

APLICACIÓN PRÁCTICA EN MATERIA DE PROTECCIÓN DE DATOS EN LA JUNTA DE ANDALUCÍA

UNIDAD 3

**Las Administraciones públicas como
responsables en el RGPD. Relaciones con sus
encargados de tratamientos**

CONTENIDO

1. PRINCIPIO DE RESPONSABILIDAD PROACTIVA	3
2. ELACIONES RESPONSABLE vs ENCARGADO. ESPECIAL REFERENCIA A LAS ADMINISTRACIONES PÚBLICAS.	6
3. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO.....	9
3.1 PROTECCIÓN DE DATOS DESDE EL DISEÑO	9
3.2 PRIVACIDAD POR DEFECTO	13
3.3 EXIGIBILIDAD DE LA APLICACIÓN DE ESTOS PRINCIPIOS	14
4. EL REGISTRO Y EL INVENTARIO DE ACTIVIDADES DE TRATAMIENTO	15
4.1 EL RAT: REGISTRO DE ACTIVIDADES DE TRATAMIENTO	15
4.2 EL INVENTARIO.....	16
5. POLÍTICAS DE PROTECCIÓN DE DATOS	17
6. ENFOQUE DE RIESGO EN EL RGPD	18
6.1 LA GESTIÓN DEL RIESGO.....	19
6.2 LA GESTIÓN DEL RIESGO EN EL RGPD	20
6.3 EL RIESGO PARA LOS DERECHOS Y LIBERTADES	21
6.4 LA GESTIÓN DEL RIESGO DE CUMPLIMIENTO VS RIESGO PARA LOS DERECHOS Y LIBERTADES	22
7. EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS	23
8. LA SEGURIDAD EN EL RGPD	27
8.1 EL PAPEL DE LA SEGURIDAD.....	27
8.2 EL RESPONSABLE DE SEGURIDAD	28
8.3 EL ESQUEMA NACIONAL DE SEGURIDAD	29
8.4 NOTIFICACIONES DE BRECHAS DE SEGURIDAD	29



Este curso ha sido cedido por la Agencia Española de Protección de Datos por medio de una licencia Creative Commons Reconocimiento-No comercial-Compartir igual, en los términos que se describen en <http://creativecommons.org/licenses/by-nc-sa/3.0/es> o texto oficial que, para esta modalidad de licencia, sustituya al indicado.

1. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El **concepto de responsabilidad proactiva** se establece en el artículo 5 del RGPD, en el que se define el conjunto de principios que se ha de aplicar para la protección efectiva de los datos personales. En concreto en el apartado 2 se establece que la responsabilidad proactiva es una de las obligaciones del responsable del tratamiento en relación con los principios establecidos en el apartado 1 del mismo artículo. Por lo tanto, es una de las nuevas obligaciones que se establecen en el RGPD para asegurar el cumplimiento de dichos principios y que consiste en la capacidad del responsable, es decir, de la organización, de demostrar y proporcionar evidencias de dicho cumplimiento.

El concepto de responsabilidad proactiva se pierde en la traducción del RGPD, desde la redacción original en inglés a la traducción al español. **En la versión en inglés se emplea el término “accountability”**. Este término es muy difícil de traducir al castellano, procede de la cultura empresarial anglosajona y no existe una palabra que lo defina en nuestro idioma de forma precisa porque, aunque sea duro de aceptar, está lejos de nuestros conceptos culturales tradicionales.

Las obligaciones del responsable se dibujan en el artículo 24 del RGPD: Artículo 24 Responsabilidad del responsable del tratamiento

1. **Teniendo en cuenta** la **naturaleza**, el **ámbito**, el **contexto** y los **finés** 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.
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**.
3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

El RGPD **se basa en la gestión del riesgo para los derechos y libertades mediante la implementación el autoanálisis, crítico, continuo, “traceable”, o rastreable, y basado en la responsabilidad, que permita implementar una verdadera gobernanza de datos personales en el seno de las empresas.**

“Traceable” o rastreable supone que existe un registro de las distintas decisiones en el tiempo, incluso cuando dichas decisiones han resultado contradictorias. Con responsabilidad implica que en dicho registro se identifica la persona que tomó las decisiones o las que no las tomó cuando debería haberlo hecho, por qué tomó esas decisiones, qué justificación había para tomarlas y cuándo las tomó. Además, dependiendo del tipo de actividad o decisión, se pueden recoger datos adicionales que pudieran resultar relevantes para el proceso de negocio o para el servicio proporcionado a los sujetos de los datos, como dónde tomo dicha decisión o desde qué dispositivo se tomó dicha decisión.

Otro aspecto relevante en relación con la implementación de la responsabilidad proactiva es el compromiso de los miembros de la organización, ya que el principio de responsabilidad proactiva implica a todo el personal de la organización involucrado en el día a día del tratamiento de datos de carácter personal y no de forma puntual. **El personal de la organización ha de tomar una actitud proactiva, comprometida y responsable, consciente de la necesidad de preservar un derecho fundamental.** En definitiva, una nueva actitud en la ejecución de las obligaciones que es activa antes que pasiva.

El conjunto de tareas que se han de implementar para hacer efectivo el principio de responsabilidad proactiva en relación a la protección de datos de carácter personal no se encuentra listado en un solo artículo, más bien al contrario, la definición del mismo se extiende a lo largo de todo el RGPD, de igual forma que se distribuye en la organización. Pero se pueden señalar las medidas más importantes y establecidas en el reglamento que están ligadas a la aplicación efectiva de la responsabilidad proactiva.

Estas, sin pretender ser exhaustivo, son las siguientes:

