por el tratamiento automatizado de datos como por su procesamiento manual, por los elementos humanos y por los recursos implicados. El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve.

El RGPD no establece un criterio práctico-metodológico para la gestión de los riesgos. En ese aspecto, el RGPD deja libertad para que este la gestión del riesgo para los derechos y libertades se integre con el resto de los recursos de gestión de riesgo, políticas y gobernanza de la organización.

Con carácter general, el RGPD tampoco exige ningún requisito explícito de formalidad a la hora de ejecutar la gestión del riesgo, sin perjuicio de las obligaciones de "accountability" ya mencionadas. Sin embargo, para tratamientos que impliquen un alto riesgo, el RGPD sí establece unos requisitos mínimos que ha de tener su gestión. Estos se derivan, especialmente, de las obligaciones establecidas en los artículos 35 "*Evaluación de impacto relativa a la protección de datos*" (EIPD), y el artículo 36 del RGPD. En este sentido, el Comité Europeo de Protección de Datos ha desarrollado el documento "*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*"[20] (a lo largo de este texto se referenciarán como Directrices WP248).

Las Directrices WP248 definen los conceptos de "riesgo" y de "gestión del riesgo":

> *Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias estimado en términos de gravedad y probabilidad.*

[18] Statement on the role of a risk-based approach in data protection legal frameworks, adoptada el 30 de mayo de 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[19] Declaración WP218 "The so-called "risk-based approach" is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20). The legal regime applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach..."

[20] https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

Por otra parte, la «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

En las Directrices WP248 se incluyen recomendaciones tanto para la realización de la EIPD como para la gestión del riesgo en general.

C. EL RIESGO PARA LOS DERECHOS Y LIBERTADES

El riesgo para los derechos y libertades atañe principalmente, como manifiestan las Directrices WP248, a los derechos a la protección de datos y a la intimidad[21].

El Considerando 75[22] desarrolla el concepto de riesgo para los derechos y libertades como cualquier efecto o consecuencia no deseados sobre los interesados o no previsto en el propio tratamiento de datos personales, capaz de generar daños o perjuicios sobre sus derechos y libertades, particularizando, entre otros: los daños y perjuicios físicos, materiales o inmateriales, problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización, perjuicios económicos o sociales, privación a los interesados de sus derechos y libertades, que se les impida ejercer el control sobre sus datos personales, etc.

De forma más específica, las propias Directrices WP248[23] interpretan que la protección se ha de extender a otros derechos fundamentales. Explícitamente, se señalan la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación y la libertad de conciencia y de religión.

Además, en la Declaración WP218 se interpreta que, en la aproximación basada en el riesgo, la protección de dichos derechos ha de realizarse evaluando tanto el impacto que tienen sobre la persona afectada el tratamiento en cuestión como el impacto social general que puede ocasionar. En este último caso, se plantea un ejemplo concreto como podría ser la pérdida de confianza social[24]. Por lo tanto, no sólo hay que gestionar los

[21] Directrices WP248: "Como se indica en la declaración del Grupo de Trabajo sobre protección de datos del artículo 29 sobre la función de un enfoque basado en el riesgo de los marcos jurídicos sobre protección de datos, la referencia a «los derechos y libertades» de los interesados atañe principalmente a los derechos a la protección de datos y a la intimidad".

[22] *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos* ***que pudieran provocar daños y perjuicios físicos, materiales o inmateriales****, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*

[23] …pero también puede implicar otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

[24] 11/ The risk-based approach …, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)

riesgos para el sujeto de los datos que se están tratando, sino los de todos aquellos individuos afectados o colectivos de afectados[25] por el tratamiento.

En conclusión, el foco de la gestión de riesgos en el RGPD es la protección de la persona, en su dimensión individual y social, como sujeto de los datos o afectado por el tratamiento. Aunque tenga una relación colateral, la gestión del riesgo para los derechos y libertades no está orientada a proteger intereses propios del responsable o encargado con relación, por ejemplo, a la continuidad del tratamiento, su eficacia o su eficiencia, el cumplimiento normativo o con relación a las posibles actividades de negocio del encargado y responsable.

D. LA GESTIÓN DEL RIESGO DE CUMPLIMIENTO VS RIESGO PARA LOS DERECHOS Y LIBERTADES

El riesgo de cumplimiento normativo se puede definir como la gestión del riesgo que corre la entidad de incurrir en sanciones legales o administrativas, pérdidas financieras significativas o de reputación por incumplimiento de la normativa legal, normas internas y códigos de conducta aplicables a las actividades, en este caso, de un responsable o encargado.

La gestión del riesgo para los derechos y libertades no está orientada a gestionar el riesgo para la organización derivado de un incumplimiento normativo. La primera está orientada al interesado, como se ha señalado en el anterior apartado, mientras que la segunda, es una gestión del riesgo que pone su foco en la protección de los intereses de la entidad. Por lo tanto, el incumplimiento o posible incumplimiento de los principios y derechos establecidos en el RGPD y la normativa de desarrollo no es objeto de una gestión del riesgo que para los derechos y libertades puede ocasionar un tratamiento a los interesados.

La Declaración WP218[26], interpreta que los derechos y principios fundamentales establecidos en el RGPD que han de cumplir los responsables deben estar garantizados, independientemente de las características del tratamiento y del proceso de gestión del riesgo para los derechos y libertades.

[25] Con frecuencia el objetivo de un tratamiento no es otro que el de clasificar a las personas en un grupo específico, si bien la dimensión habitual es el individuo, con frecuencia las decisiones que se toman por un responsable de un tratamiento pueden afectar a los derechos de grupos de personas: https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

[26] 2/ Rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved (e.g. right of access, rectification, erasure, objection, transparency, right to be forgotten, right to data portability).
4/ Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects.

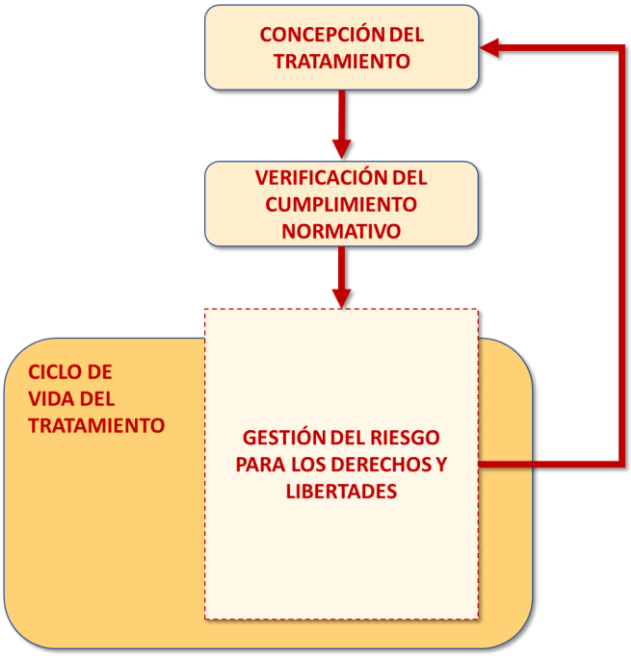

Figura 1 Cumplimiento como requisito previo a la gestión del riesgo

Es una interpretación errónea entender el enfoque de riesgos del RGPD como una forma de reemplazar los requisitos de cumplimiento normativo mediante controles o medidas técnicas y organizativas. Menos aún, el enforque de riesgos del RGPD no está orientado a solventar las posibles consecuencias que, para los afectados, pudiera suponer un posible incumplimiento normativo. En particular, las medidas legales, técnicas y organizativas que pudieran plantearse como resultado de una gestión del riesgo para los derechos y libertades no justifican, por ejemplo, la inexistencia o utilización errónea de una determinada base jurídica para un tratamiento, tampoco, por ejemplo, la carencia de que concurra alguna de las excepciones que levantan la prohibición de tratar categorías especiales de datos. Es decir, la base jurídica no puede suplirse o sustentarse en la concurrencia de alternativas al propio cumplimiento, incluyendo, en su caso, la necesaria evaluación del interés legítimo[27].

En definitiva, no sería lícito reemplazar cualquiera de los principios del RGPD por medidas técnicas y organizativas encaminadas a sustituir dichos principios o a mitigar las posibles consecuencias que dicha falta de cumplimiento pudiera tener sobre los interesados afectados.

En el mismo sentido, la gestión del riesgo para los derechos y libertades no se puede resolver mediante el uso de garantías legales que se basen en un desvío de la responsabilidad hacia terceros. La obligación de garantizar los derechos y libertades descansa en el responsable del tratamiento, como aclara la nota 6 de las Directrices WP248:

> *... Los responsables del tratamiento no pueden eludir su responsabilidad cubriendo los riesgos con pólizas de seguros*

De esta forma, una póliza de seguros que cubra los perjuicios que se puedan generar para la organización, o un acuerdo contractual que pretenda desplazar las

[27] Declaración WP218: 12/ The legitimate interest pursued by the controller or a third party is not relevant to the assessment of the risks for the data subjects. It is in applying the balancing test under the criteria for making the data processing legitimate under the Directive (Article 7 f.) or of the draft regulation (Article 6 f.) that the legitimate interest should be taken into account.

responsabilidades a un tercero, no es una medida para gestionar el riesgo para los derechos y libertades. El balance coste/beneficio, en términos económicos o financieros, derivado de la falta de cumplimiento normativo en materia de protección de datos no debe interpretarse, en ningún caso, como una gestión del riesgo para los derechos y libertades de las personas físicas, sino que, incluso, podría ser considerado por la Autoridad de Control como un posible beneficio obtenido de la propia infracción[28] y un posible factor agravante[29].

Garantía jurídica	**Gestión del riesgo para los derechos y libertades**
Contrato con el encargado de tratamiento cumpliendo los requisitos del artículo 28 del RGPD	Es una obligación de cumplimiento normativo, no una gestión del riesgo
Póliza de seguros para cubrir la responsabilidad de la organización ante una posible infracción del RGPD	Supone una gestión del riesgo de cumplimiento, pero no del riesgo para los derechos y libertades.
La firma de un acuerdo de confidencialidad por parte de personal que tratan determinados datos.	Puede ser una medida de gestión del riesgo para los derechos y libertades, en la medida que no relaja las obligaciones del responsable, sino que busca garantizar el compromiso del personal que trata los datos.

Tabla 2 Ejemplos de garantías jurídicas y su relación con la gestión del riesgo

La gestión del riesgo para los derechos y libertades tiene por objetivo el estudio del impacto y la probabilidad de causar daño a las personas, a nivel individual o social, como consecuencia de un tratamiento de datos personales. Por el contrario, la gestión de riesgo de cumplimiento normativo tiene por objetivo facilitar al responsable una herramienta para verificar el grado de cumplimiento de las obligaciones y preceptos exigidos legalmente con relación a una actividad de tratamiento. Por lo tanto, previamente al proceso de gestión de riesgos y como condición *sine qua non* para emprender una actividad de tratamiento, es preciso sistematizar la verificación de cumplimiento normativo a lo largo de todo el ciclo de vida del tratamiento.

La AEPD pone a disposición de los responsables y encargados un documento que contiene un Listado de cumplimiento normativo y una Hoja de ruta para garantizar la conformidad con la normativa de protección de datos que puede ser de utilidad a la hora de analizar el grado de conformidad con la normativa de protección de datos.

[28] Considerando 149: *"Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento."*

[29] Artículo 83.2.k: *"Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

E. LA GESTIÓN DEL RIESGO EN TODOS LOS TRATAMIENTOS

Todas las actividades de tratamiento de datos personales implican un riesgo para las personas cuyos datos son tratados y, en particular, para sus derechos y libertades. Incluso, en aquellos casos en los que el responsable, ya sea por la tipología del dato o por el tipo de actividad de la organización, pudiera asumir la existencia de un riesgo escaso para los interesados o incluso la inexistencia de riesgo.

Las Directrices WP248 aclaran la importancia de realizar la gestión del riesgo en los tratamientos aun cuando los tratamientos no sean de alto riesgo:

> *…el mero hecho de que las condiciones que dan lugar a la obligación de llevar a cabo una EIPD no se hayan cumplido no disminuye la obligación general de los responsables del tratamiento de aplicar medidas para gestionar adecuadamente los riesgos para los derechos y libertades de los interesados.*

En la misma línea, con relación a las obligaciones generales del responsable y encargado del tratamiento, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD) plantea la necesidad de tener en cuenta los riesgos que podrían producirse como resultado de un tratamiento de datos personales.

Por lo tanto, el concepto de "riesgo cero" no existe cuando hablamos de gestión del riesgo, en particular, cuando hablamos de los riesgos que pueden suponer los tratamientos de datos personales. Siempre existirá un riesgo inherente o inicial implícito en cualquier tratamiento y, una vez que se hayan aplicado medidas y garantías que lo minimicen, seguirá existiendo un riesgo residual.

La Declaración WP218 interpreta que el enfoque de riesgos ha de ser un proceso escalable y adaptable a la situación específica de cada tratamiento. La aproximación basada en el riesgo ha de ser proporcionada, y la realización del proceso de gestión del riesgo para los derechos y libertades ha de estar guiada por principios de eficacia y eficiencia. La complejidad del proceso de gestión de riesgo ha de ajustarse, no al tamaño de la entidad, la disponibilidad de recursos, la especialidad o sector de la misma, sino al posible impacto de la actividad de tratamiento sobre los interesados y a la propia dificultad del tratamiento. Si una entidad pretende abordar un tratamiento y no tiene la capacidad para hacer la necesaria gestión del riesgo, estará obligada a buscar algún tipo de ayuda, como recurrir a la consultoría externa, para realizarlo de la forma apropiada.

Cuando los tratamientos son de bajo riesgo, la AEPD dispone de herramientas para orientar y facilitar su gestión. La AEPD también proporciona herramientas para ayudar a realizar un primer análisis en tratamientos de alto riesgo.

F. LA GESTIÓN PROACTIVA EN LA GESTIÓN DEL RIESGO

La Declaración WP218[30] interpreta que la aproximación basada en el riesgo debe ir más allá de un enfoque limitado a reaccionar ante un perjuicio producido al interesado. La gestión del riesgo no se debe reducir a la mera gestión de las consecuencias que se han producido sobre el interesado, como en el caso de que exista una brecha de datos personales. La gestión del riesgo ha de incluir el enfoque preventivo.

[30] 11/ The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect.

Además, a la hora de determinar los factores de riesgo a gestionar, hay que tener en cuenta el contexto presente y los potenciales contextos futuros. La gestión del riesgo requiere realizar una evaluación a largo plazo, especialmente en aquellos escenarios cuyo impacto pudiera derivar en un perjuicio muy elevado sobre los interesados o sobre la sociedad.

G. LA GESTIÓN DEL RIESGO COMO PROCESO

La gestión del riesgo implica actividades como contextualizar, identificar, analizar, evaluar, actuar y revisar. Hay que abordar la gestión del riesgo como un proceso transversal a toda la organización y conectarlo con el resto de los procesos existentes de cara a lograr un marco de gestión del riesgo global, integral, eficaz y eficiente que abarque a la organización en su conjunto y en todas sus dimensiones. El compromiso que adopten los responsables de la entidad en dicha gestión es un factor clave para el éxito.

La Declaración WP218 interpreta que la gestión del riesgo para los derechos y libertades no debe reducirse a un "*ejercicio de checkbox*"[31]. Al contrario, la gestión de riesgos, tal y como lo entiende la norma ISO 31000[32], es un proceso formado por un conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza, mediante una secuencia de iniciativas o acciones.

Las aplicaciones, las guías o las checklist dirigidas a la gestión del riesgo pueden resultar herramientas muy valiosas de soporte, proporcionando información útil para realizar dicha gestión. Sin embargo, hay que tener presente que el análisis final, la toma de decisiones y la ejecución del plan de acción, son competencia exclusiva de la dirección y de los posibles ejecutores de dichas medidas, siendo las herramientas meros instrumentos de ayuda y apoyo a las tareas de gestión.

Figura 2 Soporte a la decisión y toma de decisiones

El proceso de gestión del riesgo ha de tener al menos las siguientes etapas:

[31] Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected.
[32] 4.4.2 Implementación del proceso de gestión del riesgo. La gestión del riesgo se debería implementar de manera que se asegure que el proceso de gestión del riesgo, descrito en el capítulo 5 se aplica mediante un plan de gestión del riesgo en todos los niveles y funciones pertinentes de la organización, como parte de sus prácticas y procesos.

- Descripción del tratamiento, tanto en lo que respecta a su naturaleza, como al ámbito, contexto y fines del mismo.
- Identificación y análisis de los riesgos en el tratamiento.
- Evaluación del nivel de riesgo y determinación de si procede o es necesario realizar una EIPD.
- Tratamiento del riesgo.
- Seguimiento y verificación de la eficacia de las medidas adoptadas y decisión sobre cuándo es necesario realizar un proceso de revisión y reevaluación de las medidas.

Existen dos tareas previas, que son la determinación de la concepción del tratamiento, a más alto nivel, y el análisis previo de los requisitos de cumplimiento de las previsiones de la normativa de protección de datos:

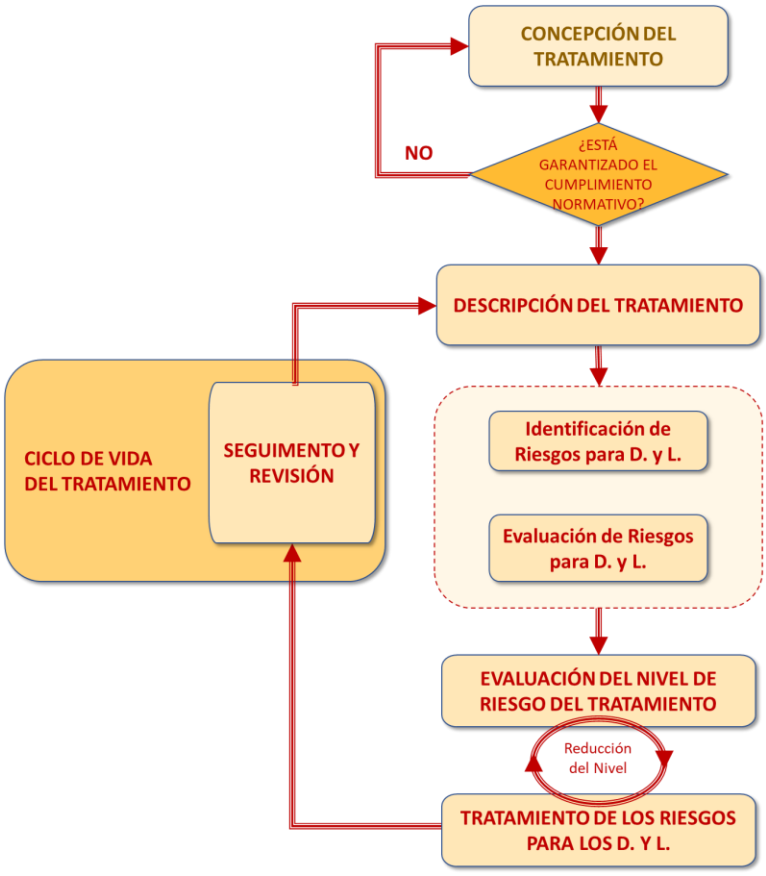

Figura 3 Esquema básico del proceso de gestión del riesgo

Estas etapas han de implementarse de forma que permitan establecer hasta qué punto una actividad de tratamiento, por el contexto, sus características, el tipo de datos tratados, su extensión, sus finalidades, o las características de los interesados, puede tener consecuencias (impacto) sobre los derechos y libertades de las personas físicas. Además, debe incluirse un subproceso de monitorización continua que debe de entenderse como la gestión de la mejora continua del proceso de análisis y gestión del riesgo.

Al ser un proceso, este ha de plasmarse en las políticas de la organización[33] y tendrá que estar documentado.

H. LA INTEGRACIÓN EN LA GESTIÓN DE LA ORGANIZACIÓN

La norma ISO 31000[34] manifiesta que la gestión del riesgo ha de estar integrada con el resto de los procesos de la entidad, en particular en la política, planificación y revisión del tratamiento, para que sea relevante, eficaz y eficiente.

Es decir, la gestión del riesgo no puede realizarse de forma aislada, independientemente o después del diseño y/o implementación de un tratamiento. La gestión del riesgo para los derechos y libertades ha de estar integrada en la gobernanza y políticas de la entidad[35] para que sea eficaz y eficiente y no meramente un simple trámite formal.

En este sentido, y referido a la EIPD, las Directrices WP248 manifiestan, con relación a la gestión del riesgo, que el mismo:

> *…esté integrado en los procesos existentes de diseño, desarrollo, cambio, riesgo y revisión del funcionamiento de acuerdo con los procesos internos, el contexto y la cultura;*

Entre los procesos con los que ha de integrarse están todos aquellos relativos a la gestión del riesgo desde otras perspectivas: financiera, fraude, coste de oportunidad, continuidad de procesos, imagen, suplantación, de negocio, ambiental, seguridad de las personas, etc., que se han de entender de una forma integral.

Figura 4: Integración de la gestión del riesgo para los derechos y libertades en el resto de procesos de gestión de riesgos de la organización.

[33] Artículo 24 RGPD: Responsabilidad del responsable del tratamiento:
2.- Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

[34] La gestión del riesgo debería estar integrada en todas las prácticas y procesos de la organización, de una manera que sea relevante, eficaz y eficiente. El proceso de gestión del riesgo debería formar parte de los procesos de la organización, y no ser independiente de ellos. En particular, la gestión del riesgo debería estar integrada en el desarrollo de la política, en la planificación y revisión de la actividad y la estrategia, y en los procesos de gestión de cambios.

[35] De hecho, sería conveniente que estuvieran integradas todas las acciones de cumplimiento RGPD

En el marco de una organización, todos estos análisis no deben gestionarse de forma independiente pues ello los haría ineficaces, sino que han de analizarse de forma unificada para alcanzar una única conclusión. De esta forma, el responsable puede alcanzar una decisión en el marco de un planteamiento holístico que tome en consideración el contexto global del tratamiento, sus requisitos y limitaciones, dentro de un marco común de gestión del riesgo para todos los procesos de la organización.

Un caso particular de esta gestión integral lo representan las obligaciones del responsable respecto de la notificación a la Autoridad de Control de las brechas de datos personales, así como la comunicación de estas a los propios interesados. En este caso, la evaluación del riesgo que sobre los derechos y libertades de los interesados pueda representar la brecha de seguridad no debería ser, en ningún caso, inferior a la evaluación que se hubiera hecho en el marco del análisis de riesgo del tratamiento. Como se ha señalado, gestión del riesgo y gestión de brechas, son dos tareas que deben ser gestionadas de manera conjunta con el fin de evitar incongruencias que pudieran repercutir negativamente en el proceso de gestión de un tratamiento de datos personales o en los propios afectados.

Figura 5: Evaluación del riesgo del tratamiento y de una brecha de datos

I. PAPEL DE ENCARGADOS, DESARROLLADORES Y SUMINISTRADORES

La gestión del riesgo para los derechos y libertades es una obligación del responsable, tal y como establece el artículo 24.1 del RGPD:

> *Teniendo en cuenta … así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.*

En el caso de encargos de tratamiento, el RGPD establece la obligación de asistir al responsable a la hora de realizar la gestión del riesgo, teniendo en cuenta la naturaleza del tratamiento y la información a su disposición, en el artículo 28, en sus apartados 3.c[36], f[37] y h[38], así como en el considerando 83[39]. Para llevar a cabo de forma efectiva dichos deberes, el encargado debe llevar a cabo una gestión del riesgo para los derechos y libertades al menos dentro de los límites del objeto del encargo.

Por otro lado, un desarrollador o suministrador de un producto o servicio con el que varios responsables van a realizar distintos tratamientos de datos puede llevar a cabo una gestión del riesgo para los derechos y libertades. En ese caso los riesgos

[36] c) tomará todas las medidas necesarias de conformidad con el artículo 32.
[37] f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.
[38] h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable
[39] A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado.

identificados y las medidas adoptadas deben incorporarse al proceso de gestión del riesgo del tratamiento que pretenda realizar el responsable. Este proceso debería de ampararse en las garantías contractuales correspondientes a la adquisición del producto o servicio.

En cualquier caso, con independencia de la gestión realizada por los encargados, desarrolladores o suministradores, el responsable seguirá manteniendo la obligación de realizar su propia gestión del riesgo, o una EIPD cuando las operaciones de tratamiento que lleve a cabo puedan entrañar un alto riesgo para los derechos y libertades de los interesados.

J. LA GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES Y LA EIPD

El RGPD establece las obligaciones relativas a la evaluación de impacto relativa a la protección de datos (EIPD), fundamentalmente, en los artículos 35 y 36. Como establece el artículo 35:

"*Cuando sea probable que un tipo de tratamiento, …, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, …, una evaluación del impacto*".

El RGPD no obliga a que para cualquier tratamiento de datos personales sea necesario realizar una EIPD, pero sí establece que es obligatorio que se realice cuando hay una probabilidad de que entrañe un alto riesgo. La existencia de un grado razonable de presunción de que el tratamiento puede entrañar un alto riesgo hace imprescindible la realización de una EIPD.

1. Definición de EIPD como proceso que obliga a actuar

En el texto del Reglamento no aparece una definición para el término "evaluación de impacto relativa a la protección de datos" o EIPD. El CEPD sí desarrolla la definición de EIPD en las Directrices WP248 como:

> *"… un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos."*

Según esto, el CEPD considera que la EIPD, es un "*proceso*" y, por tanto**:**

- Reducir la EIPD a una actividad puntual y aislada en el tiempo es incompatible con el concepto de proceso que interpreta las Directrices WP248.
- La EIPD ha de estar documentada[40], pero la EIPD es más que el informe que refleja sus resultados.
- La EIPD ha de evaluar los riesgos "*determinando las medidas para abordarlos*". La EIPD obliga al responsable a actuar y tiene una dimensión mayor que un mero formalismo plasmado en un documento sobre el que se puedan realizar cambios mínimos para adaptarlo a cualquier tratamiento.

La EIPD es un proceso de análisis de un tratamiento que se extiende en el tiempo, a lo largo de todo el ciclo de vida de un tratamiento de datos personales, y que se ha de

[40] Con objeto de dar soporte al responsable en la realización de este proceso, la AEPD ha publicado modelos para documentar ante la Autoridad de Control el resultado de este proceso. Estos modelos facilitan la labor del responsable de documentar adecuadamente una consulta previa.

revisar de forma continua, "*al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento*" (art.35.11 del RGPD).

2. Integración de la EIPD y la gestión del riesgo

La EIPD forma parte del proceso de gestión de riesgos para los derechos y libertades de las personas físicas en lo que respecta al tratamiento de sus datos personales. En la definición del CEPD, una de las misiones de la EIPD es "ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento".

Figura 6: Integración de la EIPD en la gestión del riesgo para los derechos y libertades

La EIPD y la gestión del riesgo son actividades integradas. Una vez que se toma la decisión de llevar a cabo una EIPD, esta forma parte indivisible de la gestión de riesgos para los derechos y libertades. De esta forma, no es posible ejecutar una EIPD si no existe una gestión de riesgos para los derechos y libertades y no se realiza en el marco de la misma.

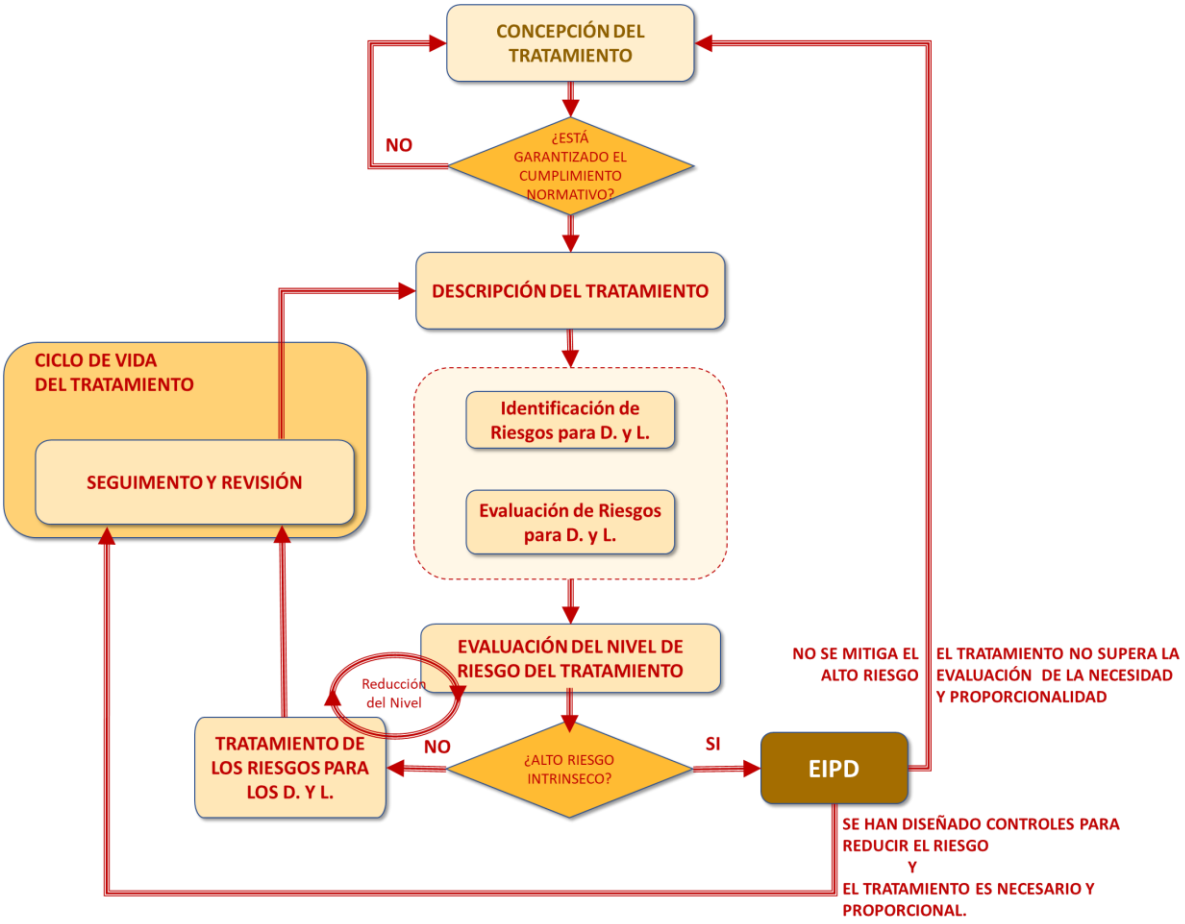

Figura 7: Esquema básico del proceso de gestión del riesgo incluyendo la EIPD

3. La EIPD amplía los requisitos de la gestión del riesgo

El RGPD, en el marco de la EIPD, añade unos requisitos adicionales a la hora de realizar la gestión del riesgo para los derechos y libertades, añadiendo un grado más elevado de dedicación, en particular, en la profundidad del análisis, en los requisitos de *accountability* (p.ej. documentación e implicación del DPD) y de control por parte de las autoridades de control.

Las características que incorpora la EIPD con relación a la gestión general del riesgo para los derechos y libertades son:

- Es exigible cuando hay un alto riesgo para los derechos y libertades.
- Es una obligación específica del responsable.
- Exige un análisis de la necesidad y proporcionalidad del tratamiento[41] con relación a sus fines.
- Exige su realización antes del inicio de las actividades de tratamiento[42].
- Exige el asesoramiento del DPD si este está nombrado.

[41] No debe confundirse el "análisis de necesidad" de llevar a cabo una EIPD frente al "análisis de necesidad del tratamiento" que es una exigencia que el RGPD requiere al responsable en su artículo 35.7.b.
[42] Con algunos matices que se desarrollan en la sección del documento dedicada específicamente a la EIPD.

- Requiere recabar la opinión de los interesados, o sus representantes, cuando proceda, en el proceso de gestión del riesgo[43], justificando en su caso la no procedencia o la limitación en la comunicación de información.
- Tendrá en cuenta el cumplimiento de los códigos de conducta aprobados, a que se refiere el artículo 40, a los que se hubiera adherido el responsable.
- Tendrá en cuenta los requisitos de las certificaciones que fueran aplicables al tratamiento en el ámbito de la organización responsable.
- Su resultado se debe tener en cuenta para evaluar la viabilidad o inviabilidad del tratamiento desde el punto de vista de protección de datos. La EIPD es una herramienta para fundamentar la toma de decisiones del responsable con relación a llevar a cabo o no la actividad de tratamiento o, en su caso, modificar el tratamiento dentro de los parámetros que establecen los principios de protección de datos.
- En caso necesario, en función del nivel de riesgo residual, obliga al responsable a realizar una Consulta Previa (art. 36) a la Autoridad de Control.

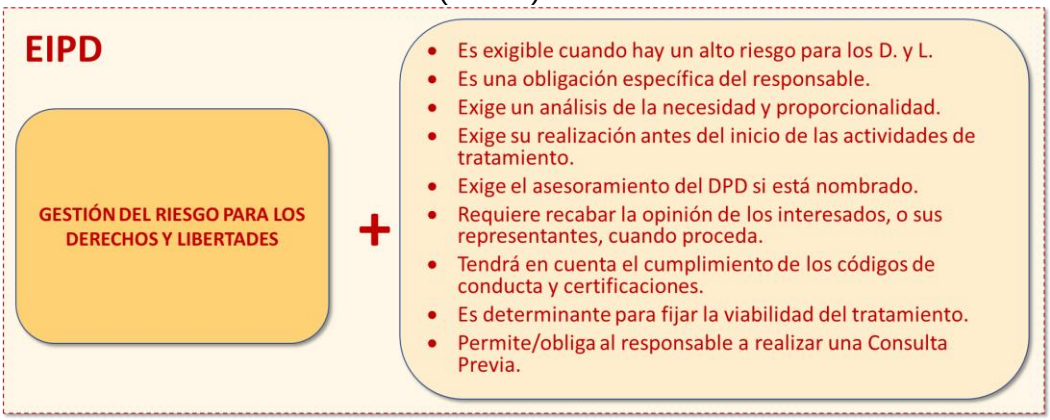

Figura 8: Qué añade la EIPD al proceso de gestión del riesgo.

4. La EIPD como herramienta para demostrar cumplimiento

En las Directrices WP248, junto a la definición de EIPD, se interpreta:

> *"Las EIPD son instrumentos importantes para la rendición de cuentas, que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento."*

De esta forma, una de las posibles medidas de "*accountability*" o de demostrar cumplimiento es la realización de una EIPD, cuando esta no sea obligatoria.

[43] Artículo 35.9 RGPD.

III. EL PROCESO DE GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES

A. DETERMINACIÓN PRECISA DE LAS FINALIDADES DEL TRATAMIENTO

Para llevar a cabo una correcta gestión del riesgo es necesario, en primer lugar, identificar y caracterizar de forma precisa los fines del tratamiento.

Los fines del tratamiento, así como su legitimación, ya han de estar fijados antes de iniciar la gestión del riesgo. Esta determinación es una tarea previa que será necesario que esté expuesta en este punto del análisis, y detallando cómo el responsable se ha asegurado de la correcta identificación de los mismos. Para tener garantías de que los fines del tratamiento han sido correctamente identificados, estos han de cumplir con las siguientes propiedades[44]:

Últimos	Han de determinarse cuál es el fin último del tratamiento y no confundirlo con objetivos intermedios, medios instrumentales u operaciones de tratamiento que tengan lugar en alguna fase del tratamiento o que pueden ser dependientes con la forma de implementar el tratamiento[45].
Específicos:	Suficientemente precisos y concretos, especificando las carencias, demandas, exigencias, obligaciones u oportunidades objetivas y finales que el fin del tratamiento viene a resolver o a dar respuesta.
Medibles	Han de definir un estado futuro deseable en términos cualitativos.
Alcanzables y realistas	Se determinan garantías para conseguir los fines del tratamiento en la medida que es posible "demostrar" que el fin último se va a conseguir.
Acotados	Los fines se han de conseguir en un periodo de tiempo y en el marco de una determinada etapa del ciclo de vida del tratamiento.

Tabla 3 Propiedades que han de cumplir unos fines del tratamiento bien definidos.

En algunos casos, se podría confundir los fines del tratamiento con alguna de las medidas que se podrían adoptar para conseguir dichos propósitos. Por ejemplo, en tratamientos que tienen como fin la seguridad de las personas, el control de acceso o el cumplimiento de normas, se pueden utilizar métodos técnicos (como videovigilancia) o métodos coercitivos (como sanciones) como medidas para conseguir dicho propósito. Las operaciones de videovigilancia o los procesos de sanción son medios técnicos u organizativos utilizados en una forma concreta de entender la implementación del tratamiento. El empleo de dichos métodos no es el fin último del tratamiento, sino que buscan objetivos intermedios o son medios instrumentales para la consecución del fin último del tratamiento.

[44] Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf

[45] En caso de que se utilice en un tratamiento, por ejemplo, videovigilancia, no supone que el fin del tratamiento sea videovigilar. El fin podría ser preservar la seguridad de las personas, controlar el acceso a un recinto o cualquier otro. Las operaciones de videovigilancia son un medio y una implementación concreta de ese tratamiento orientado a conseguir dicho fin.

Los fines del tratamiento han de describirse de forma clara, precisa y entendible, pero no simplificadora.

B. DESCRIPCIÓN DEL TRATAMIENTO

Para gestionar los riesgos que para los derechos y libertades representa un determinado tratamiento, hay que conocerlo y, para ello, es necesario analizarlo. Analizar supone examinar detalladamente, separando y considerando de forma independiente cada una de sus partes, para conocer sus características, cualidades, restricciones y limitaciones, y así poder extraer conclusiones.

La profundidad de este análisis ha de ser la suficiente como para poder llegar a conclusiones con relación al riesgo que representa para los derechos y libertades y, además, para cumplir con las obligaciones de Registro de Actividades del Tratamiento. Normalmente, en la medida que se va deduciendo que el riesgo puede ser elevado, hay que hacer una revisión de la descripción, descendiendo a bajo nivel y haciéndola más detallada, por lo que será un proceso iterativo que se desarrollará a lo largo del ciclo de vida del tratamiento.

