Confidencialidad y seguridad del tratamiento

PID_00252147

Ramón Miralles López

Tiempo mínimo de dedicación recomendado: 8 horas

Universitat Oberta de Catalunya

Índice

1. El principio de integridad y confidencialidad de los datos

El artículo 5 del Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), recoge los principios relativos al tratamiento de datos personales.

Entre esos principios se incluye el de «**integridad y confidencialidad**», que implica que los datos serán tratados garantizando su seguridad, lo que en la práctica supone adoptar de manera activa medidas técnicas y organizativas, que los protejan de tratamientos no autorizados o ilícitos, y que eviten su pérdida, destrucción o daño accidental.

Esa seguridad de los datos ha sido una constante en la regulación del derecho fundamental a la protección de los datos de carácter personal; ya en la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD), se hacía referencia a la seguridad de los datos en su artículo 9, como uno de los principios de la protección de datos.

La LORTAD regulaba exclusivamente el tratamiento automatizado de datos, alcance que posteriormente fue superado por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), en la cual la protección también debe alcanzar a los tratamientos no automatizados.

En la LORTAD el «**responsable del fichero**» venía obligado a adoptar medidas técnicas y organizativas que evitaran que los datos fueran alterados o extraviados, así como su tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, pero también el tipo de datos y los riesgos a que pudieran estar expuestos los datos.

El artículo 9.2 de la LORTAD hacía la previsión de que las condiciones de seguridad en que debían ser tratados los datos personales se establecerían vía reglamentaria; de ese modo, mediante el Real decreto 994/1999, de 11 de junio, se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contuvieran datos de carácter personal (en adelante, RMS).

En el RMS es donde se establecieron los tres niveles de medidas de seguridad, sobre la base del tipo de datos tratados, que la posterior legislación mantuvo como el modelo de selección de las medidas de seguridad de los datos que, como veremos, vendrá ahora a ser sustituido por el RGPD.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, la Directiva), también incluía la seguridad de los tratamientos de datos personales, concretándola en la obligación del responsable del tratamiento de aplicar medidas técnicas y organizativas adecuadas para proteger los datos personales de su destrucción, accidental o ilícita, su pérdida accidental, así como su alteración, difusión o acceso no autorizado o ilícito.

Según la Directiva, las medidas debían adecuarse al estado de las tecnologías, teniendo en cuenta el coste de su aplicación, y siempre en relación con los riesgos que pudiera presentar el tratamiento y la naturaleza de los datos a proteger.

La Directiva se traspone al ordenamiento jurídico español mediante la LOPD, que deroga la LORTAD, pero mantiene vigente, mediante su Disposición transitoria tercera, de subsistencia de normas preexistentes, concretamente el RMS del año 1999.

El RMS no será derogado hasta la aprobación, mediante el Real decreto 1720/2007, de 21 de diciembre, del Reglamento de desarrollo de la LOPD (en adelante, RLOPD), manteniendo en su título VIII, con pocas variaciones, el modelo de medidas de seguridad del RMS.

La LOPD, en su artículo 9, reproduce el principio de seguridad de los datos de la manera en que ya había sido recogido en la LORTAD, con algunas ligeras diferencias, especialmente en cuanto a la adopción material de las medidas de seguridad, que no incumbe ya solo al responsable del tratamiento, sino también al encargado de tratamiento.

Para la LOPD las medidas técnicas y organizativas adoptadas deben garantizar la seguridad de los datos, evitando su alteración, pérdida, tratamiento o acceso no autorizado, reiterándose la referencia a tener en cuenta, al adoptar esas medidas, el estado de la tecnología, la naturaleza de los datos y los riesgos a los que esos datos puedan estar expuestos.

Con este rápido repaso se constata que la seguridad de los datos ha sido una constante en la regulación del derecho fundamental a la protección de los datos de carácter personal; tal y como se expresa en el preámbulo del RLOPD, la seguridad de los datos es «un aspecto esencial para la tutela del derecho fundamental a la protección de datos».

1.1. El entorno: la sociedad de la información

Antes de analizar en qué consiste materialmente el deber de proteger los datos personales, y de entrar a describir sus principales características, conviene contextualizar en qué escenario se tratan los datos de carácter personal en pleno siglo XXI.

En este sentido, debe tenerse en cuenta la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre «La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI», que en enero de 2012 acompañó a la primera versión del RGPD, aprobada en mayo de 2016.

La historia de la humanidad está repleta de avances tecnológicos, a partir de descubrimientos e invenciones, que tienen como denominador común el hecho de aportar evidentes ventajas para el propio desarrollo de la humanidad, en esencia sobre la base de la mejora del bienestar, pero que a la vez han generado nuevos riesgos o potenciado los ya existentes.

Hay multitud de ejemplos contemporáneos al respecto: la energía nuclear, la industria automovilística, la industria farmacéutica, la aviación comercial, etc., simplemente por citar algunos entornos en los cuales esa paradoja de «beneficio-riesgo» resulta evidente.

En esos supuestos, el papel de las normas no ha sido otro que intentar mitigar esos riesgos mediante la incorporación de principios, derechos y obligaciones, de contenido jurídico, es decir, cumpliendo con la función social que debe asumir la regulación, que no es otra que crear unas condiciones de convivencia aceptables, o de equilibrio, entre intereses que pueden entrar en conflicto.

Para ejemplificar lo hasta aquí expresado, podemos describir brevemente el paralelismo entre las tecnologías de la información y la industria automovilística, por lo que respecta a su desarrollo y a la imprescindible regulación que ha acompañado a sus sucesivos avances, especialmente en relación con la seguridad.

Parece ser que la primera víctima de un accidente de tráfico, relacionado con un vehículo a motor, fue Mary Ward, en 1869, que iba como pasajera en un vehículo a vapor; al parecer, en una curva perdió el equilibrio y fue arrollada por el mismo vehículo en que viajaba.

El primer automóvil con motor de combustión interna data de 1886, y en 1896 está documentado el primer atropello con resultado de muerte; a partir de 1908 Henry Ford comenzó a producir automóviles en una cadena de montaje (Ford modelo T), lo que provocó que se pudieran fabricar unidades a un ritmo elevado, al menos respecto del sistema más artesanal de sus antecesores, y

con ello los precios disminuyeron, y el automóvil empezó a ser popular, y en consecuencia el número de accidentes de tráfico empezó a crecer. En esa época la velocidad máxima podía situarse alrededor de unos 20 kilómetros por hora y el combustible solo se podía comprar en las farmacias.

Para hacernos una idea del desarrollo del mercado del automóvil, baste decir que en España el primer automóvil se matriculó en Palma de Mallorca, en 1900 (matrícula PM-1); en 1919 ya se habían matriculado 20.000 vehículos a motor, superándose en 1929 el número de 250.000.

En paralelo se empezó a regular la presencia de los automóviles en «sociedad», dados los evidentes riesgos que para la integridad física de las personas estaban suponiendo; concretamente en España, el 17 de septiembre de 1900 se aprueba la primera norma orientada a regular el tráfico, concretamente el «Reglamento para el servicio de coches automóviles por las carreteras del Estado», que entre otras cuestiones, como curiosidad, incluía la limitación de velocidad máxima: 28 km/h para vías interurbanas y 15 km/h para el caso de las vías urbanas.

También empieza a aparecer la necesidad de regular y controlar el tráfico de vehículos a motor mediante agentes dedicados a esa tarea.

Las primeras regulaciones intentaban poner orden en la circulación, preservando la seguridad de conductores, pasajeros y peatones, para con el tiempo ir incidiendo en los aspectos relacionados con la seguridad activa y pasiva de los propios vehículos, e incluso, en décadas más cercanas, en relación con el impacto medioambiental de los vehículos a motor.

Hay que reconocer que el legislador, con mayor o menor fortuna, suele estar atento a los cambios sociales; otra cosa es el ritmo con que es capaz de regularlos; por eso, la idea de que el legislador va siempre por detrás de la realidad se acentúa aún más cuando esa realidad está vinculada a las tecnologías de la información y la comunicación (en adelante, TIC).

Como veremos, la velocidad de su desarrollo y de los retos y riesgos que supone el uso de las TIC complica elaborar marcos jurídicos estables en el tiempo, que puedan satisfacer en cada momento todas las necesidades e intereses enfrentados.

La «sociedad de la información» hay que entenderla inicialmente como una evolución o mutación de la sociedad industrial; en este sentido, para aquellos que quieran profundizar, conviene tener en cuenta las teorías del sociólogo japonés Yoneji Masuda (1905-1995), ya que es uno de los principales autores que conceptualizaron la idea de sociedad de la información.

En esa sociedad de la información no solo resulta relevante la incorporación de las TIC a todos los ámbitos en que se despliega la sociedad (laboral, económico, político, educativo, de justicia, de Administración pública, etc.), apor-

tando una mayor eficiencia a los procesos (por su automatización), sino que debe ir acompañado del acceso social a la información, y su uso posterior para generar conocimiento e inteligencia, constituyendo un verdadero motor del futuro desarrollo económico y social, donde la base de «la nueva economía es la transformación de la información digital en valor económico y social».

Situados en Europea, la Unión Europea, en diferentes documentos, ha ido abordando el paradigma de la sociedad de la información, especialmente a partir del informe sobre la «sociedad de la información», conocido como Informe Bangemann de 1994, que, bajo el título de «Europa y la sociedad global de la información», sirvió de base para elaborar posteriormente el plan de actuación «Europa en marcha hacia la sociedad de la información».

A partir de esos primeros pronunciamientos, la Unión Europea ha ido concretando medidas dirigidas a promover la sociedad de la información, como por ejemplo: la liberalización de las telecomunicaciones, un marco jurídico para el comercio electrónico, la protección de los datos personales o el apoyo a la industria de los contenidos; en paralelo, empieza a detectarse que uno de los aspectos que necesariamente va a tener que ser abordado es la seguridad de la información, dando como resultado, por ejemplo, la Directiva 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS.

El uso de las TIC tiene que ir necesariamente acompañado de medidas que potencien la confianza en las tecnologías de la información y la comunicación, a fin de explotar al máximo sus beneficios, tanto para los ciudadanos a título individual como para las empresas y, en general, para el conjunto de la sociedad.

Hay una clara conexión entre el desarrollo de la sociedad de la información y la necesidad de proteger la información, tanto de incidentes accidentales como malintencionados. En el contexto de la sociedad de la información resulta esencial generar confianza en el uso de los sistemas de información, de ahí la importancia de la implantación de medidas de seguridad que generen ese clima de confianza en las tecnologías de la información y la comunicación.

Si bien en general puede considerarse que las medidas de seguridad deberían formar parte de la cultura de la autoprotección, y podríamos caer en la tentación de considerar que la regulación no es necesaria, esto no es así; ya sea por desconocimiento o despreocupación, por falta de concienciación, por cuestiones presupuestarias, por falta de alineación con el negocio, por prioridades, etc., las prácticas relacionadas con la protección de los sistemas de información no han tenido históricamente un suficiente impulso por parte de los principales interesados: usuarios de las TIC (entendidos estos en un sentido amplio, es decir, tanto personas físicas como jurídicas).

El legislador se ha visto obligado, del mismo modo que en el ejemplo de la industria automovilística, y precisamente con el fin de favorecer unas condiciones adecuadas para su desarrollo, a elaborar normas que promueven la cultura de la seguridad de la información, a veces de una manera «dolorosa», ya que incluso ha llegado a recurrir a la sanción económica ante el incumplimiento de obligaciones relacionadas con la protección de la información (como ocurre especialmente en el caso del derecho a la protección de los datos de carácter personal).

El actual desarrollo de los sistemas de información basados en las TIC hace que la seguridad de los sistemas de información tenga un peso específico muy importante y un evidente protagonismo, pero no hay que olvidar otro tipo de soportes y técnicas de tratamiento de datos personales, como son los tratamientos manuales de la información, que también deben ser objeto de protección.

El uso de las tecnologías de la información y la comunicación se ha convertido en un elemento de indiscutible relevancia en el contexto de las actividades de las organizaciones, sean de tipo público o privado, ya no solo por el hecho de aportar una mayor eficacia y eficiencia a la realización de sus procesos de negocio, sino también como un elemento de generación de mayor volumen de negocio y de captación de clientes, especialmente en el contexto de los *social media*; en definitiva: las tecnologías que dan soporte a las actividades de las organizaciones constituyen ahora uno de sus principales activos, y como tales están sujetas a amenazas, lo que obliga a adoptar medidas que minimicen los impactos negativos derivados de la materialización de esas amenazas.

La información forma parte de esos activos a proteger, pero no siempre la seguridad de la información se tiene suficientemente en cuenta, al menos no hasta que se produce algún incidente que causa daños, en ocasiones irreparables, tanto de tipo material como de reputación, que al final se traducen en pérdidas económicas o de credibilidad, máxime si están involucrados datos de carácter personal.

El legislador ha decidido que determinadas actividades deben necesariamente incorporar medidas de seguridad de la información para ser llevadas a cabo en condiciones de legalidad; es el caso del tratamiento de los datos de carácter personal, respecto de los cuales, como ya hemos avanzado, se obliga a aquellos que los tratan a que tomen medidas de seguridad que, en general, se han identificado erróneamente con cargas que no aportan ningún valor al negocio, recurriendo en muchas ocasiones a un simple cumplimiento formal de las obligaciones que se derivan de la ley en relación con la seguridad de los datos.

Tal y como se ha hecho referencia, formalmente podemos considerar que la reforma del derecho a la protección de los datos de carácter personal en Europa se inicia con la Comunicación de la Comisión Europea del año 2012: «La protección de la privacidad en un mundo interconectado. Un marco europeo

de protección de datos para el siglo XXI», en la que se utiliza la expresión «nuevo y complejo entorno digital actual» para abordar el contexto en el que se le plantean retos a la protección de los datos de carácter personal.

Esa complejidad a la que hace referencia la Comisión Europea está formada por diferentes variables, todas y cada una de ellas a su vez con sus complejidades; para entenderlo, vamos a centrarnos en torno a cinco variables que nos van a permitir tomar conciencia de hasta dónde de complejo es el escenario al que nos enfrentamos:

- **La rápida evolución de las tecnologías y de su uso**, un ritmo que difícilmente pueden seguir los legisladores, al menos con los mecanismos tradicionales de regulación; asalta aquí la duda de si tal vez deberíamos pensar en adaptar las técnicas legislativas (¿se podría legislar de otra manera?).

- **La extraordinaria capacidad de procesamiento de la información, cuantitativa (volumen de información) y cualitativa (diferentes tipos de informaciones)**, tanto por lo que respecta a las posibilidades de almacenamiento como de tratamiento y análisis de la información, lo que ha llevado a una dependencia prácticamente inevitable de las actividades de negocio respecto de las TIC.

- **El hecho de que la información tenga un valor económico**, no solo desde la perspectiva de la compraventa de información (lícita o no), también como medio productivo, de manera que la información se constituye como un verdadero activo empresarial.

- **La relación entre desarrollo de la sociedad de la información y progreso económico**; poner barreras a la innovación puede implicar poner freno al desarrollo económico, cuestión clave desde una perspectiva política; la seguridad si se aborda como una dificultad obviamente también puede llegar a considerarse una barrera.

- **La globalidad del entorno digital**, lo que lleva a la desaparición de las fronteras físicas y las dificultades que ello conlleva para la determinación de la norma aplicable, la jurisdicción competente y la ejecución de las resoluciones.

Ante ese escenario, que en definitiva implica una serie de riesgos para las personas, en tanto sus datos puedan ser utilizados para dañarles o perjudicarles, el deber de proteger los datos de carácter personal se alza como una obligación esencial para garantizar la efectiva protección de las personas, que en definitiva es el fin último del derecho fundamental a la protección de los datos de carácter personal.

La seguridad, por tanto, se constituye es un instrumento, no en un fin.

1.2. La seguridad de los datos: aspectos generales

La seguridad de la información, desde la perspectiva de la protección de datos personales, implica concretar qué controles o medidas de seguridad hay que implantar en los tratamientos de datos personales a fin de preservar la disponibilidad, integridad, confidencialidad, autenticidad y auditabilidad de la información de carácter personal, que utilizan los responsables de tratamientos, para el desarrollo de sus actividades, sean de carácter público o privado.

En gran medida, las previsiones normativas relacionadas con la seguridad de los datos personales se han venido centrando tradicionalmente en los aspectos de seguridad vinculados a evitar que se produzca el daño.

La prevención está especialmente indicada para un entorno como la protección de los datos de carácter personal, ya que al vincularse a un derecho de carácter individual y fundamental (desde la perspectiva del ordenamiento jurídico español, así como en del marco regulatorio europeo), cuando se lesiona ese derecho, los efectos de la vulneración son habitualmente de carácter irreversible y de difícil reparación; por ejemplo, pensemos en la vulneración de la confidencialidad.

Pero como veremos, no es hasta la elaboración del RGPD que se pone de relieve, de una manera clara, la necesidad de que para tomar cualquier decisión sobre los tratamientos (no solo de seguridad de los datos) deben tenerse en cuenta los riesgos que las operaciones de tratamiento puedan suponer para los derechos y libertades de las personas.

Lo cierto es que el concepto de riesgo ha estado presente en la regulación, pero no se vinculaba a una obligación material concreta, como es la gestión de los riesgos, que sí recoge ahora el RGPD.

Todo aquello que permita evitar que se produzca el incidente de seguridad con los datos personales va a ser mucho más eficiente, tanto para los afectados como para los responsables. La prevención es lo que realmente puede garantizar un adecuado clima de confianza y seguridad basado en el control preventivo de los tratamientos.

El RLOPD define qué es un sistema de información (art. 5.2.m): «Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipamientos utilizados para el tratamiento de datos personales».

Las medidas de seguridad deberán ser aplicadas sobre esos elementos que conforman el sistema de información, teniendo además en cuenta el sistema de tratamiento, puesto que, las medidas de seguridad no se aplican exclusivamente al tratamiento automatizado de la información, también a los tratamientos no automatizados.

Las medidas de seguridad, ya sean técnicas u organizativas, deben proteger la información de carácter personal en todo momento y en cualquier ubicación o soporte en que se encuentre.

Como ya hemos avanzado, el principio de seguridad en el contexto de la protección de datos de carácter personal se concreta en el deber del responsable del tratamiento y, en su caso, del encargado del tratamiento, de llevar a cabo las acciones necesarias para proteger los datos de carácter personal.

Se trata de una obligación de resultado, de manera que aun habiéndose tomado medidas, si estas no han resultado eficaces, se podrán derivar responsabilidades; a ello se une ahora el principio de responsabilidad proactiva, al cual nos referiremos más delante.

El RGPD supone una verdadera reforma del derecho a la protección de los datos de carácter personal en Europa; con carácter general, una de las principales novedades del RGPD es la orientación hacia un modelo de gestión del conjunto de obligaciones relacionadas con el derecho a la protección de los datos de carácter personal.

Un modelo de gestión implica que la organización dispone de personas, procedimientos y recursos que tienen como misión principal cumplir con las obligaciones que se deriven de las operaciones de tratamiento de datos de carácter personal.

Se trata de superar el modelo actual, en general excesivamente formalista, e ir hacia un escenario de gestión de la protección de datos, una cuestión que queda muy evidenciada, por ejemplo, cuando el reglamento aborda cómo debe ser la seguridad de los datos.

Por tanto, el modelo de seguridad que plantea el RGPD gira en torno a la evaluación y gestión del riesgo; literalmente establece que «el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo», sin entrar el legislador en el detalle concreto de qué medidas hay que aplicar, como hasta ahora se hacía, al menos en la regulación española; con esta orientación las medidas a implantar vendrán determinadas precisamente por la evaluación y tratamiento de los riesgos, y su real adaptación a las necesidades de seguridad de cada tratamiento.

Por tanto, todos los agentes implicados, responsables y encargados de tratamientos, y también las autoridades de supervisión, tendrán un importante reto de adecuación a lo que prevé el RGPD en materia de seguridad de los datos.

En los siguientes apartados iremos analizando las características de ese reto.

2. Seguridad de los datos y seguridad de los tratamientos

La aún vigente LOPD se refiere a la «**seguridad de los datos**» cuando, en su artículo 9, concreta el contenido del principio de seguridad, aunque si acudimos a la Directiva, veremos que su artículo 17 se refiere a la «seguridad del tratamiento».

Concretamente, la Directiva prevé que quien trata datos personales tiene la obligación de proteger la información de carácter personal, una obligación que se considera una condición de legalidad de los tratamientos de datos de carácter personal, ya que ese artículo 17 se sitúa en el capítulo II de la Directiva, el que trata sobre las «Condiciones generales para la licitud del tratamiento de datos personales».

