EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Módulo 3.Las Administraciones públicas como responsables en el RGPD. Relaciones con sus encargados de tratamientos.

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Contenido

Este curso ha sido cedido por el Instituto Nacional de Administración Pública 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.

3.1. EL PRINCIPIO DE RESPONSABILIDAD ACTIVA.

El **concepto de responsabilidad proactiva** se establece en el artículo 5 del RGPD, en el que se definen el conjunto de principios que se han 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 a 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.

Si nos remitimos a la definición que encontramos en el diccionario Oxford, "accountability" es la situación o el estado por el cual está claramente identificado el responsable de las acciones que se toman en la organización. Y añade que, en relación a estas acciones, dicho responsable puede proporcionar una explicación, satisfactoria y demostrable, del por qué, y con qué base legal o sobre qué principios, se tomaron dichas acciones.

Desde el punto de vista de la cultura empresarial, y utilizado el término en castellano plasmado en el RGPD, la responsabilidad proactiva está en boga en las compañías actuales, y se define como la obligación y posibilidad de responder de las acciones tomadas, y de las consecuencias, positivas o negativas, de las mismas. La responsabilidad proactiva se establece, además, a distintos niveles: a nivel de la entidad como un todo, a nivel de los distintos escalones de responsabilidad, hasta finalmente a nivel del individuo. La responsabilidad proactiva es, por tanto, una característica intrínseca de la organización.

El RGPD introduce un cambio importante en la forma en la que un responsable del tratamiento ha de enfrentarse a sus obligaciones en relación a la protección de datos de carácter personal. **Mientras que la Directiva 95/46/CE utiliza una aproximación hacia la adecuación normativa basada en gran medida en una lógica de declaración de los procedimientos en avance, el RGPD se basa en un principio de autoanálisis, crítico, continuo, "traceable" y basado en la responsabilidad, que permita implementar una verdadera gobernanza de datos personales en el seno de las empresas**.

"Traceable" 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, porqué tomó esas decisiones, que

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 a la implementación de la responsabilidad proactiva es el del compromiso de los miembros de la organización, ya que el principio de responsabilidad proactiva involucra 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, como hacía la Directiva, que nos remitía a ese momento inicial y declarativo de la creación del fichero**. 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 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 implementación del **principio de transparencia** del responsable hacia el sujeto de los datos en relación al conjunto de tratamientos realizados y los datos recogidos, especialmente en el caso de enriquecimiento de datos y las subcontrataciones realizadas, incluyendo las transferencias internacionales.
- El **ejercicio de los derechos** reconocidos a los sujetos de los datos, en particular los derechos de acceso a los datos almacenados por el responsable, rectificación de los datos erróneos y cancelación de los datos no necesarios.
- 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**, obligación que sustituye a la de la notificación de ficheros a la Autoridad de Control, 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 a 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 el mismo puede ocasionar a la privacidad, intimida 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

libertadas 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 sobre la libertad de los tratamientos puedan acarrear dichos productos o servicios o en el caso de que se ha puesto en duda la legitimidad del tratamiento debido, por ejemplo, a una denuncia de un sujeto de los datos.

- Los resultados obtenidos en dicho análisis son aquellos que se tienen que utilizar como entrada en tres de los procesos definidos en el RGP: los **análisis de riesgos de seguridad, los requisitos de privacidad desde el diseño y los de privacidad por defecto**.
- La **implementación de las medidas de seguridad identificadas** como resultado del análisis de riesgo, lo que implica el mantenimiento de las mismas y la definición de un ciclo de vida implementado de forma "traceable" para realizar su seguimiento en el tiempo.
- En relación a la implementación de medidas de seguridad, 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.
- 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.
- 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.

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 forman 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 Considerando 85. Dicha referencia se realiza en relación a la comunicación de brechas de seguridad y, en particular, a la excepción de la 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 violación 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 a 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 que el impacto de la

misma es mínimo. La seguridad de ese conocimiento se fundamenta en el control efectivo y real de los procesos de datos personales.

3.2. RELACIONES RESPONSABLE VS ENCARGADO. ESPECIAL REFERENCIA A LAS ADMINISTRACIONES PÚBLICAS.

Para estudiar las relaciones entre el responsable del tratamiento y el encargado de tratamiento en el ámbito de las Administraciones públicas, debemos partir, en primer lugar, en las definiciones que al respecto establece el RGPD. En segundo lugar se mostrará como estructura la relación entre ambos la legislación en vigor, la LOPD y el RLOPD, 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"***, según el RGPD:

"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 en la todavía vigente LOPD, donde las relaciones entre el responsable y el encargado aparecen reflejadas en el artículo 12, exigiendo la celebración de un contrato o acto jurídico similar por escrito o incluso formato electrónico que los vincule. El encargado actúa de acuerdo a lo estipulado por el responsable que es quien *decide sobre la finalidad, contenido y uso del tratamiento.*