- La **gestión del riesgo** para los derechos y libertades de los interesados.
- La implementación del **principio de transparencia** del responsable hacia el sujeto de los datos en relación con el conjunto de tratamientos realizados y los datos recogidos, especialmente en el caso de enriquecimiento de datos y las subcontrataciones realizadas, incluyendo las transferencias internacionales.
- La obligación de tener un **delegado de protección de datos** que canalice dicha información tanto a las autoridades de control como a los sujetos de los datos que se dirijan a la entidad.
- La obligación de tener un **listado de tratamientos** y que dicho listado esté disponible tanto para la autoridad como para todos aquellos ciudadanos que lo requieran, aunque sus datos no se encuentren bajo tratamiento.
- La obligación de realizar los **análisis de impacto en la privacidad**, que es un análisis crítico del tratamiento de los datos personales que se llevan a cabo en un proceso, servicio o negocio. Está orientado a identificar tanto los efectos directos y previstos en el objeto de dicho tratamiento, como los efectos secundarios, laterales o indeseados que puede ocasionar a la privacidad, intimidad y libertad tanto de los clientes, usuarios o terceros. Es un estudio que trasciende el marco local de las actividades de la propia organización o los propósitos originales del tratamiento y ha de adoptar una visión global cuyo objetivo es la protección de los derechos humanos y las libertades fundamentales tal y como se desarrollan en el RGPD. Y lo más importante, ha de ponerse a disposición de las Autoridades de Control en caso de que se tengan dudas sobre el riesgo que, para los derechos y libertades de las personas, puedan suponer los tratamientos que se realizan.
- Los resultados obtenidos en dicho análisis son aquellos que se tienen que utilizar como entrada en tres de los procesos definidos en el RGPD: **los requisitos de privacidad desde el diseño, los de privacidad por defecto y los de seguridad, con la implementación de dichos requisitos.**
- La **notificación de las brechas de seguridad**, independientemente del tratamiento de la brecha, tanto a las autoridades de control como a los sujetos de los datos que han podido ser comprometidos.
- En relación con la implementación de las medidas de responsabilidad proactiva, y en general de los procesos que tratan datos de carácter personal, la **obtención de certificados y de sellos de privacidad**, lo que supone pasar procesos de certificación supervisados por terceros y la **adhesión a códigos de conducta**, que tienen el mismo papel que los procesos de certificación, pero con un

marcado carácter sectorial. Al igual que los anteriores, suponen procesos de transparencia pública controlados por terceras partes independientes.

De los párrafos anteriores se puede deducir una importante conclusión y es que la responsabilidad proactiva se refiere a la configuración de la organización desde la perspectiva de protección de datos. Una configuración que permite articular coherentemente cada una de las medidas enumeradas anteriormente, y establecidas en el Reglamento, para que actúen de forma coordinada ofreciendo una efectiva protección a los derechos de los ciudadanos. Es decir, responsabilidad proactiva supone introducir una cultura de protección de datos en la organización.

No se encuentra otra referencia a la responsabilidad proactiva en el texto del articulado. En cambio, sí se encuentra en uno de los considerandos, el 85. Dicha referencia se realiza en relación con la comunicación de brechas de seguridad y, en particular, a la excepción de informar a las autoridades de control sobre la existencia de un incidente de seguridad que afecte a los datos de carácter personal cuando, atendiendo al principio de responsabilidad proactiva, el responsable pueda demostrar la improbabilidad de que la brecha de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

Este considerando no establece, pero sí sugiere, una interpretación en relación con la seguridad jurídica que una decisión de la organización en relación a una brecha de seguridad sea contraria a realizar una notificación de brecha de seguridad. La organización se encontrará protegida porque tiene conocimiento de que el impacto de la brecha es mínimo. La seguridad de ese conocimiento se fundamenta en el control efectivo y real de los procesos de datos personales.

2. RELACIONES RESPONSABLE vs ENCARGADO. ESPECIAL REFERENCIA A LAS ADMINISTRACIONES PÚBLICAS

Para determinar las relaciones entre el responsable del tratamiento y el encargado de tratamiento en el ámbito de las Administraciones Públicas, debemos partir, en primer lugar, de las definiciones que al respecto establece el RGPD. En segundo lugar, se mostrará cómo estructura la relación entre ambos la legislación en vigor, la LOPDGGD Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, describiendo la casuística que tiene lugar en el marco de actuación de las Administraciones Públicas. Finalmente se describirán los posibles hechos diferenciales que el RGPD presenta.

El RGPD define, en su artículo 4.7, como **“responsable del tratamiento”** o **“responsable”**: “La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

Respecto a la definición de **“encargado del tratamiento”** o **“encargado”**, lo define como “la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”.

Ambas definiciones del RGPD mantienen lo descrito ya en la anterior LOPD, donde las relaciones entre el responsable y el encargado requerían la celebración de un contrato o acto jurídico similar por escrito o incluso formato electrónico que los vinculase. El encargado actúa de acuerdo con lo estipulado por el responsable que es quien decide sobre la finalidad, contenido y uso del tratamiento.

La relación entre responsable y encargado tan fácilmente reconocible en otros ámbitos aparece también en la Administración Pública generalmente a través de una encomienda de gestión, de un convenio o contrato administrativo.

En este último caso, la Disposición Adicional 25ª de la Ley 9/2017, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, determina que “Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento”, con las especificidades establecidas en tal Disposición Adicional.

Sin embargo, lo que entre entidades particulares quedaba claro con la firma de un contrato, ha suscitado dudas en muchas ocasiones en el seno de las Administraciones Públicas, donde, en muchas ocasiones, las estructuras orgánicas asignan una/s unidad/es, subdirecciones generales/servicios/negociados, funciones de gestión a otra unidad, subdirección general de informática, agencia..., funciones entre las que se encuentran:

- El desarrollo de los sistemas de información necesarios para el funcionamiento de los servicios, el portal web, la sede electrónica, la intranet, las herramientas colaborativas y los dominios de internet del/de la Ministerio/CCAA/Ayuntamiento.
- El impulso de la administración digital del/de la Ministerio/CCAA/Ayuntamiento y sus organismos

de acuerdo con el plan de acción departamental para la transformación digital y la Estrategia TIC de la Administración, así como la provisión de servicios en materia de tecnologías de la información y comunicaciones que le corresponde prestar como unidad TIC del/de la Ministerio/CCAA/Ayuntamiento.

- El impulso y coordinación en el ámbito del/de la Ministerio/CCAA/Ayuntamiento de los Esquemas Nacionales de Interoperabilidad y Seguridad, y de las medidas para garantizar la accesibilidad de los servicios electrónicos y el cumplimiento de sus obligaciones, en materia de reutilización de la información del sector público.

Así pues, en muchas ocasiones aparecen unidades transversales, con condición de encargado de tratamiento en virtud de atribución de competencias¹ que aparecen reflejadas en una norma de carácter reglamentario organizativo, como puede ser un Real Decreto (AGE) o Decreto (CCAA) de estructura, o incluso, en una ley cuando se ha creado un organismo específico para ello.

Es decir, nos encontramos con un organismo o entidad que actúa como encargado de tratamiento en el ámbito de su respectiva Administración Pública, puesto que se le atribuyen funciones y competencias que no inciden en el poder decisorio sobre la finalidad, contenido y uso de los datos, sino que fundamentalmente versan sobre la implantación y utilización de los sistemas de información para que sean utilizados por los órganos y organismos correspondientes.

En este supuesto específico, cuando el encargado de tratamiento está configurado en función de esas normas de carácter reglamentario-organizativo, o incluso legales, que fija sus competencias, supone ya la existencia de un contrato de encargo de tratamiento, sin que por tanto sea necesario la celebración de contratos específicos para cada órgano u organismo en los términos del art. 28.3 RGPD.