A efectos prácticos, esa diferencia respecto del objeto sobre el cual se van a proyectar las medidas de seguridad no resulta excesivamente relevante, pero sí que conviene contextualizar una y otra referencia ya que tiene su interés, al menos desde una perspectiva de su evolución y estudio académico.

La Directiva plantea que las medidas de seguridad, ya sean de carácter técnico u organizativo, se aplican a los tratamientos, con el fin de proteger los datos tratados, mientras que la LOPD parece plantear un escenario en el que lo esencial es adoptar medidas sobre el objeto de tratamiento (datos), no tanto sobre las operaciones que se llevan a cabo.

Lo cierto es que, técnicamente, resulta más preciso referirse a la seguridad de los tratamientos, es decir, a la seguridad aplicada a las diferentes operaciones a las que se someten a los datos, que como veremos más adelante es la orientación del RGPD.

Los artículos 9.2 y 9.3 de la LOPD insisten en esa especie de imprecisión técnica cuando ponen el énfasis en considerar, como objeto principal de las medidas de seguridad, los ficheros, un elemento material que es puramente instrumental, ya que se trata del contenedor de los datos, aunque también puede entenderse como la organización y estructuración de los datos.

Esas imprecisiones tienen unos antecedentes muy claros, el escenario tecnológico de finales de los años setenta y principios de los ochenta, a pesar de tratarse de una norma elaborada ya a finales de los noventa.

El legislador comunitario sí que prestó atención a la evolución de las TIC, haciendo un planteamiento más adaptado a las realidades tecnológicas y de gestión de la información de mediados de los noventa; posteriormente, ya entra-

dos en el siglo XXI, se fueron produciendo cambios más que transcendentales, especialmente a partir del momento en que internet se «socializa» y la tecnologías en su conjunto empiezan a evolucionar a un ritmo sin precedentes.

Precisamente esos avances tecnológicos son los que al final, al menos en parte, han provocado una reforma significativa del derecho a la protección de los datos personales en Europa sobre la base del RGPD aprobado en mayo de 2016.

La Constitución de 1978, en su artículo 18.4, se refiere a «limitar el uso de la informática», reflejando, del mismo modo que el Convenio 108 del Consejo de Europa, una realidad tecnológica muy concreta, la de hace cerca de cuarenta años, marcada en esencia por dos características:

- **Sistemas de información formados por bases de datos de carácter centralizado** (grandes ficheros de datos centralizados física y lógicamente)

- **Sistemas informáticos muy limitados**: opciones de tratamiento muy básicas, conectividad limitada, sin periféricos de usuario, sistemas operados por personal muy especializado, sin ningún tipo de interoperabilidad, con sistemas propietarios y cerrados, etc.

Operaciones de tratamiento, ficheros y datos en realidad constituían un conjunto difícilmente separable, de manera que adoptar medidas de seguridad en los ficheros, en los datos o en los tratamientos, en realidad, venía a ser lo mismo.

Resulta razonable que el Convenio 108, en su artículo 7, partiera de la seguridad de los datos como uno de los principios básicos para la protección de la información referida a las personas físicas:

> «Artículo 7. Seguridad de los datos
>
> Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.»

La LORTAD (derogada por la LOPD) parte del mandato constitucional del artículo 18.4, y se alinea con los principios y garantías del Convenio 108, manteniendo una concepción «preinternet» respecto de los sistemas de información, a pesar de que en 1992 las TIC, tal y como las conocemos en la actualidad, aunque de una manera incipiente, empezaban a ser una realidad: conectividad basada en redes TCP/IP y la informática de consumo.

Como hemos avanzado, en 1995, la Directiva orienta la seguridad hacia un concepto más amplio, superando la visión del Convenio 108 de 1981. En consecuencia, el foco de la seguridad se pone sobre los tratamientos.

En 1999, la LOPD no recoge esa «reorientación» y mantiene la seguridad centrada en el binomio dato/fichero, con un redactado del artículo que describe el principio de seguridad (art. 9), casi idéntico al de la LORTAD.

El legislador de 1999 no apreció el matiz de que la Directiva giraba alrededor de los tratamientos y no en torno a los ficheros, ni tampoco prestó atención a lo que el legislador de 1992 aclaró respecto del concepto «fichero», ya que si bien la LORTAD tenía como elemento nuclear lo que, convencionalmente, se denominan «ficheros de datos», esta introdujo en su exposición de motivos el concepto de tratamiento de datos

> «concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados».

Ya en el año 2007, el Real decreto 1720/2007 identifica el título VIII del Reglamento como «De las medidas de seguridad en el tratamiento de datos de carácter personal», pero a pesar de esta alineación con la Directiva, en el articulado se mantiene la fórmula «fichero o tratamiento», cuando identifica aquello sobre lo que hay que implantar las diferentes medidas de seguridad.

En cualquier caso, la cuestión se resume en la obligación de asegurar los tratamientos de datos personales, lo que obviamente redundará en la protección de los datos que son objeto de esas operaciones de tratamiento; si las medidas de seguridad salvaguardan correctamente todas las operaciones relacionadas con un determinado tratamiento, la información relativa a las personas estará convenientemente protegida.

2.1. El principio de la seguridad de los datos de la LOPD

El «principio de seguridad», en el contexto de la protección de los datos de carácter personal, implica con carácter general la imposición al responsable del tratamiento de un «deber de protección» de los datos personales que trata, en tanto es quien ha decidido que tal tratamiento exista, sobre la base de concretar su contenido, uso y finalidades.

El artículo 9 de la LOPD dota de contenido a ese «principio de seguridad» de los datos:

«**1.** El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.»

Por tanto, el principio de seguridad se concreta en el deber del responsable del tratamiento y, en su caso, del encargado del tratamiento, de llevar a cabo las acciones necesarias para proteger los datos de carácter personal de los riesgos derivados de su tratamiento y de la naturaleza de los datos tratados, teniendo en cuenta el estado del arte de las tecnologías, lo que se traduce a la práctica en la implantación de unas medidas de seguridad que podrán ser tanto de carácter técnico como organizativo.

El detalle de las medidas de seguridad a implantar y cuáles de ellas deben implantarse en cada caso se recoge en el RLOPD, en su título VIII.

El objetivo de esas medidas de seguridad se concreta en evitar, en relación con los datos personales:

- La alteración
- La pérdida
- El tratamiento no autorizado
- El acceso no autorizado

Debe ponerse énfasis en que el «principio de seguridad» implica una obligación de resultado, es decir, no se trata exclusivamente de implantar unas medidas de seguridad que resulten adecuadas desde el punto de vista de su definición o del cumplimiento; también, deben serlo desde la perspectiva de su eficacia; por tanto, deberán estar implantadas y funcionar adecuadamente en el sentido de proteger, de manera efectiva, los datos personales sobre la base de dotar de seguridad a las operaciones de tratamiento.

2.2. Protección de las operaciones de tratamiento

Aplicar seguridad a los tratamientos implica conocer en detalle todas y cada una de las operaciones de tratamiento que se llevan a cabo, de manera que en función del riesgo que implica cada una de ellas se puedan seleccionar e implantar aquellas medidas que resulten más eficaces para mitigar esos riesgos. Más adelante profundizaremos en el enfoque a riesgos que plantea el RGPD.

Tal y como se define el principio de «integridad y confidencialidad» del RGPD, los datos se tratarán garantizando su seguridad, de manera que, en particular, no sean tratados de manera no autorizada o ilícita, evitando su pérdida y su destrucción o daño accidental.

Las actividades de tratamiento están formadas por un conjunto de operaciones de tratamiento que se llevan a cabo utilizando los datos personales, ya sea de manera automatizada o no.

Cuando el RGPD define el concepto de tratamiento, se identifican como posibles operaciones:

> «la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

En definitiva, cualquier acción que se lleve a cabo con los datos personales implica una operación de tratamiento y, como tal, va a requerir que se prevean las medidas adecuadas para que esa operación de tratamiento no tenga como efecto «la destrucción, pérdida o alteración accidental o ilícita de datos personales», o la comunicación a acceso no autorizado a los datos personales, tal y como prevé el artículo 32.3 del RGPD.

A estos efectos, resulta de utilidad la definición que de «sistema de información» hace el RLOPD, en su artículo 5.2, letra m (definiciones en relación con lo dispuesto en el título VIII del RLOPD), que entiende como tal el «conjunto de ficheros, tratamientos, programas, suportes y, en su caso, equipos utilizados para el tratamiento».

Materialmente, las medidas de seguridad técnicas y organizativas se implantarán en los sistemas de información que soporten el conjunto de operaciones de tratamiento que constituyen la actividad de tratamiento.

En este sentido, en primera instancia, el responsable del tratamiento deberá conocer perfectamente el contexto en el que se llevan a cabo las diferentes operaciones de tratamiento de las cuales es responsable, lo que incluye tener conocimiento preciso de:

- los procesos que se aplican a los datos, es decir, qué se hace con los datos,
- qué datos se tratan, con especial atención a las categorías especiales de datos,
- quién está involucrado en esos tratamientos, incluyendo a las personas afectadas, y por supuesto a cualquiera que tenga acceso, de cualquier modo y con cualquier técnica, a los datos,

- cómo se «mueve» la información, es decir, los flujos de datos previstos,

- y, por supuesto, el detalle de las tecnologías utilizadas en esas operaciones de tratamiento, incluyendo las técnicas utilizadas en los tratamientos no automatizados.

2.3. Cambio de enfoque: de niveles de seguridad según tipo de datos hacia los riesgos derivados de los tratamientos

1) Actual escenario: LOPD y RLOPD

La vigente regulación, previa a la plena aplicación del RGPD, si bien hace referencia a tener en cuenta los riesgos que puedan suponer los tratamientos para los datos personales, en la práctica tal actividad no se ha llevado a cabo por parte de los responsables de tratamientos, al menos formalmente.

La herencia que nos dejó el RMS del año 1999, que determinó la existencia de tres niveles de medidas de seguridad, instituyendo para cada nivel unas medidas de seguridad concretas, quedó reflejada en el título VIII del RLOPD, lo que en la práctica llevó a que no fuera necesario llevar a cabo una gestión formal de los riesgos, ya que tanto la evaluación de riesgos como su posterior tratamiento se aportaban ya en el propio RMS, y posteriormente en el RLOPD, teniendo en cuenta únicamente el tipo de datos objeto de tratamiento (arts. 80 y 81 del RLOPD).

En el RLOPD, las medidas de seguridad se organizan por niveles (alto, medio o bajo); cuanto más sensible es la información que debe ser protegida, más exigentes son las medidas de seguridad; y por razones obvias, se distingue entre las medidas de seguridad que deben ser aplicadas a los tratamientos automatizados y aquellos no automatizados.

El artículo 81 determina qué nivel de medidas de seguridad debe aplicarse, teniendo en cuenta la tipología de datos objeto de tratamiento:

a) A todos los tratamientos de datos de carácter personal se les aplican las medidas de seguridad de nivel básico.

b) Las medidas de seguridad de nivel medio se aplicarán a los tratamientos:

- relativos a la comisión de infracciones administrativas o penales;

- relacionados con la prestación de servicios de información sobre solvencia patrimonial y crédito;

- que sean responsabilidad de las administraciones tributarias, en relación con el ejercicio de potestades tributarias;

- que sean responsabilidad de las entidades financieras, en relación con la prestación de servicios financieros;

- que sean responsabilidad de las entidades gestoras y servicios comunes de la Seguridad Social, relacionados con el ejercicio de sus competencias;

- que sean responsabilidad de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;

- que contengan un conjunto de datos de carácter personal que proporcionen una definición de las características o de la personalidad de las personas y que permitan evaluar determinados aspectos de su personalidad o de su comportamiento.

c) Las medidas de seguridad de nivel alto se aplicarán a los tratamientos que traten datos sobre: ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, aquellos que contengan o se refieran a datos obtenidos para finalidades policiales, sin consentimiento de las personas afectadas, o aquellos datos derivados de actos de violencia de género.

Se establecen algunas especialidades y excepciones en la aplicación de este esquema general de determinación del nivel de seguridad, concretamente:

- Los datos de tráfico y localización que traten los operadores que presten servicios de telecomunicaciones electrónicas disponibles para el público, o exploten redes públicas de comunicaciones electrónicas, son inicialmente considerados datos de nivel medio, pero esos datos también deberán estar protegidos con una medida concreta de nivel alto, la prevista en el artículo 103 del RLOPD (el registro de accesos).

- Cuando se traten datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, con la única finalidad de hacer transferencias de dinero a entidades de las que son asociadas o miembros las personas de las que se tratan eses tipos de datos, o si es un tratamiento en el que aparecen de forma incidental o accesoria este tipo de datos, sin que tengan relación con la finalidad del fichero o tratamiento. Entonces, solo se aplicarán las medidas de seguridad previstas en el nivel básico.

- Si se trata de un archivo o un tratamiento que utiliza datos de salud que se refieren exclusivamente a un grado de discapacidad o solo a la declaración de la discapacidad o invalidez del afectado, y siempre que sea necesario tratar este dato para dar cumplimiento a unos deberes públicos. En este

caso, serán suficientes las medidas de seguridad de nivel básico para este fichero o tratamiento.

En posteriores apartados se abordarán las medidas concretas previstas en el RLOPD para cada nivel de medidas de seguridad.

2) Próximo escenario: RGPD y nueva LOPD

El RGPD plantea un modelo netamente orientado a la gestión de riesgos, es decir, incorpora la gestión de riesgos como una obligación (art. 24 RGPD) del responsable del tratamiento, que le debe permitir ser capaz de seleccionar por sí mismo las medidas de carácter técnico y organizativo más adecuadas, teniendo en cuenta el riesgo que potencialmente presenten las operaciones de tratamiento.

La aprobación del RGPD, en mayo de 2016, implica necesariamente llevar a cabo una adaptación de la normativa interna de los Estados miembros.

Disponer de un RGPD supone la existencia de un «régimen uniforme que deberá ser también aplicado de forma uniforme en toda la Unión», aunque por supuesto cada Estado puede preservar sus propios principios y tradición jurídica, en tanto no se contradiga lo previsto en el RGPD.

El RGPD contiene habilitaciones e imposiciones a los Estados miembros, por lo que respecta a regular mediante el derecho interno ciertas materias relacionadas con el RGPD.

El 10 de noviembre de 2017, el Consejo de Ministros aprobó el proyecto de Ley orgánica de protección de datos (en adelante, PLOPD), que por supuesto no reitera el texto del RGPD, sino que trata de «clarificar sus disposiciones, dentro de los márgenes que el mismo establece» (exposición de motivos del PLOPD).

Tal y como también recoge la exposición de motivos del anteproyecto, se trata de «depurar el ordenamiento jurídico», a fin de eliminar la normativa interna que pueda resultar «incompatible con el derecho de la Unión».

Lo cierto es que los reglamentos europeos, a pesar de que sean aplicables directamente, pueden requerir de normas internas para que su aplicación resulte plenamente efectiva; por tanto, la futura Ley de protección de datos asumirá el papel de «desarrollo o complemento» del RGPD.

El RGPD plantea llevar a cabo una evaluación de los riesgos teniendo en cuenta que los riesgos a valorar lo son en relación a los derechos y libertades de las personas afectadas por las operaciones de tratamiento.

En el Considerando 76 del RGPD se expresa que:

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

Por tanto, según el RGPD, a la hora de valorar los riesgos habrá que tener en cuenta dos variables:

- Hasta qué punto una situación de riesgo que ha sido identificada es probable que se produzca; por tanto, las decisiones que se tomen para gestionar esa situación de riesgo tenderán a reducir la «probabilidad» de que se produzca tal situación no deseada.

- Y la «gravedad», es decir, cuánto daño o perjuicio se puede llegar a causar si una situación de riesgo llega a producirse; en este caso, las decisiones que se tomen para gestionar las consecuencias de la situación de riesgo tenderán a reducir sus efectos perjudiciales.

Este planteamiento viene sustentado en lo previsto en el artículo 24.1 del RGPD, en cuanto a la responsabilidad de aplicar medidas técnicas y organizativas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como «los riesgos de diversa probabilidad y gravedad»; y también en el artículo 25.1, al abordar la protección de datos desde el diseño, utilizando la misma fórmula para referirse a la diversidad de los parámetros que configuran el riesgo (probabilidad y gravedad).

Por lo tanto, ahora ya no se establece una «lista» de medidas de seguridad a aplicar en función de los tipos de datos objeto de tratamiento, sino que el responsable del tratamiento deberá seleccionar, de manera responsable, aquellas medidas de seguridad que resulten más adecuadas para mantener bajo control los riesgos específicos que entrañen las operaciones de tratamiento.

Respecto a la gestión de riesgos que se deriva de lo previsto en el RGPD, profundizaremos más adelante.

2.4. Protección de datos desde el diseño y seguridad por defecto

Con el RGPD se incorporan al marco jurídico que regula el derecho fundamental a la protección de datos algunos principios que podemos calificar de novedosos, al menos en el contexto europeo; concretamente, la protección de datos desde el diseño y la protección de datos por defecto.

Entra en juego aquí la denominada seguridad por defecto, que en cuanto a su alcance queda bien sintetizado en el artículo 19 del Esquema Nacional de Seguridad (en adelante, ENS).

El ENS está regulado por el Real decreto 3/2010 y tiene por objeto establecer la política de seguridad en el uso de las TIC que hacen las Administraciones públicas; el ENS está formado por una serie de principios básicos y de requisitos mínimos que deben garantizar una protección adecuada de la información que tratan las Administraciones públicas por medios electrónicos.

Como decíamos, según el artículo 19 del ENS, la seguridad por defecto implica que los sistemas de información se diseñan y configuran de manera que:

- «El sistema proporcionará la mínima funcionalidad requerida para que la organización solo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que solo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario».

En definitiva se trata de que, aplicadas a los tratamientos de datos personales, las diferentes operaciones se diseñen y se configuren teniendo en cuenta que sean seguras desde el momento en que se implantan.

En cuanto a la «protección de datos desde el diseño», hay que mencionar su origen, aunque sea brevemente, que no es otro que el denominado *privacy by design*, una propuesta definida y difundida por Ann Cavoukian, «Information and Privacy Commissioner of Ontario» entre 1997 y 2014, resultando muy relevante referirse a los que identificó como los principios básicos de la privacidad desde el diseño, recogidos en el documento «7 Foundational Principles of Privacy by Design».

Tal y como se expresa en el mencionado documento, los objetivos de privacidad por diseño se centran en asegurar la privacidad y obtener el control personal de la propia información, y por lo que respecta a las organizaciones, les permite obtener una ventaja competitiva sostenible, pudiéndose alcanzar esos objetivos aplicando siete principios básicos:

1) Proactivo, no reactivo; preventivo no correctivo: se trata de anticipar y prevenir las situaciones en que se puede producir una invasión de la privacidad, antes de que ocurra.

2) Privacidad como la configuración predeterminada: las tecnologías de la información deben estar configuradas desde el inicio para proteger la privacidad.

3) Privacidad incrustada en el diseño: la privacidad es un componente esencial de la misión o funcionalidad de la solución que requiere del tratamiento de datos personales; de este modo la privacidad pasa a ser parte integral del sistema, sin disminuir su funcionalidad.

4) Funcionalidad total / «Todos ganan», no «Si alguien gana, otro pierde»: no se sacrifica privacidad por funcionalidad, ni al revés, el equilibrio ha de ser posible.

5) Seguridad extremo-a-extremo / protección de ciclo de vida completo: debe garantizarse una administración segura del ciclo de vida de la información.

6) Visibilidad y transparencia / mantenerlo abierto: las diferentes partes del sistema de tratamiento son conocidas por las partes afectadas, las expectativas de privacidad se cumplen y, además, pueden ser verificadas por terceros.

7) Respeto por la privacidad de los usuarios / mantener un enfoque centrado en el usuario: los intereses de las personas afectadas por los tratamientos deben estar presentes en las decisiones y medidas que se adopten.

Aspectos todos ellos vinculados directa o indirectamente a decisiones que tienen que ver con la seguridad de los tratamientos, ya que esas decisiones se adoptan en el momento en el que se están diseñando las futuras operaciones de tratamiento, de manera que cuando se inicien ya existirán garantías y certeza de que se han definido teniendo en cuenta la seguridad.

Un diseño que evidentemente deberá completarse con una adecuada implantación de las medidas de seguridad, y posterior monitorización y gestión de la seguridad de los tratamientos.