Según el citado artículo 12 de la LOPD, apartados 2, 3 y 4:

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

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 26ª del Texto Refundido de la Ley de Contratos del Sector Público, Real Decreto Legislativo 3/2011 de 14 de noviembre, 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 y 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 competencias*[1] que aparecen reflejadas en una normada de carácter reglamentario-

[1] Este supuesto específico ha sido analizado por el siguiente informe jurídico de la AEPD: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2012-0333_Encargado-del-tratamiento-en-virtud-de-atribuci-oo-n-de-competencias..pdf

organizativo, como pueden ser un Real Decreto (Administración General del Estado) o Decreto (Comunidad Autónoma) de estructura.

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 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. 12.2 LOPD.

Además de este supuesto específico, 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.

Por otra parte, la aplicación del RGPD no modifica las relaciones entre responsable y encargado o las cuestiones a tener en cuenta. El contenido mínimo del contrato contendrá 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 Capítulo IV del ALOPD, 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.

Asimismo, la aplicación del RGPD a partir del 25 de mayo de 2018 supone, que los contratos ya existentes con encargados de tratamiento con vocación de prolongarse en el tiempo, para que sean conformes a la nueva norma europea, deben adecuarse, incluyendo las cláusulas con el contenido mínimo al que nos hemos referido anteriormente.

Para facilitar esta labor de adecuación, así como ayudar en la elaboración de este tipo de contratos una vez que se aplicable el RGPD, 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, señalar que el Anteproyecto de Ley Orgánica de Protección de Datos que se está tramitando incluye la siguiente Disposición Adicional Primera:

El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, 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.

3.3. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO.

3.3.1. INTRODUCCIÓN.

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.

3.3.2. PROTECCIÓN DE DATOS DESDE EL DISEÑO.

De conformidad con el apartado 1 del artículo 25, se puede establecer que el principio de **protección de datos desde el diseño** tiene como objetivo cumplir los requisitos definidos en el RGPD y por tanto, los derechos de los interesados. La palabra "requisito" utilizada en el artículo es de capital importancia, ya que implica que lo establecido en el RGPD ha de servir como entrada al conjunto de requisitos que se utilizarán para definir, es su estado inicial, la funcionalidad de un producto, servicio o aplicación de tratamiento de datos. La protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar sucesivas etapas de desarrollo.

De esta forma, la protección de datos no es algo a considerar una vez se tiene el producto encima de la mesa, sino que se ha de plantear incluso antes de que éste este en el tablero de diseño. Las medidas que permiten garantizar la protección de datos no son una capa añadida al tratamiento, un envoltorio o una funcionalidad posterior, sino

que están íntimamente incluidas en el mismo, formando parte integral del espíritu de su diseño, de forma que no es un elemento identificable que se pueda quitar o poner, sino que está impregnando toda su estructura.

Por supuesto, estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento. Es importante recalcar que la implementación de un tratamiento no descansa únicamente en un conjunto de productos hardware o software, sino que un tratamiento es un sistema formado por máquinas, personas, la interacción entre ambas y los modos de utilización y de uso. Estos tres últimos elementos se definen en las medidas organizativas.

Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore medidas para la **seudoanonimización** temprana de los datos personales o la minimización de datos.

La seudoanonimización se define en el apartado 5 del artículo 4 como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, y siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

La minimización de datos no se encuentra explícitamente definida en el RGPD, pero se interpreta en el sentido de que los datos personales objeto de tratamiento deben ser adecuados, relevantes y limitados a los que sean necesarios en relación con la finalidad del tratamiento. Ambas medidas han de incorporarse en la implementación de los tratamientos, de forma que la disociación de los datos identificativos del resto de datos forme para en sí del proceso.

No hay que olvidar que muchos tratamientos se siguen realizando en papel, parte de ellos realizando copias o utilizando el soporte de impresión como copias temporales de trabajo, y que dicha forma de trabajo ha de contemplarse a la hora de diseñar el proceso global.

La obligación de que se adopten los principios de privacidad desde el diseño recae en el responsable del tratamiento. El responsable del tratamiento podrá subcontratar tanto el desarrollo como la implementación de una parte o de la totalidad del tratamiento. En ese caso, haciendo ejercicio de sus obligaciones, debe reflejar contractualmente los requisitos que garanticen la protección de los derechos de los sujetos de los datos y hacer seguimiento de que dichos requisitos han sido efectivamente traducidos a decisiones de diseño y que son funcionales. En el caso de adquisición de productos o contratación de servicios que sean utilizados para la implementación de un tratamiento, entre los elementos que se utilizarán para determinación de la elección entre los disponibles en el mercado ha de figurar, con un peso significativo, sino crítico, el hecho de que se pueda demostrar que en su desarrollo se han implementado los principios de privacidad desde el diseño.