DESCRIPCIÓN DEL TRATAMIENTO			
Su propósito	**Su naturaleza**	**Su ámbito/ alcance[46]**	**Su contexto**
• Fines últimos. • Fines instrumentales. • Fines secundarios. • Otros…	• Las etapas en las que se implementa. • El flujo de datos personales. • Las operaciones de tratamiento que precisa (manuales y automatizadas). • Los activos/ elementos sobre los que se implementa. • Los roles que acceden a los datos. • Las características tecnologías relevantes. • La participación de encargados en distintas operaciones. • Otros…	• La extensión en la cantidad de datos. • La extensión en la cantidad de sujetos afectados. • La extensión en los tipos y categorías de datos. • La extensión geográfica. • La extensión en el tiempo del tratamiento. • La extensión en el tiempo de la conservación. • La frecuencia de recogida. • La granularidad. • Otros…	• El mercado o sector en el que se desenvuelve. • El entorno social en el que despliega. • El entorno normativo. • La interacción con otros tratamientos de la entidad. • Las cesiones de datos que son necesarias. • Las transferencias internacionales que implica. • Las brechas de seguridad o incidentes que se producen en tratamientos relacionados. • Los efectos colaterales en la sociedad • Otros…

Tabla 4 Ejemplo de la información que describe el tratamiento que es útil para la gestión del riesgo.

El estudio del tratamiento se podría realizar con distintos niveles de detalle (se detallan en el capítulo “Descripción y contextualización del tratamiento”):

- Análisis a alto nivel del tratamiento.
- Análisis de las fases del tratamiento.
- Análisis del ciclo de vida de los datos.
- Inventario de activos.
- Descripción de casos de uso.

[46] En el original en inglés del RGPD se utiliza la palabra “scope”, que ha sido traducida por “ámbito” en el artículo 24 y 25 y por “alcance” en el artículo 27, 32, 35, 37 o 39, por ejemplo.

La descripción del tratamiento puede ir más allá de las obligaciones normativas establecidas de elaborar y mantener un Registro de Actividades de Tratamiento con el contenido mínimo que exige el artículo 30 del RGPD y el artículo 31 de la LOPDGDD. Sin embargo, ha de integrarse con la solución adoptada en la organización para implementar dicho proceso de registro y, en general, para gestionar los procesos de la entidad.

Como potencial fuente de riesgos, el conocimiento de las tecnologías que se pretenda utilizar, así como sus riesgos asociados, deben ser entendidos como una obligación del responsable y parte de su deber de diligencia con relación al cumplimiento de las previsiones del RGPD. En ningún caso, el desconocimiento del contexto tecnológico puede entenderse como un eximente de las obligaciones del responsable.

Así mismo, cuando en el marco del proceso de gestión del riesgo sea necesaria una consulta previa a la Autoridad de Control a las que se refiere el artículo 36 del RGPD, en dicha consulta no cabe trasladar a la Autoridad de Control el análisis de aquellos productos, servicios y sistemas existentes en el mercado que pudieran ser empleados, así como los riesgos asociados a los mismos en función de las tecnologías que incorporan. El proceso de identificación de estos riesgos forma parte de la labor del responsable y se enmarca en las funciones de asesoramiento del DPD.

C. LA EVALUACIÓN DEL NIVEL DE RIESGO DEL TRATAMIENTO PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS

La evaluación del nivel de riesgo tiene dos objetivos. El primero, optimizar los esfuerzos para mitigar y gestionar los riesgos de forma proporcional. El segundo, determinar si el nivel de riesgo exige cumplir con lo previsto en los artículos 35 y 36 del RGPD (supuestos de alto riesgo).

1. Proceso de evaluación del riesgo

El proceso de evaluación del nivel de riesgo es una disciplina con una metodología consolidada y común a cualquier proceso de gestión del riesgo. Para la evaluación del nivel de riesgo asociado a un tratamiento hay que realizar las siguientes tareas:

- Identificar los factores de riesgo o amenazas[47] para los derechos y libertades.
- Analizar los mismos, en su impacto y probabilidad, para poder llevar a cabo la evaluación del nivel de riesgo inherente que se deriva de cada uno de los factores de riesgo.
- Evaluar el nivel global del riesgo del tratamiento para los derechos y libertades del tratamiento.

Podemos definir un factor de riesgo o amenaza como una causa potencial de la que se puede derivar un perjuicio para los derechos y libertades de las personas físicas. Los factores riesgo puede tener su origen en el propio tratamiento, como su fin, las operaciones del tratamiento, o la tecnología empleada entre otros. También pueden tener origen en efectos colaterales e indeseados que se derivan del contexto interno o externo a la organización. Todo factor de riesgo tiene un nivel de impacto potencial sobre los interesados. Además, existirá una determinada probabilidad de que dicho factor de

[47] Utilizaremos en este texto el término "factor de riesgo" como sinónimo de "amenaza". "Amenaza" es un término bien definido en la literatura de gestión de riesgos, y en dicha literatura el "riesgo" se deriva de la probable materialización con un determinado impacto de una amenaza. Pero dado que en el RGPD y su en desarrollo se utiliza el término "riesgo" como sinónimo de "amenaza" se empleará esta convenció.

riesgo se materialice de forma efectiva. La probabilidad dependerá tanto de factores internos al tratamiento como de factores externos (contextuales).

2. Riesgo inherente y riesgo residual

El **riesgo inherente** es el resultante de evaluar el nivel de riesgo **previamente** a la implantación de medidas y garantías para reducir el riesgo derivado de cada uno de los factores de riesgo. Esto supone considerar el efecto conjunto de todos los posibles factores de riesgo en los posibles escenarios en los cuales éstos podrían materializarse con una determinada probabilidad produciendo un determinado impacto. Todos ellos han de ser evaluados de forma conjunta, teniendo en cuenta su acción acumulativa y su efecto combinado.

El riesgo residual es el resultante de evaluar el nivel de riesgo resultante **después** de tomar las medidas y garantías orientadas a reducir el riesgo derivado de cada una de las fuentes de riesgo. El objetivo es que el riesgo residual se reduzca a un nivel de riesgo aceptable.

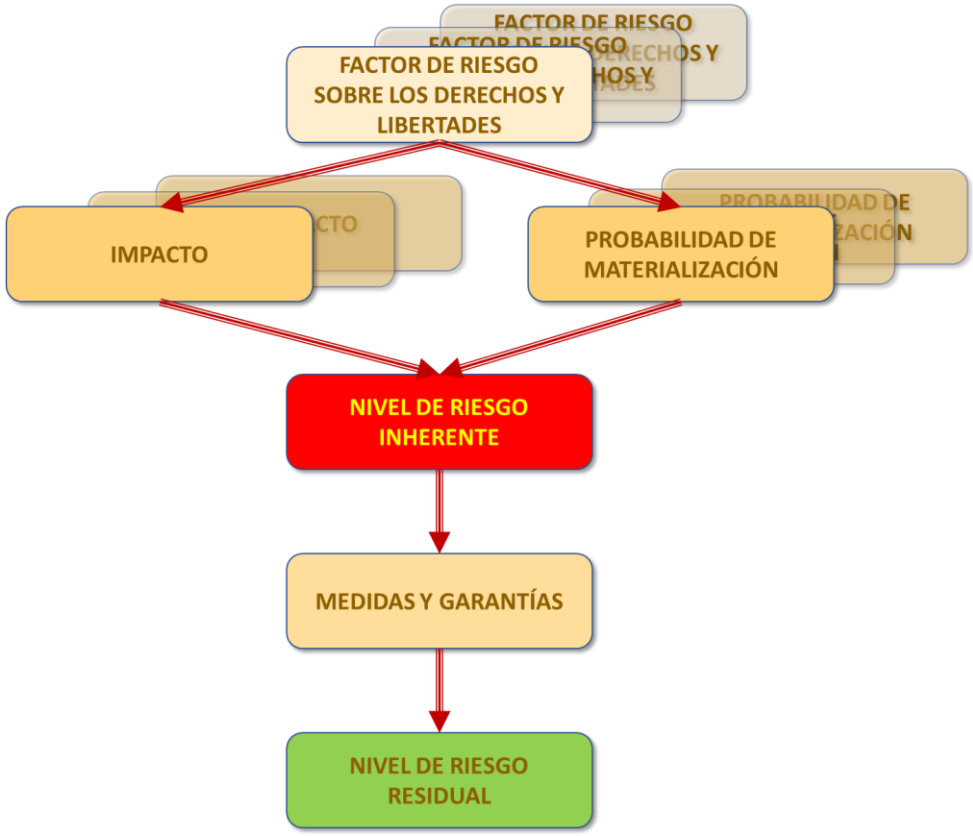

Figura 9: Evaluación del riesgo inherente y riesgo residual

3. Identificación de los factores de riesgo

Identificar un factor riesgo consiste en detectar la fuente que puede propiciar un evento capaz de ocasionar impacto en los derechos y libertades de los interesados.

La normativa anterior al RGPD, en particular el Título VIII del reglamento aprobado por R.D. 1720/2007 ya desplazado, realizaba una valoración del nivel de riesgo de los

ficheros de datos personales con relación a la seguridad de los datos y no con relación a los derechos y libertades de las personas físicas. Dicho análisis tenía las siguientes limitaciones:

- Estaba orientado a ficheros, no a tratamientos.
- Estaba basado fundamentalmente en las categorías de datos utilizados[48].
- Estaba orientado únicamente a determinar las medidas de seguridad.
- Había sido realizado por el legislador.
- Las medidas de seguridad eran una lista de mínimos, que se entendieron por muchos responsables como una lista cerrada.

Sin embargo, el contexto actual es mucho más complejo y un modelo tan simplificado no da respuesta a las situaciones actuales[49]. Por lo tanto, el RGPD requiere que:

- La evaluación del nivel de riesgo sea una tarea del responsable que debe orientarse hacia las operaciones de tratamiento que realiza y no hacia el posible contenido de un fichero de datos.
- La evaluación del nivel de riesgo tenga en cuenta todos los aspectos del tratamiento, que se derivan de la naturaleza, ámbito, el contexto y los fines del tratamiento.
- Las medidas y garantías a adoptar no se limiten a medidas de seguridad, sino que, además, impliquen medidas sobre la concepción del tratamiento, gobernanza y políticas de protección de datos, medidas de protección de datos desde el diseño (de desvinculación[50], transparencia y control), gestión de brechas de datos personales y, en su caso, la realización de una EIPD.

4. Identificación de factores de riesgo de un tratamiento de datos personales en la normativa

En el RGPD, y en su desarrollo mediante otras normas, las directrices del CEPD y la AEPD, se identifican factores de riesgo concretos. Además, en determinados casos se establecen el impacto y la probabilidad de las mismas por defecto, facilitando así el análisis al responsable. Algunos ejemplos son los siguientes:

- En las Directrices WP248 se manifiesta que:

  Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD.

  La existencia de una aplicación de IoT en el tratamiento es un factor de riesgo a gestionar. El responsable tiene que evaluar el impacto que puede tener sobre los derechos y libertades teniendo en cuenta la certeza de que dicho factor de riesgo está materializado en el tratamiento.
- En el artículo 35.3.a se establece que es de alto riesgo un tratamiento que incluya:

  Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración

[48] Se tenían en cuenta también algunas finalidades y sectores de actividad.
[49] Considerandos 7 y 9 RGPD.
[50] Desvinculación (Unlinkability): persigue que el procesamiento de la información se realice de modo que los datos personales de un dominio de tratamiento no puedan vincularse con los datos personales de otro dominio diferente o que el establecimiento de dicha vinculación suponga un esfuerzo desproporcionado

de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

En el anterior párrafo se identifican los siguientes factores de riesgo:

- Técnicas relativas a la naturaleza del tratamiento: tratamiento automatizado y elaboración de perfiles.
- Tipos de datos relativos a la naturaleza del tratamiento: aspectos personales.
- Extensión del ámbito del tratamiento: evaluación sistemática y exhaustiva.
- Finalidades del tratamiento: toma de decisiones con efectos jurídicos o similares.

Cuando se combinan todos estos factores, el impacto sobre los derechos y las libertades es de alto riesgo y el RGPD exige una EIPD. Para gestionar dicho riesgo, será preciso determinar medidas y garantías que permitan disminuir el riesgo asociado a dichos factores.

Por el contrario, si en el tratamiento no se encontraran presentes todos los factores anteriores, sino solo un subconjunto ellos, el tratamiento tendría un determinado nivel de riesgo sin que llegue a ser "alto riesgo". Este nivel de riesgo de los factores de riesgo que concurran en el tratamiento. Además, las medidas anteriormente identificadas serían válidas para gestionar dicho riesgo, teniendo en cuenta los factores que se encuentren presentes.

- En cambio, el artículo 28.2.b de la LOPDGDD establece, que hay que ponderar el alto riesgo en el caso siguiente:

  Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales

  Por lo tanto, en este caso hay que determinar la probabilidad de que se materialice en el tratamiento una erosión a los derechos de las personas, o una la falta de control de sus datos personales. Además, se debería estimar el impacto de acuerdo con otras circunstancias del tratamiento.

De los ejemplos anteriores podemos concluir que, tanto en el RGPD como en su desarrollo, ya aparecen identificados factores de riesgo que hay que gestionar, algunos de alto impacto y probabilidad total, y otros en los que hay que estimar el impacto que podrían producir y/o la probabilidad de que se materialicen.

Por lo tanto, en la tarea de identificar fuentes de riesgo, el responsable o encargado no tiene que comenzar desde cero, sino que el RGPD y su normativa de desarrollo ya han identificado fuentes específicas de riesgo en:

- Los casos del artículo. 35.3 del RGPD.
- La normativa especial que exige una EIPD para el tratamiento o identifica factores de riesgo.
- Los casos y ejemplos de las Directrices WP248.
- Los casos de la lista aprobada por la AEPD en base al artículo 35.4 del RGPD.
- Los casos del artículo 28.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Los casos del artículo 32.2 del RGPD.

- Los riesgos identificados en el Considerando 75[51].
- Los casos y condiciones específicas descritos en las directrices publicadas por el CEPD para tratamientos específicos.
- Los casos y condiciones específicas descritos en los códigos de conducta de acuerdo con el artículo 40 y mecanismos de certificación de acuerdo con el artículo 42 del RGPD.

Para facilitar esta tarea, en el capítulo "Identificación y análisis de factores de riesgo" de la sección 2 se enumera el conjunto de los factores que se han identificado en los distintos textos enumerados previamente.

5. Riesgos de impacto muy elevado

El establecer un nivel de medidas y garantías predeterminado ante un factor de riesgo en función de la probabilidad de su materialización puede ser un error, en especial, en los casos en los que el impacto puede ser de altísima intensidad. Si el impacto de un factor de riesgo es muy alto para los derechos y libertades de las personas, aunque la probabilidad de que se materialice sea muy bajo o despreciable, es necesario gestionar adecuadamente dicho factor de riesgo.

Gran parte del cumplimiento y las garantías de los tratamientos se fundamentan en el marco establecido por el Estado de Derecho, la situación social, política y económica, y el estado de la técnica. Estos cimientos se consideran normalmente "por defecto" e inamovibles al medio plazo. Además, suelen estar más allá de la posibilidad de control por parte del responsable. Dichas garantías suelen dar soporte a los principios de limitación del tratamiento, y están relacionadas con aspectos jurídicos, organizativos y técnicos.

Escenarios de baja probabilidad, pero que pueden comprometer dichas garantías básicas, podrían ser la publicación de normativa que altera radicalmente las garantías jurídicas (p.ej. la PatriotAct o la CloudAct), avances tecnológicos disruptivos (p.ej. computación cuántica, avances en criptoanálisis), cambios radicales en las relaciones internacionales (p.ej. el Brexit), situaciones de especial emergencia (p.ej. conflictos armados, pandemias), quiebras del Estado de Derecho (p.ej. estados de excepción, subversión del orden constitucional), etc.

Esta evaluación no es necesaria para todos los tratamientos, solo en aquellos que por su extensión o intrusión pudieran ser de muy alto riesgo. Tratamientos masivos de datos, especialmente categorías especiales, extendidos en el tiempo y con consecuencias sobre los derechos y libertades serían los candidatos a este análisis. Algunos casos se podrían encontrar en los tratamientos de las AA.PP., grandes

[51] *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*

entidades de telecomunicaciones, grandes entidades financieras, aseguradoras, servicios sanitarios, grandes servicios de Internet, etc.

D. EL TRATAMIENTO DEL RIESGO

El tratamiento del riesgo supone **tomar medidas e implementar garantías** que disminuyan específicamente el nivel de riesgo para los derechos y libertades. Esta tarea supone ir más allá de meras declaraciones o compromisos aparentes. Supone ejecutar acciones para reducir, eliminar o asumir de forma controlada los riesgos identificados. Tratar los riesgos se traduce en reducir el potencial perjuicio disminuyendo, bien la probabilidad de que estos se materialicen, bien el impacto que representan. Esta tarea, como parte de la gestión del riesgo, se ha de realizar con independencia de que se trate de un tratamiento de alto riesgo o no.

En la terminología de la gestión de riesgo, se denomina "tratamiento del riesgo" a la selección de medidas y garantías para reducir, eliminar o asumir de forma controlada los riesgos identificados. En el marco de la protección de datos, la forma correcta de expresarse sería la de "tratamiento de los riesgos del tratamiento[52]". Como podría resultar confusa, se emplearán indistintamente las expresiones "atender", "disminuir", "ocuparse" o "encargarse" a lo largo del texto.

Las medidas y garantías que tienen por objeto atender o disminuir el riesgo en el tratamiento se suelen denominar "controles" en la terminología de la gestión del riesgo.

El RGPD ya señala algunas garantías que se han de implementar en caso de que exista un elevado riesgo para los derechos y libertades. Estas son, por ejemplo, la oportunidad de la aplicación de políticas de protección de datos (art. 24.2), o la obligación de comunicar una brecha de datos personales a los interesados (art. 34), entre otros.

El encargarse de los factores de riesgo del tratamiento se trata de un proceso iterativo que se realiza fundamentalmente durante las etapas de concepción y el diseño del ciclo de vida de este. En cada iteración, se aplicarán controles para reducir la probabilidad o el impacto de los factores de riesgos identificados y se evaluará nuevamente el riesgo residual tantas veces como pueda ser necesario hasta alcanzar un nivel de riesgo aceptable. Las medidas de control se deben considerar de forma independiente para cada riesgo identificado, aunque más tarde se evalúe su efecto combinado, estableciéndose tantas medidas de control como sean necesarias hasta lograr un nivel de riesgo aceptable.

Los controles derivados de la gestión del riesgo pueden aplicarse a múltiples operaciones de tratamiento que sean similares. Algunos de los controles podrían también formar parte de los controles aplicados desde otras estrategias de protección de datos de una organización como son: políticas de protección de datos del responsable, políticas de protección de datos desde el diseño y por defecto o políticas seguridad desde el diseño y por defecto.

1. Clasificación de las medidas y garantías

Las medidas que se pueden adoptar para mitigar el riesgo se podrían clasificar, siguiendo la literatura de gestión de riesgos, de acuerdo con distintos criterios:

[52] En la versión en inglés del RGPD no se utiliza la expresión "treatment" sino "processing" que se traduce como "proceso", aunque en la versión en español se ha preferido emplear "tratamiento".

- En cuanto previenen la materialización del riesgo o se activan como respuesta a un riesgo materializado, se pueden clasificar en medidas proactivas/preventivas, de detección y reactivas/correctivas.
- En cuanto a la estrategia de cómo afrontar el riesgo, distinguimos entre medidas orientadas a:
    - Reducir/mitigar el riesgo: Para reducir el nivel de riesgo, se deben establecer medidas de control que disminuyan los niveles de probabilidad y/o los impactos asociados al riesgo inherente.
    - Evitar/eliminar el riesgo: Si el riesgo es muy elevado y no se quiere asumir el mismo, se puede decidir abandonar la actividad de tratamiento o, en su defecto, modificar la naturaleza, el alcance, el contexto y la finalidad del tratamiento para evitar dicho riesgo.
    - Aceptar/asumir el riesgo: Si el riesgo inherente es inferior al nivel de riesgo considerado como aceptable, se puede asumir, pero sin olvidar la necesidad de continuar gestionándolo de forma continua.
- Atendiendo a su naturaleza, los controles pueden incorporar medidas:
    - Organizativas: Medidas asociadas a los procedimientos, a la organización y/o al gobierno de la entidad relacionadas con la aplicación de políticas de protección de datos.
    - Legales: Garantías jurídicas que pudieran ser necesarias como el establecimiento de cláusulas de confidencialidad o la adopción de compromisos de no reidentificación, entre otros.
    - Técnicas: Medidas de protección desde el diseño, medidas de seguridad o medidas para auditoría (“accountability”) automática, entre otras.

<table>
<tr><th colspan="5">Gestión del Riesgo para los Derechos y Libertades</th></tr>
<tr><td>Proactivas/ preventivas</td><td rowspan="3">Garantías legales</td><td rowspan="3">Garantías técnicas</td><td rowspan="3">Garantías organizativas</td><td>Reducir/ mitigar</td></tr>
<tr><td>De detección</td><td>Evitar/ eliminar</td></tr>
<tr><td>Reactivas/ correctivas</td><td>Aceptar/ asumir</td></tr>
</table>

Tabla 5 Clasificación de medidas y garantías para la gestión del riesgo

Tomando como base el modelo de responsabilidad proactiva establecido en el capítulo IV del RGPD, las medidas y garantías que se pueden adoptar para mitigar los riesgos de protección de datos se pueden clasificar en:

Medidas y garantías en base al RGPD	Medidas sobre el concepto y diseño del tratamiento.
	Medidas de gobernanza y políticas
	Medidas de protección de datos por defecto[53] y desde el diseño
	Medidas de prevención y gestión de brechas de datos personales/ medidas de seguridad.

Tabla 6 Medidas y garantías para la gestión del riesgo en base al RGPD

A cada uno de los factores de riesgo identificados hay que asociar las medidas de control adoptadas. Es muy importante asegurarse de que la asignación de los controles es adecuada y acorde al riesgo, además de que los riesgos se gestionen de forma conjunta y teniendo en cuenta la interrelación entre ellos, con el claro objetivo de poder mitigar los niveles de riesgo del tratamiento como un todo.

Como resultado de atender los riesgos se obtiene el riesgo residual, definido como el nivel de riesgo resultante en el tratamiento una vez se hayan aplicado medidas de control para mitigar y/o reducir su nivel de exposición con relación al conjunto de factores de riesgo identificados. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre el tratamiento.

2. Transparencia y derechos como medidas para disminuir el riesgo

El RGPD establece, en su Capítulo III, obligaciones de transparencia e información, y determina un conjunto de derechos que el responsable ha de proporcionar a los interesados con una serie de condiciones mínimas. El considerando 60 interpreta que dichos deberes se han de extender en la medida que sea necesario para garantizar un tratamiento leal y transparente[54]. Estas obligaciones forman parte de los requisitos de cumplimiento del responsable y no son medidas para disminuir el riesgo del tratamiento.

Sin embargo, se pueden establecer medidas de transparencia e información que vayan más allá de lo señalado en el párrafo anterior para disminuir los riesgos del tratamiento. Una vez cumplimentadas las obligaciones de lealtad y transparencia, se pueden, por ejemplo, hacer explícito al interesado formas de prevenir los riesgos en los que incurre el tratamiento, publicando aquella información que resulte relevante sobre la EIPD o detallando los tipos de datos recogidos, lo que podría ser en determinados casos una medida para disminuir el riesgo del tratamiento.

En el mismo sentido, atender los derechos de los interesados garantizando una diligencia que va más allá de lo establecido en el artículo 12 de RGPD, por ejemplo, en plazos, en medios y en canales, podría ser una forma de disminuir determinados riesgos en algunos tratamientos.

[53] Hay que recordar que las medidas de protección de datos por defecto se han de implementar por defecto, es decir, en cualquier caso e independientemente del riesgo. Ver Guía de protección de datos por defecto.

[54] Considerando 60. Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales…

E. BRECHAS DE DATOS PERSONALES Y SEGURIDAD EN LOS TRATAMIENTOS

Todo tratamiento se implementará sobre un sistema de información, que será en parte automatizado y en parte manual. Además del riesgo que, para los derechos y libertades, puede suponer en sí mismo la existencia de dicho tratamiento, es obligatorio determinar también el riesgo que para esos mismos derechos y libertades puede suponer el que se materialice una brecha de datos personales, es decir, un tratamiento no autorizado o accidental sobre los datos[55].

Figura 10 La gestión de la seguridad como una parte de la gestión del riesgo para los derechos y libertades.

Como interpreta la Declaración WP218, hay que subrayar que abordar los riesgos que pudiera entrañar un tratamiento de datos para los derechos y libertades de las personas no puede limitarse a aplicar exclusivamente medidas de seguridad. Por lo tanto, la gestión de los riesgos de seguridad es una más de las actividades para la gestión de los riesgos para los derechos y libertades y se tiene que supeditar a esta última. Además, desde el punto de vista del RGPD, las medidas de mitigación han de estar orientadas a reducir el impacto y la probabilidad de que las brechas de datos personales afecten al interesado.

[55] Considerando 85: "Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión"

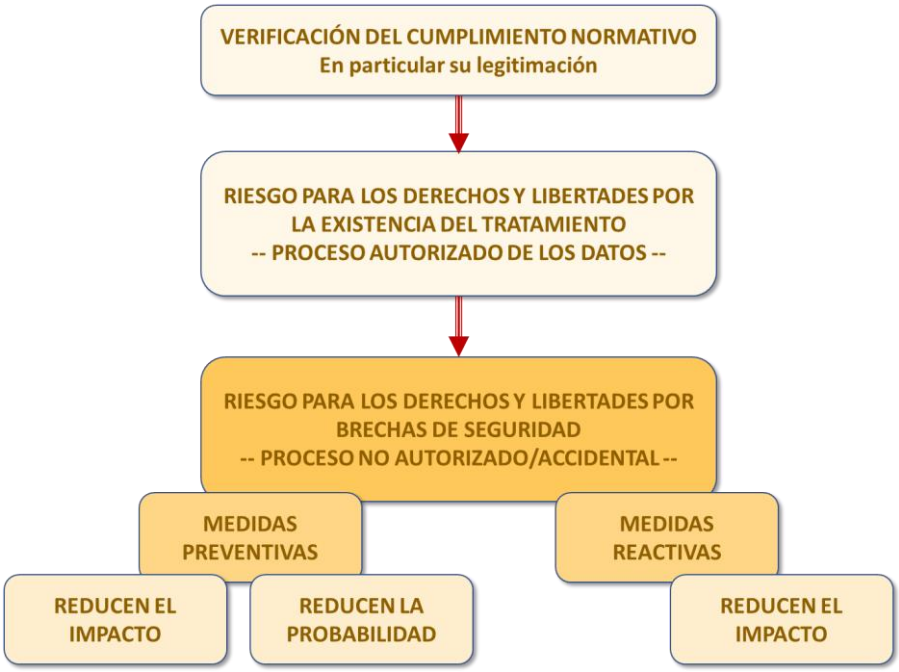

Figura 11: Las medidas de seguridad en la gestión del riesgo para los derechos y libertades.

1. La seguridad por defecto

El documento "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"[56] (Directrices sobre el artículo 25 Protección de datos desde el diseño y por defecto) del Comité Europeo de Protección de Datos, en su párrafo 47, manifiesta que las medidas de seguridad siempre se han de incluir por defecto:

> *La seguridad de la información debe estar siempre por defecto en todos los sistemas, transferencias, soluciones y opciones cuando se tratan datos de carácter personal.*

Esto significa que, aunque el riesgo del tratamiento para los derechos y libertades sea escaso[57], el responsable o encargado:

- No puede ignorar el establecimiento de medidas de seguridad, que se han de implementar independientemente de si el tratamiento es de bajo riesgo o no.
- A la hora de elegir las medidas concretas de seguridad que se han de implementar, el proceso de selección de cada una de ellas ha de estar guiado por un análisis de riesgos para los derechos y libertades de las personas físicas.
- En el caso de tratamientos de un riesgo por encima del aceptable, las medidas de seguridad deben emplearse para reducir el nivel de riesgo del tratamiento.

2. Ámbito de las medidas de seguridad

Con relación a este tipo de medidas, la sección segunda del capítulo cuarto del RGPD está dedicada a la seguridad de los datos personales. En concreto, el artículo 32 está

[56] Publicadas en versión draft en https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es

[57] El riesgo del tratamiento, por muy escaso que sea, nunca será nulo.

dedicado a las medidas que han de garantizar la seguridad del tratamiento y los artículos 33 y 34 sobre medidas específicas de contingencia en caso de que se produzca una brecha de datos personales. Es decir, el RGPD contempla tanto medidas de carácter preventivo (para evitar) como correctivo (para reaccionar ante la materialización de un riesgo).

En ese sentido, el artículo 32.1[58] enumera específicamente un conjunto, no exhaustivo, de medidas de seguridad que se podrían contemplar para un tratamiento, como son:

1. Aquellas orientadas a garantizar de confidencialidad, integridad y disponibilidad.
2. Aquellas orientadas a garantizar la resiliencia[59] de los sistemas y servicios de tratamiento, y dotar de la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
3. La seudonimización y el cifrado de datos personales.
4. Los procesos de verificación, evaluación y valoración regulares de las medidas de seguridad.

Del artículo 32.1 se concluye que hay que determinar el impacto que, para los derechos y libertades, podría tener un incidente que afectara al sistema de información, tanto con relación a la materialización de ataques, intrusiones o cualquier tipo de proceso no autorizado. También hay que evaluar dicho impacto para el caso de incidentes accidentales, tanto tecnológicos como humanos, y los asociados a eventos naturales. Del mismo modo, será preciso determinar el impacto para los derechos y libertades cuando el tratamiento no fuera automatizado.

Además, en dicha relación, se hace referencia explícita a la necesidad de gestionar los posibles errores o fallos que pudieran derivarse de las distintas medidas técnicas y organizativas que implementan estrategias de protección de datos por defecto, desde el diseño u otras garantías (los sistemas de garantías) como:

- En la seudonimización y el cifrado de datos personales ya señalados.
- Sobre los procesos de anonimización.
- En los procesos de desvinculación de datos.
- En la ejecución de la eliminación de datos.
- En la implementación de tratamientos federados.
- En la implementación de medidas de protección de datos por defecto.
- Etc.

---

[58] 32.1. 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.

[59] La resiliencia es la capacidad que tiene un sistema de continuar dando servicio ante un imprevisto, aunque sea con pérdida eficacia o eficiencia. Mientras que la disponibilidad es una razón de los días que el sistema da servicio entre los que no da servicio. Por ejemplo, un servidor con disponibilidad del 99,9% nos informa que estará parado 8,7 horas de media al año.

Finalmente, es necesario gestionar los errores técnicos derivados de la implementación automatizada de tratamientos de datos personales que se pudieran derivar de, por ejemplo:

- Sistemas de decisión automática.
- Sistemas de ayuda a la decisión.
- Tratamiento biométrico.
- Errores en la sincronización de sistemas transaccionales.
- Errores en la separación de entornos virtuales.
- Etc.

Los fallos y errores anteriores pueden derivar en problemas específicos de confidencialidad, integridad, disponibilidad, trazabilidad o autenticación, pero también otros más específicos como de calidad de datos, discriminación, etc. Además, la experiencia práctica nos demuestra que la estimación del impacto que tienen estos fallos y errores en los datos personales no se suele tener en cuenta. Por lo tanto, se considera necesario que se estudien de forma singular a la hora de analizar el riesgo para los derechos y libertades.

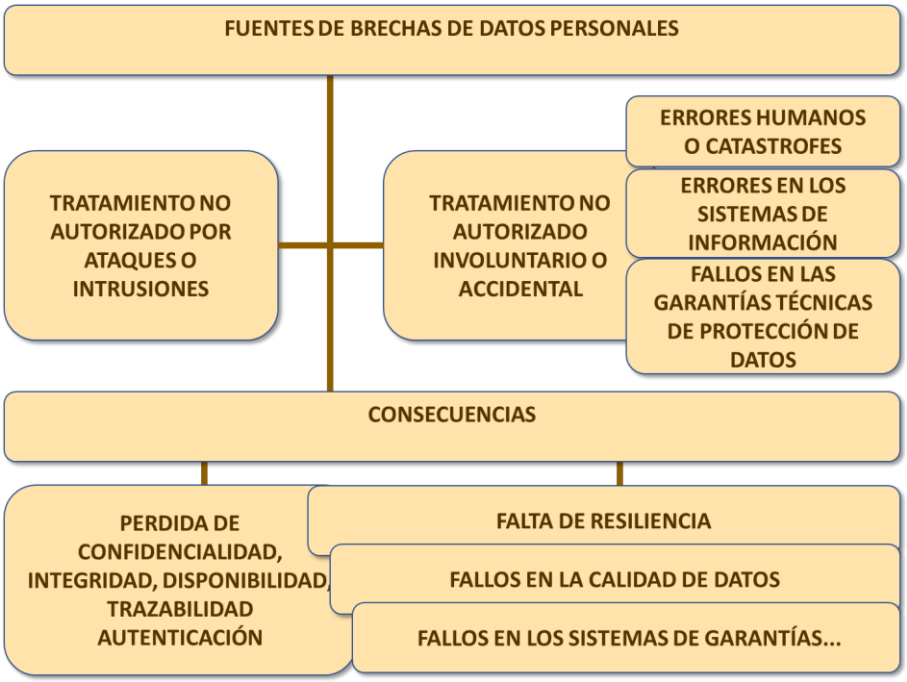

Figura 12: Fuentes de brechas de datos personales

3. Estimación del nivel de riesgo de una brecha de datos personales

Para estimar el impacto que pudiera tener una brecha de datos personales hay que plantearse las consecuencias que se derivarían de la materialización de la brecha. Una forma de hacerlo es plantearse los posibles escenarios de materialización de una brecha, determinar sus consecuencias, y evaluar cómo afecta a los derechos y libertades de los interesados, sobre todo si se trata de consecuencias irreversibles.

Ante esas consecuencias, hay que determinar medidas para disminuir la probabilidad de que suceda la brecha. Dado que la posibilidad de materialización de la brecha

siempre existe, también hay que considerar medidas para eliminar, disminuir o revertir las consecuencias de la misma sobre el interesado.

Veamos un ejemplo simplificado. Consideremos el marco de aplicaciones de domótica o de control de consumo que podrían recoger la actividad doméstica de personas físicas. En este caso, se deberían plantear varios escenarios de brecha, uno de los cuales, podría ser el siguiente:

Tratamiento basado en aplicaciones de domótica o de control de consumo	**Escenario 1**
Brecha materializada:	Confidencialidad: se accede a los registros de actividad de los usuarios de los sistemas domóticos que se almacenan en un servidor central.
Datos comprometidos:	Datos básicos, datos de contacto, datos detallados sobre eventos del sistema, uso o consumo por minuto durante un largo periodo de tiempo.
Perjuicios al interesado:	Se conoce la dirección y detalles de identificación del usuario. Se podría inferir cuándo el hogar está vacío. Se podría inferir los horarios de entrada y salida del hogar. Se podría inferir si el individuo vive solo o acompañado. Se podría inferir cuándo se va a dormir. Se pueden inferir aspectos muy personales, e incluso categorías especiales de datos. Etc.
Evaluación del impacto sobre el interesado:	Puede tener un impacto muy significativo, al afectar a los derechos y libertades fundamentales de forma irreversible.
Medidas para reducir el impacto:	Reducir la precisión temporal en la recogida de datos, y en lugar de hacerlo por minuto, hacerlo por horas, días o semanas (reducir la granularidad) Agrupar datos de diversos individuos (aumentar la agregación). Reducir el conjunto de datos recogidos (minimización de datos). Eliminar la información recogida individualmente en muy breve espacio de tiempo, casi tiempo real (conservación de datos). Disponer de un procedimiento de comunicación a los afectados muy rápido (comunicación de brechas de datos). Etc.
Medidas para reducir la probabilidad:	Medida de identificación para el acceso al sistema. Sistemas de control de acceso a los datos. Cifrar la información en tránsito y reposo. Etc.

Tabla 7 Ejemplo de escenario de brechas de datos personales

Del ejemplo anterior se pueden extraer las siguientes reflexiones:

- Los escenarios han de plantearse para casos de pérdida de confidencialidad, disponibilidad, integridad, autenticación, trazabilidad, resiliencia, fallos en las garantías (como reidentificación en datos anónimos o pseudónimos), errores en el tratamiento o cualquier otro que se considere oportuno.
- Además de medidas que reduzcan la probabilidad, es necesario implementar medidas que reduzcan el impacto de una brecha, ya que la probabilidad de que se produzca una brecha nunca es cero.
- Las medidas que reducen el impacto son, en muchos casos, medidas de privacidad desde el diseño y/o por defecto.
- Existen medidas que son preventivas, p.ej. aplicar políticas de agregación de datos, y otras que son reactivas, p.ej. tener preparada una gestión de brechas que permita la comunicación ágil a los afectados.
- En la evaluación del riesgo, hay que evaluar qué impacto puede tener para el individuo y la sociedad, ya que hay brechas cuyo impacto social hace más difícil minimizar los riesgos. En el ejemplo mostrado anteriormente, si la brecha afecta a un único individuo se pueden poner en marcha mecanismos reactivos que son inviables si afectan a miles de usuarios.

Por lo tanto, sin perjuicio de otras gestiones y medidas que se adopten, la evaluación del riesgo para los derechos y libertades no queda cubierta tan solo con la evaluación del impacto que un incidente tenga para la organización. Además, la adopción de las medidas de seguridad ha de realizarse bajo una visión de la gestión de los riesgos para los derechos y libertades que va más allá del ámbito estricto de la organización. Es decir, el análisis no puede solo centrarse en el impacto del incidente en la relación del interesado con la entidad, ya que se podrían dar situaciones como, por ejemplo:

- Una pérdida de confidencialidad en la Entidad-A puede suponer la usurpación de identidad de un sujeto. Esa suplantación se puede utilizar sobre la Entidad-B para acceder a los datos del interesado.
- La alteración de la integridad de los datos de una persona en una Entidad-A puede impedir que dicha persona acceda a servicios proporcionados por una Entidad-B.