La LOPDGDD contempla esta situación de la siguiente forma en el art. 33.5: “En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679”.

También nos encontraremos los típicos supuestos de encargados de tratamiento, como pueden ser la contratación de una empresa para que realice la destrucción de documentos o de un servicio de computación en la nube, así como cualquier otro que haya sido contratado por la Administración correspondiente para la prestación de un servicio que conlleve un tratamiento de datos de carácter personal.

A este respecto, debe tenerse también en cuenta lo que prevé la LOPDGDD en el art. 33.2: “Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público”.

¹ Este supuesto específico ha sido analizado por el siguiente informe jurídico de la AEPD: <https://www.aepd.es/informes/historicos/2012-0333.pdf>

Por otra parte, la aplicación del RGPD no modifica las relaciones entre responsable y encargado o las cuestiones a tener en cuenta. Para empezar, cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento y garantice la protección de los derechos del interesado. El tratamiento realizado por el encargado se regirá por un contrato (o acto jurídico equivalente) que vincule al encargado respecto del responsable y cuyo contenido mínimo establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Los Considerandos 79, 81 y 95 así como el Capítulo IV del RGPD y el Título V de la LOPDGDD, detallan las relaciones entre ambos, señalando que es deber del responsable la diligencia en la contratación del encargado.

En particular, el contrato o acto de encargo de tratamiento deberá contener:

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad.
- Las medidas de seguridad.
- El régimen de la subcontratación.
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los interesados.
- La colaboración en el cumplimiento de las obligaciones del responsable.
- El destino de los datos al finalizar la prestación.

Para facilitar la elaboración de este tipo de contratos, la AEPD en colaboración con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, ha publicado el documento [“Directrices para la elaboración de contratos entre responsables y encargados del tratamiento”](#), que contiene, un Anexo con un ejemplo de cláusulas contractuales para aquellos supuestos en que el encargado del tratamiento trate los datos en los locales del responsable.

Para terminar este apartado, hay que señalar que la LOPDGDD incluye la siguiente **Disposición Transitoria Quinta** sobre los contratos de encargo de tratamiento:

“Los contratos de encargo del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.”

3. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

En el texto del RGPD se hace referencia a dos principios para la implementación efectiva de la responsabilidad proactiva como son los de protección de datos desde el diseño y protección de datos por defecto. Dichas referencias se centran en los Considerandos 78 y 108 y en el artículo 25, titulado **“Protección de datos desde el diseño y por defecto”**, donde se configuran y desarrollan estos principios.

Si se repasa el artículo 4 “Definiciones” no se encontrará una definición precisa y limitada de ambos principios, por lo que hay que remitirse al texto del citado artículo 25 para determinar que se pretende con ellos. Por ello, la AEPD ha publicado la [Guía de Privacidad desde el Diseño](#) en donde se desarrolla de forma práctica la forma de implementar el artículo 25 en los tratamientos.

3.1 PROTECCIÓN DE DATOS DESDE EL DISEÑO

La idea de ‘protección de datos desde el diseño’ existe desde hace más de 20 años y se ha trabajado intensamente en ella bajo la terminología de ‘privacidad desde el diseño’ (Privacy by Design, PbD).

El RGPD, incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios. Por lo tanto, le confiere la categoría de requisito legal al principio de integrar las garantías para la protección de los derechos y libertades de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas y productos.

La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso).

Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada. Más aun, implica que se tengan en cuenta, no sólo la aplicación de medidas de protección de la privacidad en las etapas tempranas del proyecto, sino que además se contemplen también todos los procesos y prácticas de negocio involucrados en el tratamiento de datos asociado, logrando así una verdadera gobernanza de la gestión de los datos personales por parte de las organizaciones.

El objetivo último es que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema. La privacidad debe formar parte integral de la naturaleza de dicho producto o servicio.

3.1.1 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 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 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:

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

La Guía de Privacidad desde el Diseño contiene un desarrollo de la tabla anterior. A continuación, se expone un breve resumen que condensa la información de dicho documento.

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.

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 supresión².

² 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>

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.
- **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.

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.

INFORMAR

Esta estrategia pretende la implementación del objetivo y el principio de transparencia 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.

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 granulada³ 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.

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 relativas, o con impacto, en 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.

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 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. TÁCTICAS: seleccionar, excluir, podar y eliminar	Anonimización Seudonimización 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

³ 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.

ESTRATEGIAS ORIENTADAS A PROCESOS			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
	Informar	Proporcionar información extendida del tratamiento. TÁCTICAS: facilitar , explicar y notificar	Iconos de privacidad. Alertas de tratamiento. Publicar información sobre el rendimiento del tratamiento. 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.

3.2 PRIVACIDAD POR DEFECTO

El **concepto de privacidad por defecto se desarrolla** en el apartado 2 del mismo artículo 25. La idea principal estriba en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. Es decir, independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al sujeto de los datos, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario. Si fuera posible por la naturaleza del proceso, llegar incluso a que no se traten datos de carácter personal.

En particular, se destaca como uno de los principios dentro de la privacidad por defecto el que los datos personales no sean accesibles a un número indeterminado de personas físicas, sin la intervención del sujeto de los datos. Hay que tener en cuenta que el Reglamento señala “personas físicas”, no entidades, ya que se está refiriendo a la aplicación del conocido principio de seguridad denominado “need-to-know” o necesidad de conocer, como a una nueva extensión de ese principio que podríamos denominar el “need-to-disclosure” o necesidad de divulgación.

El principio de “need-to-know” o “necesidad de conocer” establece que en una organización las personas han de tener acceso sólo a la información precisa para ejecutar sus tareas. El principio se aplica a la protección de datos de carácter personal en la medida que significa que los empleados de la empresa sólo han de tener acceso a los datos de carácter personal que son estrictamente necesarios para realizar su trabajo o proporcionar un servicio. El principio de “need-to-disclosure” tiene el mismo fundamento, pero extendido a terceros que de alguna forma están relacionados con el producto o servicio solicitado, como podría ser el caso de usuarios que han utilizado el mismo servicio, han estado en el mismo sitio o se encuentran en una misma situación. **Cuatro estrategias básicas permiten implementar la privacidad por defecto:**

- Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario;
- Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;
- Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;
- Accesibilidad: limitar el acceso por parte de terceros a dichos datos personales.

Como en el caso de la privacidad desde el diseño, estos requisitos se van a traducir en medidas tanto técnicas como organizativas y en el caso de la privacidad por defecto, es necesario prestar incluso más atención a estas últimas. Incluso, se señala la oportunidad de dar transparencia a la implementación de dichos tratamientos, permitiendo a los interesados supervisar el proceso de sus datos y al responsable del tratamiento crear y mejorar elementos de seguridad.