Sea cual sea la forma de subcontratación o adquisición, el responsable nunca podrá delegar completamente sus obligaciones de aplicación de este principio, ya que siempre quedará bajo su poder de decisión al menos aquellas medidas organizativas que le compete tomar para interaccionar con el servicio subcontratado.

La selección de las medidas serán resultado de un análisis de riesgos en relación a la probabilidad y gravedad de que afecten a los derechos y libertades de las personas físicas y se aplicarán teniendo en cuenta el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento.

3.3.3. 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", como a una nueva extensión de ese principio que podríamos denominar el "need-to-disclosure".

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.

3.3.4. 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.

3.4. DEL REGISTRO DE FICHEROS AL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO.

A partir del 25 de mayo de 2018, fecha en que el RGPD será aplicable, desaparecerá la primera de las obligaciones a realizar por parte del responsable que trata datos de carácter personal con la LOPD: la notificación de ficheros ante el Registro General de Protección de Datos.

Las dos normas de aplicación en España en materia de protección de datos de carácter personal desde 1992, la LORTAD y la LOPD, habían previsto como primera obligación del responsable la comunicación a la Agencia de los ficheros que emplea en su actividad y que contengan datos de carácter personal, informando, de acuerdo al artículo 26 de la LOPD, sobre el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países fuera del Espacio Económico Europeo.

La obligación, que en el caso de ficheros correspondientes a las administraciones públicas comienza por la publicación en el correspondiente Diario Oficial, de acuerdo en lo estipulado en el artículo 20 de la LOPD y los artículos del 52 al 54 del RLOPD, de la descripción del fichero por parte del órgano responsable. Acción esta que, además de convertirse en la puerta de entrada al mundo de la protección de datos mostraba la legitimación de unos tratamientos a realizar, respaldados en una Orden Ministerial, una Orden de Consejero, o una Ordenanza en el ámbito local.

A 30 de junio de 2017 el Registro General de Protección de Datos cuenta con más de 4.700.000 ficheros inscritos, correspondientes a más de 1.600.000 entidades privadas y Administraciones públicas.

Si bien esta inscripción de ficheros desaparece, el RGPD regula en su artículo 30 el denominado **"Registro de actividades de tratamiento"** de la siguiente forma:

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:*
    a. *el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;*
    b. *los fines del tratamiento;*
    c. *una descripción de las categorías de interesados y de las categorías de datos personales;*
    d. *las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
    e. *en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo[2], la documentación de garantías adecuadas;*
    f. *cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;*
    g. *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1[3].*
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:*

[2] Artículo 49 del 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".*

[3] 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 del Anteproyecto de Ley Orgánica de Protección de Datos y que ya se especificado en el apartado anterior.

a. *el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;*

b. *las categorías de tratamientos efectuados por cuenta de cada responsable;*

c. *en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*

d. *cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.*

3. *Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.*

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.*

Es en este punto donde la existencia del Registro de Ficheros puede convertirse en una herramienta de ayuda y un punto de partida ante la tarea que ahora debe acometer. El responsable hizo en su día un ejercicio de descripción de los tratamientos de datos de carácter personal que realizaba cuando se vio en la obligación de realizar la Notificación de sus ficheros. En el caso de las Administraciones públicas las obligaciones previas a la notificación incluían un ejercicio severo de descripción exhaustiva y descripción de la legitimación que justifica el tratamiento.

Será evidente el paso de ese conjunto de ficheros a la elaboración del *Registro de las actividades del tratamiento* y la puesta al día de sus obligaciones en materia de protección de datos, pero con el contenido que ahora determina el RGPD, puesto que se añaden algunos elementos que no se exige en la actual notificación de ficheros, como puede ser los plazos previstos para la supresión de las diferentes categorías de datos, o la identificación del Delegado de Protección de Datos, si hubiese sido nombrado.

Cabe señalar que el artículo 33.2 de la redacción actual del Anteproyecto de Ley Orgánica de Protección de Datos establece que *"ciertos sujetos*[4] *harán público un*

[4] [4] El Artículo 77.1 de la actual redacción del ALOPD "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" habla de 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.

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".

Así pues parece claro que todos los tratamientos realizados por las Administraciones públicas se llevarán a cabo mostrando su legitimidad, de modo análogo, en cierta forma a la publicación de la Disposición correspondiente, como la actual LOPD dicta; además se les dará publicidad a través de la página Web de la administración pública a la que correspondiera para que el ciudadano pueda tener constancia de la base jurídica de los tratamientos a los que sus datos estén sometidos.

Por último señalar que *"Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida en el artículo 30 del Reglamento (UE) 2016/679"* ha sido descrita, por el Artículo 74 del mencionado Anteproyecto de Ley, como infracción leve.