4. La probabilidad de una brecha de datos personales

Para determinar el nivel de riesgo será necesario determinar la probabilidad de que dicho riesgo se materialice. En este punto, hay que afrontar la realidad que nos muestran todos los días los registros de incidencias de seguridad y que es la siguiente: Los sistemas fallan. No existen sistemas 100% seguros. Por lo tanto, no se pueden plantear tratamientos bajo el supuesto de que la seguridad nunca va a ser violada.

Más aún, cuando el periodo de tiempo en el que el tratamiento estará activo (ciclo de vida del tratamiento) tiende a infinito, el que se produzca una brecha de datos personales es sólo cuestión de tiempo:

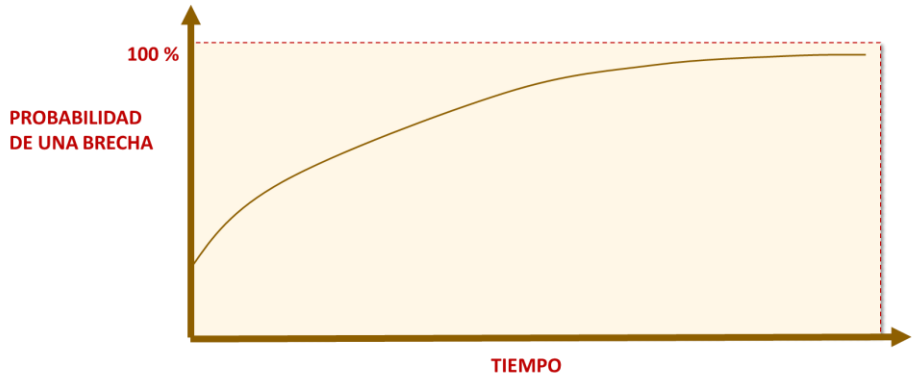

Figura 13: Evolución de la probabilidad de una brecha en el tiempo

La probabilidad de que se materialice una brecha nunca es cero, y cuanto más tiempo transcurre, mayor es la posibilidad de que ocurra un incidente. Por lo tanto, a la hora de evaluar la probabilidad, hay que tener en cuenta el plazo de tiempo que se pretender tener activo el tratamiento en cuestión.

5. Resiliencia

El artículo 32.1 del RGPD exige tanto disponibilidad como resiliencia, conceptos que pueden estar relacionados, pero son distintos. La disponibilidad es la propiedad de un activo de ser accesible y usable bajo demanda por una entidad autorizada[60].

El término resiliencia se refiere a la capacidad de adaptación de un organismo, organización, sistema o sociedad a los cambios sin que sus características básicas estructurales y funcionales se vean alteradas. Estas, han de adaptarse sin alcanzar el punto de ruptura, parálisis o crisis. Tras esa adaptación, la entidad puede volver a su estado original o incluso haber mejorado su adecuación al entorno. Esto significa la capacidad de asumir, con flexibilidad, situaciones límites y sobreponerse a ellas.

La resiliencia organizacional estudia la resiliencia en organizaciones. Para alcanzarla, la organización ha de anticiparse, prepararse, responder y adaptarse a los cambios o eventos que se puedan producir. Estos pueden ser cambios en el contexto económico, político, legal, social, ambiental, etc.; así como daños en la infraestructura, actos de terrorismo, cibercrimen, etc.

La resiliencia es inherente, relativa y ninguna organización, red o sistema puede ser totalmente resiliente. El grado de resiliencia dependerá de:

[60] Definición en la ISO-27001

Capacitación de las personas.	El personal, tanto del nivel más alto al más bajo, ha de tener la capacidad de detectar los cambios, la capacidad de comunicarlos, la capacidad de entenderlos, la capacidad de innovar ante ellos, la capacidad de actuar y la voluntad actuar de forma proactiva, en tiempo real.
Flujo adecuado de información	Ha de ser ágil, específico, mínimo, completo y desde y hacia las personas adecuadas.
Liderazgo	Han de existir puntos claros de toma de decisión con responsabilidades bien definidas.
Adaptabilidad estratégica	Las estructuras físicas, tecnológicas y organizativas han de poder evolucionar en tiempo real hacia nuevos objetivos o formas de actuar.

Tabla 8 Factores que determinan el grado de resiliencia de una organización

La resiliencia organizativa, como toda medida de seguridad, descansa fundamentalmente en las personas. La resiliencia ha de permitir adaptarse a la velocidad necesaria, teniendo una visión holística de la conectividad de todos los eventos que se producen en el contexto interno y externo a la organización. Por tanto, la resiliencia debe estar integrada en toda la organización.

A su vez, resiliencia y sostenibilidad son conceptos relacionados, pero distintos. La resiliencia está vinculada al grado de preparación para la reacción de la organización ante un contexto variable. La sostenibilidad de la organización está relacionada con las acciones para evitar o mitigar sus impactos en el interior y exterior a la empresa, en su entorno, asegurando su propia viabilidad a largo plazo, y de contribuir, a su vez, a la del entorno.

6. Integración de los requisitos de gestión del riesgo para los derechos y libertades en el SGSI

La gestión de la seguridad de la información es una disciplina muy madura, con modelos de gestión (SGSI o Sistema de Gestión de la Seguridad de la Información) y directrices (normas ISO 27000 o ENS) bien conocidas e implantadas que pueden considerarse estándares de seguridad.

Los sistemas de información son una proyección de los tratamientos de la entidad, en tanto que son los medios que le dan soporte y, por ello, las políticas de los sistemas de información deberían ser una proyección de las políticas de información de la entidad. A su vez, las políticas de seguridad son un subconjunto de las políticas de información de la entidad.

El diseño, mantenimiento y operación de los sistemas de información, manuales y automáticos, se nutre de un conjunto de requisitos funcionales y no funcionales. Uno de esos requisitos no funcionales son los requisitos de seguridad, acordes a los objetivos de la entidad y que, a su vez, se traducen en requisitos específicos de seguridad del sistema de información.

Sin embargo, en organizaciones donde los niveles de gestión eran pobres, las políticas de los sistemas de información han sido el motor de la ordenación de los procesos de la entidad. La propia naturaleza de estos exige una aproximación sistematizada a la implementación de tratamiento. Por eso, en algunas organizaciones, las políticas de los sistemas de información que surgían de los departamentos TIC venían a suplir la carencia de políticas de información y de políticas de calidad en la entidad.

Este enfoque, reactivo y de abajo a arriba, es contrario al modelo de responsabilidad proactiva, donde las decisiones se han de tomar de arriba abajo, desde el diseño de los tratamientos en la organización y con una visión holística. Además, esta aproximación ha tenido consecuencias negativas como, por ejemplo, obligar a los administradores de los sistemas de información a tomar decisiones sin que existieran directrices claras ni canales de comunicación para transmitir las necesidades finales de los procesos de la entidad, de sus políticas comerciales o respecto a los criterios de eficacia y de eficiencia. Los administradores de los sistemas de información deben implementar los requisitos de seguridad que proporcione el responsable de seguridad con una visión integral de la organización, pero no deben de llevar a cabo la toma de decisiones con relación a la seguridad más allá de las cuestiones técnicas y operativas relacionadas con la propia administración de los sistemas.

En particular, el conjunto de requisitos de seguridad, con relación a los derechos y libertades, ha de ser una de las entradas al proceso de análisis de riesgos general de los sistemas de información que ha de llegar al departamento TIC.

Los requisitos no funcionales de seguridad pueden provenir de distintos objetivos de la entidad en general y de los tratamientos de datos que se realizan, en particular: seguridad de las personas, robo, fraude, etc. A su vez, será necesario tener en cuenta otros requisitos funcionales y no funcionales, además de los que se deriven de normativas, obligaciones contractuales, certificaciones, etc.

Figura 14: Integración de los requisitos de seguridad para la protección de los derechos y libertades

La forma de implementar dichos requisitos ha de balancearse entre los distintos objetivos. Por ejemplo, si con objeto de proteger la seguridad de las personas se plantea

una solución basada en identificación biométrica, ha de valorarse que puede colisionar con protección de datos o con la imagen que la empresa quiere proporcionar. Otro ejemplo podría ser, con el propósito de evitar el fraude, la implementación de procedimientos de autenticación tan robustos que colisione con las estrategias de venta y de accesibilidad de los productos.

7. Medidas de gestión brechas[61] de datos personales.

La gestión de incidentes es uno de los objetivos de control específicos de seguridad. El RGPD dedica a este objetivo dos artículos, el 33 y 34 y tres considerandos, el 85, 86 y 88, donde establece obligaciones a los responsables con relación a la notificación de las brechas de datos personales a la Autoridad de Control y de la comunicación de su ocurrencia a los interesados en función del riesgo para los derechos y libertades que representen.

La gestión de brechas es una obligación del responsable, que debe incluir el establecimiento de medidas preventivas y reactivas en función del riesgo y que repercute en el ciclo de gestión del riesgo del tratamiento. Es decir, el responsable debe, de forma preventiva, implementar mecanismos de detección y gestión de las brechas. La detección de una brecha no solo supone el empleo de medios técnicos, sino que supone que una información completa sobre las dimensiones e impacto de la brecha llegue a tiempo a los órganos de decisión que deben actuar ante la misma.

Además, antes de que se materialice una brecha de datos personales, el responsable debe estar preparado para cumplir, al menos, las obligaciones que se derivan de la normativa. El grado de preparación que ha de tener el responsable debe determinarse en función de la evaluación del riesgo que represente la ocurrencia de una brecha de datos personales.

Por otro lado, finalizadas las acciones inmediatas de reacción ante la brecha, el responsable tendrá que abordar, dentro del ciclo de gestión del riesgo, todas aquellas medidas que fueran necesarias para prevenir que el incidente[62] o la brecha pudieran volver a ocurrir. Esta tarea implicará la revisión de los controles que estuvieran relacionados con la ocurrencia de la brecha, así como posible la implantación de nuevos controles que pudieran ser necesarios.

En otro orden de ideas, la norma establece una serie de obligaciones ante la ocurrencia de una brecha de seguridad que no dependen de la realización de un análisis de riesgos como, por ejemplo, la obligación del encargado del tratamiento de notificar, sin dilación indebida, al responsable del tratamiento las brechas de datos personales que afecten a los tratamientos encargados (art.33.2) o la obligación del responsable del tratamiento de documentar cualquier brecha de datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas (art. 33.5).

Otra de las obligaciones que no dependen de la gestión del riesgo es que el responsable ha de ser capaz de detectar la materialización de las brechas de datos de

[61] El término resultante de la traducción del RGPD al castellano es el de "violaciones de seguridad" aunque en el presente documento se ha preferido utilizar el término más comúnmente utilizado de *"brechas" de datos personales para designar a "toda violación de la seguridad que ocasione 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"*.

[62] El artículo 35.5 del RGPD obliga al responsable a documentar o registrar cualquier hecho relacionado con una brecha de datos personales incluidos los hechos relacionados con ella. Debe de considerarse un incidente de seguridad de los datos personales cualquier hecho o situación que pueda relacionarse con una brecha de seguridad en la medida que pudiera suponer o facilitar una brecha de seguridad de los datos personales con independencia de que se haya materializado en un perjuicio para cualquiera de las dimensiones de seguridad.

carácter personal y ha de tener la capacidad de gestionarlas para dar cumplimiento a las obligaciones de los artículos 33 y 34.

Lo que sí depende de la gestión del riesgo es la dimensión de las medidas técnicas y organizativas para la gestión de incidentes, como podrían ser:

- Utilización de herramientas de gestión de incidentes adaptadas al RGPD.
- Procedimientos establecidos de cumplimiento de las obligaciones relativas a los artículos 33 y 34 del RGPD.
- Protocolos de identificación de riesgos adicionales generados por la brecha y de reevaluación del nivel de riesgo para los derechos y libertades de los sujetos del tratamiento.
- Etc.

Más información sobre la gestión de brechas de protección de datos personales se puede encontrar en los siguientes recursos:

- Guía para la notificación de brechas de datos personales
- Herramienta para evaluar la obligación de comunicar a los interesados: COMUNICA-BRECHA RGPD
- Formulario de notificación de brechas a la Autoridad de Control
- Microsite sobre brechas de datos personales

F. IMPLEMENTACIÓN DE LOS CONTROLES, VERIFICACIÓN Y REEVALUACIÓN: LA GESTIÓN DEL RIESGO COMO UN PROCESO CONTINUO

Una vez decidido el conjunto de controles es necesario desplegarlos a lo largo del proceso de concepto, diseño e implementación del tratamiento, así como en su evolución o cuando se detecte la necesidad de revisión del mismo.

En la gestión del riesgo es preciso continuar la observación del tratamiento y auditar sus resultados de forma periódica a fin de garantizar que la eficacia de las medidas implementadas se mantiene, los resultados obtenidos son los esperados[63] y la naturaleza, ámbito, contexto y fines no han sido alterados.

La verificación de la correcta aplicación de las medidas y garantías, así como la revisión del nivel de riesgo y su gestión, es un proceso que hay que realizar a lo largo de todo el ciclo de vida del tratamiento. Se recomienda realizar un proceso de verificación durante la fase de implantación con el objetivo de garantizar y validar que las medidas de control definidas en el Plan de acción se han puesto en marcha correctamente.

El escenario ideal es que estas tareas, con carácter general, se integren en las políticas y procedimientos de la entidad con relación a la gestión del ciclo de vida del tratamiento. En definitiva, que estén reflejadas en un plan de acción de gestión del tratamiento.

Son varias las referencias del RGPD a esta necesidad de introducir la gestión del riesgo a lo largo de las distintas etapas del ciclo de vida del tratamiento. El artículo 24

[63] Considerando 74 "Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, 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."

establece que las medidas para la gestión del riesgo “se revisarán y actualizarán cuando sea necesario”. A su vez, el artículo 25[64], donde se establece la Protección de Datos desde el Diseño y por Defecto, establece que estas medidas se aplicarán “en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento”. El artículo 32, sobre Medidas de Seguridad, en su apartado 1.d, establece la obligación de “un proceso de verificación, evaluación y valoración regulares”. Finalmente, en el artículo 35, sobre la EIPD, establece que esta se realizará “antes del tratamiento”.

A este respecto, las Directrices WP248 señalan:

> *En la práctica, esto significa que los responsables deben evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuando es probable que un tipo de tratamiento entrañe «un alto riesgo para los derechos y libertades de las personas físicas».*

En la nota 6 de las mismas Directrices WP248 se expone:

> *Cabe señalar que, a fin de gestionar los riesgos para los derechos y libertades de las personas físicas, dichos riesgos deben identificarse, analizarse, estimarse, evaluarse, tratarse (p. ej., mitigarse) y revisarse con regularidad.*

Por lo tanto, la gestión del riesgo es un proceso continuo y cíclico. Dicha gestión ha de realizar su primer ciclo con las primeras fases del tratamiento: antes de determinar los medios del tratamiento (en su concepción, análisis, diseño, prototipado e implementación) y antes de ejecutar el tratamiento (pruebas y preparación/despliegue). Además, la gestión del riesgo ha de repetirse a lo largo del ciclo de vida del tratamiento para evaluar y tratar los cambios que se puedan producir en las fases siguientes (operación, mantenimiento, evolución y retirada).

[64] 1. Teniendo en cuenta … 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, …, e integrar las garantías necesarias en el tratamiento …

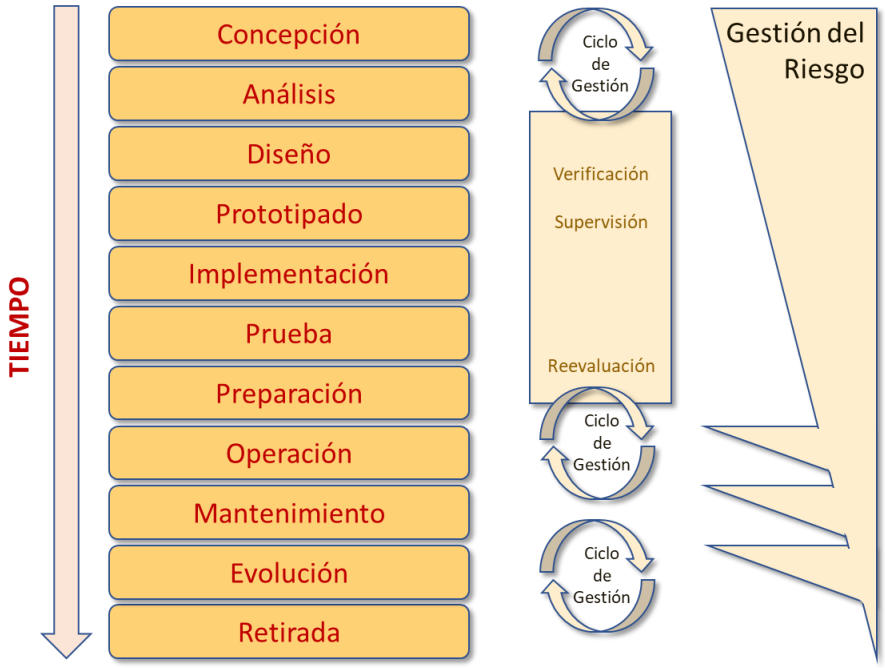

Figura 15: La gestión del riesgo en el ciclo de vida del tratamiento

La figura pretende dar una visión genérica del esfuerzo que podrían requerir las distintas iteraciones de la gestión del riesgo a lo largo del ciclo de vida del tratamiento, siendo necesario realizar algunas puntualizaciones:

- La gestión del riesgo se ha de realizar, en una primera iteración, en la concepción del tratamiento.
- Existen unas fases en las que, *a priori*, las acciones derivadas de la gestión del riesgo se tendrían que verificar, y en su caso reevaluar, y donde esta actividad podría tener una mayor intensidad, como son las fases de operación, mantenimiento y evolución.
- La reevaluación del riesgo se puede iniciar por eventos propios a fases distintas de la fase en la que se encuentre el tratamiento dentro de su ciclo de vida y depender del contexto, es decir, de eventos externos al tratamiento.

Con relación a la verificación y reevaluación, como establece el artículo 24, las medidas para conseguir la conformidad con el RGPD han de estar guiadas por "la naturaleza, el ámbito, el contexto y los fines del tratamiento", además de los riesgos. La actividad de tratamiento puede evolucionar a través de cualquiera de sus etapas debido a la variación del contexto, a la introducción de nuevos factores externos, la identificación de nuevas necesidades, la modificación de los medios tecnológicos utilizados, etc. modificándose la exposición al riesgo y haciendo necesaria la reevaluación del mismo.

Por lo tanto, la organización ha de implementar procedimientos que detecten problemas, cambios o eventos en el tratamiento o en su entorno que sean susceptibles de desencadenar la necesidad de iniciar un ciclo de revisión de la gestión del riesgo. Si no se detectan problemas, cambios o eventos que pudieran dar lugar al inicio de un ciclo de revisión será necesario establecer periodos de revisión que podrían estar fijados en el marco de las políticas de protección de datos del responsable[65].

[65] Artículo 24.2 RGPD.

En este proceso es de vital importancia la gestión de incidentes (de todo tipo) o la información que se puede inferir de las reclamaciones de los interesados en el ejercicio de sus derechos en materia de protección de datos.

En particular, en aquellos casos en los que la necesidad del tratamiento puede estar justificada por eventos externos de carácter temporal o transitorio, como situaciones de emergencia, se han de establecer cláusulas de caducidad en la reevaluación del balance entre la injerencia para los derechos y libertades que represente el tratamiento y el beneficio social que genera.

Es muy importante destacar, como se ha señalado anteriormente, que la iteración de un ciclo de gestión del riesgo no ha de suponer un esfuerzo desproporcionado, sino que ha de ser una actividad eficaz y eficiente. Lo único que exige es reflexionar, aunque sea por un momento, si se sigue teniendo el tratamiento bajo control ante condiciones cambiantes del propio tratamiento y/o del contexto en el que este se desenvuelve.

Además, esta reflexión, ha de estar integrada en los procesos de gestión del tratamiento para que sea realmente efectiva.

IV. LA GOBERNANZA DE LOS RIESGOS PARA LOS DERECHOS Y LIBERTADES

A. POLÍTICAS DE PROTECCIÓN DE DATOS

El gobierno o gobernanza de datos es el proceso por el que se implementan políticas y procedimientos para garantizar una gestión efectiva y eficiente de la información en la entidad. Estas políticas se proyectan en la gestión de cada tratamiento específico. Entre las políticas que pueden ser necesarias en una organización, al menos deben tenerse en cuenta las políticas de protección de datos, como un medio para la reducción del riesgo.

Cuando se trata de datos personales, la gobernanza de los datos establecida en la organización ha de garantizar el cumplimiento de los derechos y libertades conforme al RGPD. Para ello, los tratamientos de datos personales deben estar respaldados por la implementación efectiva de los principios relativos al tratamiento (art.5 RGPD), tomando las medidas adecuadas y ofreciendo garantías suficientes. En virtud del principio de responsabilidad proactiva, las políticas han de ser compromisos establecidos a nivel de la dirección de la organización.

El considerando 78 declara *"… el responsable del tratamiento debe adoptar políticas internas…*" y el artículo 24.2 establece "*Cuando sean proporcionadas … la aplicación … políticas de protección de datos*[66]". Si entendemos el término "políticas[67]" como el conjunto de directrices que rigen la actuación de una organización en un asunto o campo determinado, las políticas de protección de datos definen un modo de actuar de la organización ante los tratamientos de datos personales a lo largo de todo su ciclo de vida.

Por lo tanto, lo que exige el RGPD con relación a las políticas de protección de datos es el aspecto efectivo, práctico y ejecutivo de un conjunto de directrices, yendo más allá de la referencia al aspecto formal de la existencia de un documento titulado "política de protección de datos" donde se realiza la mera reproducción formal del articulado del RGPD y se reduce a una mera declaración de la voluntad de compromiso del responsable con el cumplimiento normativo. Con relación a las políticas, como en la gestión de riesgo, hay que evitar confundir el fondo con la forma, ya que es el fondo lo que reclama el RGPD.

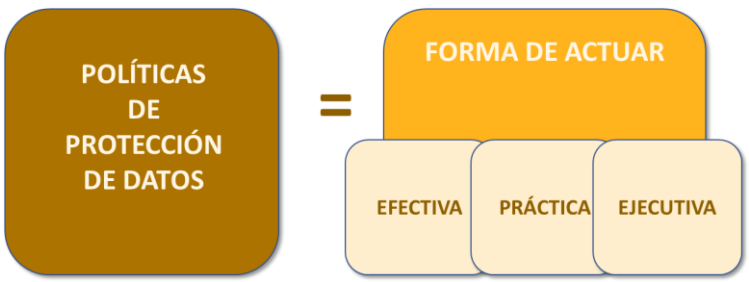

Figura 16: Las políticas de protección de datos

[66] No hay que confundir Política de Protección de Datos, con Política de Privacidad. Esta última, es un término que se aplica a las cláusulas informativas que dan cumplimiento a las obligaciones de transparencia del RGPD.
[67] Política: "Orientaciones o directrices que rigen la actuación de una persona o una entidad en un asunto o campo determinado".

Por supuesto, y con relación a la obligación de demostrar, dicha política ha de estar documentada. Pero dicho requisito no exige la existencia de un documento con ese título ni que las políticas estén definidas de forma independiente del resto de políticas de la organización. Al contrario, la aplicación práctica del RGPD necesita integrar directrices específicas para el mejor cumplimiento del RGPD en la documentación de los procedimientos aprobados por la entidad. Dependiendo de la complejidad de la organización, es recomendable que no se creen políticas o guías nuevas, sino que la protección de datos se integre con las políticas corporativas ya existentes y así disminuir la carga administrativa y de gestión.

En organizaciones más complejas, podría ser aconsejable disponer de un documento marco siempre que se emplee como guía para la adopción las directrices señaladas en procedimientos específicos como, por ejemplo, los procedimientos de recursos humanos, teletrabajo, contratación de productos y servicios, desarrollo de aplicaciones, etc. Pero siempre que tenga el objeto de garantizar la eficacia en la protección de datos y que no se limite a una pura declaración formal en un documento desvinculado de la realidad de los procedimientos de la entidad.

Figura 17: Relación entre gobernanza, políticas y procedimientos

Esta última, aunque será la expresión del compromiso de un responsable o un encargado para garantizar el cumplimiento del RGPD, tendrá utilidad siempre y cuando se emplee como directriz general a la hora de desarrollar los procedimientos específicos de la organización y sea posible demostrar que dichos procedimientos específicos están siendo utilizados de manera adecuada.

Como establece el artículo 24, la implementación de dichas políticas y gobierno de los datos dependerá de la estructura orgánica de cada entidad. Por tanto, la aplicación de políticas de protección de datos supondrá la aplicación de aquellos recursos, procedimientos y controles que pudieran ser necesarios para garantizar dicho cumplimiento en cada entidad concreta. De igual forma tendrán que adoptarse dichas políticas en las organizaciones que pudieran actuar como encargadas del tratamiento con la finalidad de abordar una gestión y control eficaces que garanticen al responsable el cumplimiento del RGPD.

Figura 18: Marco de la ejecución de las políticas de protección de datos[68]

Dichas políticas se deberán verificar, revisar, actualizar y mejorar de forma continua, de acuerdo con los criterios y métodos implantados en la organización[69].

B. DOCUMENTACIÓN

La obligación de documentar el proceso de gestión del riesgo está relacionada con el cumplimiento de la obligación de "accountability". La documentación tiene dos objetivos generales:

- En primer lugar, y siendo su objetivo más importante, dar soporte a la ejecución eficaz y eficiente de la gestión del riesgo para los derechos y libertades.
- En segundo lugar, y supeditado al primero, permitir demostrar que así se ha realizado.

Por lo tanto, la documentación de la gestión del riesgo:

Es una herramienta de trabajo	Ha de ser útil para la ejecución de la gestión del riesgo de forma eficaz.
Ha de ser eficiente	Ha de suponer una carga mínima en la gestión del tratamiento.
Ha de ser completa	Ha de recoger las decisiones tomadas en la gestión del riesgo, así como la justificación de dichas decisiones basadas en evidencias objetivas.
Ha de ser dinámica	Se ha de mantener y hacer evolucionar en la medida en que se produzcan cambios en el

[68] Basado en ISO-31000 Gestión del Riesgo – Principios y Directrices
[69] Por ejemplo, siguiendo un ciclo PDCA o de mejora continua.

	tratamiento, en su contexto o incidencias que le afecten.
Ha de ser trazable	Permitirá realizar el seguimiento y la evolución en el tiempo del proceso de gestión del riesgo.
Ha de comunicarse	Ha de llegar a los órganos adecuados de toma de decisión, de ejecución de las decisiones y de control.
Ha de transmitir información	Ha de tener el formato, lenguaje y el contenido necesario para que se puedan ejecutar dichas acciones con eficacia y eficiencia
No es monolítica	Ha de estar formada por distintos documentos, adaptados a los distintos destinatarios de la información.
Ha de estar integrada en la gestión de la organización	En línea de lo manifestado con relación a las políticas de protección de datos, ha de estar integrada con el resto de documentación asociada a la gestión del tratamiento en otros aspectos.

Tabla 9 Características de la documentación para la gestión del riesgo

Por lo tanto, en primer lugar, la documentación no es la gestión del riesgo, aunque la gestión de riesgo ha de estar documentada.

A su vez, la documentación no exige escribir un único documento compacto, sino tener un sistema de registro de los análisis, decisiones y seguimiento de las acciones. La complejidad de este sistema, como interpreta la Declaración WP218[70], se deberá adaptar a la complejidad y el impacto del tratamiento, y podría tomar diferentes formas, desde una hoja de cálculo hasta una base de datos o, incluso, un sistema de gestión documental.

La documentación de la gestión del riesgo tampoco es un informe jurídico. En la medida que la documentación adquiera un volumen engorroso que no permita la gestión eficaz y eficiente del riesgo, no será adecuada. De esta forma, ha de recogerse toda la información necesaria para una gestión eficiente y solo dicha información.

[70] 6/ The form of documentation of the processing activities can differ according to the risk posed by the processing. Yet, all data controllers should at least to some extent document their processing activities in order to further transparency and accountability. Documentation is an indispensable internal tool for controllers to manage accountability effectively and for ex-post control by DPAs as well as for the exercise of rights by data subjects. It goes beyond information to be given to the data subjects.

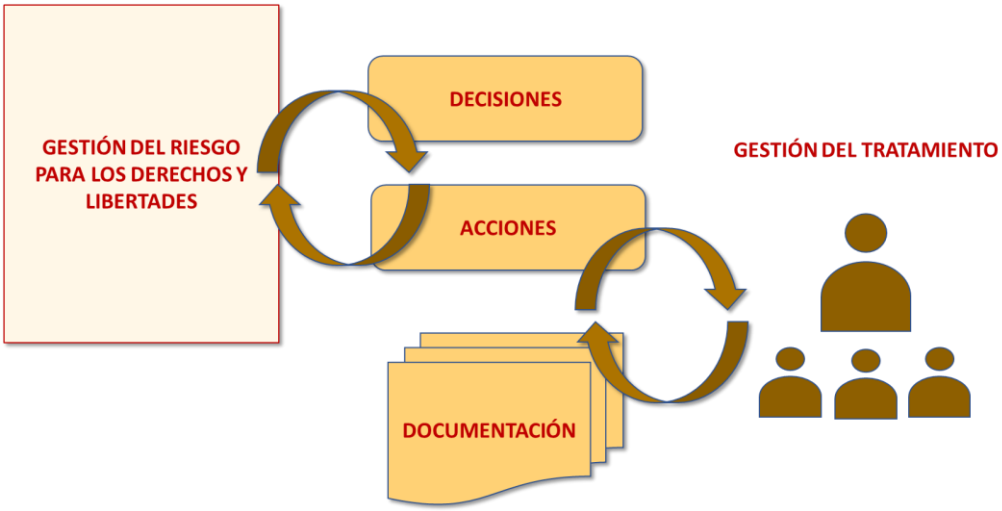

Figura 19: La documentación del proceso de gestión del riesgo

La documentación de la gestión del riesgo tendrá que contener unos elementos mínimos:

1. Quién lo realiza.
2. Quién lo aprueba.
3. La descripción del tratamiento.
4. Metodologías y guías empleadas en el proceso de gestión.
5. La identificación y análisis de riesgos para los derechos y libertades.
6. La evaluación del nivel de riesgo para los derechos y libertades.
7. La decisión de realizar o no una EIPD (análisis de obligación y análisis de necesidad de EIPD).
8. Las medidas seleccionadas y un plan de implementación y seguimiento.
9. Los criterios para reevaluar el plan y los plazos de revisión
10. Incidencias detectadas
11. Fecha de realización o revisión.

Tabla 10 Contenido mínimo de la documentación de gestión del riesgo

Como se ha comentado antes, esta información podría ser un documento aislado o estar integrado en la documentación de gestión de los tratamientos de la organización. A su vez, la descripción del tratamiento tendrá que ser congruente con la información registrada en las herramientas sobre las se ha implementado el RAT[71].

Adicionalmente, con relación a la documentación sobre las metodologías seguidas, se podría documentar:

- La decisión de elegir una determinada metodología.
- Identificación de la escala cualitativa o cuantitativa utilizada para describir la magnitud potencial del riesgo.

[71] Por ejemplo, si la descripción del tratamiento cumple las obligaciones del RAT, la misma documentación hace las funciones del RAT. Si no, el RAT deberá estar incluido en los documentos de gestión de los procesos de la entidad.

- Identificación de las posibles consecuencias (impacto) que una amenaza puede tener sobre el tratamiento y los propios interesados en el supuesto de que llegara a materializarse.
- Identificación de la probabilidad de materialización de una amenaza teniendo en cuenta sus vulnerabilidades. Con carácter general, a mayor número de vulnerabilidades, mayor probabilidad de que una amenaza llegue a materializarse.
- Criterios utilizados para la evaluación del riesgo y objetivos de nivel de riesgo considerados aceptables.

En cuanto al grado de trasparencia a aplicar a la documentación, las Directrices WP248 estipulan que no hay obligación de publicar esta información, con las siguientes apreciaciones:

> *"¿Existe la obligación de publicar la EIPD? No, pero publicar un resumen podría fomentar la confianza, y se debe comunicar la EIPD completa a la Autoridad de Control en caso de consulta previa o si así lo solicita la APD."*

Por lo tanto, la publicación, o no, de la documentación relativa a la gestión del riesgo, ya sea de forma total o parcial, puede depender de las políticas de transparencia de la entidad. Pero también habrá que valorar si la transparencia puede ayudar a la gestión de los riesgos para los derechos y libertades vista esta como una medida de privacidad desde el diseño.

Lógicamente, no sería justificable ni recomendable la publicación de información detallando elementos concretos de las medidas para la gestión del riesgo que pudieran aumentar dicho riesgo. Aunque la gestión de los riesgos no se puede sustentar sobre la ocultación de las medidas adoptadas[72], un exceso de publicidad podría suponer un riesgo tanto para la organización como para los propios interesados[73].

[72] Lo que se denomina "security through obscurity"

[73] El análisis de riesgos puede incluir detalles de los activos utilizados en el tratamiento: sistemas de información, topología de red, versiones de productos utilizados, etc. Esta información es crítica para la organización y valiosa para un atacante que pretenda acceder de forma no autorizada a la organización, además esta información puede ser utilizada en combinación con otras informaciones publicadas por la organización en diferentes medios (ingeniería social).

SECCIÓN 2: METODOLOGÍA BÁSICA PARA LA APLICACIÓN DE LA GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES

V. DESCRIPCIÓN Y CONTEXTUALIZACIÓN DEL TRATAMIENTO

Una correcta gestión del riesgo para los derechos y libertades exige conocer los detalles del tratamiento.

La mejor forma de realizar la descripción de un tratamiento es la que se ajuste a la descripción de procesos que ya se utilicen en los sistemas de gestión y de calidad de la entidad. Se exigen dos únicos requisitos para que dicha descripción sea adecuada. El primero, que dicha descripción se extienda para incluir la información establecida en el artículo 30 del RGPD, sobre los mínimos exigibles en los registros de actividades de tratamiento. El segundo, que la información que contiene sea suficiente para poder realizar una eficaz gestión del riesgo para los derechos y libertades de las personas físicas.

Existen distintas metodologías para formalizar el estudio de un tratamiento. En este capítulo se ofrece una metodología para la descripción del tratamiento que tiene carácter de mínimos y pretende servir de ayuda a aquellos que necesiten implantar una metodología desde cero. Cualquier otra podría ser adecuada si cumple con lo señalado en el párrafo anterior. A la hora de elegir una metodología u otra, se recomienda que esta esté integrada en los sistemas de gestión de la organización.

La granularidad que se debe alcanzar en la descripción del tratamiento ha de ser la suficiente para que sea posible realizar dicha gestión. En este sentido se podría estudiar el tratamiento hasta en tres niveles de detalle:

- Estudio a alto nivel del tratamiento.
- Análisis de la estructura del tratamiento, o descomposición del tratamiento en fases para realizar el estudio individual de las mismas.
- Análisis del ciclo de vida de los datos.

La profundidad en el estudio del tratamiento, es decir, la decisión de solo realizar el estudio a alto nivel o llegar hasta un análisis completo del ciclo de vida de los datos, dependerá del posible nivel de riesgo y de la complejidad del tratamiento.

Figura 20: Niveles en la descripción del tratamiento

La información proporcionada por los anteriores niveles de descripción se podría completar con análisis adicionales, como son el inventario de activos y la descripción de casos de uso. Todos estos niveles de descripción se desarrollan a lo largo de este capítulo.

Cuando el responsable, con el asesoramiento del DPD si está nombrado, alberga dudas sobre la profundidad del estudio que se debería realizar, se recomienda llevar a cabo el análisis estructurado, como mínimo.

En cualquier caso, cualquier aproximación que se adopte para la descripción del tratamiento ha de tener como objetivo disponer de un instrumento útil para "garantizar y poder demostrar"[74], de forma eficiente, la gestión del riesgo para los derechos y libertades. En ningún caso debe convertirse o interpretarse como una mera carga burocrática.

A. ESTUDIO A ALTO NIVEL DEL TRATAMIENTO

Un estudio a alto nivel del tratamiento aborda a este como un elemento monolítico, sin divisiones ni partes. Este estudio debe permitir realizar un análisis del riesgo con la formalidad que sea necesaria, y también puede servir para conseguir la información suficiente que permita cumplir con las obligaciones del art. 30 del RGPD y 31 de la LOPDGDD (RAT e inventario).

En la metodología empleada, dicho análisis debería poder proporcionar, al menos, la siguiente información:

Tratamiento	Nombre o descripción
Responsable/s	Identificación del responsable[75].
Fines de tratamiento	
Finalidad del tratamiento	

[74] Artículo 24 del RGPD
[75] En caso de corresponsabilidad, determinar dichas corresponsabilidades y sus límites.

Fines intermedios y secundarios[76]	
Alcance y ámbito del tratamiento	
Datos personales	
Datos personales tratados	Agrupados por categorías.
Precisión de los datos	Incluyendo, al menos: • La frecuencia de recogida. • La granularidad.
Ciclo de vida de los datos	Una descripción breve de su ciclo de vida, incluyendo: • Condiciones de supresión de los datos. • Tiempo máximo y mínimo de permanencia de los datos en el tratamiento.
Sujetos interesados	
Categorías de sujetos afectados	Establecer las posibles categorías de interesados para las que se pretende diseñar el tratamiento (menores, personas en riesgo de exclusión social, pacientes, alumnos, etc.). Se recomienda analizar posibles desequilibrios de poder entre los interesados y el responsable del tratamiento[77].
Volumen de sujetos	Cantidad de sujetos afectados.
Extensión geográfica	Local, regional, nacional o internacional. Especificando dicha extensión.
Duración del tratamiento	
Extensión en el tiempo del tratamiento	Tanto desde la puesta en producción hasta la propuesta de retirada del tratamiento. Descripción de circunstancias que podrían motivar la retirada del tratamiento.
Naturaleza	
Implementación del tratamiento	
Operaciones ejecutadas en el tratamiento	Por ejemplo: 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.
Casos de uso	

[76] Considerando 33: Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.
[77] Directrices WP248

Inventario de activos[78] que implementan el tratamiento	Especificando: • Humanos. • Organizativos. • Materiales. • Técnicos/Sistemas de información.
Recogida y generación de datos	
Origen de los datos	Externos al tratamiento (otros tratamientos, responsables, o entidades) o internos al tratamiento.
Datos inferidos o generados	Categorías de datos inferidos con relación a los fines del tratamiento.
Acceso a los datos	
Categorías de intervinientes en el tratamiento	Con relación a las fases del tratamiento, definir las categorías de intervinientes que participan en las operaciones.
Intervinientes externos y sus roles	Encargados, subencargados, desarrolladores, etc. Fases o etapas del tratamiento en las que intervienen y operaciones de tratamiento que tienen encomendadas por el responsable, así como el vínculo jurídico con el responsable del tratamiento.
Roles de acceso a los datos de los intervinientes	Para cada interviniente, definir sus roles con relación a las operaciones de tratamiento identificadas.
Flujos de información con otros tratamientos del responsable	Es necesario tener en cuenta los procesos de la organización relacionados con el tratamiento (gestión de calidad, inteligencia de negocio, directorios, agendas, etc.) a fin de identificar la relación de los procesos con los tratamientos de la organización en un único mapa de procesos/tratamientos.
Comunicaciones de datos	Identificación de las entidades a las que se transfieren datos, con sus localizaciones geográficas, habilitaciones legales y garantías establecidas para esa comunicación, así como cualquier otra información que sea relevante para la gestión del riesgo.
Debilidades	
Características/limitaciones y factores de riesgo relevantes de las tecnologías intervinientes	
Vulnerabilidades	Derivadas de los elementos técnicos, pero también humanos u organizativos, que pueden provocar accesos no autorizados o pérdida de calidad de datos, exactitud, disponibilidad, resiliencia, etc.