La protección de datos desde el diseño implica que, tanto en el momento de definir las diferentes operaciones de tratamiento como al determinar los medios que van a ser utilizados para tratar los datos personales, van a tenerse en cuenta, en esa toma de decisiones, los principios, derechos y obligaciones recogidos por la normativa que vaya a ser de aplicación al tratamiento de datos personales que se pretende llevar a cabo, y todo ello desde la necesidad de gestionar los riesgos que pueden suponer las operaciones de tratamiento para los derechos y libertades fundamentales; entre esos principios y obligaciones se encuentran los relacionados con la seguridad de los tratamientos.

El RGPD también obliga al responsable del tratamiento a tener en cuenta lo que denomina «protección de datos por defecto», es decir, se deberán definir y aplicar medidas técnicas y organizativas apropiadas para garantizar particu-

larmente que, por defecto, los datos sean tratados garantizando su seguridad para evitar, en especial, el tratamiento no autorizado o ilícito (principio de «confidencialidad», art. 5.1.f).

En definitiva, el RGPD introduce cambios sustanciales en la obligación de proteger los datos personales, sobre la base de implantar medidas de seguridad en los tratamientos que habrán sido seleccionadas atendiendo a los riesgos específicos que presenten las operaciones de tratamiento.

3. Encaje de la seguridad de los tratamientos en el marco de las obligaciones del responsable del tratamiento previstas en el RGPD

Tal y como ya se ha avanzado en anteriores apartados, el responsable del tratamiento viene obligado a implantar medidas que resulten eficaces para garantizar que los tratamientos de datos de carácter personal se realizan en unas condiciones de seguridad adecuadas, que en el contexto del RGPD implica controlar los riesgos que las operaciones de tratamiento puedan entrañar para los datos personales.

El capítulo IV del RGPD, en su sección 1, regula las obligaciones que con carácter general deben asumir tanto responsables como encargados de tratamiento, y la sección 2 se refiere de manera expresa a la seguridad de los datos, si bien centra la seguridad de los tratamientos en su artículo 32.

Entre las obligaciones de carácter general se incluyen también la protección de datos desde el diseño y por defecto, cuestiones a las que ya nos hemos referido en el apartado anterior.

Debemos destacar como novedad el registro de actividades de tratamiento, que no es otra cosa que la obligación de disponer de un registro de las actividades de tratamiento que efectúa el responsable del tratamiento, entendiendo como tales los tratamientos que lleva a cabo desde una perspectiva funcional en tanto se trate de operaciones de tratamiento vinculadas a una misma finalidad.

En el artículo 28 del PLOPD se prevén las obligaciones generales de responsables y encargados de tratamiento, limitándose a reiterar que las medidas de seguridad deberán ser determinadas por el responsable del tratamiento, teniendo en cuenta los riesgos que el tratamiento pueda generar en los derechos de los afectados.

3.1. Garantizar y demostrar la conformidad con el Reglamento

El responsable del tratamiento viene obligado, con carácter general, a aplicar medidas técnicas y organizativas que, por un lado, garanticen que el tratamiento se lleva a acabo conforme a lo previsto en el RGPD, pero además, en aplicación del principio de responsabilidad proactiva (*accountability*), también deberá estar en disposición de demostrar ese cumplimiento.

A la hora de adoptar esas medidas, el responsable del tratamiento deberá tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento; todo ello bajo el enfoque a riesgos al cual ya hemos hecho referencia.

En cuanto a los que debemos entender por naturaleza, ámbito, contexto y fines del tratamiento, a continuación se proporcionan algunas orientaciones sobre su significado:

1) La naturaleza del tratamiento tiene que ver con las características esenciales del tratamiento; por tanto, se trata de tener en cuenta, por ejemplo:

- si de manera prioritaria se tratan categorías especiales de datos (art. 9 RGPD),
- si se tratan datos a gran escala (gran volumen tanto en valores absolutos como relativos, o incluso teniendo en cuenta el alcance territorial),
- si se lleva a cabo un seguimiento exhaustivo de personas,
- si se combinan diferentes conjuntos de datos (diversas fuentes de información),
- si los datos se refieren a personas en situación de vulnerabilidad, lo que incluye a los menores,
- cualquier otra circunstancia que forme parte intrínseca del tratamiento.

2) En cuanto al alcance del tratamiento, se trata de valorar los efectos o consecuencias del tratamiento, es decir, hasta dónde pueden llegar los efectos del tratamiento, por ejemplo:

- toma de decisiones con efectos jurídicos,
- decisiones en procesos competitivos,
- valoración de riesgos crediticios,
- exclusión de beneficios sociales o fiscales,
- limitaciones en el acceso a servicios o contratos,
- en definitiva, con independencia de la finalidad del tratamiento, qué efectos directos o indirectos pueden tener sobre las personas las operaciones de tratamiento.

3) Respecto del contexto del tratamiento, tendremos en cuenta el conjunto de circunstancias en que se van a llevar a cabo las operaciones de tratamiento, por ejemplo:

- el uso de nuevas tecnologías, o tecnologías emergentes,

- el uso de tecnologías especialmente invasivas para la privacidad,
- el uso de tecnologías que de manera inherente impliquen riesgos significativos,
- la existencia de diversos responsables de tratamiento,
- la existencia de complejas cadenas de encargados de tratamiento,
- la existencia de transferencias internacionales,
- y cualquier otra circunstancia en la que se lleven a cabo las operaciones de tratamiento, especialmente si pueden generar un riesgo relevante para los derechos y libertades de las personas.

4) Y por último, en cuanto a los fines del tratamiento, se trata de identificar cuál es la finalidad del tratamiento, qué se pretende obtener del conjunto de operaciones de tratamiento de datos personales que se llevan a cabo, por ejemplo, si la finalidad es:

- la toma de decisiones,
- la elaboración de perfiles,
- la valoración de personas,
- el análisis predictivo,
- la prestación de servicios relacionados con la salud,
- el seguimiento, control u observación de personas,
- la vigilancia o monitorización,
- etc.

Pues bien, a la hora de adoptar cualquier decisión en relación con los tratamientos, deberá valorarse si tal decisión es conforme a los principios, derechos y obligaciones previstas en el RGPD, teniendo en cuenta los riesgos para los derechos y libertades, y además, deberán diseñarse e implantarse de tal manera que el responsable del tratamiento sea capaz de demostrar ese cumplimiento, lo que evidentemente también afecta a las decisiones relacionadas con la seguridad de los tratamientos.

3.2. Aplicación de políticas de protección de datos

Aunque muy tímidamente, el RGPD introduce el uso de las «políticas de protección de datos», cuestión no planteada en regulaciones previas, y que debemos considerar una novedad de un cierto calado, muy alineada con el ya tratado principio de responsabilidad proactiva, ya que disponer de una política de protección de datos en la organización supone, por su mera existencia, un compromiso con la gestión responsable de la información referida a personas físicas que utiliza la organización para el desarrollo de las actividades que le son propias.

Se trata de políticas de la organización o, en su caso, políticas empresariales, es decir, un conjunto de declaraciones de principios generales que la organización se compromete a cumplir, dotando los recursos necesarios para ello, y para las que se proporciona una serie de orientaciones o directrices básicas, aplicables a toda la organización, que tienen que ver con la aptitud y conductas que se espera del conjunto de los miembros de la organización, afectando tanto a empleados como a directivos, e incluso a terceros que de alguna manera participen o colaboren en las actividades de la organización.

Pueden incluir también aspectos organizativos derivados de la política, e incluso puede llegar a definir cuál es la estructura documental que se va a utilizar para desarrollarla, en tanto se vaya a sustentar materialmente en manuales, normas, protocolos, procedimientos, guías, etc. internos de la organización.

Las políticas pueden ser de carácter muy general, o bien de tipo departamental, o referirse a aspectos muy concretos, como por ejemplo, la seguridad, la calidad, el medioambiente o, como en el caso que nos ocupa: la protección de datos.

Lo cierto es que el RGPD tan solo dedica un artículo, concretamente el 24.2, a las políticas de protección de datos, que como decíamos están muy vinculadas con la capacidad de demostrar el cumplimiento; a ello se refiere el Considerando 78:

> «A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe **adoptar políticas internas** y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.»

El artículo 24.2 no prevé con carácter general que los responsables de tratamiento dispongan en todos los casos de políticas de protección de datos, de manera que solo las propone cuando resulten proporcionadas en relación con las actividades de tratamiento que se llevan a cabo, si bien no explicita cuándo se consideraría adecuado el uso de esas políticas.

Tal vez la circunstancia de que el RGPD se refiera a las «normas corporativas vinculantes» como un tipo de políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento nos da una cierta idea

del contexto en el que parecen encajar las políticas de protección de datos, aunque no hay obstáculo para que cada responsable de tratamiento pueda disponer de una política adaptada a su dimensión, y a las características de los tratamientos que lleva a cabo.

En cualquier caso, nunca está de más tener un documento que de manera sucinta y clara, y que sea conocido por el conjunto de la organización, describa cómo se piensa abordar el derecho a la protección de los datos de carácter personal desde una perspectiva de posicionamiento interno común para toda la organización.

También se puede plantear la política de protección de datos desde la perspectiva de las directrices básicas que guiarán las decisiones en materia de seguridad de los tratamientos de datos personales, ya que las políticas de seguridad de la información han tenido, y tendrán, un significativo auge en el actual escenario de escalada de los ciberataques, que pueden afectar tanto a grandes compañías como a las empresas más modestas.

Las políticas, sean de protección de datos o de seguridad, son mencionadas también cuando el RGPD define las funciones del delegado de protección de datos en su artículo 39, de manera que le asigna la función de supervisar con carácter general el cumplimiento, no solo normativo, sino también de las «políticas del responsable o del encargado de tratamiento», de manera que posiblemente esta sea otra pista para saber cuándo resultará proporcionado disponer de una política interna de protección de datos.

Probablemente, la obligación de designar un delegado de protección de datos suponga también la necesidad de plantearse la elaboración y aplicación de la mencionada política de protección de datos que, entre sus contenidos, deberá incluir directrices en relación con la seguridad de los tratamientos.

Las políticas de protección de datos implican en todo caso el compromiso del responsable de tratamiento, y por tanto, del conjunto de la organización, de tener en cuenta que las operaciones de tratamiento de datos de carácter personal implican en sí mismas riesgos para los derechos y libertades de las personas afectadas y que, en todo momento, esa constatación debe guiar las decisiones del conjunto de la organización y de las personas que forman parte de ella.

3.3. La concurrencia de responsables del tratamiento

En el artículo 26 del RGPD se prevé la posibilidad de que varios responsables de tratamiento definan de manera conjunta los objetivos y los medios de tratamiento.

En este sentido se refiere a ellos como «corresponsables», que deberán concretar claramente hasta dónde llega la responsabilidad de cada uno de ellos en relación con las diversas operaciones de tratamiento que puedan concurrir, lo que obviamente debe trasladarse a las medidas de seguridad, de manera que no existan dudas sobre qué asume cada responsable en cuanto al diseño, implantación y gestión de las medidas de seguridad a aplicar.

Obviamente, la gestión de riesgos deberá ser abordada de manera acordada entre todos ellos, evitando en todo caso que puedan quedar riesgos sin identificar, ya que ello podría suponer la falta de la aplicación de las medidas adecuadas.

Tampoco se puede producir el efecto de que las obligaciones puedan llegar a diluirse por la concurrencia de responsables; estas se mantienen intactas para todos ellos, si bien deberá preverse de qué manera se distribuyen entre los diferentes responsables del tratamiento.

3.4. Información sobre seguridad en el registro de actividades de tratamiento

Otra de las novedades del RGPD es la obligación de que responsables y encargados de tratamiento, cuando estos no se encuentren excluidos por lo previsto en el artículo 30.5, dispongan del denominado registro de actividades de tratamiento (en adelante, RAT), que no es otra cosa que un registro documentado que deberá contener una serie de informaciones relacionadas con las características de los tratamientos.

Esas informaciones que debe contener el RAT vienen indicadas en el artículo 30.1 del RGPD, por lo que respecta al responsable del tratamiento, y en el artículo 30.2 en relación con el RAT de los encargados de tratamiento.

En ambos casos, se prevé que el RAT contenga una descripción general de las medidas de seguridad técnicas y organizativas aplicadas a los tratamientos, si bien se hace la salvedad de que tal información se incluirá en tanto «sea posible».

El hecho de que el RGPD se refiera a que debe incluirse en el RAT una «descripción general» de las medidas de seguridad implica que no se trata de incluir una información detallada de cómo se protegen los tratamientos, es decir, no se trata de trasladar, por ejemplo, los contenidos del documento de seguridad previsto en la vigente regulación (art. 88 RLOPD), ni de otras normas de seguridad detalladas o procedimientos de seguridad operativos, sino de establecer el vínculo entre los riesgos que se han gestionado y la tipología de medidas de seguridad implantadas, o incluso podría bastar con hacer referencia al conjunto de buenas prácticas que en materia de seguridad de la información se

hayan podido adoptar, ya sea sobre la base de un estándar internacional, como por ejemplo la ISO 27002, o el Esquema Nacional de Seguridad para el caso de las Administraciones públicas.

En este sentido convienen destacar que el PLOPD, al referirse a las medidas de seguridad de los tratamientos en el ámbito del sector público, en su Disposición adicional primera, establece que el ENS deberá adaptarse a los criterios previstos en el artículo 32 del RGPD, para la determinación de los riesgos que potencialmente puedan generar las operaciones de tratamiento de datos personales, apuntando por tanto a que el modelo de seguridad a aplicar por las Administraciones públicas vendría a estar definido por lo previsto en el ENS.

Por otro lado, que se utilice la fórmula «cuando sea posible» obedece al hecho de que, en algunos casos, a fin de no poner en riesgos a la propia seguridad de los tratamientos, tal vez no resulte adecuado incluir en el RAT información precisa sobre las medidas aplicadas, aunque eso no obsta para incluir algún tipo de referencia, como por ejemplo la organización y responsabilidades relacionadas con las medidas de seguridad, o el sistema de gestión de la seguridad de la información utilizado (si fuera el caso), o el modelo de prácticas de seguridad que ha sido implantado, ya que se trata de información que, aun haciéndose pública, no va a poner en riesgo la eficacia de las medidas implantadas.

Hay que tener en cuenta que el RAT queda a disposición de las autoridades de control; en ese sentido, es previsible que sea un instrumento que, con frecuencia, vaya a ser solicitado por estas en aquellos casos en que, por ejemplo, como consecuencia de un incidente de seguridad, o por una queja planteada por una persona afectada, sea necesario verificar qué decisiones de seguridad se tomaron en su momento y en base a qué evaluación de riesgos.

Obviamente, sin perjuicio de que de manera complementaria, aparte de solicitar el RAT, la autoridad de control pueda acceder a otras informaciones de mayor detalle o acceder a los sistemas de información para verificar el estado de implantación y eficacia de las medidas de seguridad, en razón de los riesgos que pretenden controlar, a ello se refiere el artículo 58.1 del RGPD cuando describe los poderes de investigación de que disponen las autoridades de control.

3.5. El delegado de protección de datos y la seguridad de los datos

Para finalizar el análisis del encaje de la seguridad en el conjunto de las obligaciones de responsables y encargados de tratamientos, nos referiremos ahora a otra nueva obligación: la de designación del denominado delegado de protección de datos (en adelante, DPD), una obligación de carácter organizativo que pone en evidencia el giro que imprime el RGPD al cumplimiento, que viene a centrarlo en la gestión.

Tal obligación no aplica a todos los responsables y encargados de tratamiento; el DPD solo deberá designarse cuando concurran ciertas circunstancias, muy vinculadas a las particulares características de las actividades principales del responsable o del encargado, previstas con carácter general en el artículo 37.1 del RGPD, y con más detalle en el artículo 34 del PLOPD.

Al DPD se le atribuyen funciones de supervisión del cumplimiento de lo previsto en el RGPD; por tanto, todo aquello relacionado con las medidas de seguridad podrá ser objeto de supervisión por parte de este, un papel bien diferente al que el actual RLOPD atribuye al responsable de seguridad, cuando en su artículo 95 establece que es el «encargado de coordinar y controlar las medidas» de seguridad, es decir, lleva a cabo una actividad exclusivamente centrada en la eficacia de las medidas de seguridad, siendo el papel del DPD de un mayor alcance.

El DPD deberá supervisar las políticas de protección de datos, a las cuales ya hemos hecho referencia, así como las auditorías que puedan llevarse a cabo en relación con los tratamientos, ya sean de cumplimiento o de medidas de seguridad.

Por supervisar deberemos entender el ejercicio de «inspeccionar» lo realizado por un tercero, de manera que, en realidad, salvo cuestiones muy concretas, o como consecuencia de necesidades organizativas propias de cada responsable o encargado de tratamiento, el DPD no va a diseñar o implantar medidas de seguridad, su misión es verificar que tanto su diseño como su posterior implantación, y por supuesto su gestión ordinaria, están alineadas con lo previsto en el RGPD.

La supervisión implica un cierto nivel de jerarquía, de ahí que el artículo 38 del RGPD, al regular la posición del DPD, prevea que trate las cuestiones que son de su responsabilidad al más alto nivel jerárquico del responsable o encargado del tratamiento.

La supervisión también implica un cierto nivel de «autoridad» dentro de la organización, y por supuesto de disponibilidad de medios y recursos para llevar a cabo tal actividad, por lo que en el caso de las medidas de seguridad esto debería traducirse en la capacidad de interactuar directamente con los responsables de seguridad o áreas relacionadas con el diseño, implantación y gestión de las medidas de seguridad.

4. Seguridad y encargados de tratamiento

El encargado de tratamiento es una figura esencial en el contexto de la regulación del tratamiento de los datos de carácter personal y en la protección misma de esos datos, en tanto ejemplifica la capacidad del regulador de identificar situaciones fácticas, inherentes al escenario que ha de ser objeto de regulación, que requieren de unas previsiones específicas en la norma, que establezcan las condiciones y requisitos que permitan su aplicación sin menoscabar el derecho a la protección de los datos de carácter personal.

El tratamiento de los datos de carácter personal materialmente no siempre puede ser llevado a cabo por el responsable del tratamiento, aunque sea quien haya decidido su existencia y necesidad, sobre la base de concretar su contenido, uso y finalidades, ya que, en atención a diversos factores, que pueden ser de orden tecnológico, económico, organizativo, estructural, de oportunidad, etc., puede resultar más eficaz que algunas de las operaciones de tratamiento de los datos, a veces incluso todas ellas, sean llevadas a cabo por una persona física o jurídica que trate los datos por cuenta del responsable del tratamiento.

El artículo 4 del RGPD define al «encargado del tratamiento» (en adelante, encargado) como «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento», coincidiendo con lo que hasta ahora se venía identificando como encargado en la vigente normativa (LOPD y RLOPD).

Incluye el RGPD, también en su artículo 4, una definición de «tercero» que excluye de considerar como tal al encargado, planteamiento que ya se hacía en el nuestro RLOPD y que refuerza la idea de que el encargado no es «cualquiera» en relación con el tratamiento de los datos de carácter personal, de ahí que el RGPD venga a exigirle una mayor implicación en la protección de los datos.

Esa relevancia jurídica del papel del encargado llega hasta tal punto que el hecho de utilizar sus servicios, en tanto estos estén acordados y regulados convenientemente en un instrumento jurídico vinculante (contrato, convenio o cualquier otra forma de establecimiento de relaciones de servicio), recrea la ficción de considerar que no se esté llevando a cabo una comunicación de datos a terceros, aunque materialmente se esté produciendo.

Conviene recordar que la cesión o comunicación de datos se define en la LOPD como cualquier revelación de datos efectuada por el responsable del tratamiento a una persona diferente a la que hacen referencia los datos personales, y que tal comunicación va a requerir, con carácter general, el consentimiento de la persona afectada por el tratamiento de sus datos. En el RGPD la cesión

o comunicación de datos no vienen regulada específicamente, encontrándose subsumida en el concepto genérico de tratamiento (en el módulo 1 de estos materiales se analiza esta cuestión).

Como decíamos, la actividad de tratamiento de datos implica frecuentemente que terceros lleven a cabo operaciones de tratamiento de los datos sin ser los responsables de ese tratamiento, en tanto van a actuar por cuenta del responsable, que será quien siempre deberá determinar el alcance de los servicios de tratamiento que debe prestar el encargado, sobre la base de una serie de instrucciones que le va a trasladar en el instrumento jurídico que se utilice, típicamente un contrato de servicios, o como documentos anexos o complementarios al instrumento vinculante principal (contrato).