3.5. LA SEGURIDAD EN EL RGPD.

3.5.1. INTRODUCCIÓN.

La protección de datos se articula en un conjunto de principios básicos entre los que se encuentran las obligaciones de los responsables de proteger la información. Las medidas de seguridad son herramientas que permiten alcanzar este objetivo de proteger la información, pero tenemos que ser conscientes que todos manejamos diariamente nuestros datos y nuestra información personal y la seguridad de los datos personales no puede articularse exclusivamente desde el punto de vista de los responsables. La seguridad de los datos personales tiene, al menos, dos enfoques: uno el que corresponde a los responsables de los tratamientos y otro el que corresponde a los propios interesados e interesadas.

Diariamente manejamos nuestra información personal, navegamos por internet, instalamos apps en nuestros dispositivos móviles, accedemos a redes sociales, realizamos compras online, dejamos nuestras opiniones en foros y blogs, utilizamos el correo electrónico, utilizamos programas de mensajería instantánea, etc. Cada día son más los servicios electrónicos de los que disponemos y cada vez es más fácil su

---

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.

utilización y en cada uno de estos servicios dejamos información personal que suele ser utilizada con fines publicitarios.

Toda la información que dejamos online forma parte de lo que llamamos nuestra huella digital, que habla de nosotros y marca nuestra reputación digital que no es más que una parte de nuestra reputación social. Nuestra huella digital se asocia a nuestra persona y es necesario ser conscientes de los riesgos que esto puede implicar hacia nosotros y, en general, para nuestros derechos y libertades.

Los servicios online forman parte de nuestra vida ya que, para cualquier actividad o información que necesitemos, la realidad digital nos otorga libertad para elegir e informarnos de forma global, pero es preciso conocer la existencia de riesgos para nuestra información personal y entender cómo evitarlos. El mundo digital no es muy distinto del mundo real, los engaños también están presentes y con frecuencia su objetivo es la obtención de nuestra información personal.

Por ejemplo, el uso del Smartphone está generalizado y es un dispositivo en el que se almacena gran cantidad de información personal, es la puerta de entrada a la mayoría de servicios digitales de los que somos usuarios y se convierte en uno de los puntos más importantes a la hora de proteger nuestra información personal.

Por estas razones, la AEPD en colaboración con INCIBE (Instituto Nacional de Ciberseguridad) ha desarrollado una serie de fichas temáticas agrupadas en la "Guía de Privacidad y Seguridad en Internet" con el objetivo de dar a conocer los riesgos más frecuentes para nuestra información personal y la forma de evitarlos en la medida posible.

En esta guía se facilitan orientaciones para proteger la información que almacenamos en nuestros dispositivos, ayudas para gestionar nuestras contraseñas, recomendaciones para evitar utilizar páginas que suplantan la identidad de un sitio web, explicamos la forma de eliminar nuestros datos personales de los buscadores de internet, cómo evitar timos y engaños en internet como por ejemplo el "phising" o el "ransomware".

Con esta iniciativa desde la AEPD ponemos a disposición del usuario de servicios digitales un texto que pretende dar a conocer riesgos tecnológicos con un lenguaje asequible, dando al mismo tiempo soluciones para mitigar o evitar estos riesgos además de ilustrar algunas de las consecuencias negativas de las que podríamos ser víctimas.

Por otra parte, con frecuencia nos referimos a los "nativos digitales" como a aquellas personas que han nacido en la era digital, con una capacidad natural para manejar dispositivos electrónicos y utilizar programas y herramientas digitales, pero esta capacidad natural no evita que sea necesaria la educación digital de la misma manera que es necesaria la educación vial o la educación en cualquier otro contexto en el que se desarrolla el menor.

Por este motivo, desde la AEPD entendemos que la educación digital y la concienciación del menor son uno de los factores más importantes para garantizar la seguridad de su información personal en el mundo digital y de la información personal que ellos manejan de otras personas cuando comparten información en la red (videos,

fotos, etc.). Con estos objetivos la AEPD ha creado el espacio web www.tudecideseninternet.es en el que se ponen a disposición del menor recursos que pueden ser útiles para la labor de concienciación y educación digital y recursos para el personal próximo al menor como educadores o familiares. La AEPD ha publicado dos guías en formato ficha que se pretende sean útiles para facilitar la concienciación de del menor en su actividad online, cada una de estas guías se componen de una parte orientada al menor y otra orientada al educador o al adulto próximo al menor.

El factor de concienciación del menor es fundamental de cara a proteger su privacidad e incluso su seguridad. En buena parte de los delitos en los que puede verse implicado un menor como víctima o como responsable existe con frecuencia un denominador común: la información personal. Ciberbulliying, ciberbaiting, sexting y grooming son algunos ejemplos.