[78] Activo se define como todo bien o recurso que puede ser necesario para implantar y mantener una actividad de tratamiento a lo largo de todo su ciclo de vida, desde su concepción y diseño hasta el fin de la vida útil del tratamiento.

Medidas y garantías implementadas	
Políticas de protección de datos	
Medidas y garantías de privacidad y seguridad por defecto y desde el diseño del tratamiento	Conjunto de garantías jurídicas, organizativas y técnicas incorporadas al tratamiento con independencia del nivel de riesgo que pudiera asociarse al tratamiento.
Medidas y garantías de privacidad y seguridad adoptadas en función del riesgo.	Conjunto de garantías jurídicas, organizativas y técnicas que se adoptan en función del riesgo. Este apartado, podría estar vacío en la primera iteración del ciclo de gestión del riesgo. En función de que se vayan abordando los riesgos con distintas medidas, este apartado se iría completando.
Garantías en las transferencias internacionales	Cláusulas contractuales, BCR's u otras.
Contexto	
Sector de actividad	
Mercado o sector económico	
Marco normativo	
Marco normativo de aplicación	Se tendrán en cuenta, además de las normativas de protección de datos, las normativas sectoriales que fueran de aplicación al tratamiento.
Estándares, certificación, códigos de conducta aplicables al tratamiento	
Posibles efectos colaterales/no deseados del tratamiento	
Derivados del alcance y ámbito	
Derivados de la naturaleza de los datos	
Derivados del mercado o sector	
Otros efectos colaterales del tratamiento	
Brechas de seguridad	
Incidentes conocidos ocurridos en tratamientos similares	Por incidentes conocidos deben entenderse tanto incidentes de la propia organización como incidentes de otras organizaciones con similares o idénticos medios técnicos, organizativos, humanos, etc. En este contexto, puede resultar de ayuda la consulta del microsite de brechas de seguridad de la AEPD[79].

[79] https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-seguridad

Potenciales amenazas	Derivadas de los elementos técnicos, humanos u organizativos, así como de situaciones o contextos sociales determinados (crisis económica, pandemia, inestabilidad política o social, etc.) que aprovechando una vulnerabilidad de uno de los activos identificados pudieran dar lugar a brechas con consecuencias no deseadas para los derechos y libertades de los interesados.

Tabla 11 Información derivada de un análisis a alto nivel del tratamiento

B. ANÁLISIS ESTRUCTURADO DEL TRATAMIENTO

En el caso de que una descripción del tratamiento, como la mostrada en el apartado anterior, no sea suficiente para gestionar el riesgo para los derechos y libertades, será preciso realizar un análisis estructurado del tratamiento[80]. Para ello, se precisa identificar en el tratamiento las distintas operaciones que lo forman y la relación que existe entre ellas.

Figura 21: Elementos que describen una fase del tratamiento

Las operaciones de tratamiento que pueden formar parte de un tratamiento y que son de interés desde el punto de vista de la protección de datos, están definidas, de forma no exhaustiva, en el artículo 4 del RGPD como:

> *4.2 «tratamiento»: … 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.*

[80] Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks (WP218): *"Data subjects should have the same level of protection, regardless of the size of the organization or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner."*

A su vez, el artículo 4 del RGPD define dos tratamientos de datos que se pueden incorporar en dichas operaciones de tratamiento: la elaboración de perfiles[81] y la seudonimización[82].

El tratamiento "típico" incluirá, de forma general, las siguientes fases: captura de datos, clasificación y almacenamiento, uso y explotación, cesiones y transferencias de datos a terceros, bloqueo y/o supresión de los datos.

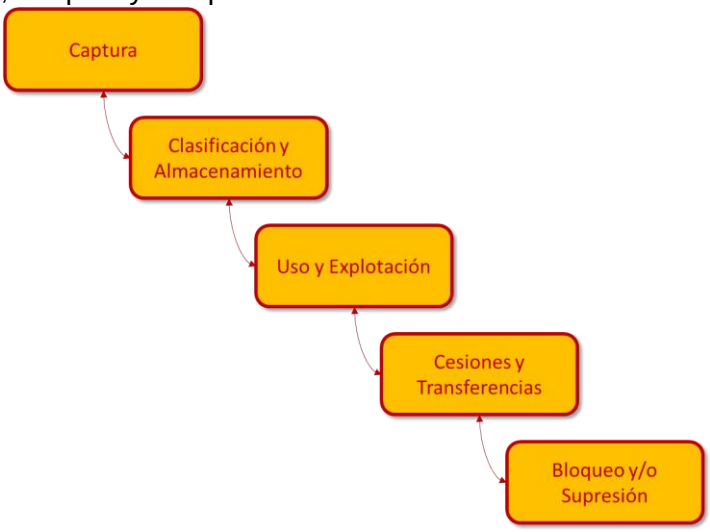

Figura 22: Estructuración en fases de un tratamiento genérico.

Esta es una aproximación simplista pero que podría ser un punto de inicio para realizar el análisis estructurado del tratamiento, el cuál podría ser más complejo e incluir varios casos de uso.

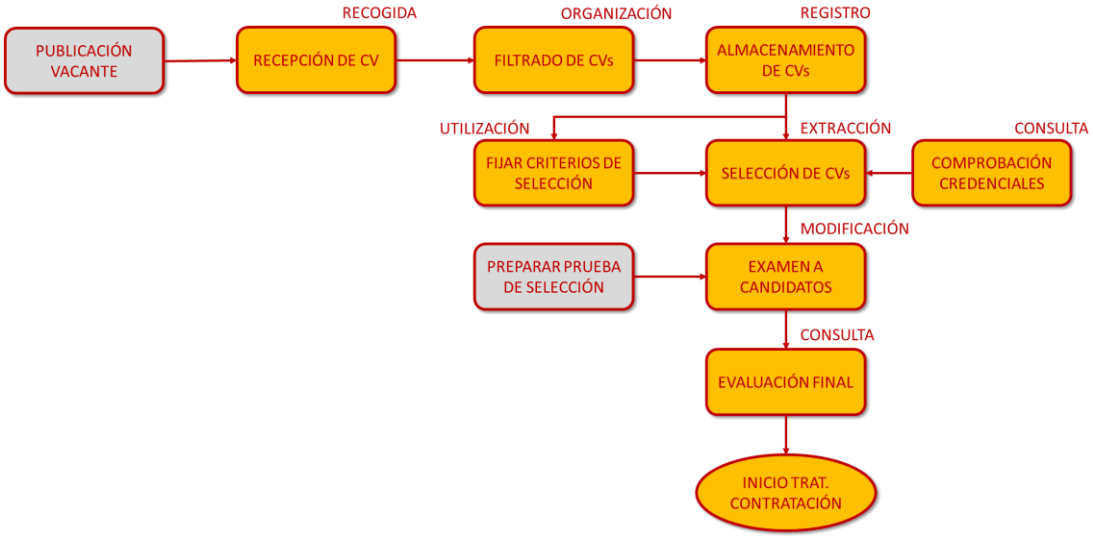

Figura 23: Ejemplo simplicado de una actividad de tratamiento relativa a la selección de personal. En este caso, se marca, para cada fase, la operación u operaciones realizadas. En

[81] 4.4 «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física

[82] 4.5 «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable

sombreado se encuentran aquellas fases que, en este ejemplo, no tratarían datos de carácter personal.

El grado de descripción de cada fase tendría que ser acorde al impacto en el riesgo que podría tener dicha fase. Como orientación, con el objeto de gestionar el riesgo, se podrían identificar los siguientes elementos para cada fase:

Nombre de la fase:	
Fases anteriores	
Fases posteriores	
Operación u operaciones realizadas	En una misma fase podrían ejecutarse varias operaciones.
Activos que implementan la operación	Entendiendo activos tal y como se han definido en el apartado anterior.
Características relevantes de la implementación de la fase	La implementación se puede realizar con medidas organizativas y/o elementos técnicos. Las medidas organizativas pueden incluir aspectos como la distribución física de las instalaciones (por ejemplo, el aislamiento de zonas de entrevista) o la generación y destrucción de informes físicos. Por otro lado, en el caso de componentes técnicos, se podrían identificar tecnologías disruptivas o uso novedoso de determinadas técnicas, entre otros.
Datos tratados	
Datos inferidos o generados	
Origen de los datos	Externos al tratamiento (otros tratamientos, responsables, o entidades) o internos al tratamiento.
Destino de los datos	Externos al tratamiento (otros tratamientos, responsables, o entidades) o internos al tratamiento.
Intervinientes externos, sus roles y funciones	Encargados, subencargados, desarrolladores, etc. y con distintas funciones: editor, soporte web, administrador, análisis, BBDD, marketing, etc.
Incidentes conocidos de fases implementadas con características similares, propios o ajenos	
Vulnerabilidades y amenazas	Derivadas de los elementos técnicos, pero también humanos u organizativos, que pueden provocar accesos no autorizados o pérdida de

	calidad de datos, exactitud, disponibilidad, resiliencia, etc.
Medidas y garantías de privacidad y seguridad por defecto	Conjunto de garantías jurídicas, organizativas y técnicas ya adoptadas.
Medidas y garantías de privacidad y seguridad adoptadas en función del riesgo	Conjunto de garantías jurídicas, organizativas y técnicas que se adoptan en función del riesgo. Este apartado, podría estar vacío o tener una primera aproximación, en la primera iteración del ciclo de gestión del riesgo. En función de que se vayan abordando los riesgos con distintas medidas, este apartado se iría completando.

Tabla 12 Descripción de una fase del tratamiento

C. DESCRIPCIÓN DEL CICLO DE VIDA DE LOS DATOS

Para tratamientos complejos, en los que la principal fuente de riesgo proviene de la sensibilidad, la extensión de los datos, las formas de recogida de estos o su comunicación a terceros, es recomendable realizar un análisis global del ciclo de vida de los datos. El análisis del ciclo de vida supone estudiar, para un conjunto o categoría de datos, las distintas etapas de su vida, desde su recogida o generación hasta su destrucción. La descripción del ciclo de vida de los datos es un análisis complementario al análisis estructurado del tratamiento.

Por lo tanto, este estudio podría limitarse a una categoría de datos, por ejemplo, datos biométricos procesados en un tratamiento, o extenderse a todas las categorías de datos, en función del ejercicio de la responsabilidad proactiva en la gestión del riesgo.

Una aproximación elemental al estudio del ciclo de vida de los datos podría estructurar el mismo en las siguientes etapas:

Figura 24: Ciclo de vida básico de los datos.

- **Recogida/Generación:** Proceso de obtención de datos para su tratamiento. La obtención de datos se puede realizar mediante diversas técnicas: formularios web o en papel, la toma de muestras y realización de encuestas, grabaciones de audio y video, información recogida por sensores, etc. Pero también se pueden generar nuevos datos en el tratamiento como ocurre en la elaboración de perfiles, la inferencia de nueva información personal o la toma de decisiones automatizadas.
- **Registro:** Consiste en establecer categorías y asignarlas a los datos para su almacenamiento, organización, estructuración, conservación o adaptación en los sistemas o archivos y bases de datos.
- **Uso:** Engloba la operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea mediante procedimientos manuales o automatizados, con relación a su modificación, extracción, consulta o utilización.

- **Comunicación a un tercero:** Comprende el traspaso o comunicación de datos a un tercero[83] por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión. Cabe la posibilidad de que la comunicación, implique a su vez, una transferencia internacional de datos.
- **Finalización:** Procesos de limitación, incluyendo el bloqueo de datos según lo exigido en el artículo 32.2 de la LOPDGDD[84], supresión o destrucción de datos.

A continuación, se muestra un posible modelo con el que documentar el ciclo de vida de una categoría de datos:

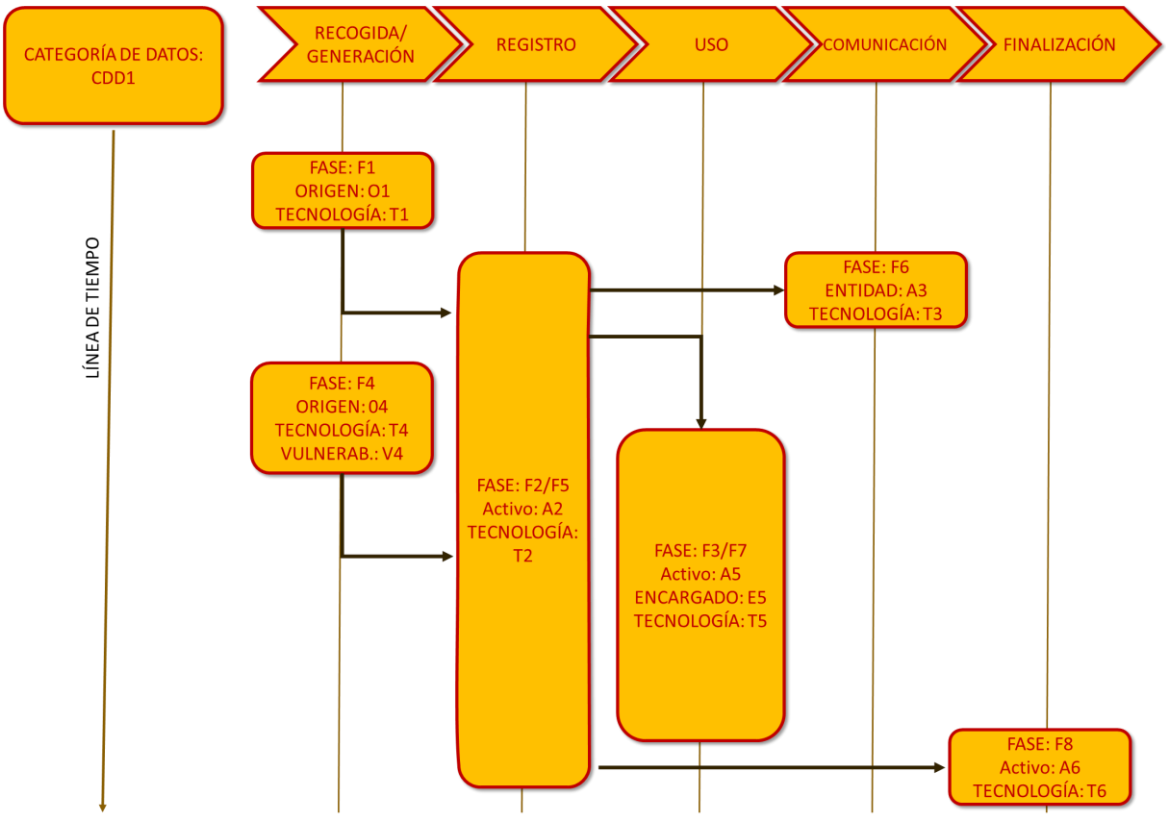

Figura 25: Ejemplo de ciclo de vida de los datos.

En el ejemplo mostrado en el gráfico anterior se ha incluido información adicional como referencia a las fases que intervienen, encargados, terceros, tecnologías u otra que pudiera ser relevante para la descripción y gestión del riesgo.

[83] Se entiende por tercero (art.4.10 del RGPD) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

[84] Artículo 32.2 LOPDGDD. "*El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.*"

D. INVENTARIO DE ACTIVOS

Activo se define como todo bien o recurso que puede ser necesario para implantar y mantener una operación de tratamiento en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada del tratamiento.

Todos los activos deberían incluirse, organizarse y mantenerse actualizados, en lo que se denomina el inventario de activos del tratamiento. Este inventario de activos no es sólo pertinente desde el punto de vista de protección de datos, sino que tiene aplicación en otras funciones básicas para la gestión de la entidad: contabilidad, amortización, mantenimiento, asignación de recursos, seguridad, etc. de modo que su existencia es esperable en aquellas organizaciones que tienen implementados modelos de calidad. En ese caso, la gestión de riesgos para los derechos y libertades se tendrá que integrar con dicho inventario.

En el caso que nos ocupa, el nivel de detalle a incluir en el inventario de activos debería ser el necesario para identificar y gestionar el riesgo de manera eficiente y, al mismo tiempo, poder demostrar dicha gestión.

El inventario de activos se debe determinar a partir del análisis estructurado del tratamiento, o mediante cualquier otro procedimiento determinado por la entidad, de igual o mayor eficacia.

Un correcto inventario de activos a nivel de organización, no solo circunscrito a las actividades de tratamiento, permitirá identificar relaciones o efectos colaterales entre distintos tratamientos. Además, puede suponer una mejora en cuanto a la economía de medios necesarios para llevar a cabo dicho inventario y la posterior labor de identificación y gestión de los riesgos que pudieran derivar de cada activo.

En una entidad será habitual que varios tratamientos puedan acceder a los mismos conjuntos de datos comunes y hacer uso de activos[85] también comunes en la recogida de datos, el procesamiento, la comunicación, etc. Estos activos que implementan operaciones comunes y que son compartidos entre distintos tratamientos son, en muchos casos, sistemas heredados[86]. En otros casos, como puede ser la implementación de apps en sistemas móviles, los tratamientos se desarrollan utilizando componentes estándar de terceros compartidos entre varias aplicaciones que hacen un uso común de acceso a servicios de proceso de datos[87].

[85] Con implementación organizativa, como puede ser un mostrador físico de atención al cliente, como tecnológica, una página web.
[86] Un sistema o aplicación de computadora que todavía se está utilizando debido a los costos de reemplazo o rediseño.
[87] En relación a los riesgos para la protección de datos que puede suponer, consultar el: Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios" https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf

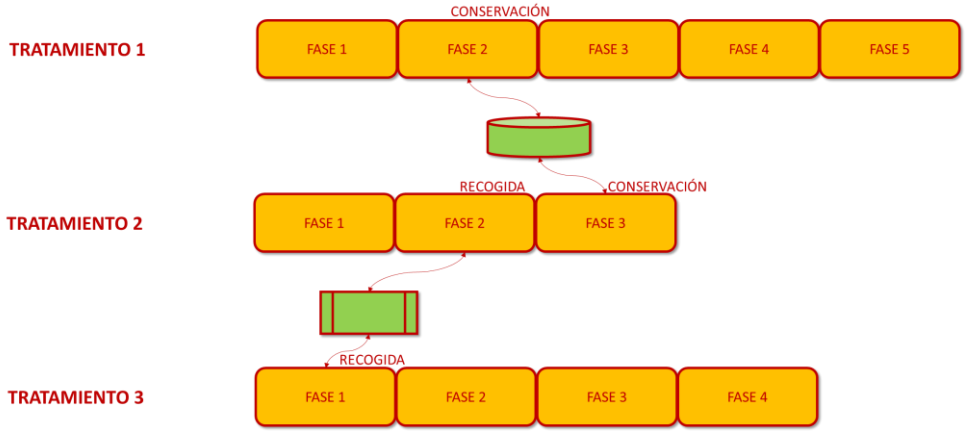

Figura 26: En este caso, los tratamientos 1 y 2 incluyen fases de conservación de datos personales, que se implementan en los servicios de bases de datos de la entidad, mientras que los tratamientos 2 y 3 incluyen fases de recogida de datos implementandas sobre las mismas librerías de captura de datos (por ejemplo, una API en Android).

Con relación a cada activo, sería posible documentar los mismos atendiendo al siguiente modelo:

Activo:	Un identificador del activo
Tecnologías involucradas:	
Tratamientos y fases en las que se emplea:	Puede utilizarse el mismo activo en distintos tratamientos
Operaciones de tratamiento en las que es necesario:	
Datos que son tratados:	
Datos que son generados:	
Roles con acceso al activo y su nivel de privilegio:	
Vulnerabilidades (inherentes al activo)	
Amenazas (internas y externas) asociadas al activo	

Tabla 13 Descripción de los activos involucrados en el tratamiento

E. CASOS DE USO

Los tratamientos pueden ser muy sencillos, formados por una secuencia simple y ordenada de fases. En otros tratamientos, más complejos, las funcionalidades, y por tanto su caracterización, podrán variar en función de la configuración del mismo, ya sea establecida por defecto o realizada por el propio usuario, o con relación a los distintos servicios que pueda proporcionar el responsable: servicios normales o premium, adecuación a un público menor de edad, adulto o de tercera edad, presencia de servicios de valor añadido, etc.

En ese caso, en la descripción del tratamiento en sus distintos niveles de detalle, se deberá identificar a qué caso de uso se refiere y marcar sus diferencias. La identificación de casos de uso, con ejemplos, se ha tratado en la **Guía de Protección de Datos por Defecto**.

VI. IDENTIFICACIÓN Y ANÁLISIS DE FACTORES DE RIESGO

La identificación y el análisis de los factores de riesgo para los derechos y libertades de las personas físicas es el paso previo a la evaluación del nivel de riesgo del tratamiento.

En este capítulo se va a desarrollar una metodología para dicha identificación y análisis. Esta metodología es orientativa, y no es la única posible, existiendo un amplio margen de libertad para que la entidad pueda elegir la más adecuada a sus características y necesidades. En particular, se recomienda utilizar (y ampliar con relación a la protección de datos) la metodología utilizada para la gestión de riesgos en la organización.

De igual forma, para PYMES y Startups en las que los tratamientos son, a priori, de bajo riesgo, la AEPD pone a disposición de responsables y encargados las herramientas **FACILITA-RGPD** y **FACILITA-EMPRENDE**, que además de ayudar al cumplimiento normativo permiten **una aproximación inicial** a la gestión del riesgo. Igualmente, la AEPD ha publicado la herramienta **GESTIONA_EIPD**, que guía a los usuarios a través de los **elementos básicos** que deben ser tenidos en cuenta en los análisis de riesgos de los tratamientos y en las evaluaciones de impacto. Esta herramienta proporciona las **bases mínimas** para iniciar las actividades de gestión de riesgos en el ámbito del RGPD, incluyendo requisitos de cumplimiento normativo con el fin de permitir a pequeñas y medianas empresas, que no dispongan de un marco para la gestión del riesgo en su organización, iniciarse en las labores de identificación, evaluación, gestión de los riesgos de los tratamientos de datos personales y ejecución de EIPD. Finalmente, se cuenta con el prototipo de herramienta EVALÚA_RIESGO RGPD, que tiene como objeto servir de ayuda a responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los interesados presentes en el tratamiento, hacer una primera evaluación del riesgo intrínseco, incluyendo necesidad de realizar una EIPD, y estimar el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgos específicos.

Todas las herramientas anteriores tienen como propósito servir de ayuda y soporte a la decisión. Estas herramientas generan la documentación básica para iniciar la gestión del riesgo, que, como se ha señalado anteriormente, es un proceso que guía la implementación eficaz de medidas y garantías para proteger los derechos y libertades de los interesados. Sin embargo, este resultado no debe entenderse como definitivo y debe ser revisado y adaptado a las circunstancias concretas del responsable en cumplimiento de la obligación de responsabilidad proactiva que le viene impuesta por la normativa

El único requisito que ha de cumplir cualquier metodología utilizada por un responsable o encargado es que tenga al menos la misma eficacia que la aquí presentada para la identificación y el análisis de los factores de riesgo para los derechos y libertades de los interesados.

En el contexto de la responsabilidad activa, la identificación y análisis de factores de riesgo estará siempre documentado y justificado a fin de que el responsable pueda demostrar que, las decisiones tomadas en cada momento con relación a la gestión del riesgo han sido las más adecuadas en función de la información de la que se disponía (“accountability”).

A. IDENTIFICACIÓN DE LOS FACTORES DE RIESGO

En el RGPD, y en su desarrollo a través de la LOPDGDD, normativa especial, y listas, guías y directrices aprobadas por las autoridades de protección de datos, se identifican un conjunto de factores de riesgo. Estos factores identificados constituyen una lista de mínimos que hay que gestionar.

Sin embargo, el responsable no puede ni debe limitarse a tratar los factores de riesgo identificados explícitamente en la normativa. En la gestión del riesgo se ha de ir más allá, y durante la fase de análisis, identificar y evaluar también aquellos factores de riesgo que derivan del tratamiento concreto en función de su naturaleza, ámbito o extensión o los fines que persigue, sin olvidar, tampoco, aquellas otras que se derivan del contexto presente (interno y externo a la organización) y futuro del tratamiento.

B. EL ANÁLISIS DE LOS FACTORES DE RIESGO

Para cada uno de los factores de riesgo identificados, el responsable deberá determinar el impacto inherente, es decir, aquel que resulta de no considerar las medidas y garantías para los derechos y libertades. El impacto dependerá del daño que se pueda ocasionar a los interesados en particular y a la sociedad en su conjunto, en el ámbito de sus derechos y libertades, a corto, medio y a largo plazo.

A su vez, también será necesario determinar la probabilidad de que el riesgo identificado se materialice.

A priori, en el RGPD podemos ver definidas dos bandas o niveles de riesgo: alto riesgo para los derechos y libertades de las personas y su ausencia, que podríamos denominar “no alto riesgo”. Ajustar el análisis a solo los dos niveles de riesgo a los que refiere el RGPD podría ser una dificultad a la hora de establecer una gestión eficaz del riesgo, pues limitaría la granularidad para la evaluación del riesgo residual[88] y, en general, para la gestión del riesgo a lo largo del ciclo de vida del tratamiento.

Bajo estas premisas, y como aproximación general para alcanzar un equilibrio entre la facilidad y la eficacia del proceso de gestión del riesgo, se propone establecer cuatro niveles de impacto del riesgo (muy significativo, significativo, limitado y muy limitado) así como cuatro niveles de probabilidad de ocurrencia (muy alta, alta, baja e improbable), de modo que sus valores combinados permiten establecer los siguientes niveles de riesgo: muy alto, alto, medio y bajo.

Como propuesta, para determinar el nivel de un riesgo específico en función de su impacto y probabilidad se puede establecer el siguiente mapa de calor:

[88] La norma ISO 31010 viene a recomendar como enfoque común dividir los riesgos en tres bandas: riesgo intolerable, riesgos donde es preciso balancear costes y beneficios y riesgos insignificantes. Por tanto, es recomendable que el número de bandas de riesgo para gestionar el riesgo inherente y residual sea al menos de tres. Si embargo, para facilitar la integración en los procesos de análisis de riesgo de la entidad, una posibilidad es la de implementar el mismo número de bandas de riesgo a todos los ámbitos en los que sea de aplicación el marco de trabajo para la gestión del riesgo (riesgos ambientales, laborales, de negocio, protección de datos, etc.).

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

Tabla 14 Matriz Probabilidad x Impacto para determinar el nivel de riesgo

Para calcular el nivel de impacto, de forma orientativa y sin perjuicio de lo expuesto en los siguientes capítulos, se podrían tener en cuenta las siguientes consideraciones:

Nivel de Impacto	Descripción	Derechos fundamentales
Muy significativo	Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución[89], y sus consecuencias son irreversibles. y/o Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible. y/o Causa un daño social significativo, como la discriminación, y es irreversible y/o Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible. y/o Causa perdidas morales o materiales significativas e irreversibles.	Igualdad No discriminación Vida Integridad física Libertad religiosa Libertad personal Intimidad personal y familiar Propia imagen Expresión Información Cátedra Reunión Asociación Libre acceso a cargos y funciones públicas en condiciones de igualdad
Significativo	Los casos anteriores cuando los efectos son reversibles. y/o Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos.	

[89] Los derechos fundamentales garantizados por la Constitución española son, entre otros, el derecho a la igualdad y no discriminación; el derecho a la vida y a la integridad física, a la libertad religiosa, a la libertad personal, a la intimidad personal y familiar y a la propia imagen, a la libertad de expresión e información, a la libertad de cátedra, a la libertad de reunión, a la libertad de asociación, al libre acceso a cargos y funciones públicas en condiciones de igualdad, a la tutela judicial efectiva, a la legalidad penal, a la educación, a la libertad de sindicación y el derecho de petición.

	y/o Se produce o puede producirse usurpación de la identidad de los interesados y/o Pueden producirse pérdidas financieras significativas a los interesados y/o Pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad y/o Existe un perjuicio social para los interesados o determinados colectivos de interesados	Tutela judicial efectiva Legalidad penal Educación Libertad de sindicación Derecho de petición
Limitado	Pérdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter irreversible y/o Pérdidas financieras insignificantes e irreversibles y/o Perdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales	
Muy limitado	En el caso anterior, cuando todos los efectos son reversibles	

Tabla 15 Criterios para determinar el nivel de impacto

Cuando existan dos o más factores de riesgo que apunten a un determinado nivel de impacto, podríamos hablar de un coeficiente de impacto acumulado dando lugar a un nivel de impacto mayor al inicialmente estimado.

Para la determinación de la probabilidad, se podrían utilizar los siguientes criterios.

Probabilidad	
Muy alta	Si el factor de riesgo está materializado y no depende de la probabilidad, p.ej. porque la Directrices wp248 identifican el uso de una tecnología como un riesgo y está presente en el tratamiento. y/o

	Si hay constancia de diversas materializaciones de dicho riesgo en el último año en distintas entidades. y/o Si hay constancia de una materialización de dicho riesgo en el último año en la misma entidad. y/o Existen auditorías/estudios que identifican importantes vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.
Alta	Si hay constancia de una materialización de dicho riesgo en el último año en alguna entidad. y/o Existen estudios que determinan que la probabilidad podría ser alta. y/o Existen auditorías/estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. y/o Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes
Baja	Si hay constancia de una materialización de dicho riesgo en los últimos 10 años en alguna entidad.
Improbable	Si no hay constancia de materialización de dicho riesgo en ningún caso.

Tabla 16 Criterios para determinar la probabilidad de materialización de un factor de riesgo

Para evaluar correctamente la tabla anterior es importante:

- Justificar que se conoce el estado del arte relativo a los elementos que implementan el tratamiento.
- Tener acceso a los catálogos de vulnerabilidades de los ya existentes en el mercado y que se encuentre debidamente actualizado.
- Consultar históricos de incidentes (p. ej. los informes publicados por la AEPD en el micro-site brechas de datos personales).

Cuando existan dos o más indicios que apunten a un determinado nivel de probabilidad, podríamos hablar de un coeficiente de probabilidad acumulado dando lugar a una tasa de probabilidad mayor a la inicialmente estimada.

C. LISTA DE FACTORES DE RIESGO IDENTIFICADOS EN LA NORMATIVA

El RGPD, y la normativa de desarrollo, identifican múltiples factores de riesgo[90]. La persona a cargo de la evaluación del riesgo de un tratamiento debería tener en cuenta todos los factores que ya están identificados y determinar si estos afectan, o son susceptibles de afectar, al tratamiento.

Esta tarea requiere recorrer todos los textos legales y realizar un esfuerzo de sistematización. Para facilitarla, en la presente guía se realiza una compilación de los factores de riesgo identificados, se han agrupado por categorías, y se ha determinado un nivel de riesgo mínimo para cada una de ellas. A su vez, la AEPD ha publicado un prototipo de herramienta de evaluación del nivel de riesgo de un tratamiento, EVALÚA_RIESGO RGPD, que permite realizar una primera aproximación a la identificación y evaluación del riesgo de un tratamiento en base a las categorías aquí mostradas.

Las categorías son las siguientes:

Operaciones relacionadas con los fines de tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.
Tipos de datos utilizados	Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.
Extensión y alcance del tratamiento	Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.
Categorías de interesados	Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.

[90] Entre ellas: el art.35.3 del RGPD, Directrices WP248, lista de la AEPD en base al artículo 35.4 del RGPD, art. 28.2 de la LO 3/2018, art.32.2 del RGPD, Considerando 75 del RGPD, "Guidelines 8/2020 on the targeting of social media users", "Guidelines 02/2021 on Virtual Voice Assistants", "Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications", "Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19", "Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19", "Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo", "Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados", "Directrices 2/2020 relativas a la aplicación del artículo 46, apartado 2, letra a), y del artículo 46, apartado 3, letra b), del Reglamento 2016/679 con respecto a las transferencias de datos personales entre autoridades y organismos públicos del EEE y de fuera de este", "Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions", "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", "Dictamen 8/2014 sobre la evolución reciente de la internet de los objetos", "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes", "Directrices sobre los delegados de la protección de datos (DPD)".

Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.
Recogida y generación de datos	Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.
Efectos colaterales del tratamiento	Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Categoría del responsable/encargado	Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
Comunicaciones de datos	Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.

Tabla 17 Categorías de factores de riesgo identificados en el RGPD o en su desarrollo.

El nivel de riesgo, determinado para cada factor de riesgo de forma aislada, agrupado por categorías, es el siguiente:

1. Operaciones relacionadas con los fines de tratamiento

Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.

Factor de riesgo	Nivel de riesgo
Perfilado P.ej. y sin ser exhaustivos: • Creación de perfiles • Uso de perfiles • Clasificación de individuos • Orientación de productos/servicios a individuos o grupos • Análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, etc.) • Otros	Alto

Evaluación de sujetos P.ej. y sin ser exhaustivos: • Valoración • Puntuación • Otros	Alto
Predicción P.ej. y sin ser exhaustivos: • Inferencia de nuevos datos personales • Otros	Alto
Control del empleado P.ej. y sin ser exhaustivos: • Evaluación del empleado • Observación del puesto de trabajo • Monitorización del puesto de trabajo • Grabación de imágenes en ámbito laboral • Grabación de audio en ámbito laboral • Monitorización por medio de imágenes en ámbito laboral • Monitorización por medio de sonido en ámbito laboral • Geolocalización de trabajadores en ruta • Tiempo invertido en realizar tareas • Monitorización y control de correo electrónico • Monitorización y control de la navegación en Internet en el puesto de trabajo • Control de uso de aplicaciones/servicios informáticos en el puesto de trabajo • Control de uso de teléfono • Otros	Medio
Control del acceso a de Internet P.ej. y sin ser exhaustivos: • Análisis o evaluación de tiempos de uso de Internet • Análisis o evaluación de la actividad de navegación en Internet • Análisis o evaluación de alarmas sobre navegación a sitios específicos en Internet • Análisis o evaluación de alarmas sobre navegación a contenidos específicos en Internet • Otros	Medio
Observación P.ej. y sin ser exhaustivos: • Vigilancia mediante imágenes • Vigilancia mediante sonidos • Vigilancia de comunicaciones • Vigilancia de emisiones de calor u otras • Vigilancia de transmisiones • Vigilancia de Internet • Otros	Alto
Monitorización P.ej. y sin ser exhaustivos: • Gestión mediante IoT • Control mediante imágenes	Alto

• Control mediante sonidos • Control de comunicaciones • Control de emisiones de calor u otras • Control de transmisiones • Control de Internet • Control mediante geolocalización • Otros	
Supervisión P.ej. y sin ser exhaustivos: • Control • Análisis mediante imágenes • Análisis mediante sonidos • Análisis de comunicaciones • Análisis de emisiones de calor u otras • Análisis de transmisiones • Análisis de Internet • Análisis mediante geolocalización • Control de tráfico rodado • Otros	Alto
Rastreo de contactos	Muy alto
Control físico de acceso P.ej. y sin ser exhaustivos: • Control de acceso al centro de trabajo • Control de acceso a local comercial • Control de acceso a eventos • Control de acceso a instalaciones deportivas • Control de acceso a edificios (públicos/privados) • Otros	Bajo
Localización P.ej. y sin ser exhaustivos: • Geolocalización • Perfilado de desplazamientos • Determinación de lugares habituales • Determinación de lugares frecuentes de acceso • Datos sobre la persona inferidos de la geolocalización • Otros	Medio
Identificación unívoca	Bajo
Decisiones automatizadas sin intervención humana	Alto
Tratamiento automatizado para soporte a la toma de decisiones P.ej. y sin ser exhaustivos: • DSS • Inteligencia de negocio que exceda datos meramente estadísticos • Minería de datos • Otros	Medio
Decidir sobre o impedir el ejercicio de derechos fundamentales P.ej. y sin ser exhaustivos: • Derecho a la igualdad	Muy Alto

• Derecho a la no discriminación • Derecho a la vida y a la integridad física • Derecho a la libertad religiosa • Derecho a la libertad personal • Derecho a la intimidad personal y familiar • Derecho a la propia imagen • Derecho a la libertad de expresión e información • Derecho a la libertad de cátedra • Derecho a la libertad de reunión • Derecho a la libertad de asociación • Derecho al libre acceso a cargos y funciones públicas en condiciones de igualdad • Derecho a la tutela judicial efectiva • Derecho a la legalidad penal • Derecho a la educación • Derecho a la libertad sindical • Derecho el derecho de petición • Otros derechos o libertades	
Decidir sobre el control del interesado de sus datos personales • Derecho de acceso. • Derecho de rectificación • Derecho de oposición • Derecho de supresión • Derecho de limitación del tratamiento • Derecho de no ser sometido a decisiones automatizadas sin intervención humana. • Derecho a la portabilidad • Otros	Alto
Decidir sobre el acceso a un servicio	Alto
Decidir sobre la realización o ejecución de un contrato	Alto
Decidir sobre el acceso a servicios financieros	Alto
Efectos jurídicos sobre las personas	Alto
Evaluación y/o predicción de posibilidad de enfermedad/salud genéticamente.	Muy Alto
Conservación con fines de archivo	Medio

Tabla 18 Factores de riesgo asociados a las operaciones relacionadas con los fines del tratamiento.