3.3 EXIGIBILIDAD DE LA APLICACIÓN DE ESTOS PRINCIPIOS

En caso de transferencia de datos a un tercer país en que no haya una decisión que constate la adecuación de la protección de los datos, el considerando 108 establece que el responsable o el encargado del tratamiento, debe tomar medidas para compensar dicha situación. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, en particular, deben referirse al cumplimiento de los principios de la protección de datos desde el diseño y por defecto.

4. EL REGISTRO Y EL INVENTARIO DE ACTIVIDADES DE TRATAMIENTO

4.1 EL RAT: REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El RGPD regula en su artículo 30 la obligación de llevar un **“Registro de actividades de tratamiento”** o RAT. El objeto de dicho registro es el de permitir un control y gestión proactiva de los procesos que realice la organización de forma eficiente. Por lo tanto, el RAT es una herramienta y no un formulario. El contenido mínimo, que no máximo, que exige la normativa es el siguiente:

1. Cada responsable y, en su caso, su representante, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
 - el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
 - los fines del tratamiento;
 - una descripción de las categorías de interesados y de las categorías de datos personales;
 - las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
 - en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo⁴, la documentación de garantías adecuadas;
 - cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
 - cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1⁵.
2. Cada encargado y, en su caso, el representante del encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:
 - el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
 - las categorías de tratamientos efectuados por cuenta de cada responsable;
 - en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
 - cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.
3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

⁴ Artículo 49 RGPD: Excepciones para situaciones específicas; Párrafo 1, b): “La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado”.

⁵ En el caso de España, las medidas de seguridad a adoptar por responsables y/o encargados de tratamiento del Sector Público [el Artículo 2 de la Ley 40/2015] deben entenderse dentro del Esquema Nacional de Seguridad como especifica la Disposición Adicional Primera de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

En aquellas entidades que, por tener implantados sistemas de calidad, ya tengan un catálogo de procesos o tratamientos, solo tendrían que asegurarse que la información ya registrada incluye la requerida en los artículos 30 del RGPD. Es decir, el artículo 30 no obliga a crear un nuevo registro de tratamientos si la entidad ya dispone de dicho registro para otros propósitos. Además, tampoco limita la información que puede haber en un registro de actividades de tratamiento. Esta información se puede ampliar tanto como sea necesaria para que dicho registro sea una herramienta de gestión eficiente.

4.2 EL INVENTARIO

La información que el RGPD exige en el RAT es una información de mínimos. Por motivos de cumplir con estándares de calidad o para control interno de los tratamientos, el RAT podrá estar integrado en las herramientas de control de procesos de la entidad e incluir información como: personas de contacto a cargo de tratamientos, referencias a contratos, controles sobre auditorías, enlaces a documentación, etc.

Por ello, el artículo 31.2 de la LOPDGDD establece que "Los sujetos⁶ enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal". El inventario es una versión mínima del RAT que mantenga la organización, sin toda la información adicional que se utilice para la gestión interna y no sea necesario hacer pública.

Así pues, parece claro que todos los tratamientos realizados por las Administraciones Públicas se llevarán a cabo mostrando su legitimidad; además, se les dará publicidad, ya sea a través de la página web, sede electrónica o Portal de Transparencia para que el ciudadano pueda tener constancia de los tratamientos que realiza cada una de ellas.

⁶ El Artículo 77.1 de LOPDGDD "Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento" se refiere a los siguientes:

- a. Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
- b. Los órganos jurisdiccionales.
- c. **La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.**
- d. Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
- e. Las autoridades administrativas independientes.
- f. El Banco de España.
- g. Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
- h. Las fundaciones del sector público.
- i. Las Universidades Públicas.
- j. Los consorcios.
- k. Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

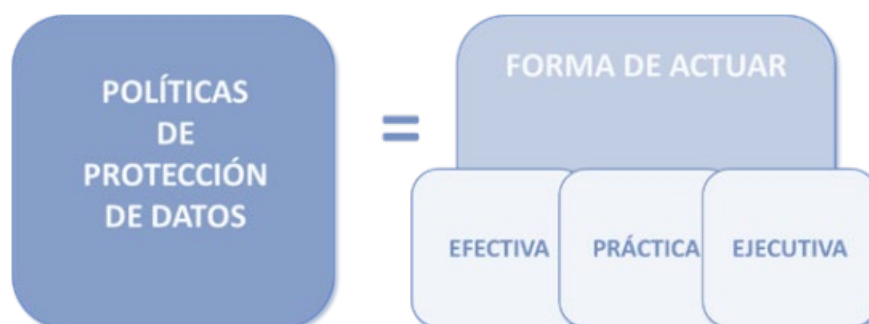
5. POLÍTICAS DE PROTECCIÓN DE DATOS

El gobierno o gobernanza de datos es el proceso por el que se implementan políticas y procedimientos para garantizar una gestión efectiva y eficiente 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 de protección de datos personales, tomando las medidas adecuadas y ofreciendo garantías suficientes.

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 datos⁷”. Si entendemos el término “políticas⁸” 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 o la LOPDGDD o una 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.



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, sino que exige que, en los procedimientos aprobados por la entidad en el que se reflejen las políticas a seguir en aquellas actividades que impliquen el tratamiento de datos personales, se encuentren directrices específicas para el mejor cumplimiento del RGPD. En el caso que nos ocupa, deben existir en las políticas directrices para la gestión del riesgo para los derechos y libertades. La inclusión de dichas directrices en, por ejemplo, los procedimientos de recursos humanos, teletrabajo, contratación de productos y servicios, desarrollo de

⁷ No hay que confundir Política de Protección de Datos, con Política de Privacidad. Esta última, es un término que se aplica a las cláusulas que dan cumplimiento al deber de informar.

⁸ Política: “Orientaciones o directrices que rigen la actuación de una persona o una entidad en un asunto o campo determinado”.

aplicaciones, etc., tendrá un carácter más eficaz, que una pura declaración formal en un documento independiente.



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.

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 controles que pudieran ser necesarios para garantizar dicho cumplimiento. 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 la responsable el cumplimiento del RGPD.

6. ENFOQUE DE RIESGO EN EL RGPD

En toda nueva actividad, el hecho de realizar una tarea de reflexión previa para identificar posibles problemas y anticiparse a las futuras dificultades, permitirá tomar decisiones racionales y actuar con garantías de éxito. El esfuerzo que se dedicará a sopesar las posibles consecuencias de las acciones, a corto o a largo plazo, deberá ser proporcional al posible perjuicio o consecuencias que éstas podrían tener. Cuando esta forma de actuar se aplica al gobierno de una organización, a esta aproximación se le denomina “gestión del riesgo”.