Por lo que hemos visto hasta ahora, la seguridad debe ser aplicada a los tratamientos de datos de carácter personal, a fin de que los datos personales no se vean afectados por los riesgos a que de manera inherente se ven expuestos por su simple recogida, almacenamiento y uso (tratamiento); en consecuencia, cuando exista un encargado, este va a tener que aplicar una serie de medidas de seguridad que den respuesta a las exigencias derivadas del principio de seguridad que, como ya nos hemos venido refiriendo, forma parte esencial del derecho fundamental a la protección de los datos de carácter personal.

Las medidas de seguridad deberán ser establecidas y trasladadas por el responsable del tratamiento, en forma de instrucciones, al encargado; en ese sentido, establece el artículo 12.2 de la LOPD que, en el contrato de servicios del que se derive ese encargo, junto con las instrucciones propias del servicio de tratamiento, deberá estipular también las medidas de seguridad que el encargado del tratamiento estará obligado a implantar.

No se nos pueden escapar las complejidades del actual escenario de aprovisionamiento de servicios TIC, en el que existen toda una serie de proveedores de servicios que tienen una posición dominante en el mercado, especialmente en el contexto de los servicios en la nube, que les permite imponer sus propias condiciones para prestar esos servicios.

Los servicios en la nube muy frecuentemente implican el tratamiento de datos de carácter personal, generando unas relaciones de servicio en las que el responsable del tratamiento se encuentra en una clara situación de inferioridad en cuanto a la capacidad de establecer pactos o acuerdos en los contratos que se le presentan por parte de esos proveedores.

Tampoco resulta evidente que los responsables de tratamientos puedan verificar, de una manera eficaz, que el prestador de servicios cumple con las exigencias que supone llevar a cabo actividades de tratamiento de datos de carácter personal en calidad de encargado del tratamiento.

Resulta de especial dificultad verificar, por parte del responsable, si las medidas de seguridad técnicas y organizativas que deben proteger los tratamientos de datos personales objeto de la prestación de esos servicios TIC están realmente implantadas y si estas resultan eficaces.

Hay que partir de la base de que, junto con las evidentes mejoras que puede suponer el uso de servicios de *cloud computing*, se produce lo que podríamos denominar «un daño colateral» al contratarlos: una clara pérdida de control sobre el uso de la TIC, que como riesgo debe ser convenientemente gestionado; no olvidemos el enfoque al riesgo a que obliga el RGPD a la hora de tomar cualquier decisión relacionada con las operaciones de tratamiento.

Una pérdida de control frecuentemente amplificada por la falta de transparencia en las condiciones de algunos servicios en la nube, que puede dificultar el cumplimiento de las diferentes obligaciones materiales del responsable del tratamiento.

Precisamente, abordar la transparencia y el fomento de condiciones más ajustadas a los requisitos relacionados con la protección de datos, y a otras normas existentes a escala europea, ha movido a las instituciones europeas a trabajar en lo que se ha venido en llamar la «estrategia europea de *cloud computing*», cuyo punto de referencia principal es una comunicación de la Comisión Europea, de septiembre de 2012: «Liberar el potencial de la computación en nube en Europa».

En particular, por lo que respecta a la protección de datos, resulta irrelevante, en cuanto a las obligaciones del responsable del tratamiento, que los datos se procesen en la «nube», ya que sus obligaciones se mantienen intactas con independencia de los medios de tratamiento utilizados, dado que es de su responsabilidad escoger los medios más adecuados; una elección que debe hacerse teniendo en cuenta los riesgos que puedan suponer para las operaciones de tratamiento, y eso por supuesto se aplica a las medidas de seguridad.

Si tuviéramos que concretar cómo se materializa la pérdida de control a la que hemos hecho referencia, podríamos decir que con carácter general se despliega en tres dimensiones:

- **Se pierde el control directo de los datos:** obviamente es una cuestión de especial relevancia en el caso de los datos de carácter personal, aunque esa pérdida de control también puede afectar a las informaciones de carácter empresarial o de negocio.

- **Se pierde el control directo de los procesos de tecnologías de la información:** el rendimiento y disponibilidad de las tecnologías de la información y su seguridad técnica pasan a depender de terceros, y todo ello con dependencia absoluta de las telecomunicaciones.

- **Se pierde el control en relación con la capacidad contractual:** porque, como ya hemos avanzado, no podremos negociar los términos y condiciones contractuales, salvo contadas excepciones.

Habrá que estar atentos a una diligente formalización de los contratos o, al menos, habrá que ser conscientes de los riesgos legales y de negocio que puede suponer la firma de determinados contratos de adhesión, muy habituales en los servicios en la «nube».

Ciertamente, las prácticas contractuales más comunes del mercado de *cloud* se ciñen a la propuesta de cláusulas estándar por parte del proveedor, pero tal y como expresa una opinión del Grupo de Trabajo del Artículo 29 (Opinión 1/2010), «el desequilibrio en la capacidad de negociar los contratos por parte de pequeños y medianos responsables de tratamientos, respecto de los grandes proveedores de servicios de *cloud computing*, no justifica la aceptación de cláusulas y condiciones que no cumplan con la legislación de protección de datos».

El RGPD ha supuesto reposicionar el marco jurídico en ese escenario complejo; precisamente ese era uno de los objetivos de la reforma (disponer de una regulación adaptada a los nuevos retos planteados por las TIC), definiendo ahora un papel del encargado que va más allá que el de simplemente seguir unas instrucciones del responsable del tratamiento.

Esa nueva perspectiva supone regular una tendencia ya marcada por las autoridades de control, que impelía a los encargados de tratamiento a mostrar una cierta proactividad en el desarrollo de sus actividades, especialmente en cuanto a las medidas de seguridad con las que debían proteger los datos de carácter personal, debiendo ir más allá de las instrucciones recibidas de los responsables de tratamiento.

El RGPD, en su Considerando 101, hace referencia a que el hecho de que los datos personales se transfieran fuera de la Unión Europea (circunstancia que puede darse con cierta normalidad en servicios en la nube) no debe «menoscabar el nivel de protección de las personas físicas garantizado en la Unión» por el RGPD.

En el Considerando 81 del RGPD se hace referencia a que las operaciones de tratamiento que deba llevar un encargado deben «regirse por un contrato u otro acto jurídico con arreglo al derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable», y que este debe concretar los aspectos relacionados con el servicio contratado teniendo en cuenta los riesgos para los derechos y libertades de las personas cuyos datos serán objeto de las operaciones de tratamiento que va a realizar el encargado; es decir, deberán tenerse en cuenta las medidas más adecuadas para mitigar esos riesgos.

4.1. La seguridad y la selección del encargado del tratamiento

Ya hemos puesto en evidencia la importancia del encargado del tratamiento en relación con la implantación y gestión de las medidas de seguridad vinculadas a los tratamientos de datos de carácter personal, ya que como encargados van a llevar a cabo materialmente diversas operaciones de tratamiento que van a estar sujetas a riesgos de diversa probabilidad y gravedad.

El artículo 20.2 del RLOPD recoge la obligación del responsable del tratamiento de «velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto» en el propio RLOPD, obviamente en relación con aquellas cuestiones que resulten de aplicación a las operaciones de tratamiento de datos personales relacionadas con el servicio objeto del encargo de tratamiento.

Por tanto, ya en la propia selección del encargado el responsable del tratamiento deberá ser diligente, optando por el más adecuado, tanto por lo que respecta a las capacidades técnicas vinculadas a los servicios objeto de encargo, y su solvencia como prestador de servicios, como en relación con su capacidad de cumplir con lo previsto en la normativa que en cada caso sea de aplicación en relación con el tratamiento de los datos, es decir, no solo la legislación de carácter general (LOPD y RLOPD en estos momentos, o RGPD y la nueva LOPD a partir de su plena aplicación), también en su caso, con aquellas normas de carácter sectorial que pudieran resultar de aplicación por las características de las operaciones de tratamiento que van a ser realizadas por cuenta del responsable del tratamiento (imaginemos, por ejemplo, las operaciones relacionadas con historias clínicas).

El RGPD es muy claro en esta cuestión, al considerar que para garantizar el cumplimiento de lo previsto en el reglamento, respecto del tratamiento que lleve a cabo un encargado, el responsable, al «encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del» RGPD, y continúa: «incluida la seguridad del tratamiento» (Considerando 81).

Eso, llevado al articulado del RGPD, se traduce en que el artículo 28.1 establece que:

> «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 presente Reglamento y garantice la protección de los derechos del interesado».

4.2. Medidas de seguridad en el contrato de encargado de tratamiento

Cuando el RGPD prevé los contenidos mínimos del acto jurídico que debe vincular al responsable y encargado (art. 28.3), identifica algunos relacionados con la seguridad de los tratamientos; así, tenemos que deberá incluir cláusulas que establezcan que:

- «tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable;
- garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
- tomará todas las medidas necesarias de conformidad con el artículo 32
- ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado».

El artículo 32 del RGPD es el que regula la seguridad del tratamiento, cuestión que trataremos en detalle en el apartado 6.

4.3. Otras obligaciones de los encargados relacionadas con las medidas de seguridad

Sin perjuicio de las obligaciones específicamente relacionadas con la seguridad de los tratamientos que prevé el RGPD, que veremos más adelante en detalle, vamos ahora a identificar otras obligaciones, también previstas en el RGPD, que de manera directa o indirecta se encuentran vinculadas con carácter general a la obligación de llevar a cabo las operaciones de tratamiento en las condiciones de seguridad más adecuadas para proteger los datos personales de los riesgos a que pueden estar expuestos, y que por tanto los encargados deberán tener en cuenta.

El punto de partida sería el Considerando 83, ya que explica que con el objeto de mantener la seguridad, y por tanto evitar que se infrinja lo previsto en el RGPD, «el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos», de tal modo que esas medidas garanticen un nivel de seguridad adecuado; por tanto, el encargado deberá evaluar los riesgos, del mismo modo que viene obligado el responsable, obviamente exclusivamente en relación con aquellas operaciones de tratamiento que le han sido encargadas.

A la hora de determinar esas medidas, también podrá tener en cuenta el estado del arte de la tecnología y el coste de su aplicación; por tanto, podrá utilizar criterios de proporcionalidad a la hora de concretar las medidas de seguridad a implantar.

En el Considerando 95 del RGPD, se hace referencia a que el encargado deberá asistir al responsable para asegurar que se cumpla con lo que pueda prever una evaluación de impacto relativa a la protección de datos o, en su caso, aquello que pueda haber determinado la autoridad de control si se hubiera realizado una consulta previa tras la evaluación de impacto (respecto de las evaluaciones de impacto, en tanto obligan a llevar a cabo una gestión de los riesgos, incluidos los que afecten a la seguridad de los datos, dedicaremos un apartado específico más adelante).

Los encargados también deberán mantener su propio registro de actividades de tratamiento, una nueva obligación prevista en el RGPD; ese registro, que quedará a disposición de las autoridades de control, se regula en el artículo 30.2 del RGPD y también se recoge en el artículo 31 del PLOPD.

Ese registro de actividades debe contener una información mínima, entre la que cabe destacar, en relación con las medidas de seguridad, que, «cuando sea posible», se incluya una «descripción general de las medidas técnicas y organizativas de seguridad»; se trata de un registro que deberá constar por escrito, obviamente incluyendo que su formato pueda ser electrónico.

Al referirse a una descripción general de las medidas de seguridad, recordemos que debemos entender que no se trata de incluir toda la documentación relacionada con la seguridad, es decir, las normas, procedimientos, manuales técnicos, guías, etc.; por tanto, no se trata del documento de seguridad que prevé el RLOPD en su artículo 88, se trata de una información mucho más sintética y que en todo caso es evidente que puede referenciar dónde encontrar información detallada, qué medidas de seguridad están implantas y cómo están implantadas, o incluso describir cuál es la organización de seguridad que gestiona las medidas.

El Considerado 97 dice que «el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del derecho y la práctica en materia de protección de datos» para supervisar internamente el cumplimiento del RGPD, lo que incluye la supervisión de las medidas de seguridad; ese Considerando se está refiriendo obviamente al delegado de protección de datos, que viene regulado en el artículo 37 del RGPD.

Además, según el artículo 28.3 del RGPD, el encargado pondrá a disposición del responsable «toda la información necesaria para demostrar el cumplimiento de las obligaciones» relacionadas con la propia existencia del encargo (art. 28 RGPD), del mismo modo que deberá facilitar la realización de auditorías, ya sea «por parte del responsable o de otro auditor autorizado por dicho responsable».

Y se establece una obligación muy relevante en el mencionado artículo 28.3, ya que el encargado debe informar de manera inmediata al responsable si considera que una determinada instrucción que le ha dado podría infringir el RGPD

«u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros», lo que pone en una posición ciertamente incómoda al encargado, ya que se le asigna también un papel de «vigilante activo» de aquello que el responsable tienen previsto llevar a cabo en relación con las operaciones de tratamiento que forman parte de los servicios objeto de encargo.

Finalmente, en el caso de que el encargado recurra a otro prestador de servicios para realizar determinadas operaciones de tratamiento que le han sido encargadas a él, deberá, entre otras cuestiones, asegurarse de que proporciona «garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del» RGPD, lo que en su caso incluye las medidas de seguridad, cuestión que resulta más que relevante porque, en caso de incumplimiento por parte del subencargado, el encargado inicial «seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado».

5. La gestión de los riesgos para la determinación de las medidas de seguridad

El RGPD considera que, al evaluar el riesgo en relación con la seguridad de los datos, hay que tener en cuenta particularmente eventos no deseados (situaciones) que potencialmente puedan producir a partir de la ejecución de las diversas operaciones de tratamiento de los datos personales, es decir, habrá que tener en cuenta cuestiones como su «destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos», en tanto el impacto de esos eventos no deseados puedan llegar a ocasionar «daños y perjuicios físicos, materiales o inmateriales» a las personas cuyos datos personales son objeto de tratamiento.

Ese impacto podemos concretarlo en dos potenciales tipos de consecuencias:

- Se puede llegar a producir un resultado de daño o perjuicio material que afecte a las personas cuyos datos están siendo objeto de tratamiento (discriminación, rechazo, daño económico, perjuicio laboral, intromisión a la intimidad, etc.).

- Se puede llegar a vulnerar algún derecho o libertad de esas personas, en especial el derecho a la protección de los datos de carácter personal, sobre la base de que las operaciones de tratamiento han vulnerado principios y/o derechos previstos por la regulación, habitualmente como consecuencia del incumplimiento total o parcial de alguna de las obligaciones de seguridad que impone la regulación a responsables y encargados de tratamientos (no olvidemos que se trata de una obligación de resultado).

Obviamente se trata de ámbitos de impacto que están conectados, de manera que por ejemplo, el incumplimiento de una obligación implicará, con carácter general, la vulneración de algún principio y/o derecho, que potencialmente puede tener como consecuencia un daño o perjuicio material para las personas, aunque no siempre se dé esa correlación.

En definitiva, la falta de adopción de medidas de seguridad adecuadas en los tratamientos constituye en sí misma una importante fuente de riesgo potencial para los derechos y libertades.

El RGPD determina que, para garantizar un nivel de seguridad adecuado al riesgo, deberá tenerse en cuenta «el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento».

Por tanto, el RGPD plantea la necesidad de que las medidas de seguridad concretas a aplicar se adapten al riesgo y a las circunstancias que rodean a los tratamientos, lo que modifica sustancialmente el modelo actual (el del título VIII del RLOPD) en el que, para determinar las medidas de seguridad en la práctica, solo se tiene en cuenta el tipo de datos; ahora las medidas de seguridad a adoptar deberán adaptarse a las circunstancias que le sean propias a cada tratamiento.

Como decíamos, por lo que respecta a la gestión de los riesgos en relación con la seguridad de los tratamientos, en particular habrá que tener en cuenta los riesgos que pueda implicar el tratamiento como consecuencia de:

- la destrucción de datos personales
- la pérdida de datos personales
- la alteración de datos personales (accidental o malintencionada)
- la comunicación no autorizada de datos personales
- el acceso no autorizado a los datos personales

Hay que insistir en la idea de que las decisiones relacionadas con la reducción de riesgo no se limitan, exclusivamente, a las medidas de seguridad. Hay otras decisiones no directamente vinculadas a la seguridad de los datos que también deberán ser adoptadas para reducir la probabilidad y gravedad de riesgo para los derechos y libertades de las personas cuyos datos son objeto de tratamiento.

La gestión del riesgo implica identificar, analizar y valorar situaciones hipotéticas (a las que podemos denominar como potenciales escenarios de riesgo o amenazas), que en el caso de materializarse podrían dar lugar a los daños y perjuicios, o vulneraciones, a las que ya se ha hecho referencia.

Una definición directa y sencilla de riesgo sería: «proximidad de un posible daño».

Existen diversas metodologías para llevar a cabo la gestión de riesgos, algunas de ellas estrechamente vinculadas a las tecnologías de la información. El RGPD no determina de qué manera deben gestionarse los riesgos; por tanto, cualquiera de esas metodologías convenientemente adaptadas a los criterios de riesgo del RGPD (en esencia, que tenga en cuenta el riesgo para los derechos y libertades) podrán ser utilizadas.

Lo que haremos a continuación es describir con carácter general qué actividades se llevan a cabo a la hora de gestionar riesgos; se trata de una simple aproximación a lo que implica ese enfoque a riesgos que plantea el RGPD.

5.1. Aspectos generales de la gestión de riesgos

La gestión de los riesgos relacionados con las operaciones de tratamiento sujetas al RGPD debe aplicarse a todas las decisiones relacionadas con el tratamiento de los datos de carácter personal, por tanto, incluyendo a aquellas vinculadas a la seguridad de los tratamientos.

Habrá que tomar decisiones sobre la base del riesgo, por ejemplo: a la hora de decidir cómo gestionar el consentimiento, o cómo facilitar el acceso a los derechos, en la designación del delegado de protección de datos o en la selección del encargado de tratamiento, por citar tan solo algunas decisiones no vinculadas directamente a la seguridad de los tratamientos.

Por tanto, con carácter general, y no limitándose exclusivamente a la seguridad de los tratamientos, el RGPD incorpora la gestión de riesgos como una actividad que necesariamente deberá llevar a cabo el responsable del tratamiento (en su caso, el encargado del tratamiento) para seleccionar y adoptar las medidas de carácter técnico y organizativo más adecuadas para:

- garantizar que el tratamiento se realiza según lo previsto en el RGPD
- y demostrar que el tratamiento es conforme con el RGPD «responsabilidad proactiva».

Según el propio RGPD, los riesgos, tanto por lo que respecta a su «probabilidad» como a su «gravedad», pueden ser «variables», así que será necesario a los efectos de la selección y aplicación de las medidas técnicas y organizativas tener en cuenta:

- hasta qué punto es probable que se produzca la situación que pone en riesgo derechos y libertades como consecuencia del tratamiento de datos personales,
- y cómo de graves pueden ser las consecuencias en caso de que se produzca la situación que pone en riesgo derechos y libertades.

Por tanto, como veremos, será necesario tener la capacidad de graduar, de la manera más objetiva posible, el nivel o zona de riesgo en que se sitúan las operaciones de tratamiento, y en su conjunto el tratamiento, es decir, habrá que evaluar los riesgos.

La evaluación de esos riesgos, que forma parte de la gestión de riesgos, deberá permitir determinar, especialmente, si el tratamiento supone un «alto riesgo», una noción a la que nos referiremos más delante de manera específica, ya que resulta muy relevante en el contexto del RGPD.

Cualquier tratamiento de datos de carácter personal implica potencialmente algún tipo de riesgo, es decir, el hecho de recopilar información relativa a personas físicas, que es susceptible de ser sometida a operaciones de tratamiento aplicando técnicas diversas, tiene como consecuencia la exposición de ese conjunto de información a riesgos de diversa índole.

Por tanto, siempre va a estar presente un riesgo inherente al propio tratamiento, es decir, por el mero hecho de llevarse a cabo, de manera que el proceso de gestión de riesgos lo que va a procurar es mantener ese riesgo en unos niveles que resulten aceptables, en tanto se creen unas condiciones adecuadas para el tratamiento de los datos de carácter personal.

Gestionar los riesgos implica, por un lado, evaluar el riesgo, y por otro, tratar el riesgo, cuestiones que abordaremos en detalle más adelante.