2. Tipos de datos utilizados

Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

Factor de riesgo	Nivel de riesgo
Documentos personales P.ej. y sin ser exhaustivos: • Correos electrónicos • Cartas personales • Diarios • Notas de lectores de libros electrónicos • Otros	Medio
Información de aplicaciones de registro de actividades vitales	Alto
Aspectos personales P.ej. y sin ser exhaustivos: • Personas o grupos con los que se relaciona • Temperamento • Carácter • Inteligencia • Roles sociales • Capacidad de adaptación • Tolerancia al riesgo • Gustos/preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales, …) • Cuidado de salud • Culturales (lectura, música, arte, …) • Pertenencia y actividades en asociaciones sociales y culturales • Otros	Medio
Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos P.ej. y sin ser exhaustivos: • Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc. • Hábitos de consumo (tarjetas de fidelización de clientes, actividad web, …) • Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales, …) • Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.) • Otros	Medio

Rendimiento laboral P.ej. sin ser exhaustivos: • Control de acceso al lugar de trabajo • Grabación de imágenes del puesto de trabajo • Grabación de audio en el puesto de trabajo • Evaluación del trabajador por medio de imágenes capturadas de los dispositivos y pantallas del trabajador • Evaluación del trabajador por medio de sonido • Grabación de imágenes en zonas de acceso o en oficinas • Grabación de audio en zonas de acceso o en oficinas. • Monitorización de los equipos de los empleados • Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos) • Otros	Medio
Situación económica P.ej. sin ser exhaustivos: • Renta personal • Ingresos mensuales • Patrimonio (bienes muebles/inmuebles) • Situación laboral • Otros	Medio
Estado financiero P.ej. sin ser exhaustivos: • Solvencia financiera • Capacidad de endeudamiento • Nivel de deuda (Préstamos personales, hipotecas) • Listas de solvencia • Impagos • Activos (fondos de inversión, rendimientos generados, acciones, cuentas a cobrar, rentas percibidas, etc.) • Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; o deudas u obligaciones • Otros	Medio
Datos de medios de pago: P.ej. y sin ser exhaustivos: • Tarjetas de crédito • Información de acceso a servicios de monedas virtuales. • Otros.	Alto
Datos de comportamiento P.ej. sin ser exhaustivos: • Fiabilidad de la persona • Hábitos y valores que facilitan la convivencia • Hábitos y valores que facilitan el trabajo y el estudio • Hábitos y valores que influyen en el bienestar personal, laboral y familiar • Hábitos y valores que influyen en el compromiso con las personas y con la sociedad • Estabilidad laboral	Medio

• Quejas sobre la persona • Otros	
Datos de localización P.ej., sin ser exhaustivos: • Registro de desplazamientos • Registro de lugares habituales • Registro de rutinas en base a localización • Registro de lugares habituales • Otros	Medio
Datos muy personales[91] no recogidos en clasificaciones anteriores	Alto
Datos sanitarios P.ej. y sin ser exhaustivos: • Historia clínica • Informes de salud • Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales • Recetas médicas • Datos relativos a salud física • Datos relativos a salud mental • Datos relativos a prestación de servicios de atención sanitaria • Datos de salud de aplicaciones de eHealth • Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido • Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente • Otros	Muy Alto
Datos biométricos P.ej. y sin ser exhaustivos: • Huella dactilar • Facciones rostro • Iris • Venas de la palma de la mano • Voz • Oreja • Gestos	Alto

[91] Wp248: *"Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales."*

• Modo de andar • Descriptores corporales de cualquier índole • Otros	
Datos genéticos	Muy Alto
Categorías especiales de datos o que permitan inferirlos P.ej. y sin ser exhaustivos: • Origen étnico • Origen racial • Opiniones políticas • Convicciones religiosas • Convicciones filosóficas • Afiliación sindical • Datos relativos a la salud • Datos relativos a la vida sexual • Datos relativos a las orientaciones sexuales • Otros	Muy Alto
Categorías especiales de datos seudonimizados	Alto
Datos personales relativos a condenas e infracciones penales	Muy Alto
Metadatos P.ej. y sin ser exhaustivos: • Datos de tráfico de las comunicaciones electrónicas • Identificación de emisor y/o receptor en las comunicaciones • Datos en conexiones a internet: localización; características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logado, conexión (IP, proveedor de servicios, velocidad de descarga), … • Otros	Medio
Identificadores únicos P.ej. y sin ser exhaustivos: • Dirección IP • Dirección MAC • IMSI • IMEI • ID de un dispositivo • N. teléfono • DNI, NIE, N. Pasaporte o equivalente • N. de la Seguridad social • Matrícula de vehículo • Número de tarjeta de crédito. • UID (identificadores únicos de registro de usuarios en sitios web) • Identificadores únicos derivados de las características del dispositivo (p. e. acceso a la información de la batería de un dispositivo, id publicitario del dispositivo) • Identificadores únicos añadidos a archivos (p. e. metadatos de fotografías subidas a redes sociales)	Medio

• Otros	
Datos y metadatos de las comunicaciones electrónicas y datos inferidos de las comunicaciones electrónicas P.ej. y sin ser exhaustivos: • Correos electrónicos • Mensajes instantáneos • Llamadas de teléfonos • Video llamadas • Otros	Medio
Datos de navegación web P.ej. y sin ser exhaustivos: • Registro de páginas visitadas (p. e. historial de navegación, logs de servidores web, …) • Registro del tiempo que se está en cada página • Registro del momento de la visita a la página • Registro del número de conexiones • Registro de actividad del ratón por las diferentes partes de la página web • Navegador utilizado • Otros	Medio

Tabla 19 Factores de riesgo asociados a los tipos de datos utilizados en el tratamiento.

3. Extensión y alcance del tratamiento

Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.

Factor de riesgo	Nivel de riesgo
Sistemático P.ej. y sin ser exhaustivos: • Se produce de acuerdo con un sistema • Es preestablecido, organizado o metódico • Tiene lugar como parte de un plan general de recogida de datos • Es llevado a cabo como parte de una estrategia • Otros	Alto
Exhaustivo sobre las personas P.ej. y sin ser exhaustivos: • Se recogen y tratan gran variedad de elementos distintos • Múltiples ámbitos de su vida • Se cubren distintos aspectos de la personalidad • Otros	Alto
Involucra a gran número de sujetos P.ej. y sin ser exhaustivos: • El número de interesados afectado es elevado en números absolutos	Muy Alto

• El número de interesados afectado es elevado en relación con la población correspondiente • El número de interesados es relevante en relación con la extensión geográfica • Otros	
El volumen de datos tratados es muy elevado	Muy Alto
La duración del tratamiento es elevada P.ej. y sin ser exhaustivos: • La permanencia del tratamiento es elevada • Otros	Medio
La actividad de tratamiento tiene un gran alcance geográfico P.ej. y sin ser exhaustivos: • Nivel regional, nacional o supranacional • Otros	Medio
Tratamiento a gran escala P.ej. y sin ser exhaustivo: • Tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital • Tratamiento de datos de desplazamiento de personas físicas que utilizan el sistema de • transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte) • Tratamiento de datos de geolocalización en tiempo real de clientes de una cadena de comida rápida internacional con fines estadísticos por parte de un encargado del tratamiento especializado en la prestación de estos servicios • Tratamiento de datos de clientes en el desarrollo normal de la actividad de una empresa de seguros o un banco • Tratamiento de datos personales para publicidad basada en el comportamiento por parte de un motor de búsqueda • Tratamiento de datos (contenido, tráfico, ubicación) por parte de proveedores de telefonía o de servicios de Internet • Otros	Alto
Recopilación excesiva de datos con relación al fin del tratamiento	Alto

Tabla 20 Factores de riesgo asociados a la extensión y alcance del tratamiento.

4. Categorías de interesados

Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.

Factor de riesgo	Nivel de riesgo
Menores de 14 años	Muy Alto
Víctimas de violencia de género	Muy Alto
Menores dependientes de sujetos vulnerables	Muy Alto
Personas bajo guardia y custodia de víctimas de violencia de género	Muy Alto
Mayores con algún grado de discapacidad	Alto
Personas mayores	Medio
Personas con enfermedades mentales	Muy Alto
Discapacitados	Alto
Personas que acceden a servicios sociales	Medio
Sujetos en riesgo de exclusión social	Alto
Empleados	Bajo
Solicitantes de asilo	Alto
Pacientes	Alto
Sujetos vulnerables P.ej. y sin ser exhaustivos: • En situación de especial vulnerabilidad • Existe un desequilibrio entre la posición del interesado y del responsable • Otros	Muy Alto

Tabla 21 Factores de riesgo asociados a la categoría de interesados.

5. Factores técnicos del tratamiento

Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.

Factor de riesgo	Nivel de riesgo
Sistema de información hospitalaria	Alto
TV interactiva	Medio
Servicios web	Medio
Aplicaciones móviles	Medio
Sistemas de registro de localización	Alto
Reconocimiento facial	Alto
Huella dactilar	Alto
Internet de las cosas (IoT)	Muy Alto
Uso innovador o nuevas soluciones organizativas	Alto
Uso innovador de tecnologías consolidadas P.ej. y sin ser exhaustivos: • Tecnologías en las que no se ha evaluado el impacto en la privacidad • Tecnologías utilizadas a una nueva escala • Otros	Alto
Tecnologías combinadas con otras	Medio

Nuevas tecnologías P.ej. y sin ser exhaustivos: • Tecnologías inmaduras • Tecnologías emergentes • Otros	Alto
Alto grado de fragmentación de los actores que intervienen en el desarrollo e implementación de los productos/servicios que implementan el tratamiento	Alto
Tratamientos automatizados P.ej. y sin ser exhaustivos: • Tratamiento realizado mediante un proceso automático sin intervención humana • Otros	Medio
Sistema Inteligente	Medio
Videovigilancia	Alto

Tabla 22 Factores de riesgo asociados a los factores técnicos del tratamiento.

6. Recogida y generación de datos

Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.

Factor de riesgo	Nivel de riesgo
Acceso a base de datos de referencia de crédito	Medio
Acceso a base de datos sobre fraudes	Medio
Acceso a base de datos sobre blanqueo de capitales o financiación del terrorismo	Alto
Datos personales obtenidos en zonas de acceso público P.ej. y sin ser exhaustivos: • Autovía • Centro comercial • Calle • Estación • Mercado • Biblioteca • Otros	Medio
Recogida de datos de los medios sociales públicos	Bajo
Recogida de datos de redes de comunicaciones.	Medio
Recogida de datos de aplicaciones	Medio
Datos procedentes de dos o más tratamientos con finalidades diferentes	Medio
Datos procedentes de dos o más responsables distintos	Medio
Asociación de conjuntos de datos	Medio
Combinación de conjuntos de datos P. ej, y sin ser exhaustivos: • Cruce de bases de datos • Fusión de datos de sensores • Otros	Alto

Enlace de registros de bases de datos de dos o más tratamientos con finalidades o responsables diferentes	Medio
Recogida de datos por un responsable distinto al que trata y aplica excepción de información 14.5 (b, c, d)	Medio
Falta de transparencia del momento preciso de la recogida de datos. P.ej. y sin ser exhaustivo: • Sistemas móviles • IoT • Asistentes domésticos • Coches conectados • Otros.	Alto
Nuevas formas de recogida de datos con riesgos para los derechos y libertades	Alto

Tabla 23 Factores de riesgo asociados a la recogida y generación de datos.

7. Efectos colaterales del tratamiento

Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.

En este caso, no se ha evaluado por la AEPD el nivel de riesgo, sino solo el impacto que podría tener. El responsable tendrá que evaluar la probabilidad de que estas amenazas se materialicen en su tratamiento, por lo que se deja la columna "Probabilidad" vacía. Una vez completada, podrá determinar el nivel de riesgo empleando, por ejemplo, la matriz de riesgo "probabilidad x impacto" mostrada al principio de este capítulo.

Factor de Riesgo	Impacto	Probabilidad
Excede las expectativas del interesado P.ej. y sin ser exhaustivos: • Exposición excesiva del interesado • Segmentación que excede expectativas razonables • Inferencia de intereses o de otras características en base a datos no evidentes y que derivan en un perfilado del sujeto • Otros	Medio	
Posible reversión no autorizada de la seudonimización	Muy Alto	
Posible pérdida de control por el responsable de los datos procesados por el encargado del tratamiento.	Alto	

Podría determinar la situación financiera	Medio	
Podría determinar la solvencia patrimonial	Medio	
Podría deducir información relacionada con categorías especiales de datos	Alto	
Pudiera privar a los afectados de sus derechos y libertades	Muy Alto	
Pudiera impedir el control sobre sus datos personales	Muy Alto	
Puede provocar exclusión	Alto	
Puede provocar discriminación	Muy Alto	
Posible usurpación de identidad	Muy Alto	
Posible fraude	Muy Alto	
Posible daño reputacional	Muy Alto	
Posible perjuicio económico significativo	Muy Alto	
Posible perjuicio moral significativo	Muy Alto	
Posible perjuicio social significativo	Muy Alto	
Posible pérdida de confidencialidad de datos sujetos al secreto profesional	Muy Alto	
Podría impedir el ejercicio de un derecho	Alto	
Podría impedir el acceso a un servicio	Alto	
Podría impedir el acceso a un contrato	Alto	
Podría recoger datos personales distintos de los usuarios de servicio. P.ej. y sin ser exhaustivos: • IoT doméstico • Altavoces inteligentes • Coches conectados • Otros	Alto	
Posible manipulación de las personas P.ej. y sin ser exhaustivos: • Influir en el comportamiento y decisiones de los individuos. • Socavar su autonomía y libertad individual. • Generar desinformación. • Focalización que afecta al acceso a información plural • Filtros burbuja • Sobrecarga de información • Otros	Alto	
Posibilidad de autocensura	Alto	
Posibilidad de provocar un cambio cultural para claudicar derechos y libertades	Alto	
Usos imprevistos o no deseados que pudieran afectar a derechos fundamentales.	Alto	

Tabla 24 Factores de riesgo asociados a los efectos colaterales del tratamiento.

8. Categoría del responsable/encargado

Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.

En este caso, entendido generalmente para tratamientos que no forman parte de los procesos de soporte[92] de la entidad:

Riesgo	Nivel de riesgo
Sociedad de la Información	Medio
Empresa de biotecnología	Alto
Empresa de mercadotecnia	Medio
Hospitales	Alto
Investigadores privados	Medio
Entidad de evaluación de información crediticia	Medio
Entidad de evaluación de fraude	Medio
Entidad financiera	Medio
Empleador	Bajo
Proyectos de investigación	Bajo
Ensayos clínicos	Alto

Tabla 25 Factores de riesgo asociados a categoría de responsable/encargado.

9. Comunicaciones de datos

Otros factores de riesgo identificados en el tratamiento que no están señalados específicamente en el RGPD o en su desarrollo.

Factor de riesgo	Nivel de riesgo
Transferencia habitual a estados u organizaciones en otros países sin un adecuado nivel de protección	Muy Alto
Falta de trasparencia de los actores involucrados en el tratamiento P.ej. y sin ser exhaustivo: • Algunos tipos de redes sociales, • Tipos de redes de marketing digital, • Tipos de tratamientos basados en blockchain, • Tipos de IA de aprendizaje continuo remoto. • Otros	Medio

[92] Los procesos de soporte o apoyo son los que dan respaldo a los procesos de negocio, clave o estratégicos de la entidad. Los "clientes" de estos procesos son internos, como son los de nóminas, control de calidad, selección de personal, formación del personal, compras, sistemas de información, etc.

Difusión libre de identificadores únicos. P. ej. y sin ser exhaustivos: • Tags RFID • SSIDs • MACs • Claves públicas • Otros.	Alto

Tabla 26 Factores de riesgo asociados a las comunicaciones de datos.

D. RIESGO DERIVADO DE BRECHAS DE DATOS PERSONALES

En la práctica, el proceso de evaluación del nivel de riesgo no puede llevarse a cabo sin tener en cuenta las posibles consecuencias de las brechas de datos personales sobre los interesados con el fin de establecer criterios de coherencia en la evaluación del riesgo impidiendo que la evaluación inicial del riesgo pueda diferir con relación a las consecuencias sobre los interesados resultante de la pérdida de confidencialidad, integridad, disponibilidad de los datos, reversión de la anonimización/seudonimización, uso de los datos para fines no compatibles, incumplimiento de garantías, etc.

En la identificación y análisis de factores de riesgo, es necesario determinar los perjuicios que puede tener la materialización de brechas de datos personales en sus distintas dimensiones. En este caso, tanto las brechas como la noción de seguridad han de entenderse de un modo extensivo, incluyendo los problemas que se pueden producir sobre las propias medidas técnicas de reducción del riesgo (p. ej. medidas de seudonimización), así como problemas técnicos en los sistemas de tratamiento de datos (p. ej. en sistemas transaccionales).

1. Análisis básico

Una aproximación básica a la determinación del nivel de riesgo es considerar el tratamiento a alto nivel, sin entrar en el detalle de los activos que implementan el tratamiento de la información y, a partir de ahí, evaluar el impacto que produciría una brecha de datos personales en cada una de las siguientes dimensiones: confidencialidad, integridad, disponibilidad, autenticación, trazabilidad, resiliencia, fallos en las garantías de privacidad y errores en las operaciones técnicas[93] del tratamiento (o C,I,D,A,T,R,F,E).

Para realizar el análisis, se pueden plantear los distintos escenarios de materialización de una brecha de datos personales, tal como se definió en el capítulo III de esta guía, de cara a determinar que impactos se podrían producir en los interesados. Para ello, y en cada uno de los escenarios, se podría completar la siguiente tabla:

[93] Por ejemplo, como errores en sistemas de reconocimiento biométrico, en inferencias en IA, en el intercambio de datos en sistema transaccionales, en la separación de máquinas virtuales, etc.,

Tratamiento	Escenario N
Brecha materializada	Descripción del tipo de brecha.
Datos comprometidos	Relación de datos comprometidos en la brecha.
Perjuicios al interesado	Detallar que perjuicios se podrían producir al interesado en sus derechos y libertades, y en general a sus intereses. También definiendo la extensión en personas afectadas.

Tabla 27 Descripción de un escenario de brechas de datos personales.

A partir de los perjuicios que se provocan a los interesados, es posible determinar el impacto utilizando el mismo criterio seguido en el apartado “El análisis del riesgo” de este capítulo. Por ejemplo, si estimamos que una brecha de confidencialidad afecta de forma irreversible a derechos constitucionales, determinaríamos que el impacto es máximo.

Dimensión de la brecha	Impacto para los derechos y libertades
Confidencialidad	Máximo / Alto / Medio / Bajo
Integridad	Máximo / Alto / Medio / Bajo
Disponibilidad	Máximo / Alto / Medio / Bajo
Trazabilidad	Máximo / Alto / Medio / Bajo
Autenticidad/Identidad	Máximo / Alto / Medio / Bajo
Resiliencia	Máximo / Alto / Medio / Bajo
Brechas en medidas y garantías técnicas y organizativas de protección de datos	Máximo / Alto / Medio / Bajo
Errores en las operaciones técnicas de tratamiento de datos	Máximo / Alto / Medio / Bajo

Tabla 28 Recopilación de nivel de impacto para casos de brechas de datos personales.

A su vez, es necesario determinar la probabilidad de que dichas brechas se materialicen, para lo que se podría utilizar la tabla empleada en el apartado “El análisis del riesgo” y obtener el siguiente resultado para cada dimensión:

Dimensión de la brecha	Probabilidad de materialización
Confidencialidad	Máximo / Alto / Medio / Improbable
Integridad	Máximo / Alto / Medio / Improbable
Disponibilidad	Máximo / Alto / Medio / Improbable

Trazabilidad	Máximo / Alto / Medio / Improbable
Autenticidad/Identidad	Máximo / Alto / Medio / Improbable
Resiliencia	Máximo / Alto / Medio / Improbable
Brechas en medidas y garantías técnicas y organizativas de protección de datos	Máximo / Alto / Medio / Improbable
Errores en los sistemas de tratamiento de datos	Máximo / Alto / Medio / Improbable

Tabla 29 Recopilación de probabilidad de materialización de brechas de datos personales.

En el análisis de probabilidad habrá que considerar si el tratamiento tiene una expectativa de operatividad a corto, medio o largo plazo, pues hay que ser consciente, como ya se ha indicado[94], que la probabilidad de materialización aumentará con el tiempo. Por ejemplo:

Probabilidad Hoy	**Evolución de la Probabilidad**		
Máxima	Máxima	Máxima	Máxima
Alta	Alta	Máxima	Máxima
Media	Media	Alta	Máxima
Baja	Baja	Media	Alta
	Corto plazo < 1 año	Medio Plazo < 5 años	Largo Plazo Mayor 5 años

Tabla 30 Evolución de la probabilidad de materialización de una brecha en el tiempo

El nivel de riesgo para cada dimensión de la brecha se evaluaría con la siguiente tabla:

[94] En el apartado sobre brechas de datos personales del capítulo III sobre el proceso de gestión del riesgo.

Dimensión: C/D/I/T/A/R/B/E					
Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

Tabla 31 Matriz Probabilidad x Impacto para determinar el nivel de riesgo de una brecha de datos personales

2. Tratamiento de grandes conjuntos de datos

En el caso de tratamientos que procesen grandes volúmenes de datos será necesario analizar el impacto y las probabilidades de que las amenazas se materialicen sobre distintos conjuntos de datos de diferentes formas:

- Sobre un conjunto pequeño de datos, o incluso de un único individuo.
- Sobre un volumen masivo, o incluso el conjunto total, de los datos del tratamiento.

A priori, podría parecer que una brecha que afecte a una gran extensión de datos e interesados es menos probable que una brecha que afecte a pocos datos o pocos interesados.

Brecha de poca extensión	< Impacto	> Probabilidad
Brecha de gran extensión	> Impacto	< Probabilidad

Tabla 32 Posible relación entre impacto y probabilidad en brechas en función del volumen de datos.

Sin embargo, dicha presunción debería ser confirmada mediante un análisis basado en evidencias. Y, aunque así fuese, habría que determinar si las variaciones son del mismo orden de magnitud, de forma que un incremento en el impacto se compensaría con la disminución en el mismo grado de la probabilidad de la materialización de la brecha.

En cualquier caso, es necesario examinar el tratamiento considerando ambas posibilidades para determinar los niveles de riesgo del peor caso.

3. Análisis de los activos identificados en el tratamiento

En tratamientos más complejos, se podría abordar un análisis más detallado partiendo del estudio de cada uno de los activos identificados en el tratamiento con relación a las distintas dimensiones de las brechas.

Para ello, se realizaría una tabla para cada dimensión. En cada tabla se incluiría el conjunto de activos identificados en la descripción del tratamiento. A partir de ahí, se determinaría, para cada activo, si es posible la ocurrencia de una brecha en la dimensión

de seguridad analizada y, en caso afirmativo, se procedería a estimar la probabilidad de que se materialice.

Dimensión:	**C/D/I/T/A/R/B/E**	
Activos	**Probabilidad**	**Impacto**
Activo 1	Probabilidad de materialización	Nivel de impacto en función de cómo una pérdida total o parcial del activo en la dimensión C/D/I/T/A/R/B/E pudiera afectar a los derechos y libertades de los interesados.
…	…	…
Activo N	…	…

Tabla 33 Análisis de los activos implicados en el tratamiento.

El nivel de riesgo para cada dimensión se podría determinar por el peor caso de los pares (Impacto, Probabilidad). Además, este tipo de análisis permitiría identificar sobre qué activos realizar el mayor esfuerzo en implementación de medidas y garantías para reducir ese nivel de riesgo.

E. FACTORES DE RIESGO NO EXPLÍCITOS EN LA NORMATIVA

Los factores de riesgo identificados en el apartado “C” de este capítulo son, exclusivamente, aquellos identificados explícitamente en el RGPD y en su desarrollo. Como se ha señalado anteriormente, es necesario estudiar las peculiaridades del tratamiento para identificar factores de riesgo para los derechos y libertades adicionales. El responsable, en aras de la aplicación de la responsabilidad proactiva, ha de realizar un análisis crítico de su tratamiento para señalar aquellas situaciones singulares que podrían suponer un factor de riesgo.

A continuación, se muestra una lista de otros posibles factores de riesgo, sin intención de ser exhaustiva, sino como ejemplo de que podrían existir otros factores en tratamientos específicos. El propósito de esta lista es de servir de ayuda para la reflexión de responsables y encargados:

Factor de riesgo	**Impacto**	**Probabilidad**
Contexto interno de la organización		
Falta de madurez en la gobernanza y procesos de la organización		
Crisis interna de la organización		

Existencia de otros tratamientos de alto riesgo en la organización		
Actuar como encargado de numerosos (cientos o miles) de responsables		
Otros		
Operaciones relacionadas con los fines		
Se produce un contacto frecuente y reiterado con los afectados de manera que pueda resultar intrusivo para la intimidad del interesado		
Exista una probabilidad real de que, en el futuro, se vayan a tratar los datos para finalidades distintas de las que se previeron en el momento de recabarlos, en particular, si estas finalidades son más intrusivas o exceden las expectativas de los afectados		
Moldeado o presentación de la realidad digital en función de un perfilado		
Nudging o refuerzo positivo para influir en el comportamiento, explotando sesgos cognitivos o debilidades psicológicas		
Otros		
Extensión y alcance del tratamiento		
El tratamiento involucra a un elevado número de intervinientes y/u organizaciones pudiendo representar un riesgo de pérdida de control de los datos personales		
Otros		
Factores técnicos del tratamiento		
Plataformas educativas		
Internet de los cuerpos/Wearables		
Interfaces neurológicos		
Inteligencia Artificial		
Blockchain		
Otros		
Categoría de responsable/encargado[95]		
Organismos públicos y Administraciones Públicas		
Centros docentes y de educación		
Entidad aseguradora		

[95] Con relación, generalmente, a los procesos que no sean de soporte.

Otros		
Recogida y generación de datos		
Tasas de falsos positivos		
Tasas de falsos negativos		
Otros		
Efectos colaterales		
Posible inferencia de categorías especiales de datos a partir de la información acumulada del usuario		
Afecta o puede afectar al interés superior del menor		
Discriminación en la oferta de opciones, productos o servicios a causa del perfilado del usuario		
Limitación de la libertad de autonomía		
Sesgos en la toma de decisiones		
Discriminación algorítmica		
Aspectos culturales que afectan a la percepción de intrusión o a la interpretación de los datos		
Otros		
Comunicaciones de datos		
Transferencia puntual a estados u organizaciones en otros países sin un adecuado nivel de protección		
Otros		
Previstos en códigos de conducta a los que la entidad está adherida		
Previstos en los esquemas de certificación		
Cualquier otro factor de riesgo		

Tabla 34 Ejemplos de otros posibles factores de riesgo

F. ANÁLISIS DE UN ALTO IMPACTO

Un análisis de alto impacto se debería llevar a cabo en casos especiales: para el caso de tratamientos en los que el compromiso de las garantías básicas de un Estado de Derecho pudiera verse afectado y tener un impacto de altísima repercusión a nivel social sobre los derechos y libertades de los ciudadanos.

En general, se estaría hablando de casos en los que haya tratamientos masivos de datos de la población. Algunos tratamientos con dichas características se podrían encontrar, p. ej., en:

- Las AA.PP.
- Entidades de telecomunicaciones.
- Entidades financieras.
- Entidades aseguradoras
- Grandes sistemas de servicios sanitarios.
- Proveedores de servicios de Internet o Cloud.
- Otros de la misma relevancia.

En esos supuestos, y solo para estos casos de muy alto impacto, sería necesario evaluar el riesgo relativo asociado a la materialización de los siguientes eventos:

Factor de riesgo	Nivel de Riesgo
Quiebras del Estado de Derecho	
Alteración radical de las garantías jurídicas	
Cambios geoestratégicos	
Avances tecnológicos disruptivos	
Situaciones de emergencia nacional	
Otros	

Tabla 35 Ejemplos de casos de alto impacto

Por supuesto, se espera que la probabilidad de materialización de estos eventos sea mínima, pero nunca se puede considerar de nivel cero o imposible, por lo que conviene tener en mente que también es preciso determinar el nivel de riesgo para este tipo de situaciones.

VII. EVALUACIÓN DEL NIVEL DE RIESGO DEL TRATAMIENTO

La evaluación del nivel de riesgo total del tratamiento se obtiene a partir del resultado de la evaluación del nivel de riesgo para cada uno de los factores de riesgo identificados en el tratamiento. La interdependencia de los distintos factores de riesgo podría elevar el nivel de riesgo del tratamiento por encima del peor caso de cada factor de riesgo tomado individualmente.

En el caso de que el tratamiento no esté dentro de los casos tasados que exigen realizar una EIPD (ver capítulo "Análisis de la obligación de realizar una EIPD), es necesario evaluar su nivel de riesgo del tratamiento. El objetivo es tanto para determinar la obligatoriedad/necesidad de realizar una EIPD como para determinar el nivel concreto de riesgo del tratamiento de cara a implementar las medidas y garantías que resulten adecuadas.

Cuando hay distintos factores de riesgo es necesario interpretar cómo dichos factores, considerados de forma independiente, podrían interactuar entre sí para incrementar el nivel de riesgo del tratamiento (factor de riesgo acumulado), mediante el análisis de sus dependencias y efectos combinados o las interacciones mutuas que existan entre ellos.

Dado un conjunto de factores riesgos identificados para el tratamiento, así como su nivel de riesgo asociado, se pueden utilizar distintas metodologías para evaluar el nivel de riesgo total resultante del tratamiento. En cuanto a la metodología concreta para determinar el nivel de riesgo del tratamiento para los derechos y libertades de los individuos, se recomienda que esté integrada dentro de la metodología general de la organización.

Por definición, en cualquier metodología, el nivel de riesgo del tratamiento no será inferior al nivel del riesgo de mayor valor que haya alcanzado un factor de riesgo identificado en ese tratamiento de forma individual.

A. APROXIMACIÓN SIMPLIFICADA

Una aproximación simplificada para determinar el nivel de riesgo de forma genérica es establecer una formula sencilla para evaluar la acumulación de factores de riesgos de la siguiente forma:

- El valor del nivel, para cada riesgo identificado, se cuantifica de la siguiente forma:
  - Bajo: 0,2
  - Medio: 0,5
  - Alto: 0,7
  - Muy Alto: 0,9
- Si para un conjunto de factores riesgos identificados {FR1, FR2, FR3… FRn} se han evaluado los siguientes niveles de riesgo {NR1, NR2, NR3… NRn}, el nivel de riesgo del tratamiento NRT del tratamiento se podría calcular como:
  - NRTa = (NR1 + NR2) – (NR1 * NR2)
  - NRTb = (NRTa+ NR3) – (NRTa * NR3)
  - …
  - NRT = (NRTn + NRn) – (NRTn * NRn)

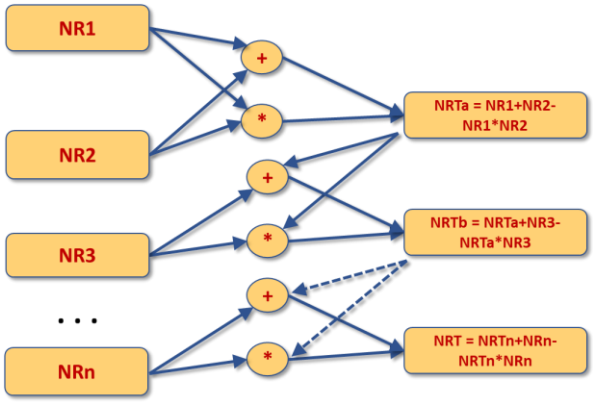

Figura 27: Un forma simplicada de calcular el riesgo del tratamiento.

- El resultado final se podría interpretar de la siguiente forma:
  - Nivel de riesgo del tratamiento Bajo: si es menor de 0,4
  - Nivel de riesgo del tratamiento Medio: de 0,4 a menor de 0,6
  - Nivel de riesgo del tratamiento Alto: de 0,6 a menor de 0,9
  - Nivel de riesgo del tratamiento Muy Alto: mayor o igual 0,9

B. APROXIMACIÓN MEDIANTE ANÁLISIS DE DEPENDENCIAS

Los factores de riesgo no son compartimentos estancos y aislados. Los factores de riesgo pueden tener relaciones entre sí, tanto con otros factores de riesgo dentro del tratamiento como con otros tratamientos que se ejecutan en la misma entidad, que tengan efectos aditivos, multiplicativos o incluso exponenciales.

El análisis de dichas dependencias se utiliza en el análisis de riesgo de seguridad con relación a los activos[96] y está estudiada de forma restringida a este campo, aunque se puede ampliar a todos los factores de riesgo en protección de datos.

En este caso, los activos son, con frecuencia, recursos compartidos entre varios tratamientos o procesos de la organización, por lo que podríamos hablar del factor del riesgo repercutido como el riesgo heredado por unos activos de aquellos otros activos de los que dependen, en particular, el resultado de acumular el riesgo heredado entre activos en términos de probabilidad e impacto. En este sentido, será necesario, cuando proceda, llevar a cabo el análisis de dependencias de los activos y asignar el valor del riesgo repercutido al activo de superior nivel en función de los riesgos de los activos de un nivel inferior de los que depende.

[96] https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/web/help/html/magerit_risk_deflected.html

VIII. CONTROLES PARA DISMINUIR EL RIESGO

Una vez identificados los factores de riesgo y determinado el nivel de riesgo del tratamiento se procederá a disminuir dicho nivel de riesgo a un valor aceptable.

A continuación, se describe un listado de medidas y garantías, denominadas de forma genérica controles, que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados en las siguientes dimensiones:

- El concepto del tratamiento
- La gobernanza y las políticas de protección de datos
- La protección de datos desde el diseño
- La seguridad en los tratamientos

Este listado no pretende ser exhaustivo, sino ilustrativo de posibles medidas que existen para afrontar los riesgos. Tampoco es un listado obligatorio de medidas mínimas que se han de adoptar en cualquier tratamiento. El responsable o encargado han de gestionar el riesgo afrontando las peculiaridades concretas de su tratamiento. En dicho sentido, el responsable o encargado ha de seleccionar o definir las medidas y garantías más adecuadas para tratar los riesgos específicos que se hayan identificado.

A. MEDIDAS SOBRE EL CONCEPTO Y DISEÑO DEL TRATAMIENTO

Estás medidas actuarán en la propia definición de la naturaleza, ámbito, contexto o fines del tratamiento, es decir, la esencia del tratamiento tal y como está concebido y diseñado. Entre las posibles medidas o garantías que se podrían adoptar estarían:

En cuanto a la naturaleza:	
	Cambiar, reordenar o reorganizar las fases del tratamiento.
	Eliminar alguna fase del tratamiento.
	Aislar y segregar fases del tratamiento entre sí para que traten datos de una forma más limitada. Por ejemplo, haciendo que algunas fases no traten datos personales (p.ej. datos anonimizados) o recurriendo a su seudonimización.
	Revisar los procedimientos de tratamiento de datos.
	Cambio de las elecciones técnicas para implementar las operaciones del tratamiento por tecnologías menos invasivas y/o más maduras.
	Cambio, en el sentido anterior, por tecnologías con mayor fiabilidad desde el punto de vista de protección de datos recurriendo, por ejemplo, al empleo de PETs (Privacy Enhanced Technologies).
	Reemplazar tratamientos automatizados por tratamientos manuales que incorporen procedimientos de supervisión y control.
	Llevar a cabo la supervisión humana de las decisiones automatizadas.
	Utilizar personal especialmente cualificado en determinadas fases del tratamiento, especialmente en su supervisión.
	Rediseñar los procedimientos de recogida, enriquecimiento o generación de datos personales.
	Reorganizar los espacios físicos donde se ejecuta el tratamiento.
	Rediseñar la orientación del trabajo en local, online o teletrabajo.

	Verificar la posibilidad de implementar medios alternativos de tratamiento: automático/manual, distintas opciones de automatización, …
	Limitar el acceso a los datos personales que es necesario que estén bajo la gestión de encargados.
	Otros.
En cuanto al ámbito:	
	Orientar el tratamiento a un número menor de sujetos.
	Orientar el tratamiento a cubrir un menor número de ámbitos de la vida de los sujetos.
	Orientar el tratamiento a una extensión geográfica limitada.
	Limitar el número de intervinientes o participantes.
	Limitar, en la concepción del tratamiento, el tiempo en el que el tratamiento trata datos de los mismos sujetos.
	Limitar el grado interacción o vinculación del tratamiento con otros tratamientos de la misma entidad.
	Limitar de la extensión del tratamiento a sujetos considerados vulnerables (ancianos, menores, personas con discapacidad, etc.)
	Definir, dentro del tratamiento, casos de uso concretos con ámbitos disjuntos.
	Otros.
En cuanto al contexto:	
	Delimitar los contextos sociales o económicos en los que se aplicará el tratamiento.
	Definir casos de uso restrictivos orientados a sectores específicos.
	Seleccionar los encargados de tratamiento para minimizar riesgos legales, sociales o políticos.
	Limitar vínculos o relaciones con tratamientos de otros responsables[97].
	Otros.
En cuanto a los fines:	
	Limitar o redefinir los fines del tratamiento.
	Eliminar fines secundarios en el tratamiento.
	Definir, dentro del tratamiento, casos de uso concretos con fines independientes.
	Otros.

Tabla 36 Ejemplos de posibles medidas sobre el concepto del tratamiento

B. MEDIDAS DE GOBERNANZA Y LAS POLÍTICAS DE PROTECCIÓN DE DATOS

Existen un conjunto de medidas y garantías que se podrían implementar a la hora de desplegar políticas de protección de datos como parte de la gobernanza del tratamiento. Estos controles están a caballo entre medidas específicas diseñadas para el tratamiento y las medidas establecidas como parte de la gobernanza de la organización.

[97] Por ejemplo, cuando los tratamientos de seguimiento de clientes en centros comerciales son soportados por un mismo servicio que da soporte a distintos responsables con una tecnología que permite vincular la actividad de una misma persona.