La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impacto) que una actividad puede tener sobre un conjunto de factores 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 exige la gestión del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. En cumplimiento del principio de responsabilidad proactiva o “accountability”, la gestión del riesgo ha de estar documentada. Sin embargo, no hay que confundir 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, es un proceso que se traduce en hechos y que se acredita documentalmente.

6.1 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 definen esta actividad como la “aproximación basada en el riesgo” (RTB de “risk based thinking”). El RTB es, con la orientación a procesos (tratamientos), 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 y hasta en el propio Código Penal. La gestión de riesgo es una garantía para el crecimiento de cualquier entidad.

Las normas ISO definen el concepto de “riesgo” como el “efecto de la incertidumbre sobre la consecución de objetivos” entendiéndose 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 surgen elementos de incertidumbre. Las incertidumbres se manifiestan desde las diferentes perspectivas desde las que esta se aborde. Por ejemplo, toda entidad ha de ser capaz de garantizar que dispondrá del capital para poner en marcha dicha actividad, es decir, ha de gestionar el riesgo financiero que puede suponer una nueva iniciativa. Una vez que financieramente se puede poner en marcha el proyecto, hay que determinar si se dispone de los recursos, humanos y materiales, necesarios y determinar su adecuación a la tarea, los posibles retrasos en entregas, su disponibilidad a lo largo de la implantación de la actividad, etc., gestionando el riesgo de ejecución del proyecto. Además, dicha actividad ha de producir alguna ganancia, material o inmaterial, por lo que será necesario determinar el coste probable que supone la actividad con relación al beneficio que aporta, y su evolución en el tiempo, es decir, el análisis coste/beneficio.

También hay que gestionar la actividad desde otras muchas perspectivas. Entre los más importantes están los riesgos de responsabilidad civil o penal. Dependiendo del proyecto o actividad en curso, se encontrará la necesidad de gestionar el riesgo relativo a la fiabilidad las tecnologías seleccionadas, el riesgo de seguridad para las personas, o con relación a la continuidad del negocio, el riesgo de que la nueva actividad cumpla unos plazos de entrega determinados, el riesgo de fraude, etc.

Además, no solo es necesario analizar la posible nueva actividad como si estuviese aislada del resto de la entidad, sino que también hay que analizar el impacto que tendrá en otras actividades de la organización, así como el riesgo de coste de oportunidad que supone relegar otras posibles opciones en favor de ésta.

Más aún, la actividad y la organización se desenvuelven en un contexto social y económico cambiante y con el que es preciso interactuar. Por tanto, la organización tiene que estudiar el riesgo legal de los futuros cambios normativos o analizar posibles efectos del riesgo de cumplimiento. Por otro lado, también hay que analizar cómo afecta la organización a la sociedad y al entorno, mediante análisis de riesgo medioambiental o de impacto social (responsabilidad social corporativa).

Por tanto, la gestión del riesgo debe entenderse como una metodología general con objetivos de gestión diferentes y determinados (riesgo financiero, legal, laboral, social, etc.).

6.2 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 en particular, 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 (en adelante la Declaración WP218) y no es un concepto novedoso en el marco de la protección de datos.

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 materiales implicados (o involucrados). El riesgo no solo surge por los fines del tratamiento o su naturaleza, sino 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 tipo de gestión del riesgo se integre con el resto de los recursos de gestión de riesgo o de 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 la gestión de riesgos. 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 (en adelante CEPD) 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” (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.

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

Asimismo, incluyen recomendaciones tanto para la EIPD en particular como para la gestión del riesgo en general. Además, aclara 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 LOPDGGDD) plantea la necesidad de tener en cuenta los riesgos que podrían producirse como resultado de un tratamiento de datos personales.

6.3 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.

El Considerando 75 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 interpretan que la protección se ha de extender a otros derechos fundamentales. Específicamente, 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 en 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. Por lo tanto, no sólo hay que gestionar los riesgos para el sujeto de los datos que se están tratando, sino los de todos aquellos individuos afectados o colectivos de afectados 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.

6.4 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, no el interesado. 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, interpreta que los derechos y principios fundamentales establecidos en el RGPD, y 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.

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 enfoque 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, en ningún caso, por ejemplo, la inexistencia o utilización de una determinada base jurídica para un tratamiento. Es decir, la base jurídica no puede suplirse o sustentarse en la concurrencia de medidas alternativas al cumplimiento, incluyendo, en su caso, la necesaria evaluación del interés legítimo.

En definitiva, no sería lícito reemplazar cualquiera de los principios del RGPD mediante medidas técnicas y organizativas encaminadas a reemplazar 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 gestionar 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 de la organización, o un acuerdo contractual que pretenda desplazar las 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 y un posible factor agravante aplicable en caso de infracción.

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 del ciclo de vida del tratamiento.

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

7. EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS

El riesgo en el RGPD tiene varias perspectivas, la primera de ellas es garantizar las medidas de seguridad acordes en cada momento al estado de la tecnología y las condiciones específicas de los tratamientos de datos personales.

Por otra parte, el enfoque del riesgo para garantizar los derechos y libertades de las personas se materializa en la protección de datos desde el diseño y las evaluaciones de impacto en la privacidad. Hablamos nuevamente del principio de proactividad de los responsables de los tratamientos.

La protección de datos desde el diseño consiste en diseñar un producto o sistema de información teniendo en cuenta, incluso antes de su diseño, los requisitos que garantice la protección de datos durante la vida útil del producto o sistema de información.

Las evaluaciones de impacto pueden definirse como un análisis de riesgos de un producto, servicio o sistema que aún no existe y se encuentra ligado a los principios de protección de datos desde el diseño y protección de datos por defecto.

El RGPD recoge las evaluaciones de impacto en su artículo 35:

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

evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
 - evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
 - tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
 - observación sistemática a gran escala de una zona de acceso público.
4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.
5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.
6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.
7. La evaluación deberá incluir como mínimo:
 - una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
 - una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
 - una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
 - las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.
8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.
9. 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.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.
11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento”.

El Grupo del Artículo 29, en el documento [Directrices sobre las Evaluaciones de Impacto en la Protección de Datos](#) introduce criterios que pueden evidenciar un elevado riesgo inherente a las actividades de tratamiento y que, se deben evaluar y pueden determinar la necesidad de realizar las mismas.

Así, podemos citar entre otras:

- Monitorización sistemática (procedimiento utilizado para observar o controlar a los interesados, incluidos los datos recopilados a través de redes o un sistema de control de un área de acceso público);
- Datos relativos a las personas vulnerables (los sujetos de datos vulnerables pueden incluir menores, segmentos más vulnerables de la población que requieren protección especial –personas con enfermedades mentales, solicitantes de asilo o ancianos, pacientes-).
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas (actividades de tratamiento realizadas mediante el uso de tecnología innovadora que pueda implicar nuevas formas de recopilación y uso de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas –por ejemplo, combinación del uso de la huella dactilar y el reconocimiento facial para mejorar el control de acceso físico-).