El tratamiento de los riesgos irá dirigido a identificar medidas de carácter técnico y organizativo, orientadas a reducir la probabilidad y gravedad vinculadas a las operaciones de tratamiento, en tanto están expuestas a situaciones hipotéticas no deseadas, que deberemos identificar.

Esas medidas, dirigidas a controlar los riesgos, deberían variar a la baja el nivel de riesgo de las operaciones de tratamiento, de lo que finalmente resultará un riesgo residual, es decir, un riesgo que ya no podemos reducir más, al menos *a priori*, por lo que deberemos reconocerlo y aceptarlo.

Dado que estamos abordando una materia que ya tiene un cierto recorrido, especialmente en el ámbito de la seguridad de las TIC, a título de complemento y de una manera muy breve, vamos a hacer referencia a algunas metodologías de análisis y gestión de riesgos.

Así tenemos:

- UNE-ISO 31000:2010 (Gestión del riesgo. Principios y directrices) y UNE-EN 31010:2011 (Gestión del riesgo. Técnicas de apreciación del riesgo), orientadas a los riesgos empresariales en un sentido amplio.

- UNE 71504:2008 Metodología de análisis y gestión de riesgos para los sistemas de información.

- La familia de Normas ISO 27000 sobre seguridad de la información, que incluyen diferentes referencias a la gestión de los riesgos derivados del uso de las tecnologías y en relación con los sistemas de gestión de la seguridad de la información (muy conocidos por sus siglas SGSI); dedicada a ello de manera específica tenemos la ISO/IEC 27005:2011.

Hay metodologías muy completas para el análisis y gestión de riesgos en relación con la seguridad de los sistemas de información, como por ejemplo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información); su primera versión fue publicada en 1997 por el entonces Consejo Superior de Informática y el Ministerio de Administraciones Públicas; ahora ya está en su versión 3. Se trata de una metodología creada por y para el sector público, pero que resulta totalmente aplicable a otros sectores.

Si bien se trata de una metodología previa, en el tiempo se ha ido actualizando, y al estar muy vinculada a la gestión de los riesgos en los sistemas de información de las Administraciones públicas, está alineada con el ENS, que establece que la gestión de la seguridad debe estar basada en los riesgos:

> «La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad» (art. 6.2 ENS).

En este sentido, hay que recordar la ya mencionada Disposición adicional primera del PLOPD, que se refiere a las «medidas de seguridad en el ámbito del sector público» y a la adaptación del ENS a lo previsto en el artículo 32 del RGPD en cuanto a los criterios de determinación del riesgo.

Se trata de una metodología muy documentada y con herramientas de apoyo a su realización; se puede acceder a una detallada información al respecto en el siguiente enlace: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WTFMUpLygdU.

Tan solo a título enunciativo, y no exhaustivo, otras metodologías, normas o herramientas de análisis de riesgos de los sistemas de información serían:

- Citicus One: software comercial de Citicus - https://www.citicus.com/.

- CRAMM (CCTA Risk Assessment and Management Methodology): se dejó de mantener en el año 2003, pero sigue siendo una referencia en cuanto a la gestión de riesgos. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - http://www.cert.org/resilience/products-services/octave/index.cfm.

- NIST SP 800-39 Gestión de riesgos de los sistemas de información, una perspectiva organizacional - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

- NIST SP 800-30: Guide for Conducting Risk Assessments - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

- Mehari: método de gestión y análisis de riesgos desarrollado por CLUSIF - https://www.clusif.asso.fr/.

Asimismo, podemos encontrar metodologías para diferentes sectores, como por ejemplo, los riesgos laborales, financieros, de seguros, medioambientales, etc.

En cualquier caso, hay una cosa que debe incorporar cualquier metodología relacionada con los riesgos, y es que debe ser repetible, a fin de que podamos ir valorando cómo evoluciona el nivel de riesgo en función de las decisiones que se van adoptando y en función de la propia evolución, en el tiempo, de aquello que es objeto de la gestión de riesgos.

5.2. El concepto de alto riesgo

Concretar si un tratamiento puede calificarse de «alto riesgo» resulta muy relevante en el RGPD, ya que tal circunstancia va a tener consecuencias que van más allá de la decisión sobre qué medidas concretas se van a aplicar para reducir la «probabilidad» y la «gravedad».

Así tenemos que, por ejemplo, en el caso de las evaluaciones de impacto relativas a los datos personales, si una vez realizada la gestión de riesgos de las operaciones de tratamiento se considera que estas suponen un «alto riesgo», el responsable del tratamiento deberá llevar a cabo una consulta previa a la autoridad competente; o cuando se produzca un incidente de seguridad que afecte a los datos personales, y del mismo se derive un «alto riesgo» para las personas afectadas, estas deberán ser informadas de las circunstancias en que se ha producido la violación de datos.

Hay actividades de tratamiento para las cuales el legislador ya ha establecido algunas prevenciones, en cuanto a considerar que el riesgo inherente que presentan para los derechos y libertades es de nivel alto, por lo que el responsable del tratamiento debe limitarse a verificar si las actividades de tratamiento que pretende llevar a cabo encajan en los supuestos en que el RGPD prevé que potencialmente se genere ese nivel significativo de riesgo, y actuar en consecuencia.

En este sentido habrá que tener en cuenta y poner en relación el Considerando 76 del RGPD, que en su primera parte determina que:

> «la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos».

Es decir, no solo las tecnologías utilizadas son relevantes para detectar potenciales riesgos, también lo es la propia definición del tratamiento, pudiendo darse la circunstancia de que la simple recogida y sistematización de determinados datos de carácter personal implique un alto riesgo para los derechos y libertades de las personas físicas, sin que la tecnología resulte ser el factor determinante de riesgo.

Por lo que respecta a la evaluación de los riesgos, el RGPD considera que:

> «el riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto».

De tal modo que se introduce la necesidad de seguir métodos objetivos de valoración de los riesgos, que permitan valorar si el riesgo debe considerarse como alto.

En una primera aproximación muy simple, podemos definir por *riesgo* la proximidad de un posible daño[1], intuitivamente calificaremos a una situación como de «alto riesgo» cuando ese daño puede resultar muy grave; por tanto, la gravedad de las consecuencias de una determinada actividad o inactividad (hacer o dejar de hacer) va a ser determinante para concluir que la situación ante la cual nos encontramos es de mucho riesgo, lo que sería equivalente a decir que hay un alto riesgo.

(1)Según el *Diccionario de la Lengua Española* de la RAE: «Contingencia o proximidad de un daño».

Hay otro parámetro que habrá que tener en cuenta a la hora de valorar el riesgo; concretamente, la probabilidad de que ese potencial daño llegue a producirse, por lo que también una alta probabilidad podemos vincularla a un alto riesgo de las operaciones de tratamiento.

Con carácter general deberemos considerar que existe un alto riesgo cuando las operaciones de tratamiento de los datos personales potencialmente puedan causar una grave vulneración de los derechos y libertades de las personas, cuyos datos son objeto de tratamiento.

Por derechos y libertades debemos entender todos aquellos reconocidos como fundamentales por el ordenamiento jurídico[2], lo que incluye también los reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea; por supuesto, entre ellos está el derecho a la protección de los datos de carácter personal (art. 8 de la Carta).

(2)Art. 1.2 del RGPD: «El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales».

¿Cuándo vamos a considerar que se puede producir una grave vulneración de los derechos y libertades fundamentales? Al menos con carácter general:

- Cuando potencialmente el tratamiento de los datos personales pueda llegar a impedir el libre ejercicio de los derechos y libertades a sus titulares (nota: obviamente, esto no quiere decir que esa sea la finalidad del tratamiento, ya que lo haría directamente ilegítimo, sino que en virtud del

riesgo inherente que implica la sola acumulación de la información y la propia ejecución de las operaciones de tratamiento, aparece esa potencial vulneración).

- Cuando potencialmente el tratamiento de los datos personales pueda dejar sin contenido al derecho o libertad (aquí debemos tener también en cuenta la nota del párrafo anterior).

- Cuando potencialmente el tratamiento de los datos personales pueda ser el origen de «daños y perjuicios físicos, materiales o inmateriales[3]» a las personas interesadas.

[(3)]Ver el Considerando 75 del RGPD

Hay situaciones en las que resulta evidente que existe un mayor riesgo de que se produzcan esas vulneraciones; por ejemplo, no es lo mismo que se traten datos de cien personas que de un millón; no es lo mismo que se traten exclusivamente los datos básicos de identificación, o que el tratamiento incluya datos relacionados con la salud; y no es lo mismo utilizar una tarjeta para identificar a alguien que implantarle un «chip» bajo la piel. En cualquier caso, hay que tener en cuenta que no suele ser un único parámetro el que provoca esa mayor gravedad, es la suma de varios factores lo que llevará a identificar el «alto riesgo».

El Grupo de Trabajo del Artículo 29 (GT29), en el WP 248 de abril de 2017, revisado en octubre de 2017 (que recoge una serie de directrices en relación con las evaluaciones de impacto), aporta una serie de criterios que pueden revelar que estamos ante un tratamiento que genera, de manera inherente, un elevado riesgo, o un riesgo significativo.

El GT29, en ese mismo documento, deja claro que el RGPD no requiere que se realice una evaluación de impacto para cada tratamiento del cual se deriven riesgos para los derechos y libertades de las personas, siendo solo obligatoria «cuando puede dar lugar a un alto riesgo».

Esos criterios se describen en el WP 248 de la siguiente manera (transcripción del contenido del WP248, traducido por el autor, por tanto no oficial):

1) Evaluación o *scoring*, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relativos al rendimiento en el trabajo de la persona afectada, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, localización o movimientos» (Considerandos 71 y 91). Ejemplos de esto podría incluir una entidad financiera (banco) que examina a sus clientes frente a una base de datos de referencia de crédito, o una empresa de biotecnología que ofrece pruebas genéticas directamente a los consumidores con el fin de evaluar y predecir los riesgos de enfermedad o salud, o una empresa de elaboración de perfiles de comportamiento o de marketing basado en el uso o la navegación en su sitio web.

2) Toma automatizada de decisiones con efecto jurídico o similar significativo: tratamiento que tenga por objeto la toma de decisiones sobre personas físicas que produzcan «efectos jurídicos en relación con la persona física» o que «afecten de manera similar a la persona física» (art. 35.3.a). Por ejemplo, el tratamiento puede conducir a la exclusión o discriminación contra individuos. El tratamiento **con poco o ningún efecto en los individuos** no coincide con este criterio específico. En las próximas directrices sobre perfiles del GT 29 se proporcionarán más explicaciones sobre estas nociones.

3) Vigilancia sistemática: tratamiento utilizado para observar, supervisar o controlar a los interesados, incluidos los datos recogidos mediante el «control sistemático de una zona accesible al público» (art. 35.3.c), o los que son captados en redes de comunicaciones.

Vigilancia sistemática

El GT29 interpreta que «sistemático» tiene uno o más de los siguientes significados (ver el GT29 Directrices sobre el delegado de protección de datos WP243):

- ocurrir de acuerdo con un sistema;
- predeterminados, organizados o metódicos;
- que se realicen en el marco de un plan general de recogida de datos;
- realizado como parte de una estrategia.

El GT29 interpreta el «área de acceso público» como cualquier lugar abierto a cualquier persona, por ejemplo una plaza, un centro comercial, una calle o una biblioteca pública.

Este tipo de seguimiento es un criterio para detectar el riesgo elevado, debido a que los datos personales pueden recopilarse en circunstancias en que los sujetos de los datos **pueden no estar al tanto de quién está recopilando sus datos y cómo se utilizarán**. Además, puede llegar a ser imposible que las personas eviten estar sometidas a ese tratamiento en espacios públicos (o accesibles al público).

4) Datos sensibles o de naturaleza muy personal: incluye categorías especiales de datos tal como se definen en el artículo 9 del RGPD (por ejemplo, información sobre las opiniones políticas de los individuos), así como datos personales relativos a condenas o delitos penales. Un ejemplo sería un hospital general que mantenga los expedientes médicos de los pacientes o un investigador privado que disponga de información de delincuentes. Este criterio también incluye datos que, en términos más generales, puede considerarse que aumentan el posible riesgo para los derechos y libertades de las personas, como **datos de comunicaciones electrónicas, datos de localización, datos financieros** (que podrían utilizarse para el fraude de pagos). A este respecto, puede ser relevante el hecho de que los datos ya hayan sido puestos a disposición del público por el interesado o por terceros. El hecho de que los datos personales estén a disposición del público puede considerarse un factor en la evaluación, si existe la expectativa de que estos van a seguir siendo utilizados

para unos ciertos fines relacionados por la publicación de los mismos. Este criterio puede incluir también la información tratada por una persona física en el curso de actividades puramente personales o domésticas (tales como servicios de computación en nube para la gestión de documentos personales, servicios de correo electrónico, diarios, lectores electrónicos equipados con funciones de toma de notas, que pueden contener información muy personal), cuya divulgación o tratamiento para cualquier otro propósito, fuera de las actividades domésticas, puede ser percibida como muy intrusiva.

No obstante, si los datos sensibles no se tratan sistemáticamente y a gran escala, su tratamiento no presenta de manera automática riesgos elevados para los derechos y libertades de los interesados. Por ejemplo, un responsable de tratamiento que organiza un evento corporativo, y quisiera saber a qué tipo de alimento son alérgicos los participantes, podría tratar estos datos sensibles excepcionalmente y no necesitaría realizar una EIPD. Del mismo modo, el tratamiento de categorías especiales de datos por un solo médico, en su consulta, no debe considerarse «a gran escala» (ver Considerando 91).

5) Datos tratados a gran escala: el GDPR no define lo que constituye «a gran escala», aunque el Considerando 91 proporciona algunas orientaciones. En cualquier caso, el GT 29 recomienda que se tengan en cuenta, en particular, los siguientes factores para determinar si el tratamiento se realiza a gran escala[4]:

(4)Ver las directrices del GT29 sobre el delegado de protección de datos WP 243.

a) El número de sujetos afectados, ya sea como número específico o como proporción de un conjunto de población.

b) El volumen de datos y/o el rango de diferentes tipos de datos que se están tratando.

c) La duración o permanencia de la actividad de tratamiento de datos.

d) La extensión geográfica del tratamiento.

6) Conjuntos de datos que han sido emparejados (vinculados) o combinados, por ejemplo, datos procedentes de dos o más operaciones de tratamiento de datos realizadas con fines diferentes y/o por diferentes responsables de tratamientos, de tal modo que las operaciones de tratamiento excedan las expectativas razonables de las personas a las cuales hacen referencia los datos[5] combinados.

(5)Véase la explicación en el Dictamen del GT29 sobre la limitación de la finalidad WP 203, pág. 24.

7) Datos relativos a sujetos vulnerables (Considerando 75): el tratamiento de este tipo de datos puede requerir una EIPD debido al aumento del desequilibrio de poder entre el interesado y el responsable del tratamiento, lo que significa que el individuo no puede consentir u oponerse al tratamiento de sus datos. Por ejemplo, los empleados a menudo se enfrentan a serias dificultades para oponerse al tratamiento realizado por su empleador, cuando está vinculado a la gestión de recursos humanos. Del mismo modo, los niños pueden considerarse incapaces de tomar conciencia de qué supone el tratamiento, de prestar su consentimiento de manera informada, o de oponerse al tratamiento de sus datos. También se puede tratar de un segmento más vulnerable de la pobla-

ción que requiere una protección especial, como por ejemplo, los enfermos mentales, los solicitantes de asilo o los ancianos, un paciente o, en cualquier caso, cuando se identifica que se produce un desequilibrio en la relación entre la persona afectada y el responsable del tratamiento, en razón de su situación de vulnerabilidad.

8) Utilizar o aplicar soluciones tecnológicas u organizativas de forma innovadora, como combinar el uso de la huella dactilar y el reconocimiento facial para mejorar el control de acceso físico, etc. El RGPD determina claramente (art. 35.1 y Considerandos 89 y 91) que el uso de una nueva tecnología puede desencadenar la necesidad de llevar a cabo una EIPD. Esto se debe a que el uso de dicha tecnología puede implicar nuevas formas de recolección y uso de datos, posiblemente con un alto riesgo para los derechos y libertades individuales. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a entender y tratar tales riesgos. Por ejemplo, ciertas aplicaciones de «internet de cosas» podrían tener un impacto significativo en la vida cotidiana de los individuos y su privacidad; y por lo tanto, requieren de una evaluación de impacto.

9) Cuando el tratamiento en sí mismo «**impida a las personas afectadas ejercer un derecho o utilizar un servicio o un contrato**» (art. 22 y Considerando 91). Esto incluye tratamientos realizados en un área pública, que las personas que acceden no pueden evitar, o procesamientos que tienen por objeto permitir, modificar o denegar el acceso de los sujetos a un servicio, o a la formalización de un contrato. Un ejemplo de esto es cuando un banco examina a sus clientes frente a una base de datos de referencia de crédito para decidir si les ofrece un préstamo.

El GT29, en el WP 248, considera que cuantos más criterios de esa relación se cumplan en un tratamiento, o en operaciones concretas de tratamiento, será más probable que el tratamiento presente un alto riesgo para los derechos y libertades de los interesados.

5.3. Riesgos para la seguridad de los datos y riesgos para los derechos y libertades

Debemos insistir en una cuestión que resulta muy relevante y que supone un diferencia esencial en el enfoque a riesgos que plantea el RGPD, ya que cuando este se refiere a los riesgos que pueden suponer los tratamientos, los concreta en «riesgos para los derechos y libertades fundamentales», es decir, en la estimación de hasta qué punto pueden ser vulnerados los derechos y libertades de las personas como consecuencia del tratamiento de sus datos personales.

La gestión de riesgos a la que se enfoca el RGPD ciertamente va más allá de estimar la exposición al riesgo de los sistemas de información, o de los datos, es decir, la gestión de los riesgos estrictamente vinculados a la seguridad, sino que en el momento de proceder a gestionar los riesgos de los tratamientos, el responsable o el encargado deberá tener en cuenta aquellas situaciones que pueden suponer una potencial vulneración de derechos y libertades fundamentales.

Respecto a las situaciones en que el RGPD considera que existe riesgo para los derechos y libertades, identifica las siguientes:

- cuando «se prive a los interesados de sus derechos y libertades», lo que incluye impedir su normal y libre ejercicio,
- cuando se provoquen «daños y perjuicios físicos, materiales o inmateriales» a las personas interesadas,
- cuando, al realizar el tratamiento, se revelen categorías especiales de datos personales,
- si se crean o utilizan perfiles personales,
- cuando se realice el tratamiento de datos personales de colectivos especialmente vulnerables, lo que incluye a los niños,
- cuando las operaciones de tratamiento se realicen sobre una gran cantidad de datos personales y/o sobre un gran número de personas.

5.4. Identificación, análisis y valoración de riesgos

Para evaluar el riesgo se llevarán a cabo, principalmente, tres tipos de actividades.

1) Las que tienen por objeto **identificar el origen de los riesgos**, es decir, reflexionar sobre los potenciales escenarios de riesgo o amenazas a los que puedan estar expuestos los datos personales, en tanto se puedan llegar a producir ciertos eventos no deseados.

2) Las de **análisis de esas situaciones que generan riesgo**, teniendo en cuenta los diversos factores que pueden entrar en juego a la hora de determinar, de la manera más precisa posible, el nivel de riesgo.

3) La **valoración de los riesgos**, sobre la base de determinar, por un lado, la probabilidad de que un evento no deseado se produzca, y por otro, su potencial gravedad, es decir, las consecuencias o impacto que puede tener ese evento en caso de producirse.

En general la valoración de riesgo, si bien puede objetivarse parcialmente, lo cierto es que algunas de las variables o factores que forman parte de la evaluación de riesgos pueden tener una componente subjetiva; aquí el conocimiento y la experiencia del profesional que identifica, analiza y valora los riesgos resultan clave para que el diagnóstico sea lo más preciso posible.

Ese conocimiento y esa experiencia deberán aplicarse siempre como mecanismo de corrección de aquellas valoraciones de riesgos que puedan considerarse desviadas o no alineadas con la realidad de cada potencial escenario de riesgo analizado.

Para llevar a cabo la evaluación de riesgos (identificación, análisis y valoración), resulta imprescindible disponer de una información detallada del conjunto de operaciones de tratamiento que se tiene previsto llevar a cabo, y de sus características, y por supuesto resulta recomendable utilizar alguna de las metodologías a las que ya hemos hecho referencia, o cualquier otro método de trabajo que permita reproducir (método repetible) y documentar la gestión de riesgos.