Estas medidas deberán estar integradas en las medidas de gobernanza de la organización[98]. Entre las medidas sugeridas, como especificidad con relación a la gestión del riesgo de los derechos y libertades, podrían considerarse las siguientes:

En cuanto al marco de gobernanza:	
	Existe un mandato y compromiso concreto de la dirección de la organización con relación a la gestión del riesgo para los derechos y libertades de los interesados.
	Está integrada la gestión del riesgo para los derechos y libertades de los interesados en los procesos de gestión de la organización.
	Existe una referencia explícita a la política de gestión del riesgo para los derechos y libertades en el marco de gestión del riesgo de la organización.
	Están diferenciadas las medidas que implementan las políticas de gestión de riesgos para los derechos y libertades de las políticas de gestión del riesgo de cumplimiento, legal o del riesgo de responsabilidad civil y penal.
	Están definidos los roles y asignación de responsabilidades y recursos necesarios para garantizar la protección de datos en la organización.
	Existen los recursos necesarios para garantizar la protección de datos en la organización.
	Está procedimentado el ciclo de mejora continua que permita garantizar la efectividad y adecuación de las políticas de protección de datos a la naturaleza, el contexto, el alcance y los objetivos de los distintos tratamientos a lo largo de su ciclo de vida.
	Existen indicadores tangibles sobre la implementación efectiva de las políticas de protección de datos.
En cuanto a la asesoría en materia de protección de datos:	
	Se ha realizado el nombramiento del DPD o la definición del órgano colegiado que ejercerá las funciones del DPD en la organización (artículos 37,38 y 39 RGPD) aun no siendo obligatorio[99].
	Está establecida la implicación del DPD en los procedimientos de decisión y definición de los tratamientos.
	Están definidos los canales internos para la comunicación con el DPD, la asesoría en protección de datos y/o los responsables de la gestión de los riesgos para los derechos y libertades.
	Se han implementado acciones para que los integrantes de la organización conozcan el rol del DPD, la asesoría en protección de datos y/o el responsable de la gestión de los riesgos para los derechos y libertades sus funciones y los canales para comunicarse con él.
	Las obligaciones de asesoría y supervisión (art. 39.1.a y b) del DPD o de la asesoría en protección de datos se extienden al desarrollo, mantenimiento y supervisión de las políticas de protección de datos.
	Otros.

[98] Por ejemplo, si la organización ha adoptado la norma ISO 31000, con las medidas de implementación del marco de trabajo de la gestión del riesgo.
[99] Cuando el nombramiento de un DPD es obligatorio, este nombramiento no está sujeto al resultado o la necesidad derivada de la gestión del riesgo.

En cuanto a las políticas de protección de datos integradas en los procedimientos:	
	Están incluidos, en los procedimientos de concepción, diseño e implementación de nuevos tratamientos, estrategias de responsabilidad activa para la protección de datos: la gestión del riesgo para los derechos y libertades, la protección de datos desde el diseño, la protección de datos por defecto, la transparencia del tratamiento y la seguridad desde el diseño y por defecto.
	Están incluidos en los procedimientos de adquisición de productos, sistemas o servicios que van a implementar operaciones dentro de la actividad de tratamiento el requerir información y garantías[100] para asegurar y poder demostrar que dicho tratamiento cumple con el RGPD.
	Están designados los puntos de contacto dentro de la organización para cada tratamiento de datos personales.
	Los buzones de denuncia implementan la gestión de abusos en temas de protección de datos.
	La protección de datos está integrada en los procedimientos de trabajo en local, remoto y teletrabajo.
	Existe una política BYOD en la que se integran los requisitos de protección de datos.
	En la política de gestión del tratamiento se establecen las condiciones para la verificación y tratamiento de la gestión del riesgo para los derechos y libertades de las personas.
	En la política de gestión del tratamiento se establecen cláusulas de caducidad en las condiciones del tratamiento.
	Otros.
Con relación a la atención a los interesados[101]	
	En la medida que puedan resultar en una disminución del riesgo, ofrecer procedimientos para la atención de derechos que vayan más allá de los mínimos establecidos en el Capítulo III del RGPD.
	En la medida que puedan resultar en una disminución del riesgo, disponer de políticas de transparencia que vayan más allá de los mínimos establecidos en el Capítulo III del RGPD[102].
	Disponer de canales de comunicación con los interesados con relación a la protección de su privacidad.
	Existen procedimientos de consulta a los interesados con relación a la protección de sus derechos.
	Otros

[100] Estas pueden ser de diverso tipo: auditorias independientes, certificaciones u otras; tanto a nivel técnico, cumplimiento, procedimiento u otros.

[101] Recordad que los interesados no son solo los clientes, sino también son interesados, en la medida que se tratan sus datos personales, los empleados, otras personas físicas con las que la entidad tiene relación y cualquier otra persona afectada indirectamente por el tratamiento.

[102] Estas políticas de transparencia se concretarán en cada tratamiento como estrategias de protección de datos desde el diseño.

Con relación a la seguridad (tanto de la organización como de la información):	
	Una referencia a la gestión del riesgo para los derechos y libertades en la política de la seguridad aplicable a los tratamientos de datos personales, así como en la política general de seguridad que fuera aplicable a la organización.
	Una integración de la protección de los derechos y libertades en el sistema de gestión de seguridad de la información (SGSI).
	Una correcta diferenciación de roles entre el DPD y los responsables TIC o de seguridad de la información.
	Una implementación de la necesaria coordinación entre el DPD y el responsable de seguridad de la organización, del sistema de información y otros en función de la entidad.
	Una clara definición del alcance de la participación del DPD en los comités de seguridad.
	Otros.
Respecto de las garantías jurídicas:	
	Están establecidos compromisos de confidencialidad para aquellos que tengan acceso a datos de carácter personal.
	Establecimiento de garantías a los encargados que vayan más allá de lo establecido en el artículo 28 del RGPD.
	Están establecidos compromisos para no llevar a cabo esfuerzos que pudieran dar lugar a la reidentificación de las personas en conjuntos de datos disociados.
	Están habilitados instrumentos con validez jurídica que protejan los derechos y libertades de los interesados en caso de materialización de riesgos específicos.
	Están habilitados instrumentos con validez jurídica que compensen equilibradamente a los interesados (no al responsable) de los daños a sus derechos y libertades en caso de materialización de riesgos específicos.
	Otros.
En relación con la formación y preparación del personal con relación a la protección de datos:	
	Están establecidas medidas de concienciación y formación del personal implicado en la definición o concepción de nuevos tratamientos
	Establecimiento de medidas de concienciación y formación del personal implicado en las operaciones de tratamiento de datos personales.
	En las guías orientadas a trabajadores, según sus roles específicos, está incluida información con relación a las obligaciones relativas a la protección de datos.
	En las guías orientadas a trabajadores, según sus roles específicos, está incluida información con relación a cómo actuar ante reclamaciones de derechos.
	En las guías orientadas a trabajadores, según sus roles específicos, está incluida información con relación a cómo actuar ante una brecha de datos personales.

	En las guías orientadas a trabajadores, según sus roles específicos, está incluida información con relación a sus derechos y canales de denuncia relativos a la protección de datos.
	Otros.
Respecto a la relación responsable-encargado	
	Está incluida en los modelos de contratos la referencia a las cláusulas contractuales aplicables en las relaciones responsable-encargado.
	En los procedimientos de contratación de encargados están incluidas las obligaciones del artículo 28 del RGPD.
	En los procedimientos de contratación de encargados están detallados procedimientos de evaluación del encargado que garantizarán que se elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas en función del riesgo del tratamiento[103].
	Las cláusulas contractuales se extenderán más allá de los requisitos establecidos en el artículo 28 del RGPD para la adecuada gestión del riesgo del tratamiento[104].
	Las cláusulas contractuales incluyen elementos que pueden ayudar al encargado a comprender los riesgos para los derechos y libertades de los datos derivados del tratamiento[105].
	Las cláusulas contractuales contemplan las medidas de seguridad aplicables al tratamiento.
	Las cláusulas contractuales contemplan la obligación del encargado de obtener la aprobación del responsable con anterioridad a realizar cualquier cambio sobre las medidas de seguridad[106].
	Las cláusulas contractuales contemplan la obligación del responsable de revisar dichas medidas periódicamente en función del riesgo[107].
	Están incluidos en los procedimientos de contratación diligencias adicionales para garantizar el cumplimiento de la normativa de datos personales.
	El responsable realiza auditorías propias sobre los encargados con relación al tratamiento.
	Terceros independientes auditan o certifican al encargado con relación al tratamiento.
	Otros.
En cuanto a las comunicaciones de datos:	
	Existen mecanismos para tener trazabilidad de las comunicaciones de datos personales realizadas por el responsable y encargado a encargados, subencargados y terceros.
	Está procedimentado la definición de mecanismos, garantías y límites aplicables a las transferencias internacionales de datos para cada tratamiento.

[103] "94. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment" Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[104] Párrafo 112 de las Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[105] Párrafo 110 y 131 de las Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[106] Párrafo 123 de las Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[107] Párrafo 123 de las Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

	Está procedimentado la referencia a las normas corporativas vinculantes que se aplicasen a la organización, con el detalle de aquellos ámbitos y tratamientos específicos aplicables, así como sus límites.
	Otros.
Dentro de la política de gestión documental:	
	Existe una definición de documentos que permiten al responsable demostrar el cumplimiento
	Está incluida la gestión del riesgo para los derechos y libertades.
	Existe trazabilidad y control de versiones de la documentación de gestión del riesgo para los derechos y libertades que se vaya generando.
	Otros.
En relación con los procedimientos para la gestión de brechas de datos personales e incidentes en el tratamiento:	
	Están definidos procedimientos para detectar brechas, incidentes o errores en los tratamientos de datos personales.
	El papel del DPD está claramente definido en los procedimientos relativos a la gestión de brechas de datos personales, garantizando, al menos, que cumple con 39.1.
	Existen procedimientos definidos para reaccionar ágilmente, a nivel de organización, ante brechas, incidentes o errores en los tratamientos de datos personales.
	Están definidos canales de comunicación, información y consulta sobre brechas de datos e incidentes con las partes implicadas en los tratamientos de datos personales.
	Están definidas medidas para identificar, en las comunicaciones de los propios interesados al responsable/encargado, información sobre brechas, incidencias o errores.
	Existen procedimientos para la notificación de brechas de datos personales a la Autoridad de Control.
	Existen procedimientos para la comunicación a los interesados de brechas de datos personales.
	Se han planteado escenarios concretos de potenciales brechas, errores o incidentes de especial gravedad, y se ha definido la forma de gestionarlos, específicamente, para proteger los derechos y libertades de los interesados.
	Existe conexión entre los procedimientos para la gestión de brechas e incidentes en el tratamiento y el proceso de gestión riesgos, incluyendo la gestión de los controles asociados.
	Otros.
En cuanto a la profundidad de la gestión del riesgo:	
	Realizar una EIPD aun no siendo esta obligatoria.
	Existen procedimientos internos que hacen necesaria la EIPD con independencia de que exista o no obligación legal de llevarla a cabo.
	Otros.

Respecto a las actividades de seguimiento y verificación de las medidas de gobernanza:	
	Están implementados planes de auditorías internas o externas que evalúen el cumplimento de las políticas de protección de datos.
	Están establecidas políticas de certificación en protección de datos.
	Están identificados, en su caso, los mecanismos de adhesión a códigos de conducta.
	Están implantados mecanismos, normas y procedimientos, para detectar cambios en la naturaleza, ámbito, contexto o fines del tratamiento.
	Están implementados mecanismos de decisión para que, en función de los cambios anteriores o incidencias detectadas, se realice un nuevo ciclo de revisión del riesgo.
	Otros.

Tabla 37 Ejemplos de posibles medidas de gobernanza y politicas de protección de datos

C. MEDIDAS DE PROTECCIÓN DE DATOS DESDE EL DISEÑO

Los controles de protección de datos desde el diseño son una de las medidas a tener en cuenta en la gestión del riesgo para los derechos y libertades, tal como establece el apartado 1 del artículo 25 del RGPD.

La AEPD, en su "Guía de Privacidad desde el Diseño", traslada a la práctica el principio de protección de datos desde el diseño, entendiéndolo como la necesidad de incluir la protección de los datos personales como uno más de los factores a ser tenidos en cuenta en cuenta en la fase de especificación de requisitos de productos y servicios, junto a otros como los requisitos de seguridad, de protección de datos por defecto, de accesibilidad o de rendimiento.

Los objetivos de protección de datos personales desde el diseño que deben ser tenidos en cuenta para productos, aplicaciones y servicios que se desarrollen son seis. Por un lado, están los tres orientados a proteger la seguridad de la información, confidencialidad, integridad y disponibilidad clásicamente y que se desarrollan en el siguiente apartado "Medidas de seguridad para la protección de los derechos y libertades". Por otro lado, están los específicos de desvinculación, transparencia y control:

OBJETIVOS DE PROTECCIÓN DE LA PRIVACIDAD		
DESVINCULACIÓN	TRANSPARENCIA	CONTROL
Minimización de datos Limitación del plazo de conservación Integridad y confidencialidad	Licitud, lealtad y transparencia Limitación de la finalidad	Limitación de la finalidad Exactitud Integridad y confidencialidad Responsabilidad proactiva

Tabla 38 Objetivos de protección de la privacidad desde el diseño.

La Guía de Privacidad desde el Diseño contiene un desarrollo de los seis objetivos. A continuación, se expone un breve resumen que condensa la información de los relacionados con desvinculación, transparencia y control.

1. Minimizar

El objetivo que persigue esta estrategia es evitar el procesamiento de datos que no sean necesarios para las finalidades perseguidas en el tratamiento. Supone la implementación de medidas orientadas a:

- **Seleccionar:** elegir únicamente la muestra de individuos relevante y los atributos necesarios.
- **Excluir:** excluir de antemano los sujetos y atributos que resulten irrelevantes para el tratamiento realizado.
- **Podar**: eliminar parcialmente los datos personales tan pronto dejen de ser necesarios.
- **Eliminar**: suprimir por completo los datos personales tan pronto dejen de ser relevantes.

2. Ocultar

Esta estrategia se centra en limitar la exposición de los datos, estableciendo las medidas necesarias para garantizar la protección de los objetivos de confidencialidad y desvinculación. La ocultación exige aplicar las siguientes estrategias:

- **Restringir:** gestionar de forma restrictiva el acceso a los datos personales.
- **Ofuscar:** hacer que los datos personales sean ininteligibles para aquellos que no estén autorizados a su consulta.
- **Disociar:** eliminar la vinculación entre conjuntos de datos que se han de mantener independientes, así como los atributos identificativos de los registros de datos para evitar correlaciones entre ellos.
- **Agregar:** Agrupar la información relativa a varios sujetos utilizando técnicas de generalización y supresión [108].

3. Separar

El objetivo que persigue esta estrategia es evitar, o al menos minimizar, el riesgo de procesamiento, en una misma entidad, de diferentes datos personales pertenecientes a un mismo individuo y utilizados en tratamientos independientes. Las medidas pueden ser:

- **Aislar:** recoger y almacenar los datos personales en diferentes bases de datos o aplicaciones que sean independientes desde el punto de vista lógico o incluso que se ejecuten sobre sistemas físicos distintos, adoptando medidas adicionales para garantizar esa desvinculación.

  Otra forma de aislar en el tiempo los datos personales es la renovación periódica de los identificadores únicos que señalan a un individuo.

[108] Agencia Española de Protección de Datos (AEPD) – Unidad de Evaluación y Estudios Tecnológicos. *La K-anonimidad como medida de la privacidad,* Jun 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf

- **Distribuir:** diseminar la recogida y el tratamiento de los diferentes subconjuntos de datos personales correspondientes a diferentes tipos de tratamiento sobre unidades de tramitación y gestión que, dentro de la organización, sean físicamente independientes y utilicen sistemas y aplicaciones distintos, intentando implementar arquitecturas descentralizadas y distribuidas con procesamiento local de la información siempre que sea posible en lugar de soluciones centralizadas con accesos unificados y que dependan de una misma unidad de control.

4. Abstraer

El objetivo es limitar al máximo el detalle de los datos personales que son tratados. A diferencia de la estrategia 'minimizar' que realiza una selección previa de los datos recogidos, esta estrategia se centra en el grado de detalle con el que los datos son tratados y en su proceso de agregación mediante:

- **Sumarizar:** generalizar los valores de los atributos utilizando intervalos o rangos de valores, en lugar de utilizar el valor concreto del campo.
- **Agrupar:** agregar la información de un grupo de registros en categorías en lugar de utilizar la información detallada de cada uno de los sujetos que pertenecen al grupo, trabajando con los valores medios o generales.
- **Perturbar:** utilizar valores aproximados o modificar el dato real mediante el empleo de algún tipo de ruido aleatorio en lugar de trabajar con el valor exacto del dato personal.

5. Informar

Esta estrategia pretende la implementación del objetivo y el principio de trasparencia más allá de los mínimos establecido por el Reglamento, cuando los mecanismos adicionales implementados permitan disminuir los riesgos para los interesados, de la siguiente forma:

- **Facilitar:** proporcionar a los interesados detalles adicionales en relación con el tratamiento.
- **Explicar:** facilitar la información relativa a los tratamientos de forma concisa, transparente, inteligible y de fácil acceso utilizando un lenguaje claro y sencillo.
- **Notificar:** comunicar a los interesados particularidades, incidencias o cambios en la naturaleza, ámbito, contexto, fines del tratamiento o en sus riesgos, más allá de las obligaciones establecidas en el RGPD.

6. Controlar

Persigue el objetivo de proporcionar a los interesados control en relación con el tratamiento de sus datos más allá de lo establecido en el RGPD permitiéndoles gestionar el riesgo, de la siguiente forma:

- **Consentir:** mecanismos más garantistas para la recogida y retirada del consentimiento.
- **Alertar:** permitir al usuario determinar alertas relativas al tratamiento de sus datos personales.

- **Elegir:** proporcionar el control al usuario de la funcionalidad granulada [109] de aplicaciones y servicios.
- **Actualizar:** implementar mecanismos más ágiles que faciliten a los usuarios la revisión, actualización y rectificación de los datos.
- **Retirar:** proporcionar mecanismos para que los usuarios puedan suprimir o solicitar el borrado de los datos personales de manera más ágil.

7. Cumplir

Esta estrategia hace referencia a la implementación, desde el diseño y de forma efectiva, de las garantías procedimentales, de las políticas y las medidas de gobernanza vinculadas a la protección de datos como parte del tratamiento concreto, buscando:

- **Definir:** especificar políticas de protección de datos en la entidad previamente al diseño de los tratamientos y determinar cuáles son aplicables a los mismos.
- **Mantener:** Revisar la efectividad de las políticas implementadas.
- **Defender:** Implementar mecanismos en los tratamientos que garanticen la aplicación de las políticas.

8. Demostrar

El objetivo es la implementación de las políticas de *accountability,* desde el punto de vista de demostrar cumplimiento, en el tratamiento en cuestión. Para ello hay que:

- **Registrar:** documentar todas y cada una de las decisiones tomadas en el tiempo con relación al concepto, diseño e implementación del tratamiento aun cuando hayan resultado contradictorias, identificando quién las tomó, cuándo y la justificación para hacerlo. El registro debe apoyarse en mecanismos de autenticidad como la firma electrónica o sellos de tiempo.
- **Auditar:** revisar de forma sistemática, independiente y documentada el grado de cumplimiento de las políticas de protección de datos en el tratamiento.
- **Informar:** poner dicha información a disposición de la Autoridad de Control, los interesados o posibles terceros como, por ejemplo, la entidad de supervisión de un código de conducta, en la medida en que proceda y que tenga por objeto la posible reducción de los riesgos.

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a datos	Minimizar	Evitar el tratamiento de datos personales innecesarios.	Anonimización Seudonimización

[109] Las funcionalidades que requieran una legitimación basada en el consentimiento han de poderse seleccionarse de forma independiente tanto del propósito principal del objeto como entre ellas.

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
		TÁCTICAS: **seleccionar**, **excluir**, **podar** y **eliminar**	Bloqueo de correlación en sistemas de gestión de identidad federada Depuración de entrada de datos y metadatos
	Ocultar	Limitar la exposición de los datos personales. TÁCTICAS: **restringir**, **ofuscar**, **disociar** y **agregar**)	Control de accesos Anonimización selectiva en el acceso a grupos de datos personales. Cifrado Cifrado homomórfico Redes de mezcla Atributos basados en credenciales Modelos de conocimiento cero (ZKP)
	Separar	Mantener separados los conjuntos de datos personales. TÁCTICAS: **aislar** y **distribuir**	Listas negras anónimas Separación física y lógica Técnicas de desvinculación de datos
	Abstraer	Limitar al máximo el nivel de detalle utilizado en los tratamientos de datos personales. TÁCTICAS: **sumarizar**, **agrupar** y **perturbar**	Agregación en el tiempo K-anonimidad Ofuscación de medidas mediante agregación de ruido Granularidad dinámica. Privacidad diferencial
Estrategias orientadas a procesos	Informar	Proporcionar información extendida del tratamiento. TÁCTICAS: **facilitar**, **explicar** y **notificar**	Iconos de privacidad. Alertas de tratamiento. Publicar información sobre el rendimiento del tratamiento.

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
			Publicar detalles sobre las limitaciones y consecuencias del tratamiento. Publicar información relativa a los análisis de riesgos.
	Controlar	Proporcionar a los sujetos de datos un control extendido sobre sus datos personales. TÁCTICAS: **consentir**, **alertar**, **elegir**, **actualizar**, **retirar**	PIMS (personal information management systems) Paneles de preferencias de privacidad Transmisión activa de presencia Selección de credenciales
	Cumplir	Aplicación de las políticas de protección de datos de la entidad al tratamiento. TÁCTICAS: **definir**, **mantener**, **defender**	Aplicar políticas de protección de datos al ciclo de vida del tratamiento.
	Demostrar	Poder demostrar que los tratamientos se han desarrollado de acuerdo con las políticas de la entidad. TÁCTICAS: **registrar**, **auditar** e **informar**.	Auditoría del tratamiento Registro y control documental del tratamiento.

Tabla 39 Estrategias, descripción, tácticas, controles y patrones de protección de datos desde el diseño.

D. MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DERECHOS Y LIBERTADES

Las medidas de seguridad para la protección de los derechos y libertades han de entenderse en sentido amplio. Es decir, no solo cubriendo aspectos relativos, por ejemplo, a accesos no autorizados, sino otras posibles amenazas. Ejemplos de dichas amenazas son las causas naturales, los accidentes, los errores humanos y posibles errores en el funcionamiento de los tratamientos automatizados, en particular aquellos que se derivan de sistemas que infieren nuevos datos personales o toman decisiones automatizadas sobre los individuos.

Como se ha señalado en los apartados anteriores, los requisitos de seguridad para la protección de los derechos y libertades forman parte de la gestión integral de la seguridad de una organización (seguridad de la organización, de las personas, de la información, continuidad de procesos, lucha contra el fraude, imagen corporativa, etc.). La selección de controles, para el caso que nos ocupa, ha de estar guiada para una adecuada gestión del riesgo para los derechos y libertades de los interesados.

En los siguientes apartados, se describirá una de las posibles formas de conseguir esa integración. Sin embargo, se recomienda integrar la gestión de la seguridad para los derechos y libertades en las políticas ya establecidas en la entidad.

1. Tratamientos sometidos al ENS

En el caso de tratamientos sometidos al Esquema Nacional de Seguridad (ENS) [110] se podría realizar la siguiente correspondencia en función del nivel de riesgo para los derechos y libertades determinado en el tratamiento:

Nivel de riesgo para los derechos y libertades	Categoría ENS
Muy Alto	Alto
Alto	Alto
Medio	Medio
Bajo	Bajo

Tabla 40 Correspondencia entre el nivel de riesgo para los derechos y libertades y la categoría ENS

Dicha propuesta está basada en la experiencia de las Autoridades de Control con relación a las brechas de datos personales notificadas y, en ningún caso, se trata de una propuesta que limite al responsable quien, en última instancia, siempre tiene la obligación de aplicar las medidas necesarias para garantizar los derechos y libertades de los interesados atendiendo a la naturaleza, el ámbito o alcance, el contexto y la finalidad de los tratamientos que lleve a cabo tal y como se expresaba en la declaración wp218.[111]

2. Aproximación básica a la implementación de medidas de seguridad

En el caso de tratamientos que no estén sometidos a la obligación de cumplimiento del ENS, se tendrán que implementar las medidas necesarias para gestionar el nivel de riesgo de los activos necesarios para dar soporte al tratamiento en cada una de sus fases. Estas medidas se establecerán y se integrarán de diferente manera en función

[110] Disposición adicional primera LOPDGDD: *"Medidas de seguridad en el ámbito del sector público: 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan a las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado."*

[111] "El cumplimiento nunca debería reducirse a un ejercicio de checklist, sino a garantizar que los datos personales sean suficientemente protegidos. La forma en la que esto se haga puede ser distinta para cada responsable….. Los interesados deberían tener el mismo nivel de protección, con independencia del tamaño de la organización o la cantidad de datos tratados."

de la metodología empleada en la organización para la gestión de riesgos de seguridad de la información. Guías enumeran posibles medidas se pueden encontrar en distintos estándares internaciones, como la ISO-27002 o en la extensión para temas de protección de datos en la ISO-27701.

Como orientación, se recomienda no implementar un nivel menor de seguridad que el criterio establecido en el Anexo II del Esquema Nacional de Seguridad, y que se traslada aquí, de forma íntegra, con las siguientes claves:

- Categoría del sistema: B-básico, M-medio, A-alto
- Dimensión: C-confidencialidad, D-disponibilidad, I-integridad, T-trazabilidad, A-autenticidad.
- "aplica" indica que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad.
- 'n.a.' significa 'no aplica'.
- "=" indica que las exigencias de un nivel son iguales a las del nivel inferior.
- Los signos "+" y "++" indican un incremento de las exigencias, graduado en función del nivel inferior de la dimensión de seguridad.
- El color verde se utiliza para indicar que una cierta medida se aplica en sistemas de categoría básica o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría media o superior; el rojo para indicar las medidas que sólo se aplican en categoría alta.
- En el listado de medidas, se ha marcado en rojo con fondo amarillo la variación respecto al listado original del ENS para reflejar la obligación marcada en los artículos 33 y 34 del RGPD de gestionar y documentar brechas de datos personales.

Dimensión	Nivel			**MEDIDAS DE SEGURIDAD**	
	B	**M**	**A**		
				org	**Marco organizativo**
Todas	aplica	=	=	[org.1]	Política de seguridad
Todas	aplica	=	=	[org.2]	Normativa de seguridad
Todas	aplica	=	=	[org.3]	Procedimientos de seguridad
Todas	aplica	=	=	[org.4]	Proceso de autorización
				op	**Marco operacional**
				[op.pl]	Planificación
Todas	aplica	+	++	[op.pl.1]	Análisis de riesgos
Todas	aplica	+	++	[op.pl.2]	Arquitectura de seguridad
Todas	aplica	=	=	[op.pl.3]	Adquisición de nuevos componentes

D	n.a.	aplica	=	[op.pl.4]	Dimensionamiento / Gestión de capacidades
Todas	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificados
				[op.acc]	Control de acceso
A T	aplica	=	=	[op.acc.1]	Identificación
I C A T	aplica	=	=	[op.acc.2]	Requisitos de acceso
I C A T	n.a.	aplica	=	[op.acc.3]	Segregación de funciones y tareas
I C A T	aplica	=	=	[op.acc.4]	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	[op.acc.5]	Mecanismo de autenticación
I C A T	aplica	+	++	[op.acc.6]	Acceso local (local logon)
I C A T	aplica	+	=	[op.acc.7]	Acceso remoto (remote login)
				[op.exp]	Explotación
Todas	aplica	=	=	[op.exp.1]	Inventario de activos
Todas	aplica	=	=	[op.exp.2]	Configuración de seguridad
Todas	n.a.	aplica	=	[op.exp.3]	Gestión de la configuración
Todas	aplica	=	=	[op.exp.4]	Mantenimiento
Todas	n.a.	aplica	=	[op.exp.5]	Gestión de cambios
Todas	aplica	=	=	[op.exp.6]	Protección frente a código dañino
Todas	aplica	=	=	[op.exp.7]	Gestión de incidentes
T	aplica	+	++	[op.exp.8]	Registro de la actividad de los usuarios
Todas	aplica	=	=	[op.exp.9]	Registro de la gestión de incidentes
T	n.a.	n.a.	aplica	[op.exp.10]	Protección de los registros de actividad
Todas	aplica	+	=	[op.exp.11]	Protección de claves criptográficas
				[op.ext]	Servicios externos
Todas	n.a.	aplica	=	[op.ext.1]	Contratación y acuerdos de nivel de servicio
Todas	n.a.	aplica	=	[op.ext.2]	Gestión diaria
D	n.a.	n.a.	aplica	[op.ext.9]	Medios alternativos
				[op.cont]	Continuidad del servicio

D	n.a.	aplica	=	[op.cont.1]	Análisis de impacto
D	n.a.	n.a.	aplica	[op.cont.2]	Plan de continuidad
D	n.a.	n.a.	aplica	[op.cont.3]	Pruebas periódicas
				[op.mon]	Monitorización del sistema
Todas	n.a.	aplica	=	[op.mon.1]	Detección de intrusión
Todas	aplica	+	++	[op.mon.2]	Sistema de métricas
				mp	**Medidas de protección**
				[mp.if]	Protección de las instalaciones e infraestructuras
Todas	aplica	=	=	[mp.if.1]	Áreas separadas y con control de acceso
Todas	aplica	=	=	[mp.if.2]	Identificación de las personas
Todas	aplica	=	=	[mp.if.3]	Acondicionamiento de los locales
D	aplica	+	=	[mp.if.4]	Energía eléctrica
D	aplica	=	=	[mp.if.5]	Protección frente a incendios
D	n.a.	aplica	=	[mp.if.6]	Protección frente a inundaciones
Todas	aplica	=	=	[mp.if.7]	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	[mp.if.9]	Instalaciones alternativas
				[mp.per]	Gestión del personal
Todas	aplica	=	=	[mp.per.1]	Caracterización del puesto de trabajo
Todas	aplica	=	=	[mp.per.2]	Deberes y obligaciones
Todas	aplica	=	=	[mp.per.3]	Concienciación
Todas	aplica	=	=	[mp.per.4]	Formación
D	n.a.	n.a.	aplica	[mp.per.9]	Personal alternativo
				[mp.eq]	Protección de los equipos
Todas	aplica	+	=	[mp.eq.1]	Puesto de trabajo despejado
A	n.a.	aplica	+	[mp.eq.2]	Bloqueo de puesto de trabajo
Todas	aplica	=	+	[mp.eq.3]	Protección de equipos portátiles
D	n.a.	aplica	=	[mp.eq.9]	Medios alternativos

				[mp.com]	Protección de las comunicaciones
Todas	aplica	=	+	[mp.com.1]	Perímetro seguro
C	n.a.	aplica	+	[mp.com.2]	Protección de la confidencialidad
I A	aplica	+	++	[mp.com.3]	Protección de la autenticidad y de la integridad
Todas	n.a.	n.a.	aplica	[mp.com.4]	Segregación de redes
D	n.a.	n.a.	aplica	[mp.com.9]	Medios alternativos
				[mp.si]	Protección de los soportes de información
C	aplica	=	=	[mp.si.1]	Etiquetado
I C	n.a.	aplica	+	[mp.si.2]	Criptografía
Todas	aplica	=	=	[mp.si.3]	Custodia
Todas	aplica	=	=	[mp.si.4]	Transporte
C	aplica	+	=	[mp.si.5]	Borrado y destrucción
				[mp.sw]	Protección de las aplicaciones informáticas
Todas	n.a.	aplica	=	[mp.sw.1]	Desarrollo
Todas	aplica	+	++	[mp.sw.2]	Aceptación y puesta en servicio
				[mp.info]	Protección de la información
Todas	aplica	=	=	[mp.info.1]	Datos de carácter personal
C	aplica	+	=	[mp.info.2]	Calificación de la información
C	n.a.	n.a.	aplica	[mp.info.3]	Cifrado
I A	aplica	+	++	[mp.info.4]	Firma electrónica
T	n.a.	n.a.	aplica	[mp.info.5]	Sellos de tiempo
C	aplica	=	=	[mp.info.6]	Limpieza de documentos
D	aplica	=	=	[mp.info.9]	Copias de seguridad *(backup)*

				[mp.s]	Protección de los servicios
Todas	aplica	=	=	[mp.s.1]	Protección del correo electrónico
Todas	aplica	=	+	[mp.s.2]	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	[mp.s.8]	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	[mp.s.9]	Medios alternativos

Tabla 41 Selección de medidas de seguridad.

3. Gestión de brechas[112] de datos personales.

La gestión de brechas de datos personales se ha de dimensionar en función del riesgo para los derechos y libertades. Entre los controles específicos orientados a garantizar una correcta detección y gestión de la brecha podrían considerarse:

Controles específicos en la gestión de brechas de datos personales
Planes de contingencia ante una brecha de datos personales.
Establecimiento de medios técnicos para la detección automática de brechas de datos personales.
Herramientas de gestión de incidentes adaptadas a los requisitos del RGPD.
Protocolos para la identificación de potenciales brechas en las quejas o comunicaciones de los usuarios o interesados.
Capacidad de evaluar la gravedad de la brecha.
Procedimientos para describir con precisión el impacto de una brecha para los derechos y libertades.
Canales internos ágiles para la comunicación de la brecha al DPD, si este está nombrado.
Canales ágiles de comunicación responsable-encargado con relación a las brechas.

[112] El término resultante de la traducción del RGPD al castellano es el de "violaciones de seguridad" aunque en el presente documento se ha preferido utilizar el término más comúnmente utilizado de *"brechas" de datos personales para designar a "toda violación de la seguridad que ocasione 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"*.

Procedimiento de decisión sobre cómo actuar con relación a la protección de los derechos y libertades ante la brecha.
Procedimientos de notificación a la Autoridad de Control para poder cumplir con los requisitos del artículo 33.
Procedimientos de comunicación a los interesados para poder cumplir con los requisitos del artículo 34.

Tabla 42 Controles específicos en la gestión de brechas de datos personales.

4. Resiliencia

Entre los controles específicos orientados a implementar un adecuado grado de resiliencia de los datos personales y los sistemas que los soportan, podrían considerarse los siguientes:

Objetivo	Controles
Capacitación de las personas.	Capacidad de detectar los cambios
	Capacidad de comunicarlos
	Capacidad de entenderlos
	Capacidad de innovar ante ellos
	Capacidad de actuar en tiempo real
	Voluntad de actuar de forma proactiva
Flujo adecuado de información	Ágil
	Específico
	Mínimo
	Completo
	Desde y hacia las personas adecuadas
Liderazgo	Puntos claros de toma de decisión Responsabilidades bien definidas.
Adaptabilidad estratégica	Las estructuras físicas, tecnológicas y organizativas han de poder evolucionar en tiempo real hacia nuevos objetivos o formas de actuar.

Tabla 43 Controles relativos a la resiliencia.

5. Fallos en las garantías técnicas de protección de datos y errores en las aplicaciones

Las medidas para el caso de brechas en las garantías técnicas de protección de datos, como en seudonimización, así como posibles errores en las aplicaciones, se pueden proyectar en las siguientes medidas de la siguiente forma:

Dimensión	Nivel			MEDIDAS DE SEGURIDAD	
	B	M	A		
				org	Marco organizativo
F,E	aplica	=	=	[org.4]	Proceso de autorización
				op	Marco operacional
				[op.pl]	Planificación
F,E	aplica	+	++	[op.pl.1]	Análisis de riesgos
F,E	n.a.	aplica	++	[op.pl.5]	Componentes certificados
				[op.exp]	Explotación
F,E	n.a.	aplica	=	[op.exp.3]	Gestión de la configuración
F,E	aplica	=	=	[op.exp.4]	Mantenimiento
F,E	n.a.	aplica	=	[op.exp.5]	Gestión de cambios
F,E	aplica	=	=	[op.exp.7]	Gestión de incidentes
F,E	aplica	=	=	[op.exp.9]	Registro de la gestión de incidentes
				[op.ext]	Servicios externos
F,E	n.a.	aplica	=	[op.ext.1]	Contratación y acuerdos de nivel de servicio
F,E	n.a.	aplica	=	[op.ext.2]	Gestión diaria
				[mp.per]	Gestión del personal
F,E	aplica	+	++	[mp.per.3]	Concienciación
F,E	aplica	+	++	[mp.per.4]	Formación
				[mp.sw]	Protección de las aplicaciones informáticas
F,E	aplica	+	++	[mp.sw.1]	Desarrollo
F,E	aplica	+	++	[mp.sw.2]	Aceptación y puesta en servicio

Tabla 44 Controles relativos a fallos en las garantías técnicas de protección de datos y errores en las aplicaciones

6. Aproximación avanzada a la implementación de medidas de seguridad

Una gestión más detallada de la gestión del riesgo de seguridad se podría realizar partiendo de un análisis completo de cada uno de los activos identificados en el tratamiento. En ese caso, se analizaría cada una de las dimensiones de seguridad que

se vean afectadas para cada activo (ver el apartado Identificación y análisis de factores de riesgo -> Riesgo derivado de brechas de datos personales -> Análisis completo) aplicando los controles específicos más apropiados para cada uno de los activos, atendiendo a su nivel de riesgo y la categoría en que se haya enmarcado.

A partir de la categoría establecida para cada activo, se procedería a la implementación de las mismas para dicho activo en concreto. Para cada amenaza identificada debe de establecerse uno o varios controles teniendo en cuenta las características del activo a proteger, así como el coste del control o los controles que se pretenden implementar.

En este caso, se recomienda aplicar los criterios seguidos para el sistema de gestión de los sistemas de información de la entidad.

IX. VALORACIÓN DEL RIESGO RESIDUAL Y REVISIÓN

A. VALORAR EL RIESGO RESIDUAL

La evaluación del nivel de riesgo del tratamiento hay que realizarla antes de implementar las medidas, de cara a determinar el nivel de riesgo intrínseco. Pero, también es preciso volver a calcularlo después de aplicar las medidas y garantías para disminuir el riesgo. De esa forma, se podrá determinar si se ha conseguido reducir el riesgo al umbral deseable. Esta es la manera en la que se han de implementar las medidas y calcular el riesgo residual hasta que este alcance unos niveles aceptables.