Estas Evaluaciones deben llevarse a cabo antes del tratamiento. Para facilitar su realización, la AEPD pone a su disposición la herramienta [GESTIONA](#) y ha publicado la [Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD](#).

Por otra parte, señalar que, a la hora de realizar una Evaluación de Impacto de la Protección de Datos, se debe disponer de una metodología que considere los requisitos exigidos por el RGPD en su artículo 35.7, donde se indica que como mínimo será:

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

La estructura con las diferentes etapas de una EIPD y el flujo a seguir en su ejecución podría ser la mostrada en la Figura 1 de la página siguiente.

Del mismo modo que se ha mencionado en el análisis de riesgos, en las evaluaciones de impacto también es necesario tener una política de revisión y análisis de los riesgos continuado, llevando a cabo auditorías periódicas en las que se ponga de manifiesto la eficacia de las medidas que se hayan adoptado para minimizar los riesgos de los tratamientos y en especial los riesgos para los derechos y libertades de los interesados. En definitiva, el enfoque de riesgos implica un proceso de revisión mejora continua de las actividades de tratamiento.

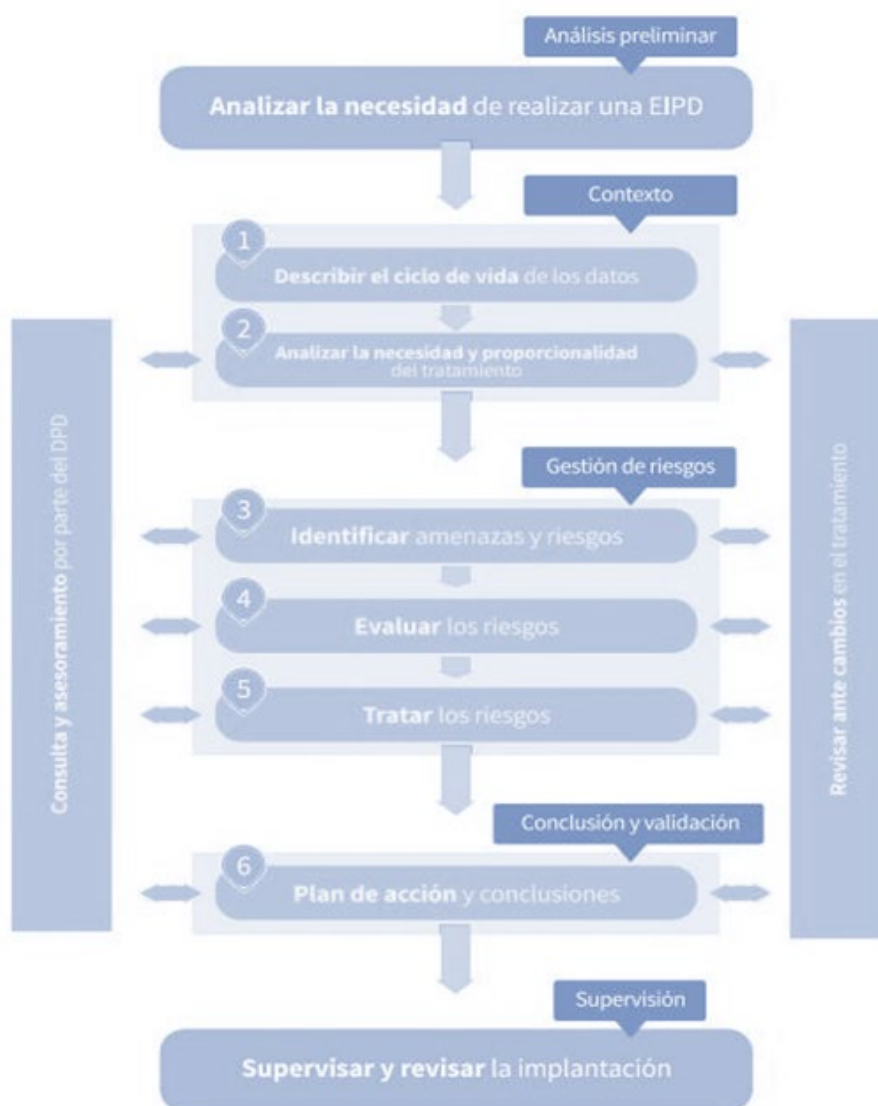


Figura 1 –Fases de realización de una EIPD

8. LA SEGURIDAD EN EL RGPD

8.1 EL PAPEL DE LA SEGURIDAD

La seguridad de la información se orienta a preservar la integridad, la disponibilidad y la confidencialidad de los datos y los sistemas mediante recursos materiales técnicos y organizativos adecuados y proporcionales para conseguir uno o varios objetivos: garantizar la continuidad de negocio, la seguridad del Estado, evitar el fraude, preservar la imagen institucional, o, por ejemplo, garantizar la privacidad.

Cuando nos referimos a **confidencialidad** nos referimos a cualquier medida que impida el acceso no autorizado a los datos personales, mecanismos para evitar la vulneración del deber de secreto o medidas encaminadas para garantizar los privilegios de acceso a la información o los datos personales. Por ejemplo, hablamos de medidas por la que se conceden o deniegan los permisos para acceder a un sistema de información o la gestión de las altas y bajas del personal de una organización. En seguridad se viene refiriendo a la confidencialidad con el principio de la “necesidad de saber” (“need-to-know”) principio mediante el cual únicamente deben acceder a la información aquellas personas que lo precisen en virtud de las funciones que deben desempeñar en su trabajo o su cargo.

La **integridad** de los datos personales o de la información se relaciona con el principio de exactitud o de calidad de los datos. De acuerdo con este principio, el responsable del tratamiento de los datos debe garantizar que aquellos datos que vienen siendo tratados son acordes a la realidad o veraces y adecuados a la finalidad para la que fueron obtenidos y, además, se garantiza su inalterabilidad.

La **disponibilidad** es la característica de la seguridad por la que se intenta mantener los datos accesibles para su consulta, localización y rectificación cuando sea necesario. Dicho de otra forma, esta característica garantiza los derechos de acceso, rectificación, supresión, derecho de limitación del tratamiento y el derecho a la portabilidad de los datos. En definitiva, se trata de una característica de la seguridad estrechamente vinculada a los derechos de los interesados.