No hay que olvidar que proteger los datos personales, a partir de la adopción de medidas de seguridad, no deja de ser una obligación de resultado que, en el marco del RGPD, está sustentada, en cuanto a las medidas a implantar, en una evaluación previa de los riesgos que para la seguridad de los datos puedan derivarse de las operaciones de tratamiento.

5.4.1. Identificación del riesgo

Deberán identificarse qué potenciales escenarios de riesgos podrían implicar, en el caso de producirse, algún daño o perjuicio para las personas afectadas por el tratamiento de los datos, ya sea porque las consecuencias implican un daño o perjuicio material directo, o porque vulneran principios o derechos y libertades, o bien directamente suponen el incumplimiento de alguna obligación por parte del responsable del tratamiento.

Podemos disponer de listas «preelaboradas» de situaciones de riesgo o de amenazas a tener en cuenta respecto de la seguridad de los tratamientos, y deberemos establecer si aplican, o no, en las diferentes operaciones de tratamiento; por ejemplo, un potencial escenario de riesgo o amenaza podría ser que se produzcan accesos no autorizados a los datos personales, o que un incidente

con la base de datos pueda hacer desparecer la información, o bien que nuestro proveedor de servicios en la nube tenga un problema con la disponibilidad de sus sistemas.

Una vez tenemos identificados todos los potenciales escenarios de riesgo que consideramos que pueden producirse en el tratamiento, pasaremos a la siguiente etapa de evaluación de los riesgos: la del análisis de los riesgos.

5.4.2. Análisis del riesgo

El objetivo que se persigue con el análisis de riesgos es determinar hasta qué punto, en las operaciones de tratamiento, pueden darse eventos no deseados, teniendo en cuenta cómo de vulnerables son las operaciones de tratamiento a los potenciales escenarios de riesgo.

Deberemos analizar hasta qué punto es probable que se produzca un evento no deseado, y cuál sería su impacto en términos de gravedad para las personas cuyos datos son objeto de tratamiento.

Para ello, deberemos conocer las medidas previstas para:

- Alejarnos del potencial escenario de riesgo o de la amenaza, es decir, **reducir la probabilidad** de que se produzcan.

- Minimizar su impacto negativo en el caso de que se produzca; en definitiva, **reducir su gravedad**.

En general, las metodologías de gestión de riesgos plantean analizar las diferentes medidas que se han previsto inicialmente, para efectuar una primera evaluación de riesgos, en tanto estas puedan incidir en la reducción de los riesgo del tratamiento (en sus dos dimensiones: probabilidad y gravedad); de ese modo, podremos valorar el nivel de riesgo inicial que generan las operaciones de tratamiento.

Con carácter general, podemos considerar que las medidas orientadas a reducir la probabilidad serán de carácter preventivo, en tanto que las medidas destinadas a reducir el impacto serán de tipo reactivo o de recuperación, ya que van dirigidas a intentar reducir la gravedad.

Hay que tener en cuenta que, si no se toma ningún tipo de medida para mitigar la probabilidad o la gravedad de un potencial escenario de riesgo, podemos considerar que es altamente probable que se produzca y, *a priori*, podría tener unas consecuencias muy graves, ya que afectaría a la protección de los datos de carácter personal (la valoración más específica del nivel de riesgo se lleva a cabo en la siguiente etapa de evaluación de los riesgos: la de valoración de los riesgos).

5.4.3. Valoración del riesgo

Una vez tenemos identificadas todas las medidas previstas inicialmente, se procede a valorar tanto la probabilidad como la gravedad, lo que nos proporcionará información del nivel de riesgo inicial del tratamiento y nos va a permitir, por ejemplo, elaborar un primer mapa de riesgos del tratamiento que conecte las variables probabilidad y gravedad.

Habitualmente, las metodologías de gestión de riesgos recurren a una escala de valores para determinar la probabilidad y la gravedad; esa escala puede ser cualquiera que nos permita situar, de la manera más precisa posible, en qué nivel de riesgo de sitúa el tratamiento; pueden ser valores que vayan de 1 a 10, o de 1 a 3, valores porcentuales, o incluso niveles sobre la base de un esquema de colores; así, por ejemplo, en una escala de riesgo del 1 al 5 podríamos tener:

Probabilidad		**Gravedad**	
Descripción	**Nivel**	**Descripción**	**Nivel**
Inminente	5	Extremadamente grave	5
Muy probable	4	Significativamente grave	4
Probable	3	Grave	3
Poco probable	2	Leve	2
Improbable	1	Irrelevante	1

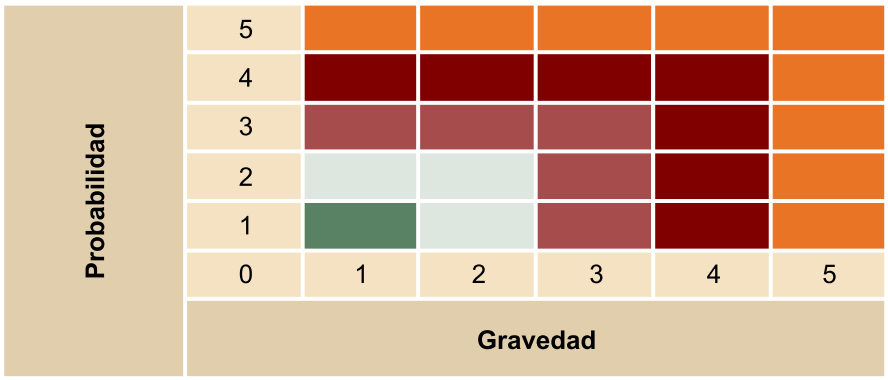
Los valores superiores de cada factor de riesgo (probabilidad y gravedad) indican en su conjunto altos niveles de riesgo, ya que nos encontramos muy cerca de que se produzca la situación de riesgo y las potenciales consecuencias de producirse el evento no deseado serían muy graves para los derechos y libertades de las personas afectadas; los valores inferiores indican un nivel bajo de riesgo en cuanto a su impacto o gravedad.

5.4.4. Mapa de riesgos

Por mapa de riesgos vamos a entender una representación visual o gráfica del nivel de riesgo en que se sitúa inicialmente el tratamiento; no es más que una herramienta que ayuda a comprender el riesgo, y por tanto ese mapa puede ser elaborado de la manera que se considere más adecuada para la organización destinataria.

Los niveles de riesgo, en cuanto a los factores de probabilidad y gravedad, deberán convertirse a una segunda escala que permita determinar si los riesgos que presentan las operaciones de tratamiento son inaceptables, tolerables o aceptables.

La equivalencia, por ejemplo, podría ser la siguiente:



Todos los potenciales escenarios de riesgo que sean valorados con un nivel de riesgo igual o superior a 3 deberán ser considerados riesgos inaceptables, por lo que habrá que considerar aplicar medidas para reducir ese nivel de riesgo (tratamiento de los riesgos), ya que las operaciones de tratamiento estarían situadas en un nivel alto de riesgo.

Cuando el nivel de riesgo sea igual a 2, el riesgo resulta tolerable, pero deberá prestarse especial atención a la eficacia de las medidas previstas; por tanto, es recomendable intentar tratar esos riesgos para bajarlos aún más de nivel.

Cuando el nivel de riesgo se sitúe por debajo de 2 este resulta aceptable, ya que los datos se están tratando en unas condiciones donde los riesgos están razonablemente controlados, si bien, como veremos, los riesgos deben ser revisados con una cierta periodicidad por si estos pudieran llegar a variar, a causa de diversos factores, y por tanto se vea afectada la eficacia de las medidas implantadas en cuanto a su capacidad de mantener controlados los riesgos.

El nivel de riesgo global del tratamiento será el de aquel potencial escenario de riesgo que alcance el nivel más alto de riesgo de todos los que han sido valorados; por tanto, si un potencial escenario de riesgo, o un grupo de ellos, implica un riesgo inaceptable, el nivel de riesgo del tratamiento será ese.

5.5. Tratamiento de los riesgos

Una vez se tienen fijados los riesgos iniciales, deberá tratarse el riesgo mediante la adopción de medidas que permitan «alejarnos» del riesgo (probabilidad) o que reduzcan, en la medida de lo posible, las potenciales consecuencias negativas (gravedad).

Sobre la base de la teoría del riesgo, debemos tener en cuenta que para la gestión del riesgo podemos al menos adoptar hasta cuatro posturas diferentes:

- **Eliminarlo:** para evitar por completo el riesgo hay que eliminar la probabilidad de que este se materialice; si prescindimos del proceso o de la

operación que puede dar lugar al potencial escenario de riesgo, podremos decir que hemos eliminado ese riesgo (por ejemplo: si decidimos que en ningún caso vamos a tener encargados de tratamiento, todos los riesgos relacionados con esa figura van a desaparecer).

- **Aceptarlo:** hemos llegado a la conclusión de que no podemos hacer más de lo que ya hemos previsto, por lo que vamos a asumir de manera consciente e informada que tenemos un determinado nivel de riesgo; no debe aceptarse un riesgo alto, solo se aceptan aquellos riesgos que, por ejemplo, se encuentren en la zona de riesgo tolerable o aceptable.

- **Transferirlo:** en este caso tomamos la decisión de no actuar directamente sobre el riesgo, sino sobre sus consecuencias, de manera que optamos por desviar el impacto, por ejemplo, contratando una póliza de seguro que nos cubra de posibles multas o indemnizaciones. La mayoría de compañías aseguradoras, entre las coberturas que ofrecen, incluyen la de cubrir la contingencia que pueda suponer la imposición de una multa por parte de una autoridad de control. Esta postura es compleja de adoptar y debe sospesarse cuál puede ser su alcance real, ya que hay otras cuestiones a considerar como, por ejemplo, la imagen de la organización. En cualquier caso, desde la perspectiva del RGPD, no debería considerarse como mecanismo de tratamiento del riesgo, ya que precisamente lo que nos plantea el RGPD es que modifiquemos el riesgo para reducirlo.

- **Reducirlo:** se trata de tomar decisiones que impliquen la aplicación de nuevas medidas, adicionales, complementarias o sustitutorias de las ya previstas, que reduzcan, ya sea la probabilidad o cercanía del riesgo, o las consecuencias negativas que puedan tener.

Por tanto, procederemos a seleccionar medidas que reduzcan la probabilidad y gravedad, ya sea añadiendo nuevas o modificando las existentes; en cualquier caso, se trata de que una vez seleccionadas las medidas volvamos a analizar y valorar el nivel de riesgo, para ver de qué modo van a modificar el nivel de riesgo inicial; finalmente, este será el riesgo residual, es decir, aquel que ya no podemos seguir tratando.

Una vez se han identificado las medidas adicionales, los riesgos se verán modificados, por lo que las metodologías de riesgos plantean volver a «dibujar» el mapa de riesgos.

6. Adopción de las medidas de seguridad

Como ya hemos venido reiterando, asegurar los tratamientos de datos personales implica adoptar medidas de seguridad, tanto de carácter técnico como organizativo; se trata de una obligación de resultado que afecta en primer lugar a responsables de tratamiento, pero también a los encargados, por su singular participación en los tratamientos de datos personales, ya que dado que materialmente tratan los datos, a ellos les va a corresponder generalmente implantar y gestionar las medidas de seguridad, a partir de las instrucciones que el responsable del tratamiento necesariamente debe transmitirles.

Ya hemos hecho referencia a una diferencia sustancial entre el modelo de medidas de seguridad a aplicar que prevé la LOPD (recogido en el RLOPD) y el planteamiento que se hace desde el RGPD.

El cambio de paradigma que en la protección de los datos supone el RGPD implica que las decisiones sobre la seguridad de los tratamientos se van a tomar sobre la base de la gestión de los riesgos (como ya hemos abordado), mientras que en el RLOPD las decisiones sobre las medidas de seguridad a implantar quedan prácticamente limitadas a determinar qué tipo de datos van a ser objeto de tratamiento y, en función del tipo de datos tratados, el legislador ya nos plantea con una cierta precisión qué medidas deben implantarse y de qué manera.

En el RGPD se hace referencia a la posibilidad de adoptar algunas medidas de seguridad (ya veremos con más precisión qué son exactamente), pero se hace desde una perspectiva muy generalista, y en ningún caso en el sentido de establecer que necesariamente deban ser esas las medidas a adoptar, máxime teniendo en cuenta que el detalle en su descripción es mínimo.

En este apartado vamos a tratar, de manera separada, las medidas de seguridad que se derivan de la LOPD, recogidas en el RLOPD, y las medidas de seguridad vistas desde la perspectiva del RGPD.

6.1. Medidas de seguridad en la LOPD

6.1.1. Descripción de las medidas de seguridad

Las medidas de seguridad se describen en el RLOPD a lo largo de treinta y seis artículos (del 79 al 114) que, junto con otras referencias a las medidas de seguridad, representan aproximadamente un 30 % del conjunto del reglamento.

La legislación vigente parte de la base de que, para una adecuada salvaguarda de los derechos y las libertades, hay que obligar a los responsables de tratamientos a adoptar medidas técnicas y organizativas que protejan la información de carácter personal, ponderando aspectos como el estado de la tecnología en cada momento o la naturaleza de los datos a proteger.

Como ya hemos visto, las medidas de seguridad, en relación con los datos personales, deben evitar (art. 9.1 LOPD):

- La alteración de la información (sea accidental o malintencionada)
- La pérdida de la información de carácter personal
- El tratamiento no autorizado de los datos
- El acceso a los datos por parte de personas no autorizadas

El RLOPD regula las medidas de seguridad en su título VIII, de la siguiente forma:

- Primero prevé unas medidas de carácter general que afectan a todo tipo de tratamientos y todos los niveles de seguridad (caps. I y II, arts. 79 al 88).
- Continúa la regulación específica de las medidas de seguridad para los tratamientos automatizados, y se utiliza la asignación de niveles de seguridad de acuerdo con el tipo de datos tratados: nivel básico, nivel medio y nivel alto (cap. III, arts. 89 al 104).
- Finalmente, se regulan las medidas de seguridad para los tratamientos no automatizados, y se sigue el mismo esquema de los tres niveles de seguridad (cap. IV, arts. 105 al 114).

Recordemos que las medidas de seguridad se aplicarán a:

- centros de tratamiento
- locales
- equipos
- sistemas
- programas

En definitiva, hay que aplicarlas a todos aquellos elementos físicos y lógicos que intervienen en el tratamiento de los datos de carácter personal.

Con carácter general, las medidas de seguridad deben proteger los datos de carácter personal con independencia de su ubicación o del sistema de tratamiento: allí donde se trata información personal debe estar implantada la correspondiente medida de seguridad.

Por último, hay que tener en cuenta que la LOPD prevé una infracción directamente relacionada con la falta de medidas de seguridad o con su ineficacia. Dedicaremos el último apartado a las cuestiones relacionadas con las infracciones relacionadas con las medidas de seguridad.

> Infracciones graves (art. 44.3): «h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que se determinen por vía reglamentaria».

6.1.2. Aplicación de los niveles de seguridad

¿Cómo sabemos las medidas de seguridad a aplicar en cada caso?

Las medidas de seguridad se organizan en niveles: concretamente hay tres niveles de seguridad (básico, medio y alto), que se aplican de acuerdo con el tipo de datos objeto de tratamiento (arts. 80 y 81 RLOPD); por tanto, deberemos analizar qué datos se tratan para determinar las medidas a aplicar.

Para cada nivel se describen una serie de requerimientos de protección de los datos, es decir, qué protección debe proporcionar la medida de seguridad; los niveles son acumulativos, de manera que, por ejemplo, a unos datos de nivel medio se les aplican también las medidas de seguridad de nivel básico.

El artículo 81 determina qué nivel de protección se aplicará a cada tipo de información:

1) A todos los tratamientos de datos de carácter personal se les aplicarán las medidas de seguridad de nivel básico.

2) Las medidas de seguridad de nivel medio se aplicarán a los tratamientos:

- relativos a la comisión de infracciones administrativas o penales;
- relacionados con la prestación de servicios de información sobre solvencia patrimonial y crédito;
- que sean responsabilidad de las Administraciones tributarias, en relación con el ejercicio de potestades tributarias;
- que sean responsabilidad de las entidades financieras, en relación con la prestación de servicios financieros;

- que sean responsabilidad de las entidades gestoras y servicios comunes de la Seguridad Social, relacionados con el ejercicio de sus competencias;

- que sean responsabilidad de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, o

- que contengan un conjunto de datos de carácter personal que proporcionen una definición de las características o de la personalidad de las personas y que permitan evaluar determinados aspectos de su personalidad o de su comportamiento.

3) Las medidas de seguridad de nivel alto se aplicarán a los tratamientos que traten datos sobre:

- ideología,
- afiliación sindical,
- religión,
- creencias,
- origen racial,
- salud,
- vida sexual,
- aquellos que contengan o se refieran a datos obtenidos para fines policiales, sin consentimiento de las personas afectadas, o
- aquellos que traten datos derivados de actos de violencia de género.

Hay algunas especialidades y excepciones en la aplicación de este esquema general de determinación del nivel de seguridad:

- Los datos de tráfico y localización que traten los operadores que presten servicios de telecomunicaciones electrónicas disponibles para el público, o exploten redes públicas de comunicaciones electrónicas, son inicialmente considerados datos de nivel medio, pero también deben estar protegidos con una medida concreta de nivel alto, la prevista en el artículo 103 del RLOPD (el registro de accesos).

- Cuando se traten datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, con la única finalidad de hacer transferencias de dinero a entidades de las que son asociadas o miembros las personas respecto quienes se tratan estos tipos de datos. También si se trata de un fichero o tratamiento no automatizado en el que aparecen de forma incidental o accesoria este tipo de datos sin que tengan relación con la finalidad del fichero o tratamiento. Entonces, solo se aplicarán las medidas de seguridad previstas en el nivel básico.

- Si se trata de un archivo o un tratamiento que utiliza datos de salud que se refieren exclusivamente a un grado de discapacidad o solo a la declaración de la discapacidad o invalidez del afectado, y siempre que sea necesario

tratar este dato para dar cumplimiento a unos deberes públicos. En este caso, serán suficientes las medidas de seguridad de nivel básico para este fichero o tratamiento.

Las medidas de seguridad tienen por objeto proteger la información personal, con independencia del sistema utilizado para el tratamiento. En aplicación de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el principio de seguridad es aplicable a cualquier sistema de tratamiento de los datos personales, automatizado y no automatizado.

6.1.3. La seguridad debe documentarse y gestionarse

Los modelos de buenas prácticas en materia de seguridad de la información parten de la base de que la seguridad requiere ser documentada para garantizar su correcta implantación, y debe gestionarse para garantizar su eficacia. El artículo 88 del RLOPD prevé que las medidas de seguridad relacionadas con la protección de datos de carácter personal sean concretadas en lo que se conoce como documento de seguridad.

El artículo 88.1 obliga al responsable del fichero o del tratamiento a elaborar un documento de seguridad que recoja las medidas técnicas y organizativas que sean de aplicación, según la normativa vigente, a los tratamientos y ficheros de su responsabilidad, y que serán de obligado cumplimiento para el personal con acceso a los sistemas de información.

Por lo tanto, todas las medidas de seguridad que el responsable del fichero o tratamiento está obligado a implantar deberán estar documentadas.

El Reglamento deja en manos del responsable decidir la forma de este documento, es decir, puede optar por hacer un único documento para todos los tratamientos, hacer uno para cada fichero o tratamiento, tener un cuerpo documental central y luego ir añadiendo anexos, etc. Lo que sí que regula el Reglamento son los contenidos mínimos del documento de seguridad.

La seguridad debe gestionarse. Tal y como exige el artículo 88.7, el documento de seguridad debe mantenerse en todo momento actualizado, con el fin de hacer efectiva esa gestión.

En relación con la necesaria gestión de la seguridad, el RLOPD prevé la figura del responsable de seguridad, que se encarga de coordinar y controlar las medidas de seguridad definidas en el documento de seguridad.

6.1.4. Detalle de las medidas de seguridad a implantar

Este apartado lo dedicaremos a revisar todas las medidas de seguridad que recoge el título VIII del Reglamento de desarrollo de la LOPD.

La metodología que se ha seguido para describir las medidas de seguridad está centrada en lo que deben proteger, y en cada caso se indica el nivel de medida de seguridad, el tipo de tratamiento al que aplica, su localización en el RLOPD (artículo) y una breve descripción de la medida de seguridad.