De igual forma, si la naturaleza, ámbito, contexto o fines del tratamiento se alteran, será necesario realizar de nuevo la evaluación.

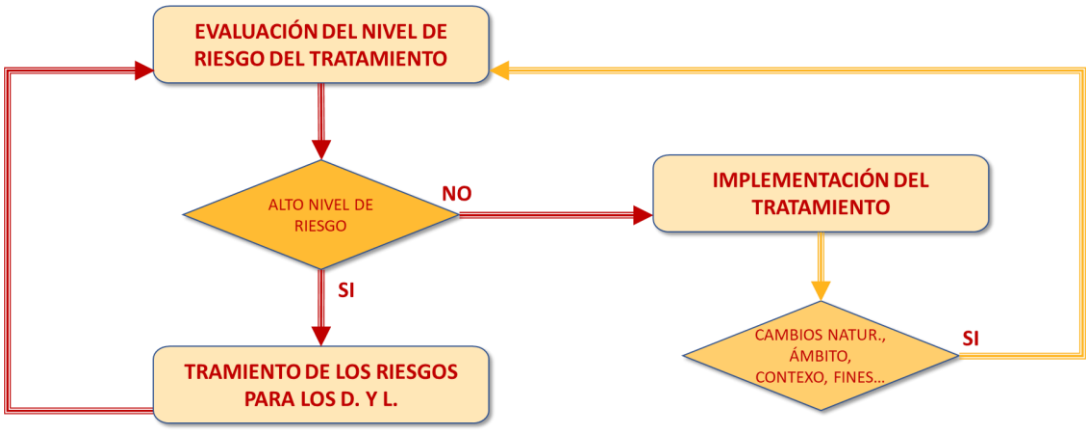

Figura 28: Ciclo de evaluación del riesgo.

Cada factor de riesgo podrá tener asociados varios controles (medidas y/o garantías) asignados para disminuir su nivel de riesgo y, para cada uno de estos controles se deberá valorar, en primer lugar, la efectividad de forma individual y seguidamente, de forma agregada.

Estos pueden influir en la probabilidad y/o en el impacto de una posible amenaza y su eficacia puede valorarse de acuerdo con la experiencia propia o ajena con relación a dichos controles. Por otro lado, un mismo control puede disminuir el nivel de riesgo de más de un factor de riesgo.

El valor de la efectividad (efectividad agregada) deberá determinarse por cada factor de riesgo identificado, clasificándose en los siguientes niveles:

- **Efectividad despreciable o limitada**: La probabilidad e impacto de la amenaza no se verán afectados por la implementación de los controles, se mantienen prácticamente en el mismo nivel o sufren pequeñas variaciones. El nivel de riesgo de dicho factor de riesgo no se reducirá.
- **Efectividad significativa**: La probabilidad e impacto de la amenaza se reducen significativamente. En ese caso, se estimará el nuevo nivel de riesgo.
- **Efectividad máxima**: La probabilidad y/o el impacto de la amenaza se reducen drásticamente hasta valores despreciables o próximos a estos. El nivel de riesgo de dicho factor de riesgo se reducirá a bajo.

Como resultado de la efectividad de los controles identificados se obtendrá una valoración del nivel de riesgo residual. Si en un primer momento, el nivel de riesgo del tratamiento se ha calculado a partir de los niveles de riesgo intrínseco para cada factor de riesgo, en esta fase de la gestión del riesgo se calcula a partir de los niveles de riesgo residuales.

Factor de riesgo	Nivel de riesgo intrínseco	Controles y sus características	Nivel de riesgo residual.
Factor 1	Nivel intrínseco 1	Control 1	Nivel residual 1
		Control 2	
		…	
..			
Factor N	Nivel intrínseco N	Control M	Nivel residual N
		Control M+1	
		…	
	Nivel de riesgo intrínseco del tratamiento		**Nivel de riesgo residual del tratamiento**

Tabla 45 Evaluación del riesgo residual vs. riesgo intrínseco.

B. RIESGOS ASUMIBLES

Como se ha señalado anteriormente, el nivel de "riesgo cero" no existe. Hay que encontrar un compromiso entre el nivel de riesgo residual alcanzado y la viabilidad del tratamiento, lo que significa tomar una decisión de cuándo un nivel de riesgo es asumible.

Sin perjuicio de las obligaciones del responsable, se podrían considerar como niveles de riesgo residual asumibles aquellos de valor bajo y medio que exigirán esfuerzos de gestión proporcionales a lo largo del ciclo de vida del tratamiento.

Esto significa que, si el responsable, durante el análisis, determina que su tratamiento tiene un nivel de riesgo residual de valor superior a medio, tendrá que adoptar nuevas medidas y garantías necesarias para gestionar los riesgos identificados. Una vez diseñadas para ser incorporadas en el tratamiento, en un proceso iterativo, se reevaluará el nivel de riesgo y repetirá el proceso hasta que el nivel de riesgo residual resulte asumible.

Tal como se expresa en las Directrices WP248: "Un ejemplo de riesgo residual elevado inaceptable incluye casos en los que los interesados pueden encontrarse con consecuencias importantes, o incluso irreversibles, de las que no puedan recuperarse (p. ej.: un acceso ilegítimo a datos que suponga una amenaza para la vida de los interesados, un despido, un peligro financiero) o cuando parezca obvio que existirá un riesgo (p. ej.: por no poder reducir el número de personas que acceden a los datos debido a sus modos de intercambio, uso o distribución, o cuando no se corrige una vulnerabilidad conocida)."

Si la entidad se limita a "ajustar" su evaluación para que el resultado obtenido se acerque exclusivamente a sus intereses, entonces no se habrá realizado un correcto tratamiento de los factores de riesgo, y el responsable incurrirá en las responsabilidades que le competan.

C. REVISIÓN DEL NIVEL DE RIESGO

Para determinar cuándo realizar una revisión en el proceso de gestión del riesgo de un tratamiento que se encuentra en ejecución hay que, antes que fijar marcos temporales, identificar aquellas circunstancias que hay que utilizar como disparadores para realizar dicha revisión.

Estos eventos serán cambios en la naturaleza, ámbito, contexto o fines del tratamiento. En la siguiente tabla se adjuntan algunos ejemplos de factores que podrían ser utilizados para determinar cuándo es necesario realizar la revisión del nivel de riesgo:

Elementos que activan un ciclo de revisión en la gestión del riesgo	
Naturaleza	• Cambios en la identidad del responsable. • Cambios en la implementación del tratamiento. • Cambios o actualización de elementos tecnológicos. • Sustitución de elementos humanos por elementos técnicos. • Cambios sustanciales en los elementos organizativos. • Cambios sustanciales en los encargos de tratamiento. • Detección de falta de eficacia en las medidas y garantías incluidas en el tratamiento.
Ámbito	• Cambio en la extensión del tratamiento. • Modificación en las categorías de los datos recogidos. • Cambio en el volumen de los datos recogidos. • Cambio en la frecuencia de la recogida de datos. • Modificación del alcance (temporal o espacial).
Contexto	• Cambios importantes en los objetivos de la organización, sus modelos de gobernanza o su cultura. • Cambio en las situaciones que justificaron el tratamiento. • Ocurrencia de incidencias y brechas que se han producido en el tratamiento o tratamientos similares. • Evolución del modelo de amenazas, las incidencias, las brechas o las tecnologías aplicables. • Cambios en el volumen o tipología de solicitudes en el ejercicio de los derechos de los interesados. • Cambios en los marcos o garantías jurídicas. • Cambios en el marco normativo de aplicación. • Cambios sociales, políticos, económicos o estratégicos.
Fines	• Cambio o ampliación de los fines principales o secundarios del tratamiento.

Tabla 46 Elementos que activan un ciclo de revisión en la gestión del riesgo.

Estos cambios pueden suponer tanto que disminuya el nivel de riesgo como que aumente, llegando incluso a ser obligatoria la realización de una EIPD.

SECCIÓN 3: EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

X. LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

La EIPD y la gestión del riesgo son actividades integradas. La EIPD forma parte indivisible de la gestión de riesgos para los derechos y libertades y se ha de ejecutar en el marco de la misma.

La evaluación de impacto relativa a la protección de datos se ha introducido en el apartado “La gestión del riesgo para los derechos y libertades y la EIPD” del capítulo “Conceptos asociados a la gestión del riesgo”.

En dicho apartado se han descrito de forma más extensa los siguientes conceptos:

- La EIPD es obligatoria cuando hay una probabilidad de alto riesgo en el tratamiento.
- La EIPD es un proceso.
- La EIPD está integrada en la gestión del riesgo para los derechos y libertades.
- La EIPD amplía los requisitos de la gestión del riesgo.
- La EIPD se tiene que traducir en acciones positivas para la implementación de medidas y garantías para gestión del riesgo.
- La EIPD es también una herramienta para demostrar cumplimiento.

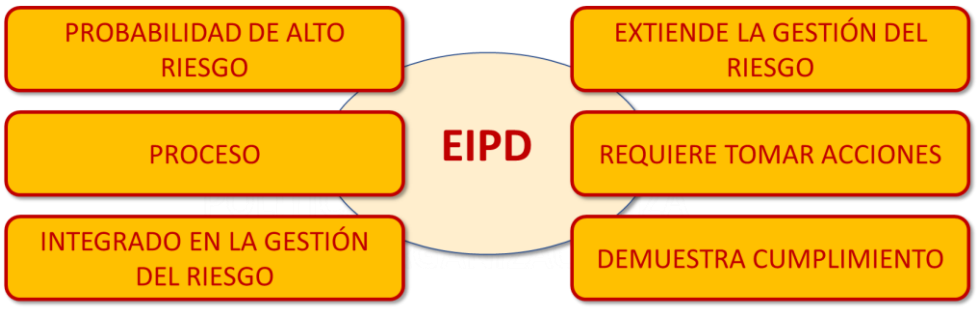

Figura 29: Caracterísiticas básicas de la EIPD

Todos los capítulos previos a esta sección son necesarios y forman parte de la EIPD. En los capítulos siguientes se desarrollan las especificidades de la EIPD.

A. QUIÉN REALIZA LA EIPD

La EIPD es una obligación específica del responsable del tratamiento, tal y como se establece en el artículo 35.1. Esto supone que es este quien asume las responsabilidades que se derivan de su ejecución y de los resultados que arroje.

Como se interpreta en las Directrices WP248:

> *“Cualquier otra persona, de dentro o fuera de la organización, puede llevar a cabo una EIPD, pero el responsable del tratamiento sigue respondiendo en última instancia por la tarea.*

El encargado del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado (artículo 35, apartado 2), y dicho asesoramiento, junto con las decisiones adoptadas por el responsable, debe ser documentado en la EIPD. El delegado de protección de datos también debe controlar la realización de la EIPD [artículo 39, apartado 1, letra c)]. Se ofrece más orientación en las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243.

Si un encargado lleva a cabo el tratamiento total o parcialmente, dicho encargado debe ayudar al responsable a realizar la EIPD y debe ofrecer la información necesaria."

Por lo tanto, los encargados del tratamiento tienen como obligación ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, es decir, en la gestión del riesgo y en la realización de la EIPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado (art. 28.3.f). Además, puede ser aconsejable que el responsable recabe el apoyo de terceros.

B. EN QUÉ MOMENTO SE REALIZA LA EIPD

Respecto al momento en que debe realizarse, el artículo 35.1 del RGPD establece que:

…, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, ...

La EIPD es un proceso que se integra en el propio proceso de gestión de riesgos para los derechos y libertades. Dentro de ese proceso de gestión, un aspecto importante de la EIPD es su carácter *a priori*, es decir, la obligación de ejecutarla antes del inicio de las actividades de tratamiento.

El RGPD incide en este carácter previo con relación a la ejecución efectiva del tratamiento. Explícitamente, no exige que se haya de realizar con carácter previo a otras etapas del ciclo de vida del tratamiento, como podrían ser su diseño o implementación. De esta forma, el RGPD se limita al ejercicio de sus competencias, es decir, no entra a valorar otras consideraciones que vayan más allá de la protección de datos de carácter personal. Los derechos y libertades de los ciudadanos se verán afectados cuando el tratamiento se ejecute de forma efectiva, por lo tanto, es antes de que se vean comprometidos dichos derechos y libertades cuando debe realizarse la EIPD.

Sin embargo, y aunque el RGPD no entra en la valoración, sería altamente recomendable que la entidad lleve a cabo la EIPD antes de iniciar el proceso de diseño e implementación efectiva. Toda fase del ciclo de vida de desarrollo de un tratamiento previo a la puesta en explotación del mismo supone realizar inversiones para llevar a cabo desarrollos, adquisiciones, cambios organizativos, contrataciones, etc. En este sentido, las Directrices WP248 se expresan literalmente en los siguientes términos:

"La EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento"

De donde se deduce que la EIPD es recomendable realizarla en las fases de concepción y diseño del tratamiento. Existen dos razones que aconsejan esta aproximación. La primera es la de proteger la inversión realizada por el responsable en

el tratamiento, pero esta razón no entra dentro de las competencias de protección de datos.

La segunda es para cumplir con los principios de protección de datos desde el diseño. Estos principios obligan a que las garantías seleccionadas estén guiadas por la gestión del riesgo y se implementen durante la fase de concepción y diseño del tratamiento, estando integradas en el mismo y extendiéndose a todas las etapas de su ciclo de vida. La protección de datos desde el diseño no es una capa adicional o un elemento que se puede añadir a posteriori[113]. Por lo tanto, una EIPD, que puede implicar que hay que realizar cambios en el tratamiento para introducir modificaciones, garantías o medidas para reducir los riesgos, se ha de realizar antes y durante la fase de diseño.

C. EXCEPCIONES PARA REALIZAR LA EIPD ANTES DEL INICIO DE LAS ACTIVIDADES DE TRATAMIENTO

El enfoque de riesgos del RGPD supone que la EIPD debe entenderse como un proceso y no como un estado. Por lo tanto, si bien la EIPD se ha de realizar antes de la implementación del tratamiento, su revisión y adaptación se extiende a todas las etapas del ciclo de vida de este.

Si durante la vida del tratamiento se producen cambios ajenos al responsable, como cambios contextuales o una ampliación no prevista del ámbito/alcance, será necesario actualizar la EIPD y, en su caso, generar un nuevo informe y plan de acción con las medidas de control adicionales que fuera necesario implantar en el marco de la gestión del riesgo antes de continuar con el tratamiento. Si no se hubiera realizado la EIPD porque las circunstancias iniciales no obligaban o no lo recomendaban, entonces sería necesario realizar la EIPD desde cero. En los casos anteriores, la EIPD se ha de ejecutar de forma inmediata.

Si el responsable pretende cambiar la naturaleza, el ámbito o los fines del tratamiento, y las nuevas circunstancias obligan o recomiendan una EIPD, esta se ha de llevar a cabo antes de iniciar las actividades de tratamiento con las nuevas actualizaciones.

Entre los casos anteriores se encuentran aquellos tratamientos que estaban ya en curso antes de la plena entrada en vigor del RGPD. Con relación a este último caso, hay que tener en cuenta que las Directrices WP248 establecen:

> *…incluso si el 25 de mayo de 2018 no se requiere una EIPD, será necesario, en el momento oportuno, que el responsable del tratamiento lleve a cabo una evaluación de este tipo como parte de sus obligaciones generales de responsabilidad proactiva*

Por lo tanto, es obligación del responsable realizar una revisión del nivel de riesgo en los tratamientos ya en curso (ver el capítulo relativo a la revisión del nivel de riesgo) de cara a determinar el momento oportuno para realizar la EIPD.

[113] El RGPD no trata sobre la protección de datos DESPUES del diseño.

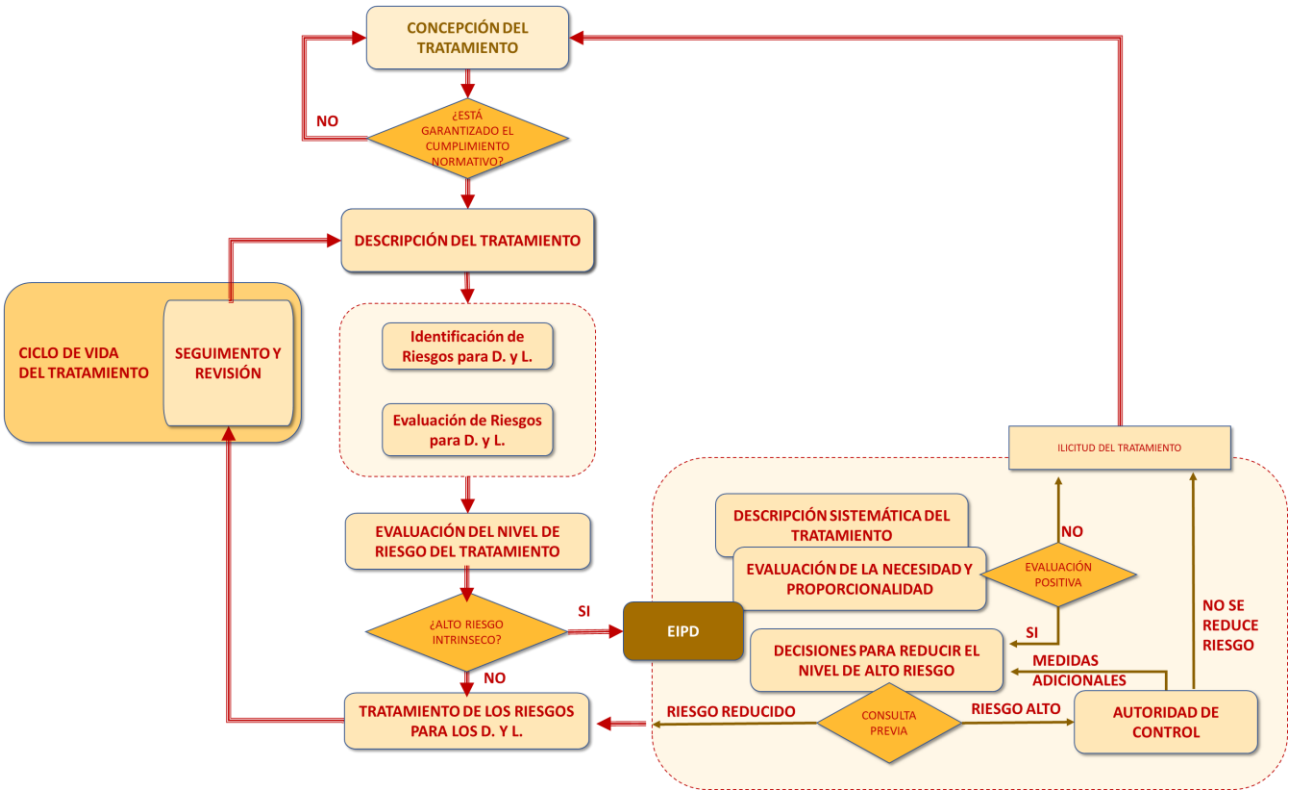

Figura 30: La EIPD en el proceso de gestión del riesgo.

XI. ANÁLISIS DE LA OBLIGACIÓN DE LLEVAR A CABO LA EIPD

El análisis de la obligación de realizar una EIPD forma parte del proceso de evaluación del riesgo para los derechos y libertades. Este proceso se ha descrito en los capítulos anteriores, aunque, con el objeto de facilitar la lectura del texto, se ha separado en un capítulo independiente este análisis.

A. CUANDO NO ES OBLIGADO REALIZAR UNA EIPD

No es obligado realizar una EIPD, sin perjuicio de otras obligaciones establecidas en el RGPD, cuando el tratamiento:

- *«No sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas»* (artículo 35, apartado 1);
- Entra dentro de lo establecido en la *Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD* publicada por la AEPD y validada por el CEPD.
- Cuando la naturaleza, el alcance/ámbito, el contexto y los fines del tratamiento sean muy similares al tratamiento para el que se ha realizado una EIPD previa. En esos casos, se pueden utilizar los resultados de dicha EIPD realizada para tratamientos similares (artículo 35, apartado 1);
- Cuando una actividad de tratamiento, de conformidad con el artículo 6, apartado 1, letra c) o e), tenga una base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro, cuando tal Derecho regule la operación específica de tratamiento y cuando ya se haya realizado una EIPD en el contexto de la adopción de dicha base jurídica (artículo 35, apartado 10), excepto si un Estado miembro considera necesario proceder a dicha evaluación previa a las actividades de tratamiento concretas que venga a regular;
- Cuando las actividades de tratamiento hayan sido comprobadas por la Autoridad de Control antes de mayo de 2018 en condiciones específicas que no hayan cambiado (véase III.C);

B. CUANDO ES OBLIGATORIO REALIZAR UNA EIPD

Las condiciones para considerar que el responsable está obligado a realizar una EIPD del tratamiento, vienen determinadas de la siguiente forma:

OBLIGACIÓN DE REALIZAR LA EIPD
"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas"[114]
Está dentro de alguno de los supuestos establecidos en el artículo 35.3 del RGPD
Existe una norma especial que exige una EIPD para el tratamiento.
Cuando el tratamiento corresponde con alguno de los ejemplos de obligación enumerados en las Directrices WP248.
Cuando el tratamiento cumple al menos dos de las condiciones de las enumeradas en las Directrices WP248 para realizar una EIPD.
Cuando el tratamiento cumpla con dos o más criterios de las *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)* publicada por la AEPD.
Cuando se haya apreciado un alto riesgo teniendo en cuenta los supuestos enumerados en el artículo 28.2 de la LOPDGDD.
Cuando en alguna de las directrices publicadas por el CEPD, el tratamiento esté identificado como obligado a realizar una EIPD.
El tratamiento se encuentre sujeto a un código de conducta o a un mecanismo de certificación que exijan al responsable la realización de una evaluación de impacto.

Tabla 47 Obligación de realizar la EIPD

La evaluación de estas condiciones hay que realizarla a partir de la descripción del tratamiento y los factores de riesgo identificados en el proceso de análisis de riesgo para los derechos y libertades. La evaluación del riesgo se ha desarrollado en el capítulo "Evaluación del nivel de riesgo del tratamiento".

La Directrices WP248 interpretaban que para tratamientos en curso en el momento de la entrada en vigor del RGPD que hubieran sido ya revisados por la Autoridad de Control o por el DPD no era obligatorio realizar la EIPD.

Sin embargo, las mismas Directrices WP248 interpretan que:

> *"deberán someterse a una EIPD los tratamientos cuyas condiciones de aplicación (alcance, fin, datos personales recogidos, identidad de los responsables o destinatarios del tratamiento, periodo de conservación de datos, medidas técnicas u organizativas, etc.) hayan cambiado desde la anterior comprobación realizada por la Autoridad de Control o el delegado de protección de datos y que probablemente entrañen un alto riesgo".*

Teniendo en cuenta que a la hora de publicar esta guía ya han transcurrido más de tres años desde la plena entrada en vigor del RGPD, y por la potencial evolución en la naturaleza, el contexto e incluso el alcance al que están sujetos los tratamientos, en línea con la obligación del responsable de revisar y actualizar las medidas cuando sea necesario[115], se recomienda llevar a cabo una EIPD para aquellos tratamientos de alto

[114] Artículo 35.1 del RGPD y Considerando 76
[115] Artículo 24.1 RGPD

riesgo que, en su momento, no la realizasen en base a la excepción anterior. No llevar a cabo ninguna revisión o no realizar la EIPD de estos tratamientos *sine die*, no puede entenderse, en ningún caso, como una forma de demostrar el cumplimiento de lo previsto en el RGPD con relación al marco de responsabilidad activa.

XII. ANÁLISIS DE LA NECESIDAD DE REALIZAR UNA EIPD

El conjunto de tratamientos obligados no es una lista cerrada ni una limitación para el responsable. En ocasiones puede ser necesario o recomendable realizar una EIPD de un tratamiento que no consta en dicha lista de tratamientos obligados, ya sea por el potencial del riesgo intrínseco que el responsable ha identificado en el tratamiento, porque el responsable pone en práctica la EIPD como herramienta para demostrar cumplimiento o, como manifiestan las Directrices WP248, no esté claro si se requiere o no una EIPD:

> *En los casos en los que no esté claro si se requiere una EIPD, el GT29 recomienda realizar una, ya que esta evaluación representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos.*

Y como se manifiesta en las Directrices, cuando, aunque no se cumplan todos los criterios para que una EIPD sea obligatoria concurren algunos de ellos, en tal medida, que el responsable considere la necesidad de llevarla a cabo:

> *Sin embargo, en algunos casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla solo uno de estos criterios requiere una EIPD.*

Por lo tanto, es importante tener en cuenta que, el hecho de que un tratamiento de datos personales no esté incluido en los supuestos obligados, no siempre implica que no sea necesario llevar a cabo la EIPD. El RGPD no limita la capacidad de decisión del responsable a la hora de decidir si esta se lleva a cabo o no. El RGPD viene a establecer un mecanismo de proactividad que permite al responsable decidir sobre la necesidad de llevar a cabo la EIPD en línea con los riesgos inherentes asociados al tratamiento en función de su naturaleza, alcance, contexto y finalidades (Considerando 76 y Artículo 35.1 del RGPD).

En particular, es preciso tener en cuenta que las listas de tratamientos obligados y excluidos establecidos por las autoridades de control y referidas en el artículo 35 del RGPD (35.4 y 35.5) son orientativas y no limitan la potestad de decisión del responsable sobre sus tratamientos de datos personales y sobre el ejercicio de la responsabilidad proactiva.

En particular, las Directrices WP248 interpretan:

> *el responsable principal de la seguridad de la información (CISO), en caso de ser nombrado, así como el delegado de protección de datos, podrían sugerir que el responsable llevara a cabo una EIPD sobre una operación de tratamiento específica, y deberían ayudar a las partes interesadas en la metodología, ayudar a evaluar la calidad de la evaluación de riesgo y si el riesgo residual es aceptable, y a desarrollar conocimientos específicos para el contexto del responsable del tratamiento;*
>
> *el responsable principal de la seguridad de la información (CISO), en caso de ser nombrado, o el servicio informático, deberían ofrecer ayuda al responsable y podrían proponer la realización de una EIPD sobre una operación de tratamiento específica, dependiendo de las necesidades de seguridad y operativas.*

De ahí que, tanto el DPD, o si no está nombrado el asesor en protección de datos, como el CISO puedan sugerir la realización de una EIPD. Estas sugerencias han de registrarse documentalmente, así como las decisiones tomadas a partir de ellas.

Por lo tanto, con independencia de que se trate de un tratamiento obligado o no a la realización de una EIPD, el responsable puede tomar la decisión de efectuarla con el fin de llevar a cabo un análisis más detallado del tratamiento de datos personales en aras de una mayor diligencia a la hora de implementar la responsabilidad proactiva. También son motivos válidos mejorar la calidad de sus productos y servicios, fomentar la cultura de protección de datos en su organización o bien como simple mecanismo para garantizar la confianza de sus clientes.

XIII. EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

Una de las exigencias del artículo 35 del RGPD con relación a la EIPD, es la que aparece en el apartado 35.7.b del RGPD, la obligación de que se realice "*una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en cuanto a su finalidad*".

El Supervisor Europeo de Protección de Datos ha publicado dos guías para realizar dicho análisis con relación al desarrollo normativo europeo[116]. Aunque no son de directa aplicación al análisis de cualquier posible tipo de tratamiento, sí resultan de gran utilidad al recoger los fundamentos de la evaluación de la necesidad y proporcionalidad[117]. En ellas se precisa el principio de proporcionalidad seguido por los jueces y tribunales[118] a la hora de realizar una ponderación cuando distintos derechos o bienes jurídicamente protegidos entran en conflicto.

Este principio de proporcionalidad, llevado a la evaluación de la necesidad y proporcionalidad del tratamiento, se traduce en realizar una ponderación atendiendo a tres criterios:

Juicio de idoneidad	Hay que determinar si el tratamiento es adecuado para el fin que persigue. El tratamiento da respuesta a determinadas carencias, demandas, exigencias, obligaciones u oportunidades objetivas y puede conseguir los objetivos propuestos con la eficacia suficiente.
Juicio de necesidad	Hay que determinar si la finalidad perseguida no puede alcanzarse de otro modo menos lesivo o invasivo, es decir, no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida.

[116] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.

[117] Considerando 4 RGPD: *"El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística."*

[118] El Tribunal Constitucional ha señalado en su STC14/2003, de 28 de enero, FJ9 que *"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*

Juicio de proporcionalidad en sentido estricto	La gravedad del riesgo para los derechos y libertades del tratamiento, y su intromisión en la privacidad, ha de ser adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de esta. Hay que ponderar el beneficio que el tratamiento, desde el punto de vista de la protección de datos[119], proporciona a la sociedad manteniendo un equilibrio con el impacto que representa sobre otros derechos fundamentales. Sin embargo, aunque pueda ceder parcialmente, en ningún caso, se puede asumir la negación absoluta del derecho a la protección de datos y vaciarle de su contenido esencial.

Tabla 48 Juicio de idoneidad, necesidad y proporcionalidad en sentido estricto.

Esta evaluación ha de terminar con una decisión de llevar o no a cabo el tratamiento, o en su caso, modificarlo para que cumpla con los tres juicios exigidos.

Durante el proceso de evaluación se pueden identificar elementos que, incluidos en el tratamiento, lo modifiquen y lo hagan ser conforme al principio de proporcionalidad, por lo que este proceso de evaluación y adecuación debe ser entendido como un proceso de mejora que puede y debe realizarse en varias iteraciones hasta conseguir un diseño del tratamiento adecuado.

Antes de abordar esta evaluación desde cero es imprescindible consultar los análisis de necesidad y proporcionalidad que se hayan podido realizar previamente sobre tratamientos similares, consultar las directrices del CEPD, las resoluciones o informes jurídicos de la AEPD, o la jurisprudencia, donde pueden existir evaluaciones de tratamientos que guarden similitud en función de la naturaleza, ámbito, contexto o fines del tratamiento y que permitan identificar los límites a los que el tratamiento en cuestión ha de sujetarse. Las conclusiones de estas evaluaciones han de ser tenidas en cuenta a lo largo de la evaluación.

En ningún caso se recomienda continuar con la EIPD cuando el tratamiento no supera la evaluación de la necesidad y/o la proporcionalidad. Téngase en cuenta que se trata de requisitos de cumplimiento que exige el RGPD; requisitos que no pueden abordarse con medidas alternativas al propio cumplimiento como, por ejemplo, medidas técnicas y organizativas.

De cara a su aplicación práctica, en esta guía proponemos un proceso de análisis secuencial, comenzando por el juicio de idoneidad. Este proceso debe ser ajustado por el responsable a su metodología de trabajo, a las características y a las circunstancias particulares del tratamiento concreto. El único requisito es que se realice un análisis completo de las tres dimensiones indicadas.

[119] Considerando 4: "*El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad...*"

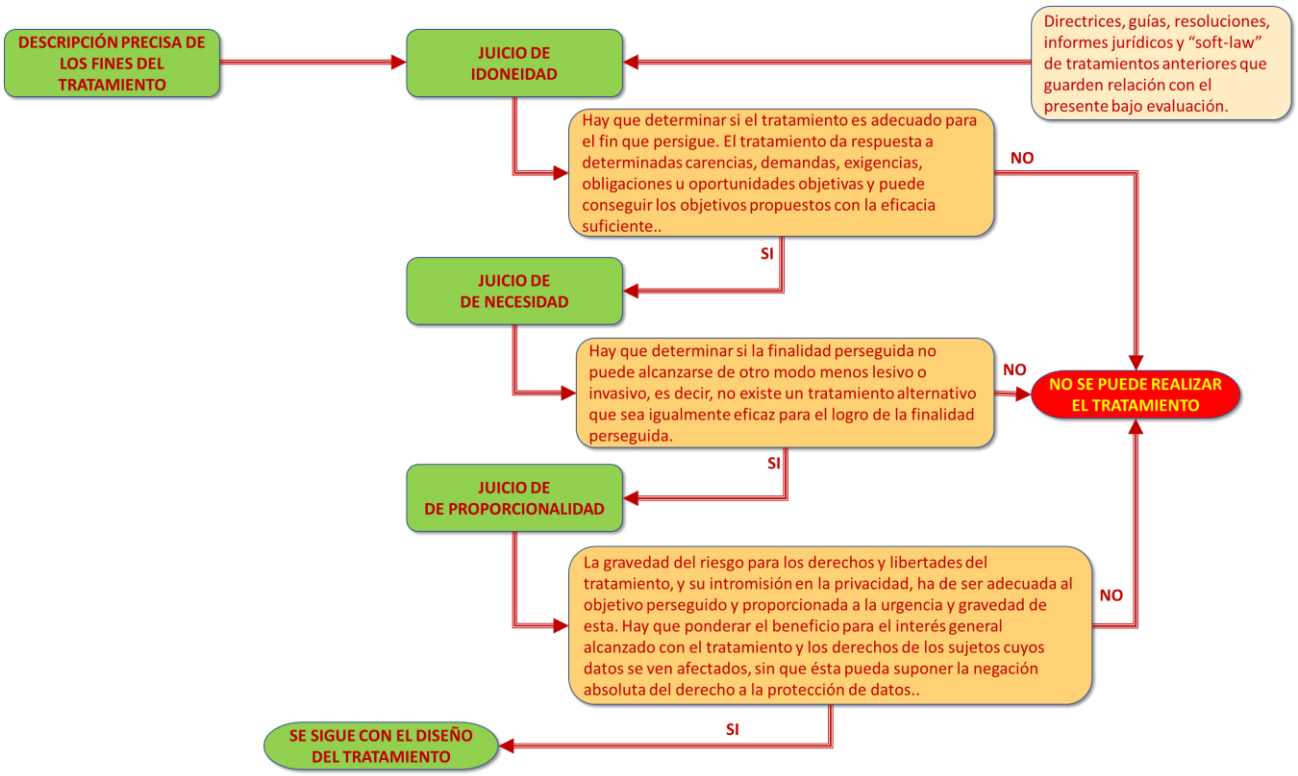

Figura 31: Proceso de evaluación de la necesidad y proporcionalidad.

Entre las medidas que el responsable tiene la obligación de revisar y actualizar (artículo 24.1) se incluirá la evaluación del juicio de idoneidad, necesidad y proporcionalidad, llevando a cabo la cuantificación objetiva de los resultados del tratamiento y la aplicación, cuando exista, de las correspondientes cláusulas de caducidad.

A. EQUÍVOCOS HABITUALES CON RELACIÓN A LA EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

Durante la aplicación práctica del RGPD se han observado los siguientes equívocos con relación a la evaluación de la necesidad y proporcionalidad del tratamiento.

En primer lugar, la EIPD es un análisis en el marco de la gestión del riesgo para los derechos y libertades, y no tiene como objeto determinar la legitimación del tratamiento o sus bases jurídicas.

En segundo lugar, no hay que confundir esta evaluación con el análisis de necesidad de realizar una EIPD (ver capítulo "Análisis de la necesidad de realizar una EIPD"), que estará en función del nivel de riesgo del tratamiento que se haya identificado.

Para finalizar, téngase en cuenta que la evaluación de la proporcionalidad de las operaciones de tratamiento con relación a sus fines (artículo 35.7.b RGPD) no debe confundirse con la obligación del responsable de utilizar únicamente los datos que fueran adecuados, pertinentes y limitados para la finalidad del tratamiento (artículo 5.1.b y artículo 25.2 RGPD). El artículo 5.1.b y el artículo 25.2 del RGPD exigen al responsable un ejercicio de análisis encaminado a la aplicación del principio de minimización y que pasa por determinar, en cada una de las operaciones que constituyen el tratamiento, los

datos y operaciones de tratamiento mínimas y necesarias para abordar los fines del tratamiento.

B. JUICIO DE IDONEIDAD

En el juicio de idoneidad se debe evaluar si la propuesta de tratamiento, tal y como está planteada, alcanza la eficacia necesaria para cumplir los fines que persigue. Esa eficacia, necesariamente, deberá ser demostrada de forma objetiva por el responsable del tratamiento, para lo cual hay que realizar la:

1. Definición del umbral de efectividad del tratamiento: Establecer de forma objetiva, cualitativa y basada en evidencias, cuál es el umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento (algunos ejemplos podrían ser, un margen de error del 5% en un valor resultado, una detección de un 95% de casos o una posibilidad de fraude por debajo del 1%).
2. Evaluación de la efectividad de la propuesta de tratamiento: Evaluar de forma objetiva, cualitativa y basada en evidencias, la efectividad del tratamiento, tal y como se ha planteado, verificando si da respuesta a las necesidades planteadas y con qué extensión (determinar si genuinamente resuelve dichas carencias).

La evaluación de la idoneidad ha de ser racional, analítica y basada en hechos y datos objetivos.

En base a la información obtenida en este análisis, se decidirá seguir o no adelante con el tratamiento tal y como está planteado.

C. JUICIO DE NECESIDAD

Para llevar a cabo el juicio de necesidad hay que seguir los siguientes pasos:

1. Determinación de la relevancia de los fines del tratamiento: Evaluar que los fines del tratamiento tienen la importancia suficiente para ser abordados con un tratamiento de alto riesgo (previo a un juicio de proporcionalidad que se describe más adelante).
2. Verificación de la adecuación de las operaciones del tratamiento: Verificación de que cada una de las operaciones concretas del tratamiento está orientada a cumplir con los fines del tratamiento de una forma objetivamente demostrable.
3. Justificación de la configuración actual del tratamiento: Evaluar que no existen otros tratamientos, que ya están en curso o que se podrían plantear, que resuelven los fines declarados sin incurrir en un alto riesgo, incluso aunque sea necesario introducir alguna modificación para cumplir los fines perseguidos.

En la práctica, no suele existir una única forma de conseguir los fines a los que está orientado un tratamiento de datos. En función de cómo se implemente este se pueden plantear diferentes escenarios de riesgo. A la hora de considerar esos otros posibles tratamientos alternativos hay que identificar aquellos que, empleando medios menos intrusivos, alcancen, al menos, igual eficacia.

Es decir, se debe evaluar si la finalidad perseguida se puede conseguir por otros medios, como, por ejemplo, utilizando otros datos (de distinta naturaleza, extensión o anonimizados), reduciendo el universo de personas afectadas (cuantitativa o

cualitativamente hablando), haciendo uso de otras tecnologías menos invasivas, aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc. e incluso, determinar si modificaciones menores de los tratamientos existentes cubren las necesidades identificadas en el primer punto.