El artículo 32 establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas. No se establece un catálogo de medidas de seguridad estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

A las características generales de la seguridad antes mencionadas (confidencialidad, integridad y disponibilidad) el RGPD añade la **resiliencia** de los sistemas y servicios de tratamiento. El RGPD define la resiliencia como la característica de la seguridad que permite garantizar la confidencialidad, la integridad y la disponibilidad de los tratamientos de datos personales, es decir, la característica de la seguridad por la que podemos garantizar la continuidad de un sistema de información o servicio de un tratamiento de datos personales en condiciones adversas.

Es importante destacar que, aunque la seguridad es un elemento necesario, no es suficiente para garantizar los derechos y libertades de las personas con relación a la protección de datos de carácter personal. Las medidas, técnicas y organizativas, para garantizar la seguridad de los datos personales

constituyen parte de las garantías que permiten implementar, de forma efectiva, la protección de datos. Pero para que dichas medidas estén realmente orientadas hacia la privacidad, la seguridad de la información debe ser vista sólo como un paso más en proceso de aplicación de los principios de protección de datos y no como el fin último. Este proceso comienza por el establecimiento de la licitud del tratamiento y continúa con la aplicación de los principios de lealtad, transparencia, finalidad, proporcionalidad, exactitud, limitación, aplicación de derechos, responsabilidad proactiva y, finalmente y derivado de los requisitos fijados, por la implementación de todos los anteriores a través de las medidas de seguridad apropiadas. En ningún caso la seguridad de la información es un elemento previo, ni puede anteponerse o sustituir, al resto de principios.

Con **la visión del riesgo para los derechos y libertades** establecida en el RGPD se permite a los responsables asignar medidas de seguridad de forma dinámica en función de las características y el contexto de cada tratamiento. La **seudonimización**⁹ y la **anonimización**¹⁰ son ejemplos de medidas que pueden ayudar a reducir el nivel de riesgo en los tratamientos realizados.

Cuando el RGPD se refiere a las medidas de seguridad de los tratamientos de datos personales, se refiere tanto a las obligaciones del responsable como a las obligaciones del **encargado o subencargado** del tratamiento. Tanto el encargado del tratamiento como el responsable del tratamiento deben de tener en cuenta el establecimiento de medidas técnicas y organizativas que permitan garantizar la seguridad de los datos personales.

En definitiva, las medidas de seguridad del RGPD son el resultado de lo que se denomina principio de responsabilidad proactiva de los responsables, mediante este principio el RGPD demanda a los responsables una actitud activa frente, entre otras, la adopción de las medidas de seguridad. Se trata de actuar anticipándose a los riesgos y evitando los perjuicios que un determinado tratamiento de datos pueda ocasionar a los interesados, en especial aquellos perjuicios que supongan un daño o un riesgo para sus derechos y libertades.

8.2 EL RESPONSABLE DE SEGURIDAD

Un papel clave en la aplicación de las medidas de seguridad es la figura del responsable de seguridad en las organizaciones. Su designación dentro de una organización debe realizarse mediante su nombramiento correspondiente que será conocido por todo el personal y su papel será el de determinar las decisiones para satisfacer los **requisitos** de seguridad de la información y los servicios (artículo 10, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en adelante ENS).

Por lo tanto, **el papel del responsable de seguridad es distinto al papel que se asigna al Delegado de Protección de Datos (DPD)**, el responsable de seguridad tiene la responsabilidad de aplicar la política de seguridad de los datos del responsable mientras que el papel del DPD está orientado al asesoramiento al

⁹ La seudonimización o disociación de los datos personales, supone eliminar aquellos datos que a priori permiten una identificación de los interesados, dejando accesibles aquellos datos o información personal que se necesita para el tratamiento. Es un mecanismo que oculta la identidad de los interesados pero que es reversible y siempre podremos reidentificar a las personas.

¹⁰ La anonimización es un procedimiento de disociación de la información diseñado para evitar la reidentificación de los interesados. Sin embargo, el propio RGPD también pone de manifiesto los límites de la anonimización de forma que en ningún caso podremos hablar en términos absolutos de datos anónimos y siempre existirá un riesgo de reidentificación de las personas que debe cuantificarse.

responsable para aplicar la política de protección de datos, que incluirá los requisitos de seguridad para la protección de los datos personales.

8.3 EL ESQUEMA NACIONAL DE SEGURIDAD

El artículo 17.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas establece con relación al archivo de documentos que “los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que4 garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.”, esta consideración supone que lo previsto en el ENS es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, y por otra parte añade a la seguridad de la información la dimensión o característica de la **trazabilidad** que en términos prácticos podría decirse que es el factor de la seguridad que permite identificar unívocamente a las personas o procesos que acceden a la información y las acciones que han realizado.

Por su parte el ENS en su artículo 1 establece que está constituido por los “principios básicos y requisitos mínimos para una protección adecuada de la información” que “será aplicado por las Administraciones Públicas para asegurar el **acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios** utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias”. La aplicación de esta norma se refiere a cualquier información en poder de las AA.PP. sin distinción acerca de su contenido, tanto si está constituida por datos personales como por cualquier otra información.

Por los motivos expuestos, la LOPDGDD en su Disposición Adicional Primera sobre las medidas de seguridad en el ámbito del sector público para los tratamientos de datos de carácter personal, determina que el ENS “incluirá las medidas que deban implantarse en caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado, **adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679**”. En definitiva, en cuanto a las medidas de seguridad se refiere, **el ENS es acorde al enfoque de riesgo del RGPD cuando se tiene en cuenta en la selección de sus medidas el riesgo para los derechos y las libertades**, es decir, si no solo tiene en cuenta un análisis del riesgo para la continuidad de los tratamientos o la seguridad de la información y los servicios electrónicos.

8.4 NOTIFICACIONES DE BRECHAS DE SEGURIDAD

La **notificación de las brechas de seguridad** es una obligación del responsable del tratamiento y también del encargado que se desarrolla, fundamentalmente, en los artículos 33 y 34 del RGPD. El artículo 33 se refiere a las obligaciones de notificación del responsable a la Autoridad de Control y del encargado al responsable, mientras que el artículo 34 se refiere a las obligaciones de comunicación al interesado.

Dicha obligación de notificación es más amplia para el responsable. Implícitamente, se está emplazando al responsable para que implemente un procedimiento de gestión de incidentes de seguridad que afecten

a datos de carácter personal, cuyo resultado visible al exterior son las notificaciones tanto de las brechas de seguridad como de las acciones y decisiones relativas a las mismas. Además, establece una obligación para la Autoridad de Control, que es la de, si lo estima oportuno, intervenir de conformidad con las funciones y poderes establecidos en el presente Reglamento.

En primer lugar, es necesario definir qué es una brecha de seguridad y para eso es necesario remitirse al artículo 4.12, según el cual: “Es 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 autorizado a dichos datos”.