3.5.2. PRINCIPIOS BÁSICOS DE LA SEGURIDAD.

Como ya se ha comentado las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos, no es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de nuestros datos. Para garantizar estos tres factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo, además, en ocasiones será también necesario tener en cuenta medidas de seguridad física como la presencia de un servicio de seguridad o un sistema de control de accesos que nos asegure quienes son las personas o procesos que acceden a la información en un momento determinado.

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, derecho a la portabilidad de los datos, 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.

3.5.3. RGPD Y SEGURIDAD.

El artículo 32 del RGPD 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 establecen medidas de seguridad estáticas, 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.

En definitiva el primer paso para determinar las medidas de seguridad será la **evaluación del riesgo**, una vez evaluado el riesgo será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

Una de las medidas que pueden contribuir a reducir el nivel del riesgo es la **seudonimización**. 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. Cuando hablamos de seudonimización siempre hay que tener en cuenta que se trata de un mecanismo que oculta la identidad de los interesados pero este ocultamiento de la identidad es reversible y siempre podremos reidentificar a las personas. Frente a la seudonimización hablamos de **anonimización** cuando el procedimiento para disociar la información está diseñado para evitar la reidentificación de los interesados e interesadas, 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, siempre existirá un riesgo de reidentificación de las personas.

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.

Cuando el sistema de información o servicio del tratamiento de datos personales no es capaz de garantizar su funcionamiento se produce una pérdida de servicio, como por ejemplo en caso de un ciberataque. Otro de los parámetros o características de la seguridad en el RGPD es la **capacidad de restaurar la vuelta a la normalidad** del sistema de información o servicio de tratamiento, o la capacidad de recuperar el funcionamiento normal del sistema de información o servicio de tratamiento.

Para acreditar el cumplimiento de los requisitos de seguridad que establece el RGPD, el artículo 32.3 permite a los responsables de los tratamientos la posibilidad de utilizar **mecanismos de certificación** para garantizar y demostrar el cumplimiento de los

requisitos de seguridad, o la adopción de un **código de conducta**. Mediante un mecanismo de certificación, un tercero examina las medidas de seguridad implantadas por el responsable del tratamiento y evalúa los riesgos con el fin de determinar si dichas medidas de seguridad son acordes a los riesgos implícitos en el tratamiento, mediante un código de conducta estaríamos hablando de un tratamiento de datos tipo con un catálogo de riesgos definido, sobre este catálogo de riesgos el responsable añadiría sus propios riesgos derivados de sus especificidades en el tratamiento para, finalmente, establecer las medidas o controles de seguridad encaminados a garantizar la seguridad del tratamiento. La certificación y los códigos de conducta pueden ser herramientas útiles para el cumplimiento de lo previsto en el RGPD en cuanto a medidas de seguridad pero no exime a los responsables del enfoque de riesgo.

El RGPD no fija unas medidas de seguridad únicamente en consonancia con la sensibilidad de los datos utilizados en un determinado tratamiento, **la visión del riesgo** permite a los responsables asignar medidas de seguridad de forma dinámica en función de las características y el contexto de cada tratamiento.

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 e interesadas, en especial aquellos perjuicios que supongan un daño o un riesgo para sus derechos y libertades.

3.5.4. 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 de 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 decide sobre las medidas de seguridad mientras que el papel del DPD está orientado al asesoramiento al responsable: informar, asesorar, supervisar el cumplimiento, cooperar con la autoridad de control, etc. en lo que concierte a los tratamientos de datos personales.

3.5.5. 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, que 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, en el momento de elaborar los contenidos de este curso, el anteproyecto de la LOPD 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 de carácter personal, 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 RGPD. En definitiva, en cuanto a las medidas de seguridad se refiere, **el ENS es acorde al enfoque de riesgo del RGPD** y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las AA.PP.

3.6. ENFOQUE Y ANÁLISIS DEL RIESGO.

3.6.1. INTRODUCCIÓN.

Hasta ahora hemos visto que el enfoque de riesgos está estrechamente relacionado con las medidas de seguridad, pero esta es una única visión del enfoque de riesgos del RGPD. El enfoque de riesgos del RGPD tiene una mayor utilidad que la que se refiere a la determinación de las medidas o controles de seguridad, antes de entrar en este detalle es necesario conocer más en detalle algunos conceptos relacionados con el riesgo.

El riesgo es un elemento con el que convivimos habitualmente, cualquier actividad que realizamos tiene implícito un riesgo. Las modalidades del riesgo son tan variadas como nuestra propia actividad, algunos de los riesgos que habitualmente son analizados pueden ser: de negocio, laborales, corporativos, de salud, medioambientales, riesgos para la seguridad de la información, etc. A esta variedad de riesgos cabría añadir una nueva vertiente: los **riesgos para los derechos y libertades de las personas** derivados de los tratamientos de datos personales.