1) La seguridad y el factor humano

Tal como prevé el artículo 88 del RLOPD, las medidas técnicas y organizativas que deban ser aplicadas por el responsable del tratamiento son de obligado cumplimiento para el personal con acceso a los sistemas de información.

Por lo tanto, el factor humano es básico para garantizar la eficacia de las medidas de seguridad, y es por eso que el RLOPD prevé toda una serie de medidas directamente relacionadas con las personas, aunque en la práctica, en casi todas las medidas de seguridad intervienen personas.

Medidas directamente relacionadas con las personas con acceso a los datos			
Nivel básico	**Todos los tratamientos**	Funciones y obligaciones del personal (arts. 89 y 105.2)	Las funciones y obligaciones de los usuarios con acceso a datos personales estarán recogidas en el documento de seguridad, y es obligación del responsable del fichero o tratamiento que el personal con acceso a datos conozca todas y cada una de las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en caso de incumplimiento.
	No automatizados	Custodia de los documentos por parte del personal (art. 108)	Cuando la documentación en papel se encuentre fuera de los lugares destinados a su almacenamiento o archivo, habitualmente porque se está utilizando, la persona que esté a cargo de esos documentos debe impedir, en todo momento, que personas no autorizadas tengan acceso a la documentación.
Nivel medio	**Automatizados**	Control de acceso físico (art. 99)	Solo las personas autorizadas en el documento de seguridad pueden acceder físicamente a los espacios donde se encuentren instalados los equipamientos físicos que dan apoyo a los sistemas de información.

2) Protección del acceso a los datos personales

Ya hemos mencionado que una de las exigencias del principio de seguridad es evitar el acceso no autorizado a los datos, así como su tratamiento no autorizado. Por tanto, el RLOPD obliga a implantar medidas de seguridad que tienen por objetivo evitar ese tipo de accesos y tratamientos.

Medidas para proteger el acceso a los datos			
Nivel básico	**Todos los tratamientos**	Control de acceso (arts. 91 y 105.2)	Cada usuario debe estar autorizado solo a acceder a aquella información necesaria para el desarrollo de sus funciones, por lo tanto debe existir una relación, siempre actualizada, de los usuarios y de los accesos autorizados. Se establecerán controles para evitar que se produzcan accesos a información personal por parte de usuarios no autorizados. Estas medidas de seguridad afectan tanto a personal propio como externo.
	No automatizados	Dificultar el acceso a los dispositivos que contienen documentos (art. 107)	El acceso a los archivos, armarios, cajones, etc. donde se guarden documentos se realizará mediante algún mecanismo que obstaculice el libre acceso (cerraduras o similares).
		Evitar el acceso de personas no autorizadas (art. 107)	Si por las características de lugar donde se almacenan los documentos no es posible implantar mecanismos que obstaculicen el libre acceso (estanterías, por ejemplo), el responsable del tratamiento debe adoptar otras medidas que impidan el acceso de personas no autorizadas.
		Identificación y autenticación (art. 93)	El responsable del fichero o tratamiento establecerá los mecanismos necesarios para garantizar la identificación y autenticación inequívoca y personalizada de los usuarios. Las contraseñas se deben proporcionar y almacenar de forma que quede garantizada su confidencialidad e integridad; con una periodicidad no superior a un año las contraseñas deben ser modificadas.
Nivel medio	**Automatizados**	Limitación de los intentos de acceso no autorizado (art. 98)	Debe existir un mecanismo que impida que se pueda intentar reiteradamente el acceso no autorizado a un sistema de información (por ejemplo, prever un número máximo de errores al introducir la contraseña).
Nivel alto	**Todos los tratamientos**	Registro de accesos a la información o documentación (arts. 103 y 113)	Cuando se trata de datos especialmente protegidos, se exige el registro de la actividad de los usuarios (qué hacen con los datos). De este modo, cada vez que un usuario intenta acceder a los datos personales se registrará la identificación del usuario, la fecha y hora del intento de acceso, el archivo sobre el que se intenta el acceso, el tipo de acceso (consulta, modificación o borrado) y si el acceso es denegado o autorizado por el sistema de control de acceso. En aquellos casos en que el acceso haya sido autorizado, también se ha de guardar información que permita identificar a qué datos se accedió. Los mecanismos de registro de acceso no pueden ser desactivados, ni la información que recogen puede ser manipulada. Esta información se conservará durante dos años y como mínimo cada mes el responsable de seguridad debe revisarla y hacer un informe. Si el responsable del fichero o tratamiento es una persona física y garantiza que únicamente él puede acceder y tratar los datos, entonces no es necesario que implante esta medida de seguridad. En caso de documentos en papel se registrará la información de qué usuarios han accedido a la documentación.
	Automatizados	Cifrado de las telecomunicaciones (art. 104)	Cuando se transmitan datos de nivel alto por redes públicas de telecomunicaciones o redes inalámbricas de comunicaciones electrónicas, la información debe ir cifrada o implantar cualquier mecanismo que haga ininteligible la información e impida su manipulación.

Medidas para proteger el acceso a los datos			
	No automatizados	Dispositivos de almacenamiento en espacios cerrados (art. 111)	Los armarios, archivadores y dispositivos en los que se almacene la información deben estar ubicados en áreas protegidas mediante puertas de acceso que permanecerán cerradas y que incorporarán dispositivos de cierre, tales como llaves u otros mecanismos, que impidan el libre acceso a las salas. Si los locales no permiten implantar esta medida, el responsable del fichero o tratamiento adoptará medidas alternativas motivadas y descritas en el documento de seguridad.
		Control de la copia o reproducción de documentos (art. 112.1)	Cualquier copia o reproducción de un documento en papel solo podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

3) Salvaguarda y custodia de la información

La información que gestionan los sistemas de información puede estar ubicada en diferentes lugares. Cuando se trata de tratamientos automatizados, habitualmente nos encontramos con dos tipos de ubicaciones: el almacenamiento relacionado con los sistemas de información de explotación habitual de los datos, y el almacenamiento en dispositivos externos, ya sea con el fin de disponer de copias de seguridad de la información o para su transporte y posterior descarga en otros sistemas de información o dispositivos de explotación de datos (estaciones de trabajo).

Si se trata de documentos en papel, también nos podemos encontrar con las ubicaciones relacionadas con la gestión y tramitación ordinaria de la documentación y las situaciones de archivo de la documentación.

En todos los casos, la información siempre debe estar protegida para dar respuesta tanto al requerimiento de evitar el acceso o tratamiento no autorizado como el de evitar la alteración descontrolada de la información o la pérdida de los datos.

Medidas de salvaguarda y custodia de la información			
Nivel básico	**Todos los tratamientos**	Gestión de soportes y documentos (arts. 92 y 105.2)	Tanto los soportes digitales de información como los documentos que contengan datos de carácter personal deberán permitir identificar qué tipo de información contienen: los soportes informáticos deben poder ser inventariados y solo deben poder acceder a ellos las personas autorizadas. Cualquier salida de información fuera de los locales habituales de tratamiento de los datos debe ser autorizada por el responsable de fichero o tratamiento, y esto incluye los envíos por correo electrónico. El transporte de soportes y documentación debe hacerse con medidas que impidan la sustracción, la pérdida o el acceso no autorizado a los dispositivos y documentos. Si un soporte o documento debe ser destruido, se deben tomar medidas para que la información no pueda ser recuperada posteriormente.

Medidas de salvaguarda y custodia de la información			
	Automatizados	Copias de soporte y recuperación (art. 94)	Se deben hacer copias de seguridad como mínimo semanalmente, y cada seis meses el responsable del fichero o tratamiento deberá verificar que los procedimientos de copia y restauración funcionan correctamente.
	No automatizados	Archivo. Garantizar la conservación (art. 106)	El archivo de documentos se hará según lo establezca la legislación específica, pero en todo caso se debe garantizar que la información se conserva en correctas condiciones.
		Archivo. Localización y consulta (art. 106)	El sistema de archivo debe facilitar la localización y consulta de la documentación.
		Archivo. Ejercicio de derechos (art. 106)	En ningún caso el sistema de archivo debe ser obstáculo para que las personas afectadas puedan ejercer los derechos de acceso, rectificación, cancelación y oposición en las condiciones previstas en la legislación.
Nivel alto	**Todos los tratamientos**	Cifrado de soportes durante el transporte y protección de la documentación (arts. 101 y 114)	El RLOPD obliga a tomar ciertas cautelas durante el transporte de soportes con información o documentación que incluya datos personales. En el caso de los soportes, los datos deben ir cifrados, o bien se deben utilizar mecanismos alternativos que impidan el acceso o la manipulación de la información durante el transporte (esto se aplica tanto a los soportes como a los documentos en papel).
	Automatizados	Identificación de soportes mediante codificación (art. 101.1)	Los soportes que contengan datos personales de nivel alto se etiquetarán de forma que sólo las personas autorizadas conozcan el tipo de información contenida en el soporte.
		Cifrado de dispositivos portátiles (art. 101.2)	Si la información es en ordenadores portátiles, fuera de los locales habituales de tratamiento, la información también deberá ser cifrada. Se debe evitar el tratamiento de datos sensibles en dispositivos portátiles que no puedan ser cifrados.
	No automatizados	Destrucción de las copias sin utilidad (art. 112.2)	Una vez las copias de documentos dejan de ser útiles deben ser destruidas, de manera que se evite el acceso a la información que contenían o que esta información pueda ser recuperada (esto implica la utilización de destructoras de papel o procedimientos con resultados similares).

4) Gestión de los incidentes

Las medidas de seguridad no siempre pueden evitar que se produzcan incidentes con la información; por lo tanto, como medida que puede servir a la prevención de futuros incidentes de las mismas características, la legislación obliga a llevar un registro y documentar los incidentes en los que se puedan ver afectados datos de carácter personal.

Medidas relacionadas con la gestión de incidentes de seguridad			
Nivel básico	**Todos los tratamientos**	Registro de incidentes (arts. 90 y 105.2)	El responsable del fichero o tratamiento debe implantar procedimientos para comunicar los incidentes con los datos y debe crear un registro donde conste el tipo de incidente, cuando se ha producido o detectado, la persona que ha notificado el incidente, que ha recibido la comunicación, qué actuaciones se han llevado a cabo y qué medidas correctoras se han implantado con el fin de que no vuelva a suceder el mismo incidente.
Nivel medio	**Automatizados**	Registrar los procedimientos de recuperación como incidentes (art. 100)	Aparte de las informaciones previstas en el artículo 90, cuando se trate de datos que requieren medidas de seguridad de nivel medio, el registro de incidencias también debe incluir información sobre los procedimientos de restauración que hayan sido necesarios realizar con motivo de un incidente. En estos supuestos se indicará qué persona ha realizado el proceso de restauración de los datos, qué datos se han recuperado y, si se da el caso, si estos han sido recuperados manualmente.

5) Medidas de seguridad de carácter organizativo

La seguridad no es exclusivamente una cuestión de tecnología; algunas medidas son exclusivamente de carácter organizativo. La combinación de ambos tipos de medidas, técnicas y organizativas, es probablemente lo que mejor garantiza un alto grado de eficacia en la protección de la información.

Medidas organizativas			
Nivel medio	**Todos los tratamientos**	Responsable de seguridad (arts. 95 y 109)	El documento de seguridad contiene la designación del responsable de seguridad, que es quien coordina y controla las medidas de seguridad previstas. Esta designación en ningún caso supone ninguna rebaja en la responsabilidad de los responsables o los encargados de tratamiento.
		Auditoría (arts. 96 y 110)	Cada dos años, como mínimo, se debe verificar mediante una auditoría, que puede ser interna o externa, si las medidas de seguridad previstas funcionan correctamente. Si hay cambios sustanciales en los sistemas de información, se debe hacer esta auditoría antes del plazo de dos años. Como consecuencia de la auditoría, se redactará un informe, donde se dictamine sobre el grado de adecuación de las medidas previstas a lo que establece la legislación, identificando las deficiencias y proponiendo medidas correctoras necesarias. Es importante tener en cuenta que los informes de auditoría deben ser revisados por el responsable de seguridad, el cual debe informar sobre las conclusiones al responsable del fichero o tratamiento afectado por la auditoría. Estos informes de auditoría deben quedar a disposición de las autoridades de control competentes (autoridades de protección de datos).
		Registro de entrada y salida de soportes (arts. 97 y 105)	Debe existir un registro de entrada y salida de soportes y documentos, el cual debe permitir conocer el tipo de soporte o documento que ha entrado o salido, junto con la fecha y hora, quién es el remitente, el número de documentos o soportes, el tipo de información que contienen, el mecanismo de envío y quién ha sido la persona responsable de la recepción.

Medidas organizativas			
Nivel alto	**Automatizados**	Evitar concurrencia de riesgos en copias y procedimientos de recuperación (art. 102)	El RLOPD obliga a que las copias de seguridad y los procedimientos de recuperación se conserven en un lugar diferente a los equipos informáticos que contienen los datos, es decir, que no estén bajo las mismas amenazas físicas. Evidentemente, en esta ubicación diferenciada se deben adoptar también medidas de seguridad.

6) Supuestos especiales

El RLOPD regula algunas situaciones muy concretas relacionadas con los tratamientos de datos personales, que completan las obligaciones de los responsables de ficheros y tratamientos en materia de seguridad y protección de datos.

a) Prestaciones de servicios sin acceso a datos (art. 83): el responsable del fichero o tratamiento adoptará medidas que afectarán a personas que en principio no deben acceder a datos personales, pero que en el desarrollo normal de sus funciones pueden estar en disposición de acceder a ese tipo de datos (personal de mantenimiento, limpieza, vigilancia, etc.). Como principio general se debe limitar, en la medida de lo posible, el acceso a la información y, cuando se trate de personal externo, en los contratos se hará constar expresamente la prohibición de acceso a datos personales y, en todo caso, la obligación de guardar secreto.

b) Acceso mediante redes de comunicaciones (art. 85): cuando se transmitan datos personales utilizando redes de comunicaciones, sean públicas o no, se debe garantizar un nivel de protección equivalente al previsto para los accesos en local.

c) Trabajo fuera de los locales o ubicaciones habituales de tratamiento (art. 86): para almacenar los datos personales en dispositivos portátiles, o para tratarlos fuera de los locales habituales del responsable del fichero o tratamiento, o en su caso, del encargado del tratamiento, será necesaria la autorización previa del responsable del fichero o tratamiento, y obviamente se deberá garantizar el nivel de seguridad exigido por el RLOPD.

d) Archivos de trabajo y copias de trabajo de documentos (art. 87): los archivos temporales o copias de trabajo deben estar protegidos según el nivel de medidas de seguridad que sean de aplicación a los datos que contengan; deberán ser borrados o destruidos una vez dejen de ser útiles para los fines que motivaron su creación como soportes temporales.

6.1.5. Tabla resumen de las medidas de seguridad LOPD

Medidas de seguridad	Básico	Medio	Alto
Nivel básico			
Funciones y obligaciones del personal	YX		
Registro de incidentes	YX		
Control de accesos	YX		
Gestión de soportes y documentos	YX		
Identificación y autenticación	Y		
Copias de respaldo y recuperación	Y		
Archivo: garantizar conservación	X		
Archivo: localización y consulta de los datos	X		
Archivo: ejercicio de derechos	X		
Dificultar la apertura de dispositivos que contienen documentos	X		
Evitar el acceso a personas no autorizadas (si no es posible lo anterior)	X		
Custodia personal de los documentos	X		
Nivel medio			
Responsable de seguridad		YX	
Auditoría		YX	
Registro de entrada y salida de soportes		Y	
Limitar los intentos de acceso no autorizado		Y	
Control de acceso físico		Y	
Registrar los procedimientos de recuperación como incidentes		Y	
Nivel alto			
Identificación codificada de los soportes			Y
Cifrado de soportes durante el transporte y protección de la documentación			YX
Cifrado de dispositivos portátiles			Y
Evitar concurrencia de riesgos en copias y procedimientos de recuperación			Y
Registro de accesos a la información o documentación			YX
Cifrado de las telecomunicaciones (redes públicas o inalámbricas)			Y
Dispositivos de almacenamiento en espacios cerrados			X

Y: Medidas de seguridad automatizadas. **X:** Medidas de seguridad no automatizadas.

Medidas de seguridad	Básico	Medio	Alto
Control de la copia o reproducción de documentos			X
Destrucción de las copias sin utilidad			X

Y: Medidas de seguridad automatizadas. **X:** Medidas de seguridad no automatizadas.

6.2. Medidas de seguridad en el RGPD

El RGPD regula, en su artículo 32, la «seguridad del tratamiento»; en ese artículo se establece que, para determinar las medidas de seguridad a adoptar, se debe llevar a cabo, de manera previa, una evaluación de los riesgos que puedan suponer las operaciones de tratamiento para los derechos y libertades de las personas.

No hay por tanto una «lista» de medidas de seguridad, sino que el conjunto de medidas a implantar deberán ser seleccionadas por el responsable o por el encargado del tratamiento, según el caso, tal y como ya hemos analizado en apartados anteriores.

Para seleccionar las medidas de seguridad a adoptar, junto con la evaluación de esos riesgos en sus dimensiones de probabilidad y gravedad, el responsable y el encargado del tratamiento deberán tener en cuenta el estado de las tecnologías y sus costes de implantación, así como la naturaleza, alcance, contexto y finalidades del tratamiento, con el objeto de garantizar que los tratamientos se lleven en las condiciones de seguridad más adecuadas en relación con los riesgos que pueden suponer, es decir, que el riesgo se mantenga en un nivel aceptable.

De una manera orientativa, incluye el artículo 32.1 algunas propuestas de medidas de control de ese riesgo, aunque en realidad más bien se trata de lo que, en el contexto de la seguridad de la información, se denominan «objetivos de control», no tanto unas medidas detalladas como hemos podido apreciar que en estos momentos prevé el RLOPD en el ordenamiento jurídico español.

En la ISO/IEC 27000 se define, como objetivo de control, la «declaración que describe lo que se debe lograr como resultado de la implementación de controles», teniendo en cuenta que por «control» debemos entender cualquier «medida que modifica un riesgo» (UNE-ISO GUÍA 73:2010), y según la UNE-ISO/IEC 27000:2014, «los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo»; en definitiva, control en relación con la seguridad de los tratamientos es sinónimo de medidas de seguridad.

Pues bien, lo que plantea el RGPD en su artículo 32.1 son objetivos de control, es decir, aquello que pretende obtenerse como resultado a la aplicación de las medidas de seguridad, en tanto estas deben reducir el riesgo que puedan presentar las operaciones de tratamiento.

De manera que, sin determinar en qué circunstancias deben implantarse, ni entrar en mayores detalles, se alude a:

1) La seudonimización, entendiendo por tal, según el propio RGPD, «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional», teniendo en cuenta que esa información que permitiría tal atribución debe conservarse de manera separada, y además deberá ser objeto de la aplicación de medidas técnicas y organizativas que impidan *a priori* la reatribución; sería el caso, por ejemplo, de que determinados datos identificativos son sustituidos por un código, y la relación de ese código con tales datos identificativos se mantiene protegida para evitar que personas no autorizadas puedan vincular uno y otro conjunto de datos (datos identificativos con la vinculación y datos seudonimizados).

2) El cifrado de datos personales, es decir, la aplicación de técnicas que permiten proteger la información sobre la base de «transformarla» en conjuntos de datos, *a priori* ininteligibles, de manera que para que puedan ser conocidos debe recurrirse a algún tipo de técnica de descifrado, que suele sustentarse en conocer o poseer un elemento que permite ese descifrado, sea una contraseña, una clave de cifrado o cualquier otro medio que permita que esa posibilidad de descifrado solo esté al alcance de personas autorizadas.

Resulta evidente que mantener los datos personales cifrados, o incluso seudonimizados, facilita su protección, reduciendo el riesgo de que sean accedidos o tratados por personas no autorizadas.

3) La capacidad de garantizar de manera permanente algunas de las típicas dimensiones vinculadas a la seguridad de la información respecto de los sistemas y servicios de tratamiento, como:

- La confidencialidad: medidas para evitar el acceso por parte de personas no autorizadas.

- La integridad: medidas para asegurar que los sistemas o servicios de tratamiento funcionan tal y como se ha previsto y que, por tanto, la información no se vea afectada en su integridad, ya sea de manera accidental o malintencionada.

- La disponibilidad: medidas para garantizar el funcionamiento ordinario de los sistemas y servicios.

- Y la resiliencia: medidas para que los sistemas de información y servicios vinculados al tratamiento de datos personales sean capaces de recuperarse de situaciones adversas o incidentes que puedan afectarles.