Realizada esa evaluación, ha de optarse por la alternativa que, alcanzando la efectividad necesaria, resulte lo menos lesiva e intrusiva en los derechos de las personas. En definitiva, se decidirá seguir o no adelante con el tratamiento tal y como está planteado.

1. Cláusulas de caducidad

Un aspecto muy importante que se deriva del análisis de necesidad es que hay que determinar si la justificación del tratamiento se basa en la exigencia de responder a una situación concreta de urgencia (por ejemplo, en caso de un interés público esencial como podrían ser temas de seguridad o sanitarios, en cuyo caso tendría que estar recogido en una norma con rango legal). En ese caso, es imprescindible identificar si existe un alto riesgo para el responsable, el Estado o la ciudadanía (riesgo distinto de aquel sobre los derechos y libertades de los interesados) y, en particular, sobre aquellos colectivos de ciudadanos que pudieran considerarse en situación de especial vulnerabilidad.

La ponderación de las circunstancias ha de realizarse caso por caso y en función de las circunstancias del momento, pues no existen derechos absolutos ni limites absolutos de los mismos. Justo porque esos límites pueden variar con el tiempo fruto de la evolución y cambio de las condiciones que los han impuesto, es necesario establecer, en el caso expuesto y en otros casos similares que pudieran identificarse, las llamadas cláusulas de caducidad del tratamiento, entendidas estas como aquellas circunstancias que puedan acaecer y hacer que el tratamiento devenga innecesario en función de su naturaleza, ámbito, contexto y fines.

En estos casos, el responsable ha de incorporar medidas para monitorizar la vigencia real de las circunstancias que justificaron el tratamiento. En el caso de que estas desaparezcan, se ha de reevaluar la idoneidad y licitud del tratamiento (artículo 6 RGPD). De esta forma, se evitará que tratamientos originados sobre la base de medidas provisionales orientadas a dar respuesta a una situación extraordinaria y de urgente necesidad, se conviertan en permanentes, definitivos y carentes de justificación.

D. JUICIO DE PROPORCIONALIDAD EN SENTIDO ESTRICTO[120]

En el momento de realizar el juicio de proporcionalidad en sentido estricto, partiendo de los análisis anteriores, y una vez acreditada la idoneidad y necesidad del tratamiento de forma objetiva y justificada, es preciso llevar a cabo la:

1. Identificación del grado de impacto del tratamiento en los derechos y libertades: Expresar, de forma detallada, las limitaciones o intrusiones a los

[120] Considerando 4. "El tratamiento de datos personales debe estar concebido para servir a la humanidad**. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad**. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística."

derechos y libertades que puede suponer el tratamiento para el interesado. Esta evaluación es una tarea previa que ya se ha debido realizar en la determinación de los factores y niveles de riesgo analizados previamente (Ver capítulo “Identificación y análisis de factores de riesgo”), exponiendo, en este punto de la evaluación, sus conclusiones.

2. Identificación y descripción de medidas compensatorias: Detallar los controles establecidos en el diseño del tratamiento para disminuir dicho impacto.
3. Identificación de los beneficios del tratamiento: Determinar las ventajas y beneficios que, de forma objetiva y con evidencias, tiene el tratamiento para los interesados, considerados de forma individual y como colectivo. Es decir, también ha de considerarse el beneficio social.
4. Confirmación de existencia de identidad en la calidad de la información utilizada: Hay que evaluar si existe simetría en la información analizada para el juicio de ponderación, es decir, si el nivel de análisis con relación al impacto es igual al nivel alcanzado en base a la información proporcionada respecto de las ventajas.
5. Análisis BDB (Balance Daño-Beneficio): Evaluar de si los beneficios para los interesados y la sociedad, previamente determinados, compensan y justifican el impacto para los derechos y libertades identificados en el punto 1 de este juicio de proporcionalidad en sentido estricto.

Un aspecto que permite determinar que la EIPD está incompleta es si hay una asimetría entre la información proporcionada con relación a las limitaciones que supone el tratamiento y la información proporcionada respecto a las ventajas que aporta, por ejemplo, intentar justificar la necesidad del tratamiento exclusivamente en términos de intereses de negocio sin tener en cuenta los derechos y libertades de los interesados en particular y de la sociedad en general.

E. CASO PARTICULAR DE TRATAMIENTO: NECESIDAD Y PROPORCIONALIDAD EN EL DESARROLLO NORMATIVO

En el caso de que la EIPD se realice sobre una iniciativa legislativa que plantee una limitación de derechos (artículo 35.10 RGPD), el análisis realizado para evaluar la necesidad y proporcionalidad del tratamiento en base a los juicios descritos, en especial los de idoneidad y necesidad, cobra mayor importancia habida cuenta del alcance y el grado de afectación que supone el tratamiento[121].

F. DECISIÓN FINAL Y DOCUMENTACIÓN DE LA EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD

La evaluación de la necesidad, y la proporcionalidad debe conducir a la toma de una decisión sobre si el tratamiento es viable o, por el contrario, no lo es de acuerdo a la forma en que está planteado.

Cuando no sea posible demostrar la necesidad y la proporcionalidad de un tratamiento de alto riesgo o de las operaciones de tratamiento que pudieran formar parte de este, no se recomienda avanzar en la evaluación de impacto en protección de datos o siquiera plantear la consulta previa a la que refiere el artículo 36 del RGPD. Las

[121] En el siguiente enlace pueden consultarse algunos ejemplos de EIPD en este contexto: https://ec.europa.eu/transparency/regdoc/?fuseaction=ia&year=2020&serviceId=&s=Buscar

herramientas de responsabilidad activa no sirven para justificar, en ningún caso, la necesidad y/o la proporcionalidad del tratamiento.

En el caso de que se concluya que el tratamiento no es necesario o no es proporcional, hay que señalar los aspectos que conducen a esa conclusión y, si es posible, realizar las modificaciones necesarias para adecuar el tratamiento a los criterios adecuados de necesidad, idoneidad y proporcionalidad.

En el proceso de realizar la evaluación de la necesidad y la proporcionalidad hay que proporcionar las evidencias adecuadas, registrar y guardar toda la información relevante para realizar este análisis y plasmar en un informe todo el proceso de la evaluación realizada con sus oportunas conclusiones.

Como se ha señalado reiteradamente, esto no significa que tenga que estar toda la información incluida en un documento singular, en múltiples documentos o formando parte del informe final que documente el proceso de EIPD que se haya seguido. La forma de presentación dependerá de cómo la documentación pueda organizarse de la forma más eficiente posible dentro de la organización, constatando, como mejor proceda, que se ha realizado dicho análisis y que el responsable del posible tratamiento lo conoce, lo respalda y se obliga, desde el punto de vista normativo, hasta sus últimas consecuencias.

En cualquier caso, la información que ha de encontrarse en la documentación es la siguiente:

Determinación precisa de las finalidades del tratamiento.	Últimos, específicos, medibles, alcanzables y acotados.

Juicio de idoneidad

Definición del umbral de efectividad del tratamiento	Establecer de forma objetiva, cualitativa y basada en evidencias, cuál es el umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento.
Evaluación de la efectividad de la propuesta de tratamiento	Evaluar de forma objetiva, cualitativa y basada en evidencias, la efectividad del tratamiento, tal y como se ha planteado, verificando si da respuesta a las necesidades planteadas y con qué extensión.

Juicio de necesidad

Determinación de la relevancia de los fines del tratamiento	Evaluar que los fines del tratamiento tienen la importancia suficiente para ser abordados con un tratamiento de alto riesgo.
Verificación de la adecuación de las operaciones del tratamiento	Verificación de que cada una de las operaciones concretas del tratamiento está orientada a cumplir con los fines del tratamiento de una forma objetivamente demostrable.
Justificación de la configuración actual del tratamiento	Evaluar que no existen otros tratamientos, que ya están en curso o que se podrían plantear, que resuelven los fines declarados sin incurrir en un alto riesgo, incluso aunque sea necesario introducir alguna modificación para cumplir los fines perseguidos.

Cláusulas de caducidad previstas en el tratamiento	Por su naturaleza
	Por su ámbito
	Por su contexto
	Por sus fines

Juicio de proporcionalidad en sentido estricto	
Identificación del grado de impacto del tratamiento en los derechos y libertades	Expresar, de forma detallada, las limitaciones o intrusiones a los derechos y libertades que puede suponer el tratamiento para el interesado. Esta evaluación es una tarea previa que ya se ha debido realizar en la determinación de los factores y niveles de riesgo analizados previamente, exponiendo en este punto de la evaluación sus conclusiones.
Identificación y descripción de medidas compensatorias	Detallar los controles establecidos en el diseño del tratamiento para disminuir dicho impacto.
Identificación de los beneficios del tratamiento	Determinar las ventajas y beneficios que, de forma objetiva y con evidencias, tiene el tratamiento para los interesados, considerados de forma individual y como colectivo. Es decir, también ha de considerarse el beneficio social.
Confirmación de existencia de identidad en la calidad de la información	Hay que evaluar si existe simetría en la información analizada para el juicio de ponderación, es decir, si el nivel de análisis con relación al impacto es igual al nivel alcanzado en base a la información proporcionada respecto a las ventajas.
Análisis BDB (Balance Daño-Beneficio)	Evaluar de si los beneficios para los interesados y la sociedad, previamente determinados, compensan y justifican el impacto para los derechos y libertades identificados en el punto 1 de este juicio de proporcionalidad en sentido estricto.

Tabla 49 Información mínima requerida en la evaluación de la necesidad y proporcionalidad del tratamiento.

XIV. OBLIGACIÓN DE DOCUMENTACIÓN

La EIPD es un proceso que es necesario documentar[122], tanto en sus conclusiones como en su proceso de desarrollo.

En las Directrices WP248 se manifiesta que:

> *...aunque una operación de tratamiento se corresponda con los casos anteriormente mencionados, puede que un responsable no considere que dicho tratamiento «entraña probablemente un alto riesgo». En estos casos, el responsable debe justificar y documentar los motivos por los que no se realiza una EIPD e incluir/registrar las opiniones del delegado de protección de datos.*

La justificación y la decisión de no realizar la EIPD, efectuada en el marco de la gestión del riesgo, también debe estar adecuadamente documentada. No llevar a cabo actividades de documentación con relación a las actividades de responsabilidad activa desarrolladas, o no documentar adecuada y motivadamente las decisiones del responsable, impedirá a este demostrar el cumplimiento de sus obligaciones y podría dar lugar al inicio de un procedimiento de infracción por la Autoridad de Control.

A. ACCESO DE LA AUTORIDAD DE CONTROL A LA EIPD

Toda la documentación relativa a la EIPD debe estar disponible para la Autoridad de Control en dos casos:

- Presentación de una consulta previa (artículo 36 RGPD).
- Solicitud por parte de la Autoridad de Control en el ámbito de los poderes que le otorga el artículo 58 del RGPD.

Por lo tanto, no existe obligación de remitir toda la EIPD realizada por el responsable a la Autoridad de Control de forma sistemática. Sin embargo, cuando se cumplan las condiciones de obligación, el no remitir a la Autoridad de Control una EIPD o hacerlo de forma incompleta podría considerarse información inexacta y, por lo tanto, constituir una infracción.

En lo que respecta a la remisión de la consulta previa a la Autoridad de Control, el RGPD, en su artículo 39 letra e), establece que el DPD ha de ser el punto de contacto para dicha gestión:

> *"e) actuar como punto de contacto de la Autoridad de Control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto".*

B. TRANSPARENCIA DE LA EIPD

No existe la obligación de hacer pública toda la documentación relativa a una EIPD, ni siquiera se considera recomendable. Sin embargo, en las Directrices WP248 se estipula que:

[122] Como se ha señalado en este documento, la palabra "documentar" no implica la realización de un único documento, sino tener registradas las acciones, los análisis y las decisiones de la EIPD, los criterios por los que se determinan determinados valores de probabilidad o impacto sobre los interesados, los motivos por los que una determinada medida supone una reducción de la probabilidad o el impacto, los motivos por los que se considera que una determinada evaluación del riesgo es aceptable, etc..

"¿Existe la obligación de publicar la EIPD? No, pero publicar un resumen podría fomentar la confianza, y se debe comunicar la EIPD completa a la Autoridad de Control en caso de consulta previa o si así lo solicita la APD. ...

En este contexto, se debe facilitar toda la EIPD [artículo 36, apartado 3, letra e)]".

Por tanto, la publicación de aquellos elementos que derivan de la realización de una EIPD que pudieran resultar en una acción de transparencia y fomentar la confianza de los interesados es una práctica aconsejable. En este caso, el responsable ha de evitar publicar detalles innecesarios que no añadan valor a dicha transparencia o que no resultasen proporcionales con relación a nuevos riesgos que la publicidad de los mismos podría crear[123].

[123] Por ejemplo, podrían surgir riesgos de seguridad TIC si se publican detalles del software utilizado (versiones, parches, etc.), topología de red, información organizativa que facilite o permita ataques de ingeniería social, detalle de las medidas de seguridad (firewalls, antivirus, etc.). También podrían surgir riesgos de seguridad para las personas, secretos comerciales, contractuales, etc.

XV. RECABAR LA OPINIÓN DE LOS INTERESADOS O DE SUS REPRESENTANTES

Uno de los requisitos a los que obliga la EIPD a la hora de realizar la gestión de riesgos (art. 35.9) es que, "*Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento*".

Esta consulta tiene por objeto hacer conscientes a los interesados, o sus presentantes, de que el tratamiento es de alto riesgo, detallando los factores de riesgo, los potenciales impactos de las brechas de datos y la intrusión a sus derechos y libertades que este supone. Además, la consulta ha de hacer conscientes a los interesados que dichos riesgos se están corriendo en aras de un bien mayor que los compensa, identificándolo de forma precisa. En todo caso, la consulta ha de ofrecer y recoger de los interesados alternativas para cumplir los mismos objetivos de forma menos intrusiva para sus intereses colectivos.

Por lo tanto, la consulta a los interesados tiene el objeto de ser un instrumento de transparencia y de valoración de si la idoneidad y necesidad del tratamiento está justificada y la proporcionalidad es adecuada. La consulta no se puede reducir a una encuesta de satisfacción en la que sólo se ofrezca una imagen de los beneficios, y mucho menos, si esos beneficios no están directamente relacionados con el objeto del tratamiento y no repercuten en un bien general.

XVI. CONSULTA PREVIA A LA AUTORIDAD DE CONTROL

El artículo 36 del RGPD establece las obligaciones que ha de cumplir directamente el responsable del tratamiento, e indirectamente el encargado, en caso de que se haya realizado una EIPD y, como resultado de esta, se haya concluido que el riesgo residual[124] de dicho tratamiento podría poner en peligro los derechos y libertades de los ciudadanos.

La consulta previa no es una acción aislada, sino que ha de integrarse en la estrategia de gestión del riesgo para los derechos y libertades a la que obliga el RGPD. De esta forma, la consulta previa es más que la simple remisión de la EIPD a la Autoridad de Control. La consulta previa implica colaboración activa, seguimiento del proceso y facilitar a la Autoridad de Control toda aquella información adicional que precise durante el proceso de evaluación de la consulta y de la que se podrían derivar acciones por parte del responsable.

No obstante, debe señalarse que, independientemente de si se debe consultar o no a la Autoridad de Control a causa del nivel de riesgo residual, siguen estando vigentes las obligaciones de conservar un registro documental de la ejecución de la EIPD y de las actualizaciones que se puedan realizar de la evaluación[125].

A. OBJETO DE LA CONSULTA PREVIA

El proceso de consulta previa tiene como objeto presentar ante la Autoridad de Control un tratamiento que sea conforme con el RGPD, que tenga obligación o se haya valorado la oportunidad, o conveniencia, de realizar una EIPD, pero que entrañe un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptable.

No es objeto de la consulta previa:

- Solicitar a la Autoridad de Control la evaluación de la licitud de un tratamiento.
- Solicitar a la Autoridad de Control que establezca las bases jurídicas para llevar a cabo un tratamiento.
- Trasladar a la Autoridad de Control la obligación del responsable de llevar a cabo la evaluación de la proporcionalidad y necesidad del tratamiento.
- La validación sistemática de cualquier tratamiento por la Autoridad de Control.
- La validación de la EIPD por la Autoridad de Control.
- La solicitud a la Autoridad de Control para que lleve a cabo la identificación y evaluación de los riesgos o el nivel de riesgo inherente de un determinado tratamiento.
- Solicitar el asesoramiento de la Autoridad de Control para la realización de la EIPD[126].
- Requerir a la Autoridad de Control para que indique al responsable alternativas a los requisitos de cumplimiento como la proporcionalidad, necesidad, deber de información, bases jurídicas, condiciones del consentimiento, etc. entendiendo

[124] El riesgo residual no es el riesgo que originalmente podría derivarse del tratamiento, sino es aquel que persiste aun después de haber implementado el conjunto de medidas que el responsable ha considerado oportunas para tratar los riesgos identificados
[125] Directrices WP248
[126] Con este objetivo las autoridades de control publican recursos de ayuda, en el caso de la AEPD pueden consultarse el siguiente enlace: https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia

dichas alternativas como posibles medidas técnicas y organizativas sustitutorias de determinados requisitos de cumplimiento.

- Proporcionar seguridad jurídica al responsable[127].
- Solicitar a la Autoridad de Control que determine las medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento o solicitar la conformidad de la Autoridad de Control con relación a las medidas de seguridad que haya establecido el responsable.
- Solicitar a la Autoridad de Control que determine los supuestos para la realización de transferencia internacionales.
- Tampoco es objeto de la consulta previa evaluar la posibilidad de obviar el respeto de un derecho específico o cualquier otro aspecto que no esté directamente relacionado con un tratamiento legítimo o que implique un elevado nivel de riesgo residual para los derechos y libertades.

En general, no es objeto de la consulta previa trasladar a la Autoridad de Control cualquiera de las obligaciones que el RGPD y la LOPDGDD exigen a los responsables y encargados del tratamiento.

B. LA OBLIGACIÓN DE REALIZAR UNA CONSULTA PREVIA

Debe consultarse a la Autoridad de Control sobre la procedencia de una actividad de tratamiento, y siempre antes de iniciarla, cuando una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, dicho tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación[128].

Además, los responsables del tratamiento deberán consultar a la Autoridad de Control siempre que el Derecho de los Estados miembros les obligue a consultar a dicha autoridad o a recabar su autorización previa en relación con el tratamiento puesto en marcha por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública (artículo 36, apartado 5)[129].

Por lo tanto, la consulta previa a la Autoridad de Control no es una obligación para cualquier tratamiento, ni siquiera para aquellos tratamientos en los que el responsable ha realizado una EIPD. Tampoco la existencia de un riesgo en el tratamiento, entendido como un riesgo para los derechos y libertades de los ciudadanos, es una condición que obliga a realizar una consulta previa a la Autoridad de Control, de igual manera que la obligación o necesidad de realizar una EIPD tampoco es equivalente a la obligación de realizar una consulta previa.

---

[127] El principal objetivo del RGPD es el de proteger los derechos y libertades de los interesados cuyos datos personales son objeto de tratamiento. Además, y, en segundo lugar, el RGPD también proporciona un marco de seguridad jurídica al responsable basado en el enfoque de riesgos y la autorregulación. En este marco de responsabilidad activa, la seguridad jurídica se garantiza en la medida que el responsable ha adoptado y ejecutado con eficacia la gestión de los tratamientos que lleva a cabo y dispone de capacidad para demostrar dicho proceso de gestión mediante las medidas de control que considere idóneas en base a las particularidades existentes en cada uno de sus tratamientos en cada momento y teniendo en cuenta las variables ya mencionadas y definidas en el propio RGPD: naturaleza, ámbito o alcance, contexto y fines.

[128] Considerando 94.

[129] Directrices WP248

Además de lo establecido en el artículo 36 del RGPD, en el artículo 28[130] de la LOPDGDD también se establece la consulta previa entre las obligaciones generales de responsables y encargados.

El encargado del tratamiento ha de ser consciente de que está sujeto a ciertas obligaciones con relación a la consulta previa. Estas han de entenderse en el marco del proceso de ejecución de dicha consulta, tal y como se establece en el apartado 2 del artículo 36 cuando trata del papel de la Autoridad de Control: *"…asesorar por escrito al responsable, y en su caso al encargado, …*". También, en el considerando 95, se describe cómo parte de las obligaciones del encargado la de asistir al responsable tanto durante la realización de la EIPD como durante la consulta previa a la Autoridad de Control[131].

C. REQUISITOS PARA REMITIR UNA CONSULTA PREVIA

Existen una serie de requisitos básicos que han de cumplirse para remitir una consulta previa a la Autoridad de Control. El siguiente *checklist* identifica dichos requisitos:

[130] Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.
"Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento".

[131] Considerando 95. El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la Autoridad de Control.

El responsable del tratamiento presenta la consulta previa	
Si existe DPD u obligación de nombrarlo, este ha asesorado acerca de la evaluación de impacto relativa a la protección de datos y ha, o está, supervisando su aplicación	
Si existe DPD u obligación de nombrarlo, este actúa como punto de contacto con la Autoridad de Control	
La consulta previa tiene carácter previo a la puesta en marcha del tratamiento[132]	
Los fines del tratamiento están objetivamente determinados	
Existe una descripción sistemática de las operaciones de tratamiento	
Está realizada la evaluación de que el tratamiento es conforme con el RGPD en el cumplimiento de principios y derechos	
Está documentada y realizada una gestión de los riesgos para los derechos y libertades de los interesados de forma sistemática	
El tratamiento tiene en cuenta medidas sobre el concepto del tratamiento, de gobernanza y políticas, de protección de datos desde el diseño, por defecto y de seguridad acordes para la gestión del riesgo para los derechos y libertades de los interesados	
Está realizado el análisis de la obligación de llevar a cabo la EIPD o, en su caso, de la necesidad	
El tratamiento supera el análisis de necesidad y proporcionalidad con relación a los fines	
Todas las acciones anteriores están formalmente documentadas	

Tabla 50 Requisitos mínimos para la presentación de una consulta previa.

D. OBLIGACIÓN DE CONSULTA PREVIA EN CASO DE MISIONES EN INTERÉS PÚBLICO

La segunda excepción a la condición de que exista un alto riesgo residual para que sea obligatorio realizar la consulta previa se establece en el apartado 5 del artículo 36 donde se da la posibilidad a cada Estado miembro de desarrollar normativamente la obligación de consulta y autorización previa para determinados tipos de tratamiento, específicamente, aquellos relativos al ejercicio de una misión realizada en interés público[133].

Hasta el momento, no se han desarrollado estas obligaciones en el ámbito nacional.

E. REQUISITOS TEMPORALES ADICIONALES PARA LA PRESENTACIÓN DE LA CONSULTA PREVIA

Antes se ha descrito que el RGPD establecía como único requisito temporal para realizar la consulta previa que esta se realizase antes de ejecutar el tratamiento. La AEPD podría, mediante circulares, establecer condiciones adicionales.

[132] Ver apartado "Excepciones a realizar la EIPD antes del inicio de las actividades de tratamiento"

[133] 36.5 "No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la Autoridad de Control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública".

F. CÓMO SE MATERIALIZA UNA CONSULTA PREVIA

1. Documentación

El apartado 3 del artículo 36 establece la documentación que es obligatorio remitir a la Autoridad de Control para realizar una consulta previa:

> *"3. Cuando consulte a la Autoridad de Control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:*
>
> *a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;*
>
> *b) los fines y medios del tratamiento previsto;*
>
> *c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;*
>
> *d) en su caso, los datos de contacto del delegado de protección de datos;*
>
> *e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y*
>
> *f) cualquier otra información que solicite la Autoridad de Control".*

En la norma se hace explícito que el responsable ha de adjuntar a la consulta previa, además de la EIPD, una información adicional descrita en las letras a), b), c) y d) del apartado 3 del artículo 35 del RGPD; información que tendría más sentido que estuviese integrada en la propia documentación que forma parte de la EIPD. Esta información tiene carácter de mínimos y ha de cumplimentarse de forma efectiva.

2. Remisión de la consulta previa

Las remisiones a la AEPD de la consulta previa relativas al artículo 36 del RGPD deberán realizarse a través de su sede electrónica. Esta ofrece un apartado específico para la presentación de consultas previas bajo el epígrafe "Consulta previa al inicio de tratamientos de alto riesgo (art. 36 RGPD)". Este trámite electrónico está dirigido exclusivamente a responsables del tratamiento para la remisión de consultas previas, no siendo oportuno para otro tipo de consultas sobre otros aspectos de cumplimiento del RGPD.

En el caso de disponer de DPD, este ha de ser el punto de contacto con la Autoridad de Control[134].

G. RESPUESTA DE LA AUTORIDAD DE CONTROL

1. Solicitud de información adicional por parte de la Autoridad de Control

La posibilidad de solicitar información adicional directamente al responsable se enmarca en el apartado 2 del artículo 36 y en el apartado 3, letra f del mismo artículo que establece que el responsable ha de facilitar "*cualquier otra información que solicite la Autoridad de Control*".

[134] 39.e) actuar como punto de contacto de la Autoridad de Control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto

Además, a la hora de gestionar una consulta previa, el RGPD establece la posibilidad de hacer uso del mecanismo de asistencia mutua descrito en el artículo 61, tanto para el asesoramiento con relación a la consulta como para resolver las posibles autorizaciones para realizar el tratamiento[135].

El recurso al mecanismo de asistencia mutua no está reglado en la normativa excepto por la referencia a cumplir con el fin de aplicar el RGPD de manera coherente. De esta forma, la solicitud de asistencia mutua es una acción que queda a discreción de las autoridades de control y permite suspender el cómputo de plazos. Este mecanismo se está implementando de forma efectiva, por ejemplo, en el marco de las reuniones de los subgrupos del Comité Europeo de Protección de Datos.

2. Plazos de respuesta

Los plazos de respuesta de la Autoridad de Control a una consulta previa se establecen en ocho semanas, pero se podría extender a un total de catorce semanas. La extensión del plazo de contestación se podrá realizar "en función de la complejidad del tratamiento", siendo obligado informar al responsable, y en su caso al encargado, de los motivos de tal extensión. Por lo tanto, la extensión del plazo de consulta ha de ser motivada sobre lo problemático que pudiera resultar el análisis del tratamiento. La fundamentación de la complejidad del estudio se podría establecer, por ejemplo, en función de la innovación tecnológica que represente el tratamiento propuesto.

De todos modos, estos plazos podrán suspenderse en caso de que la Autoridad de Control haya solicitado información adicional con fines de consulta, siendo esta necesaria para emitir su respuesta, durante el tiempo en que tarde en recibirse dicha información.

3. Extensión del Asesoramiento

En el artículo 57.1.l se establece que incumbirá a cada Autoridad de Control, en su territorio, el ofrecer asesoramiento sobre el tratamiento sobre el cual se está realizando la consulta previa: "*57.1.l ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2*".

Con carácter general y sin perjuicio de otras consideraciones que pudieran ser aplicadas al caso específico de una solicitud de consulta previa, la extensión del asesoramiento de la Autoridad de Control podrá incluir, entre otros, alguno de los siguientes aspectos:

- Señalar al responsable que el tratamiento podría infringir el RGPD o la LOPDGDD.
- Determinar si el tratamiento puede ejecutarse en las condiciones de riesgo descritas por el responsable.
- Informar al responsable con relación a la adecuación del análisis de riesgos aportado en su EIPD.
- Informar al responsable con relación a la adecuación de las medidas previstas para paliar o evitar los riesgos del tratamiento para los derechos y libertades de las personas físicas.

[135] "1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones".

- Informar al responsable sobre el correcto análisis entre las distintas alternativas de implementación del tratamiento presentadas por el responsable.
- Informar al responsable sobre la correcta evaluación de la necesidad y proporcionalidad.
- Llevar a cabo recomendaciones relacionadas con los recursos de ayuda de las autoridades de control.

El responsable no ha de esperar como respuesta de la Autoridad de Control un informe con la extensión que se derivaría de un proceso de auditoría. Tampoco es objeto de respuesta proporcionar al responsable un conjunto de soluciones concretas para el tratamiento que correspondería al resultado de un proceso de consultoría. Menos aún, el objeto del asesoramiento es obtener respuesta a una nueva consulta previa por parte del responsable con el fin de que la Autoridad de Control lleve a cabo la validación/revisión/aprobación/seguimiento de las medidas aplicadas en reacción a una consulta previa.

Una auditoría ha de señalar, con precisión, el estado en el que se encuentra la entidad (o el tratamiento) con relación al objeto de la auditoría[136]. Por su parte, la consultoría ofrece soluciones específicas para la consecución de un objetivo concreto planteado por la entidad. Ninguno de los dos casos constituye el propósito de la consulta previa ni son parte de las competencias de la Autoridad de Control.

Finalmente, este asesoramiento no debe entenderse en términos absolutos con relación al tratamiento sino con relación a aquellos aspectos que motivan la consulta previa y a la información aportada por el responsable.

4. Ejercicio de los poderes establecidos en el artículo 58 del RGPD

Además del asesoramiento, en el apartado segundo del artículo 36 se establece que, ante la información remitida por el responsable, se deja a la Autoridad de Control la potestad de ejercer los poderes establecidos en el artículo 58 del RGPD.

Esta referencia implica que, en caso de una consulta previa, la acción de la Autoridad de Control no está limitada a su capacidad de asesoramiento, que se establece en el artículo 58.3.a, sino que puede extender su acción a la totalidad de los poderes establecidos en el artículo 58, esto es, los poderes de investigación establecidos en el artículo 58.1 y los poderes correctivos del artículo 58.2 que, entre otras posibilidades, con relación a la consulta previa, permiten a la Autoridad de Control:

- Requerir al responsable información adicional a la proporcionada en la consulta.
- Realizar investigaciones al responsable en forma de auditorías que podrían incluir el acceso a los locales, equipos, datos y la información necesaria para el ejercicio de las funciones de la Autoridad de Control.
- En caso de que el tratamiento se estuviera llevando a cabo, notificar y sancionar al responsable, entre otros casos, cuando:
    - no se hubiera llevado a cabo la obligada EIPD existiendo obligación legal de llevarla a cabo (35 RGPD, apartados 1, 2, 3 y 4) 137,

[136] El proceso de auditoría que puede realizar la Autoridad de Control queda definido, en otro contexto, en la Sección 2 "Potestades de investigación y planes de auditoría preventiva" de la LOPDGDD.

[137] Según se señala en el documento de "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679", el incumplimiento de los requisitos de la EIPD puede dar lugar a la imposición de multas por parte de la Autoridad de Control competente, y así se determina en Título IX de la LOPDGDD (artículos 73.t, 73.u y 74.o).

- la EIPD se hubiera llevado a cabo de forma incorrecta (Artículo 35 RGPD apartados 2, 7, 8, y 9) ,
- y, en su caso, se hubiera facilitado información inexacta a la Autoridad de Control en la consulta previa.

- Requerir al responsable o al encargado que lleven a cabo las modificaciones necesarias en los tratamientos para ajustar el tratamiento a lo previsto en el RGPD y la LOPDGDD.
- Prohibir o imponer limitaciones temporales o definitivas sobre los tratamientos.

H. TRANSPARENCIA Y CONFIDENCIALIDAD DE LAS CONSULTAS PREVIAS

Las consultas previas, como hemos visto anteriormente, han de incluir información detallada de la implementación del tratamiento e, incluso, aspectos técnicos y organizativos de la entidad responsable. Estos aspectos pueden tener una gran importancia en cuanto reflejan cuestiones tan relevantes para la entidad como sus políticas, valores, procedimientos, fortalezas, debilidades, medidas de seguridad corporativas y objetivos de negocio que resultan cruciales para entender el alcance del tratamiento y su contexto.

1. Transparencia

En cuanto a determinar si a la información remitida a la Autoridad de Control en el marco de una consulta previa, prevista en el artículo 36 del RGPD, le resulta de aplicación la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTAIBG), cabe señalar que, por una parte, dicha información estaría excluida del ámbito de la publicidad activa, por cuanto que no se encuadraría en ninguno de los supuestos contemplados en los artículos 7 y 8 de la LTAIBG.

Por otra parte, dicha información tampoco sería en principio objeto del derecho de acceso a la información pública. Aunque sea información pública, ésta se vería afectada por los límites al derecho de acceso establecidos en el artículo 14, en la medida que su difusión supusiera un perjuicio para (i) la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, (ii) las funciones administrativas de vigilancia, inspección y control, (iii) los intereses económicos y comerciales; (iv) la política económica y monetaria, o (v) el secreto profesional y la propiedad intelectual e industrial.

2. Confidencialidad

Con relación a la confidencialidad de la información remitida a la Autoridad de Control, el RGPD establece en el párrafo 2 del artículo 54 que la información confidencial obtenida en el cumplimiento de sus funciones está protegida por el deber de secreto al que están sometido los miembros y el personal la Autoridad de Control[138].

De igual forma en las Directrices WP248 se estipula que la Autoridad de Control no pondrá en peligro los secretos comerciales ni divulgará vulnerabilidades de seguridad,

[138] Artículo 54. Normas relativas al establecimiento de la Autoridad de Control
"2. El miembro o miembros y el personal de cada Autoridad de Control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento".

lo que obliga a su vez, no solo al deber de secreto de su personal, sino a implementar las medidas de seguridad necesarias que garanticen la consecución de dicho objetivo[139].

I. NORMATIVA RELACIONADA

La obligación de realizar una consulta previa con relación a los riesgos derivados de un tratamiento de datos personales se encuentra presente también en otra normativa como, por ejemplo, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que traspone la Directiva (UE) 2016/680. En su artículo 35 establece las condiciones para que sea obligatoria la realización de la EIPD y su artículo 36, extiende la obligación de la consulta previa a cualquiera de las siguientes circunstancias:

> *a) Cuando la evaluación del impacto en la protección de los datos indique que el tratamiento entrañaría un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños.*
>
> *b) Cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos.*

A su vez, en la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), con la prudencia necesaria de que se trata de una propuesta sujeta a profunda revisión en el momento de redactar este texto, en el artículo 6 sobre el "Tratamiento autorizado de datos de comunicaciones electrónicas", se hace referencia a que los proveedores de servicios de comunicaciones electrónicas únicamente podrán tratar contenido de comunicaciones electrónicas cuando todos los usuarios finales interesados hayan dado su consentimiento para el tratamiento del contenido de sus comunicaciones electrónicas con uno o más fines específicos que no puedan alcanzarse mediante el tratamiento de información anonimizada, y el proveedor haya consultado a la Autoridad de Control siendo aplicable el artículo 36, puntos 2 y 3, del Reglamento (UE) 2016/679 a la consulta previa.

[139] "La Autoridad de Control puede facilitar su asesoramiento, y no pondrá en peligro secretos comerciales ni revelará vulnerabilidades de seguridad, sujeto a los principios aplicables en cada Estado miembro sobre acceso público a documentos oficiales"

XVII. CONCLUSIONES

Como se señalaba en la introducción, la gestión del riesgo supone un ejercicio de reflexión que hay que llevar a cabo antes de realizar una actividad de tratamiento de datos personales. Su objetivo es el de identificar y poder anticiparse a los posibles efectos adversos, o no previstos, que el tratamiento podría tener sobre los interesados. La gestión del riesgo ha de permitir que el responsable tome las decisiones y acciones necesarias para conseguir que el tratamiento cumpla los requisitos del RGPD y la LOPDGDD, garantizando y pudiendo demostrar la protección de los derechos de los interesados.

La gestión del riesgo es una tarea que confronta las expectativas e ilusiones del responsable del tratamiento con la realidad que se deriva de las consecuencias de la implementación efectiva del mismo para los interesados. También confronta los objetivos a corto plazo del responsable con una visión a largo plazo de las consecuencias que las operaciones de tratamiento pueden suponer sobre los interesados. Además, obliga a realizar un análisis crítico de las relaciones de un tratamiento con el entorno.

La gestión del riesgo que exige el RGPD es aquella que está orientada específicamente a proteger los derechos y libertades de los interesados, y no hay que confundirla con otras orientaciones de riesgo, como la gestión de riesgo de cumplimiento. A su vez, la gestión del riesgo para los derechos y libertades se extiende más allá de únicamente una gestión de riesgos de seguridad.

El correcto desempeño de esta tarea obliga al responsable a realizar algo más que elaborar documentos o utilizar herramientas de ayuda a la toma de decisiones. La gestión del riesgo que obliga a estudiar, analizar, actuar y asumir responsabilidades, así como a realizar su seguimiento continuo y permanente. Por lo tanto, la gestión del riesgo es un proceso y, como tal, ha de ser eficaz (conseguir sus objetivos) y eficiente (realizarse con el mínimo coste y empleo de recursos).

Como herramienta básica para la ejecución de la responsabilidad proactiva, la gestión del riesgo para los derechos y libertades ha de estar incluida y formar parte indivisible de las políticas de gestión de la organización. Por lo tanto, la gestión del riesgo para los derechos y libertades es una tarea que debe ser realizada “por defecto” cuando se están tratando datos de carácter personal.

La gestión del riesgo y la Evaluación de Impacto para la Protección de Datos son procesos íntimamente vinculados. La EIPD es una especificidad dentro de la gestión del riesgo. Por lo tanto, la EIPD no puede existir sin estar formando parte de la gestión de riesgos para los derechos y libertades, extendiéndola con una serie de requisitos adicionales. Mientras que la gestión del riesgo es obligatoria para todo tratamiento, las obligaciones concretas que se establecen para la EIPD son obligatorias, exclusivamente, para tratamientos de alto riesgo.

La obligación de realizar una EIPD, establecida en el RGPD y en su desarrollo, es una declaración de mínimos. Es decir, la EIPD puede ser recomendable o necesaria en otros casos, independientemente de que sea obligatoria para casos específicos. En ocasiones su utilización puede ser aconsejable, como herramienta para “garantizar y poder demostrar”[140] la conformidad con el RGPD. En cualquier caso, independientemente de guías o listas de obligación, la gestión del riesgo incluyendo las garantías de una EIPD ha de realizarse “Cuando sea probable que un tipo de

[140] Artículo 24.1 del RGPD

tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas"[141].

[141] Artículo 35.1 del RGPD