Algunos de los riesgos para los derechos y libertades de las personas que podrían estar implícitos en los tratamientos de datos personales y que pone de manifiesto el considerando 75 del RGPD son: daños y perjuicios físicos, discriminación, usurpación de identidad, reputación, confidencialidad, perjuicio social. Esta sería una muestra inicial de los riesgos de los tratamientos de datos para los derechos y libertades de las personas, habría que tener en cuenta que el mismo riesgo no tendría las mismas consecuencias en los derechos y libertades de todas las personas, por ejemplo, el aislamiento social en un menor podría tener unas consecuencias distintas que el que pudiera producirse en un anciano, en el caso del menor este riesgo de aislamiento social o discriminación podría condicionar su desarrollo como persona mientras que el anciano o adulto, aunque inicialmente el impacto es el mismo, las consecuencias para su desarrollo como persona son más limitadas que en el caso de un menor.

Esta es el nuevo enfoque de riesgos que aporta el RGPD, no se trata de evaluar las consecuencias que podría tener un riesgo para mi negocio, mi salud, mi información como responsable, etc. en esta ocasión se trata de evaluar el riesgo que tiene un tratamiento de datos para un tercero, los riesgos o consecuencias que podría tener un tratamiento de datos que no fuera realizado de acuerdo a lo previsto en el RGPD. Por ejemplo, si no garantizo la confidencialidad de los expedientes médicos y se produce una vulneración del deber de secreto, esta circunstancia podría acarrear consecuencias negativas para mí como responsable pero las consecuencias para las personas cuyos datos hubieran sido revelados y el impacto en sus vidas podría tener consecuencias impredecibles, imaginemos lo que podría suponer para una persona que públicamente fuera conocidas sus limitaciones cognitivas, tal vez estaríamos limitando su libertad para encontrar un trabajo o para relacionarse con otras personas porque podría estar expuesta a un aislamiento social con consecuencias poco favorecedoras para ejercer sus derechos y libertades como persona.

Cuando hablamos de riesgos siempre tenemos que tener en cuenta tres conceptos básicos, lo que protegemos (**el activo**), aquello de lo que pretendemos proteger al activo (**la amenaza**) y lo que pretendemos evitar (**el impacto**). Las amenazas frecuentes para la seguridad de la información pueden ser: naturales, fallos de infraestructura, error humano, vulnerabilidades frente ataques, falta de formación y concienciación de las personas, etc.

Por otra parte, **la cuantificación del riesgo** es el resultado de multiplicar el impacto que tendría una amenaza por la probabilidad de que esta amenaza llegue a materializarse:

RIESGO=IMPACTO x PROBABILIDAD

Por ejemplo, cuando el impacto es muy alto y la probabilidad de que una amenaza se materialice también es alta, tendremos un nivel de riesgo muy alto. En definitiva, estamos manejando una escala con unos valores que serán específicos en cada organización. La importancia del impacto tiene en cuenta dos tipos de daños, el daño sobre los bienes materiales o tangibles y el daño sobre los bienes intangibles. Por ejemplo, la falta de medidas de seguridad podría dar lugar a la pérdida de datos personales en una empresa, esta pérdida repercutiría sobre el negocio generando pérdidas materiales, pero con frecuencia puede ocurrir que se produzca también la pérdida de clientes o pérdida de negocio ya que esta posible negligencia implicaría una mala imagen para la entidad y posiblemente los clientes buscarían una alternativa más negligente o con mayores garantías para sus datos personales. A la posible lista de daños intangibles sería necesario añadir también la lista de daños o consecuencias para los derechos y libertades de las personas afectadas por esta posible negligencia de un responsable.

Con frecuencia el riesgo se mide con valores numéricos, **valoración cuantitativa**, pero también es posible trasladar el valor cuantitativo a una escala más comprensible con valores del tipo: escaso, medio, alto, no admisible. En definitiva son escalas de referencia que nos permiten disponer de valores con los que medir el riesgo, dicho de otra forma, la valoración de los riesgos nos permite pasar de una referencia abstracta y a veces subjetiva del riesgo a un valor concreto.

3.6.2. ANÁLISIS Y GESTIÓN DEL RIESGO.

Analizar el riesgo no serviría de nada si posteriormente no se realiza un esfuerzo para evitarlo, reducirlo o mitigarlo, transferirlo o aceptarlo. En general estas son las estrategias básicas para tratar el riesgo, en el mejor de los casos siempre habrá un riesgo residual o umbral de riesgo con el que tendremos que convivir. La actividad por la que evitamos, reducimos o mitigamos el riesgo, lo transferimos o aceptamos es la "gestión del riesgo".

Un análisis de riesgo es una **actividad sistemática** por la que se pretende identificar cada uno de los riesgos implícitos en una determinada actividad. Los riesgos no son estáticos, evolucionan según el estado de la tecnología y las situaciones específicas de cada tratamiento de datos personales, cada organización debería de tener una política de riesgos corporativa o un marco en el que se identifique a los responsables del

análisis, los recursos, los procesos, los activos, la metodología necesaria para realizar el análisis de riesgos, las herramientas necesarias, la gestión del riesgo, la periodicidad de los análisis, las medidas de seguimiento, las legislaciones aplicables, la formación del personal, etc.