En caso de que el encargado del tratamiento sufra una brecha de seguridad, éste debe notificar sin dilación al responsable la existencia de la misma. El RGPD no indica ni el formato de dicha notificación ni el plazo máximo para que ésta se realice, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la brecha de seguridad. Por lo tanto, el responsable deberá fijar las obligaciones de notificación del encargado, de tal forma que le permitan cumplir con los requisitos que a dicho responsable sí obliga el RGPD, en particular, en relación con los datos que es necesario notificar a terceros.

El responsable ha de notificar la brecha de seguridad, siempre que exista riesgo para los derechos y libertades de las personas, riesgo que ha de ser evaluado por él. El Comité Europeo de Protección de Datos será el encargado de emitir las guías, recomendaciones o directrices para determinar los niveles de riesgo y las condiciones de la comunicación.

Por otro lado, el artículo 40 relativo a códigos de conducta permite establecer condiciones de aplicación para la obligación de notificación de las brechas de seguridad de los adheridos a los códigos. En este caso, también es necesario contemplar lo establecido en el Considerando 85 donde establece un caso específico sobre la excepción de informar a las autoridades de control y éste es que, atendiendo al principio de responsabilidad proactiva, el responsable pueda demostrar la improbabilidad de que la brecha de seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable debe notificar la brecha de seguridad a la autoridad competente y comunicarla a los interesados que, en el primer caso, en relación con las Administraciones Públicas, y sin menoscabo de lo establecido en la normativa nacional en relación con las competencias de las autoridades autonómicas de protección de datos, será la Agencia Española de Protección de Datos.

La comunicación a los interesados ha de realizarse en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la notificación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir brechas de seguridad de los datos personales continuas o similares.

A pesar de ello, el RGPD establece una serie de excepciones a la necesidad de comunicar la brecha a los interesados:

- Cuando el responsable haya adoptado las medidas de protección técnicas y organizativas apropiadas y éstas se hayan aplicado a los datos personales afectados por la brecha de seguridad,

en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como puede ser el caso de que estén cifrados.

- Cuando el responsable haya tomado medidas ulteriores que garanticen que ya no existe la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
- Cuando dicha comunicación suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de forma igualmente efectiva a los interesados.

Hay que tener en cuenta que la decisión del responsable de no comunicar a los interesados puede ser revocada por la Autoridad de Control y ésta exigir que dicha comunicación se ejecute.

La notificación a la Autoridad de Control se ha de producir antes de las 72 horas, es decir, en los tres días siguientes al conocimiento por el responsable de la existencia del incidente de seguridad. Por tanto, hasta que no exista evidencia de conocimiento por el responsable de la existencia de una brecha de seguridad no se inicia el cómputo de los plazos. Pero la norma deja abierta la posibilidad de una notificación más allá de las 72 horas, y además de forma genérica, sin establecer ninguna condición o restricción, tan sólo la obligación de adjuntar a la notificación una justificación de dicha dilación.

La comunicación a los interesados no tiene un plazo temporal establecido en el RGPD, sólo se señala que debe producirse cuanto antes, teniendo en cuenta, en particular, la naturaleza y gravedad de la brecha y sus efectos adversos para el interesado.

La comunicación de la brecha a la Autoridad de Control va más allá de la mera indicación de que la misma se ha producido. Al contrario, el RGPD detalla un conjunto de datos que es obligado incorporar como mínimo:

- Una descripción de la naturaleza de la misma. Para ello hay que incluir, siempre que sea posible:
 - Las categorías de interesados afectados, es decir, qué tipo de personas han sido afectadas por la brecha. Esta clasificación puede atender a la vulnerabilidad de los interesados, como menores o discapacitados, a la relación con la empresa, como clientes o empleados, o a la relevancia de los sujetos, como podría ser jueces o policías.
 - El número aproximado de interesados afectados. Será recomendable desglosar ese número por las categorías anteriores.
 - Las categorías de datos comprometidos. No es necesario una descripción exhaustiva de los distintos campos de datos, sino una descripción genérica de los mismos, teniendo especial cuidado de señalar aquellos que sean de especial sensibilidad.
 - El número aproximado de registros de datos personales afectados.
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o, en su caso, de otro punto de contacto en el que pueda obtenerse más información. Estas opciones no son exclusivas.
- Describir las posibles consecuencias de la brecha.
- Describir las medidas adoptadas o propuestas por el responsable para mitigar los posibles efectos negativos de la brecha.

Destacar que esta información es un mínimo, no un máximo. En particular, hay que destacar que otra información de interés es la relativa a cuándo se ha producido la brecha, su extensión en el tiempo, la información técnica o procedimental relativa a la causa, etc. Por otro lado, también hay que informar de la

política de comunicación a los interesados que ha establecido el responsable y las razones para implementarla en cuanto a si se ha realizado esa comunicación, la información revelada, temporización de la información, canales utilizados, nivel de cobertura del conjunto de interesados potencialmente afectados, etc.

Gran parte de esta información no se podrá proporcionar en ese plazo de 72 horas, por lo que el RGPD establece la prioridad de realizar una notificación a la Autoridad en dicho plazo, aunque sea incompleta, y la obligación de mantener informada a la Autoridad de los nuevos datos que relativos a la brecha vayan apareciendo. La AEPD y sus funcionarios tienen la obligación de guardar secreto de la información recibida en el marco de sus actuaciones.

Al interesado se ha de comunicar tanto el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información sobre las posibles consecuencias de la brecha, así como de las medidas adoptadas o propuestas por el responsable para mitigar los posibles efectos negativos. Esta información ha de trasladarse al interesado con un lenguaje claro y sencillo, por lo que tendrá que adecuarse a la categoría del sujeto y su capacidad para entender la información que se le está suministrado. El objetivo de esta notificación es que el interesado pueda conocer las implicaciones de lo que ha pasado y qué medidas personales, para proteger sus derechos, puede adoptar. Por lo tanto, ha de ser una información eminentemente práctica.

El responsable ha de implementar un procedimiento documentado de gestión de las brechas de seguridad, que registrará todos los hechos relacionados con ellas, no sólo la información anteriormente señalada, sino cuándo, cómo y dónde se ha producido la brecha, el personal o entidades implicadas, los sistemas afectados, etc. Además, hay que incluir una evaluación de si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para su detección. Hay que documentar también los efectos producidos por la brecha y qué medidas correctivas se han adoptado tanto para minimizar sus efectos como para evitar que vuelva a producirse. Toda esta información ha de ponerse a disposición de las Autoridades de Control en su misión de verificar, si procede, la diligencia del responsable en el tratamiento de los datos y en la gestión de la brecha de seguridad.

Para una información más detallada, la Agencia ha publicado la [Guía para la gestión y notificación de brechas de seguridad](#).