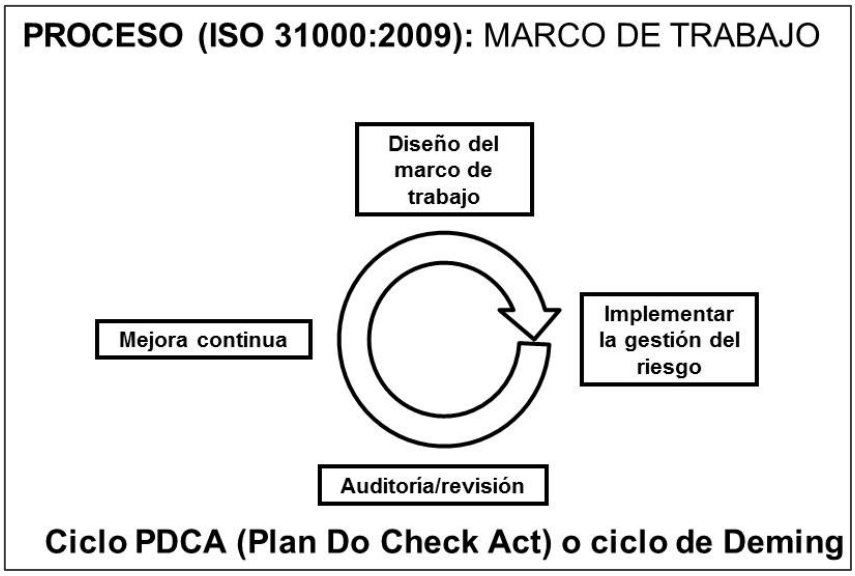
Para poder establecer el marco de referencia del análisis y la gestión del riesgo en una organización, pueden utilizarse **normas y metodologías** como las siguientes:

- Las normas ISO 31000 Y 31010, son normas generales que pueden servir de ayuda para configurar el marco de referencia para el análisis de riesgos en general.
- La norma ISO 27005 es una norma que puede utilizarse como marco para el análisis de riesgos para la seguridad de la información.
- La metodología MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

A modo de ejemplo, la norma ISO 31000 define el proceso del análisis y la gestión de riesgos en cuatro fases:

- Diseño y definición del marco de trabajo
- Implementar y gestionar el riesgo
- Verificar los resultados mediante procesos de auditoría
- Añadir mejoras al marco inicial del trabajo

La propuesta de esta norma, similar a cualquier metodología de análisis y gestión del riesgo, se basa en un sistema de mejora continua de la calidad. Un sistema en permanente evolución que técnicamente se conoce como ciclo PDCA o ciclo de Deming:



En otros términos podemos decir que el riesgo es cambiante según el entorno (marco físico, tecnológico, intervención humana, etc.) y la adecuación de las medidas para paliar riesgos también debe de ser cambiante y en permanente adecuación y revisión. El proceso por el que se revisan las medidas para paliar los riesgos se denomina **auditoría** y es un mecanismo básico y necesario para garantizar la efectividad de las

medidas para la seguridad de los tratamientos de datos y garantizar los derechos y libertades de las personas.

3.7. NOTIFICACIONES DE BRECHAS DE SEGURIDAD.

La **notificación de las violaciones 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 notificación al interesado.

Pero lo que subyace a dicha obligación de notificación es una obligación 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 seguridad como de las acciones y decisiones relativas a dichas violaciones. 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 violación de la seguridad y para eso es necesario remitirse al artículo 4, titulado definiciones, en su apartado 12 en donde se define dicho concepto:

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 violación 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 se realice dicha notificación, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la violación de seguridad. Por lo tanto, el responsable deberá fijar por tanto 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 a los datos que es necesario notificar a terceros.

El responsable ha de notificar la violación de la seguridad, siempre que exista riesgo para los derechos y libertadas de las personas físicas, riesgo que ha de ser evaluado por el responsable. El Comité 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 comunicación de las brechas de seguridad de los adheridos a los mismos. En este caso, también es necesario contemplar lo establecido en el Considerando el considerando 85 donde establece un caso específico sobre la excepción de informar a las autoridades de control y este es que, atendiendo al principio de responsabilidad proactiva, el responsable pueda demostrar la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

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

La notificación 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 comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la 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 violación a los interesados y estas son las siguientes:

- Caso de que el responsable del tratamiento haya adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la 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 los datos estén cifrado.
- El responsable ha 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.
- Que el realizar esa 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 manera igualmente efectiva a los interesados

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

La notificación de la brecha 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 de la violación. Es decir, hasta que no exista evidencia de conocimiento por el responsable de la existencia de una brecha se 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 deja abierta es posibilidad de forma genérica, sin establecer ninguna condición o restricción, tan sólo la obligación de adjuntar a la notificación una justificación del porqué de dicha dilación.

La notificación a los interesados no tiene un plazo temporal establecido en el RGPD, sólo se señala que esta ha de producirse cuanto antes, teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado.

La comunicación de la violación a la Autoridad de Control va más a allá de la mera indicación de que la brecha 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 violación de la seguridad de los datos personales. Para describir la naturaleza hay que incluir, siempre que sea posible:

    - Las categorías de interesados afectados, es decir, que tipo de personas han sido afectadas por la violación. Esta clasificación pueda atender a la vulnerabilidad de los interesados, como menores o discapacitados, a la relación con la empresa, como clientes o empleados, o 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. Lo que significa que no es necesario una descripción exhaustiva de los distintos campos de datos, sin una descripción genérica de los mismos, teniendo especial cuidado de señalar aquellos datos 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 violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales. Esto ha de incluir, si procede, las medidas adoptadas para mitigar los posibles efectos negativos

Destacar que esta información es un mínimo no un máximo. Es importante señalar que en la redacción del RGPD se considera de forma implícita que cualquier información adicional que permita a la Autoridad de Control tomar acciones presentes o futuras para garantizar la protección de los derechos de los interesados, y que la AEPD y sus funcionarios tienen la obligación de guardar secreto de la información recibida en el marco de sus actuaciones. En particular, hay que destacar que otra información de interés es la relativa a cuándo se ha producido la violación, su

extensión en el tiempo, la información técnica o procedimental relativa a la causa de la brecha, etc. Por otro lado, también hay que informar de la política de notificación a los interesados que ha establecido el responsable y las razones para implementar la misma en cuanto a si se ha realizado esa notificación, 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 comunicación 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.

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 las posibles consecuencias de la violación de la seguridad de los datos personales, como las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas 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 violaciones de seguridad. Ese procedimiento registrará todos los hechos relacionados con la violación, lo que implica que se anotará 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 detectar la violación de seguridad. Hay que registrar los efectos producidos por la violación, efectos que pueden ir más allá del compromiso de los datos de carácter personal, sino que sean relativos a la prestación de determinados servicios, por ejemplo. A su vez, se han de documentar qué medidas correctivas tanto para minimizar los efectos de la violación como 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 violación de seguridad.

3.8. 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.

Una de las cuestiones básicas a tener en cuenta en la realización de una evaluación de impacto es la participación del delegado de protección de datos. La AEPD dispone de una guía para la realización de evaluaciones de impacto en protección de datos que puede servir como referencia aunque en el momento de elaborar estos materiales se encuentra en proceso de adecuación a lo previsto en el RGPD.

En términos generales podemos decir que las fases mínimas que pueden tenerse en cuenta en la elaboración de una evaluación de impacto son las siguientes:

- **ANÁLISIS DE NECESIDAD**: fase o estudio inicial en el que tienen en cuenta los datos a tratar y su finalidad.

- **DETERMINACIÓN DE LOS FLUJOS DE DATOS Y PROCESOS**: detalles relativos al tratamiento, almacenamiento, niveles o privilegios de acceso a la información, etc.

- **IDENTIFICACIÓN DE RIESGOS:** primera aproximación a los riesgos específicos de un tratamiento de datos personales.

- **GESTIÓN DE RIESGOS:** determinación de las medidas para evitar o atenuar los riesgos iniciales del tratamiento.

- **CUMPLIMIENTO NORMATIVO NECESARIO:** análisis de toda la normativa aplicable según el tipo de tratamiento. Por ejemplo, si es un tratamiento de datos sanitarios sería conveniente tener en cuenta toda la normativa sanitaria aplicable.

- **INFORME FINAL:** conclusiones que pongan de manifiesto el nivel de riesgo y si es asumible/aceptable por el responsable del tratamiento.

- **CONSULTA PREVIA A LA AUTORIDAD DE PROTECCIÓN DE DATOS:** cuando el responsable tiene dudas sobre si el nivel de riesgo podría afectar en

exceso a los derechos y libertades de las personas deberá elevar consulta a una autoridad de protección de datos quien a su vez emitirá una respuesta en el plazo de ocho semanas para asesorar por escrito al responsable del tratamiento y/o al encargado del tratamiento.

- **IMPLANTACIÓN DE RESULTADOS:** una vez que el nivel de riesgo ha sido reducido a un nivel aceptable, se implantarán las medidas con los respectivos mecanismos de control.

- **SEGUIMIENTO:** los resultados de las medidas serán revisados periódicamente y los fallos o riesgos no previstos se introducirán dentro de lo que sería el mapa de riesgos de una organización.