4) La capacidad para «restaurar la disponibilidad y el acceso a los datos» de una manera rápida, en caso de que se produzca algún incidente con los datos, sea de tipo físico o técnico; por tanto, deberán preverse medidas vinculadas a planes de contingencia y de continuidad de los sistemas de información (o de continuidad de negocio).

5) Y por último, apunta la posibilidad de que se lleve a cabo la «verificación, evaluación y valoración regular de la eficacia» de las medidas de seguridad; en definitiva, el regulador europeo se refiere a la monitorización y auditoría de las medidas de seguridad implantadas.

Como podemos apreciar, en ningún caso hay una concreción de medidas de seguridad al estilo del RLOPD, sino que el RGPD se limita a establecer el resultado que deberían proporcionar las medidas de seguridad a adoptar; por tanto, corresponderá al responsable del tratamiento, o en su caso al encargado, determinar qué medidas se van a adoptar y de qué manera, lo que resulta una clara manifestación del principio de responsabilidad proactiva que incorpora el RGPD.

Por supuesto, el factor humano es esencial en el contexto de la seguridad de la información, y por tanto también en lo que respecta a la seguridad de los tratamientos de datos de carácter personal. Así, el artículo 32.4 del RGPD establece que los responsables y encargados de tratamiento deberán tomar las medidas adecuadas para que las personas que actúan bajo su autoridad traten los datos exclusivamente siguiendo sus instrucciones.

Como fácilmente podemos constatar, hay una evidente diferencia en el contenido regulatorio referido a las medidas de seguridad entre el LOPD y el RGPD, habiendo pasado de un conjunto amplio de artículos dedicados a describir con un cierto nivel de detalle las medidas de seguridad a adoptar (controles), por una descripción de lo que deben conseguir esas medidas (objetivos de control), dejando un amplio margen a responsables y encargados de tratamiento para llevar a cabo esa concreción, ya sea respecto de las medidas a aplicar como en la manera de aplicarlas.

El RLOPD plantea un modelo de seguridad de los tratamientos que hasta ahora se ha considerado aceptable y que, por tanto, *a priori* ha dado respuesta a los requisitos que se derivan del principio de seguridad que recoge la LOPD.

El RGPD obliga a tener en cuenta los riesgos para seleccionar las medidas de seguridad más adecuadas; por tanto, podría llegar a considerarse que el conjunto de medidas previstas en el RLOPD, y que ya están siendo aplicadas a los tratamientos, serían aptas per dar respuesta a los requisitos de protección que plantea el RGPD.

Ahora bien, podría ser así siempre y cuando responsables y encargados de tratamiento realicen la correspondiente evaluación de riesgos, a fin de verificar que, efectivamente, las medidas de seguridad implantadas conforme al RLOPD responden a los riesgos concretos que presentan las operaciones de tratamiento; no hay que olvidar que ahora el concepto de «alto riesgo» juega un papel importante y, por tanto, hay que verificar en qué nivel de riesgo se sitúan las operaciones de tratamiento.

7. Transparencia y seguridad: gestión de las violaciones de la seguridad de los datos

Entre los nuevos principios del RGPD destaca el de la «transparencia» en el tratamiento de los datos de carácter personal; en el artículo 5.1 se incluye el principio de transparencia junto con la licitud y la lealtad, por tanto formando parte de lo que podríamos considerar un «núcleo duro» de los principios de la regulación europea, al menos en cuanto a lo que podemos catalogar como principios de orden ético que deben ser tenidos en cuenta a la hora de asumir la responsabilidad de iniciar operaciones de tratamientos de datos personales.

El Considerando 39 hace referencia a lo que implica el principio de transparencia; se trata de que los interesados reciban ciertas informaciones relacionadas con las operaciones de tratamiento a que son sometidos sus datos y, entre otras informaciones, se menciona que las personas cuyos datos son objeto de tratamiento deben conocer los riesgos que este pueda entrañar, así como las salvaguardas implantadas.

Las complejidades tecnológicas que pueden llegar a confluir en las operaciones de tratamiento obligan a que, para dar una adecuada repuesta al principio de transparencia, la información que se proporcione a los interesados deba ser «concisa, fácilmente accesible y de fácil entender», utilizando un lenguaje claro y sencillo (Considerando 58).

En cuanto a la protección material de los datos personales (seguridad), la transparencia tiene una aplicación directa en el cumplimiento de lo previsto en el artículo 34 del RGPD, dedicado a la comunicación de las violaciones de seguridad de los datos personales, cuestión que abordaremos en detalle más adelante; también en el contexto de las evaluaciones de impacto relativas a los datos personales los riesgos y las medidas pueden llegar a ser objeto de unos altos niveles de transparencia.

En ese sentido, el artículo 12.1 del RGPD establece que, en relación con la comunicación prevista en el artículo 34, el responsable del tratamiento deberá facilitar al interesado la información sobre el incidente de seguridad que afecta a los datos: «en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo».

7.1. Concepto de violación de la seguridad de los datos

En la «Guía de seguridad de las TIC CCN-STIC 817» para la gestión de ciberincidentes, publicada por el Centro Criptológico Nacional, un incidente es cualquier suceso que:

«pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información; o la información que el sistema procesa, almacena o transmite; o que constituye una violación o amenaza inminente de violación de las políticas, normas o procedimientos de seguridad de la organización».

El RGPD define, en su artículo 4, lo que debe entenderse por «*violación de la seguridad* de los datos personales», a los efectos del Reglamento, considerado como tal: cualquier evento que tenga como resultado «la destrucción, pérdida o alteración accidental o ilícita de datos personales» objeto de tratamiento, o «la comunicación o acceso no autorizados a dichos datos».

Por tanto, podemos concretarlo en el hecho de que la violación de la seguridad de los datos es un incidente de seguridad que afecta a la confidencialidad, integridad o disponibilidad de datos personales, de modo que se refiere a situaciones en las que las medidas de seguridad o no estaban implantadas, o estaban implantadas pero no eran las adecuadas, o no han funcionado de la manera prevista en cuanto a la protección de los datos personales, sin perjuicio de que determinadas violaciones de datos tengan su origen en un incidente imprevisible o desproporcionado en cuanto a los medios utilizados para violentar la seguridad de los datos.

En todo caso, en cualquiera de las tres circunstancias mencionadas, nos encontraremos con que la seguridad de los tratamientos, en tanto es una obligación de resultado para responsables y encargados de tratamientos, no ha sido atendida adecuadamente, afectando a los datos personales, de tal modo que los derechos y libertades de las personas a las cuales hacen referencia esos datos podrían resultar vulnerados.

7.2. Notificación de violaciones de la seguridad a las autoridades de control

El artículo 33 del RGPD regula cómo debe actuar el responsable del tratamiento cuando detecte que los datos que trata se han visto afectados por un incidente de seguridad; obviamente, lo previsto en el artículo 33 no se refiere a la gestión interna o protocolos internos de gestión de incidentes de la organización, aunque estos deberán hacer referencia a lo previsto en el mencionado artículo 33, como veremos al final de este apartado.

El responsable del tratamiento deberá notificar a la autoridad de control competente que se ha producido una violación de los datos personales, y deberá hacerlo sin que se produzca una «dilación indebida», y en todo caso en un plazo no superior a 72 horas desde el momento en que el responsable del tratamiento tuvo conocimiento del incidente de seguridad que afecta a los datos personales.

Se establece una excepción a tal notificación cuando resulte improbable que la violación de seguridad de los datos pueda constituir un riesgo para los derechos y libertades de las personas.

Por ejemplo, imaginemos que se pierde o es sustraído un ordenador portátil que contiene datos personales; es evidente que, desde la perspectiva de seguridad de la información, estamos ante un incidente de seguridad. Ahora bien, si el contenido de ese portátil estaba cifrado (con un cifrado robusto), por ejemplo mediante una clave privada de descifrado, que está ubicada exclusivamente en una tarjeta criptográfica que está bajo el control del usuario del portátil y esta no ha sido objeto de sustracción, o bien se debe utilizar algún dispositivo biométrico para descifrar el contenido del ordenador (huella dactilar, por ejemplo), podemos decir que es improbable (que no imposible) que los datos sean accedidos de manera no autorizada en el caso de que terceros tengan acceso físico al mencionado ordenador portátil.

El Considerando 85 se refiere a esta cuestión, conectando la capacidad de demostrar tal improbabilidad para los riesgos de las personas con el principio de responsabilidad proactiva.

En el caso de que tal notificación no pueda ser realizada en el plazo de 72 horas, deberá informarse a la autoridad de control del motivo por el cual no se ha notificado dentro del plazo previsto.

En el caso de que las operaciones de tratamiento afectadas por el incidente de seguridad sean llevadas a cabo por un encargado, este también deberá notificar al responsable del tratamiento, «sin dilación indebida», que se ha producido tal circunstancia, para que este a su vez proceda a notificarlo a la autoridad de control, según lo descrito en párrafos anteriores.

El contenido mínimo de la notificación que debe efectuar el responsable del tratamiento a la autoridad de control se concreta en el artículo 33.3 del RGPD:

- Se describirá la naturaleza de la violación de la seguridad de los datos (pérdida, acceso no autorizado, indisponibilidad de los sistemas, etc.), incluyendo, si es que puede concretarse, el tipo y número de personas afectadas, así como el tipo o categoría de datos y el volumen de información que se ha visto afectado por el incidente (el RGPD se refiere al «número aproximado de registros»).

- Los datos de contacto del delegado de protección de datos.

- Se describirán las potenciales consecuencias del incidente de seguridad.

- Se describirán qué medidas han sido adoptadas, o bien se han propuesto, por el responsable del tratamiento, a raíz de la violación de la seguridad de los datos.

Si bien se establecen unos contenidos mínimos de esa notificación, se permite que, si se da el caso de que no puede ser aportada toda la información en un mismo momento, se puedan ir notificando nuevas informaciones o datos sobre el incidente a medida que se vaya disponiendo, y siempre sin retrasos innecesarios.

Hay que tener en cuenta que, en función del tipo de incidente, la situación puede resultar grave incluso para el funcionamiento de la organización del responsable del tratamiento, por lo que podría ser que determinadas informaciones sean complicadas de obtener en los primeros momentos.

En todo caso, va a implicar que entre el responsable del tratamiento y la autoridad de control se establezca una fluida comunicación, a fin de avanzar en concretar la magnitud del incidente de seguridad que haya podido afectar a los datos personales, y determinar de qué manera los potenciales efectos negativos se han minimizado.

7.3. Comunicación a las personas afectadas de la violación de la seguridad de los datos personales

Establece el RGPD una segunda obligación relacionada con la violación de la seguridad de los datos personales, que consiste en comunicar tal circunstancia a las personas cuyos datos se han visto afectados por el incidente de seguridad.

El Considerando 86 introduce tal obligación al hacer referencia a que el responsable del tratamiento «debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades», de modo que las personas afectadas puedan adoptar las necesarias precauciones para reducir o eliminar los efectos negativos de esa violación.

Esa comunicación, según el mismo considerando, debe realizarse «tan pronto como sea razonablemente posible», y en este punto aún se pone un mayor énfasis en que, en tales circunstancias, debe existir una fluida interacción entre el responsable del tratamiento y la autoridad de control; concretamente, se refiere a que la comunicación se lleve a cabo «en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones». Incluso, si fuera el caso, atendiendo las recomendaciones u orientaciones de otras autoridades u organizaciones, como por ejemplo, la policía o los centros de atención y respuesta a emergencias de redes, en sus diferentes modalidades.

En relación con estas comunicaciones, habrá que valorar el escenario que se dé en cada caso. En ocasiones, una comunicación rápida o inmediata será lo adecuado, ya que podría mitigar eficazmente los potenciales daños y perjuicios a las personas afectadas. Por el contrario, puede ser más conveniente llevar a cabo la comunicación una vez se han adoptado ciertas medidas dirigidas a impedir que se continúe produciendo la violación de la seguridad o que esta no se agrave, con lo que tal comunicación ya no sería tan inmediata.

Por ello, va a ser necesario llevar a cabo un análisis de cómo actuar caso por caso; de ahí la necesidad de estar en contacto fluido con la autoridad de control, a fin de que pueda aportar su criterio a la hora de tomar ciertas decisiones relacionadas con el cumplimiento de obligaciones previstas en el RGPD para los casos de incidentes de seguridad que puedan afectar a los datos.

El artículo 34.1 del RGPD prevé que, sin dilación, se comunique a las personas afectadas que la seguridad de sus datos se ha visto comprometida, en tanto sea probable que el incidente de seguridad que han padecido sus datos pueda suponer un alto riesgo para sus derechos y libertades (recordemos que en su momento ya hemos analizado el concepto de alto riesgo utilizado en el RGPD).

Como ya hemos dicho, esa comunicación debe realizarse en un lenguaje claro y sencillo, describiendo en qué ha consistido el incidente de seguridad, junto con información sobre sus potenciales consecuencias y las medidas adoptadas.

Se establecen algunas circunstancias por las que el RGPD exime al responsable del tratamiento de llevar a cabo la comunicación a las personas afectadas por la violación de la seguridad de sus datos personales (art. 34.3):

- Si el responsable del tratamiento había adoptado medidas de protección de los datos afectados por la violación de la seguridad, como por ejemplo el cifrado, o cualquier otra solución que impida el acceso por parte de personas no autorizadas (serían claramente medidas preventivas).

- Si el responsable del tratamiento ha tomado medidas de protección una vez conocido el incidente de seguridad que pueden evitar, a pesar el incidente, que se genere un alto riesgo para los derechos y libertades (serían claramente medidas reactivas).

- Cuando la comunicación suponga un esfuerzo desproporcionado, no pudiéndose llevar a cabo con una comunicación individual, se podrá efectuar una de carácter público, siempre y cuando permita informar a las personas afectadas de una manera efectiva.

No habiendo comunicado el responsable del tratamiento todavía la violación de la seguridad de los datos a los afectados, la autoridad de control, una vez se ha valorado si existe, o no, un alto riesgo, podrá exigir al responsable del tratamiento que proceda a efectuar la comunicación, o bien podrá decidir que

concurre alguno de los supuestos que eximen de efectuarla (supuestos del párrafo anterior) y, por tanto, que no resulta necesario llevar a cabo la comunicación del incidente de seguridad.

7.4. Gestión y registro de los incidentes de seguridad

Según el artículo 33.5 del RGPD, el responsable del tratamiento debe documentar los casos de violaciones de la seguridad de los datos personales, recopilando la información relacionada con los hechos y circunstancias en que se haya producido, sus consecuencias y las medidas de carácter correctivo que se hayan adoptado para que no vuelva a suceder; una información que quedará a disposición de las autoridades de control.

De hecho, se trata de una previsión muy similar a la prevista en la actual regulación (ya se citó en el apartado dedicado a las medidas de seguridad del RLOPD), que dispone que para todos los tratamientos de datos exista lo que denomina un «registro de incidencias» (arts. 90 y 100 RLOPD).

No solo se trata de que exista un registro donde conste: el tipo de incidencia, cuándo se ha producido o detectado, quién hizo la notificación interna, a quién se le comunicó, junto con los efectos del incidente y medidas aplicadas (en definitiva, circunstancias del incidente de seguridad), sino que deben existir también unos procedimientos internos de notificación y gestión de las incidencias.

Es evidente que la exigencia del RGPD de efectuar la notificación de la violación de seguridad, sin dilación, a la autoridad de control, y en su caso la comunicación a las personas afectadas, va a requerir que los responsables y encargados de tratamientos diseñen e implanten unos protocolos o procedimientos a aplicar en caso de que se produzca una violación de la seguridad de los datos.

Esos protocolos deberán ser conocidos por toda la organización, estableciendo claramente cómo se efectúan las comunicaciones y cómo se toman las decisiones, y en particular deberán prever quién, cómo y cuándo notifica la violación de seguridad a la autoridad de control, así como la operativa relacionada con la comunicación del incidente a las personas afectadas por este.

La existencia de esos procedimientos, obviamente, también supone una evidencia más de que se mantiene una actitud activa de cumplimento del RGPD, y por tanto atiende al principio de responsabilidad proactiva al que nos hemos venido refiriendo en diversas ocasiones.

En cuanto a las notificaciones y comunicaciones, hay que hacer una observación de carácter general en relación con lo ajustado de los plazos y la inmediatez con la que se espera que responsables y encargados de tratamiento actúen, ya que requerirá de una respuesta también ágil por parte de las autoridades de control.

Habrá que establecer canales de comunicación muy directos y de respuesta inmediata entre los operadores implicados, ya que atender la notificación de incidentes detectados en determinados momentos (fines de semana, días festivos, etc.) puede tener su dificultad si las autoridades de control no están preparadas para ello y, además, esa preparación también debe incluir tener personal cualificado para valorar los incidentes de seguridad que les puedan ser planteados.

En este caso, las autoridades de control también deben adaptar su organización para dar respuesta a las exigencias que el RGPD plantea en relación con la violación de la seguridad de los datos.

8. Verificación de las medidas de seguridad y responsabilidad proactiva

Ya hemos hecho referencia a lo que implica la incorporación del principio de responsabilidad proactiva en el RGPD, tanto desde la perspectiva del conjunto del cumplimiento del reglamento como, por supuesto, en relación con las medidas de seguridad.

En la práctica, atender a ese principio obliga a que, en el momento de diseñar e implantar los tratamientos, tengamos en cuenta que no solo es cuestión de definir las operaciones de acuerdo a lo previsto en el RGPD, es decir, teniendo en cuenta los principios, derechos y obligaciones que regula, sino que deberemos concretar de qué manera vamos a acreditar que, efectivamente, las decisiones que hemos ido tomando cumplen con las previsiones del RGPD.

En relación con las medidas de seguridad, habrá dos instrumentos que resultarán eficaces en esa necesidad de demostrar el cumplimiento: las auditorías y la revisión de los riesgos.

8.1. El principio de responsabilidad proactiva en relación con la seguridad de los datos: la gestión de la protección de datos

En la adopción de medidas de seguridad, sean de carácter tecnológico u organizativo, habrá que plantearse no solo qué protección aportan a los tratamientos de datos personales, sino también de qué manera podemos demostrar que tales medidas están implantadas y dan respuesta eficaz a la obligación se seguridad de los tratamientos que impone el RGPD sobre la base del «principio de integridad y confidencialidad».

No basta plantearse exclusivamente la implantación de medidas de seguridad cualesquiera; deberemos contar con medios que nos permitan acreditar, especialmente ante la autoridad de control, que las motivaciones para adoptar una determinada medida tienen que ver con el compromiso de cumplimiento de lo previsto en el RGPD y que no obedecen a otros criterios (coste, oportunidad, facilidad, etc.).

Tal y como recoge el artículo 24.1 del RGPD, en función de la naturaleza, ámbito, contexto y finalidad del tratamiento, junto con la gestión de los riesgos para los derechos y libertades, el responsable del tratamiento deberá aplicar medidas apropiadas para «garantizar y poder demostrar que el tratamiento es conforme» con el RGPD.

El propio RGPD aporta directamente algunos instrumentos que pueden ser útiles «para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento», como por ejemplo la adhesión a códigos de conducta, cuando estos especifiquen cuestiones relacionadas con la seguridad de los tratamientos (art. 40.2.h RGPD); o las certificaciones, sellos y marcas de protección de datos que también van a facilitar la capacidad de demostrar el cumplimiento del RGPD (art. 42 RGPD).

La reforma de la protección de datos, en buena medida, ha supuesto pasar de un escenario de cumplimiento, a partir de formalismos, a un cumplimiento sustentado en la gestión real de la protección de datos.

Ese evidente giro hacia la gestión de la protección de datos implica la superación de algunas formalidades y prácticas de un cierto carácter burocrático, desarrolladas a partir de la actual normativa (LOPD y RLOPD).

La tendencia obligada, para responsables y encargados de tratamiento, será la implantación de sistemas de la gestión de la protección de datos (por ejemplo, tipo BS 10012), de manera que ese sistema sea una parte más de la arquitectura de gobernanza de las organizaciones, dejando de ser la protección de datos una cuestión accesoria (no esencial) respecto de las necesidades de las actividades de negocio o de servicio público que precisan el uso de datos personales.

Un sistema de gestión de la protección de datos supone proveerse de un marco de trabajo interno orientado a mantener y mejorar el cumplimento de la normativa de protección de datos, y permite adoptar buenas prácticas en la gestión de la información de carácter personal, por tanto más allá del estricto cumplimiento.

Por supuesto, como en cualquier sistema de gestión, deberán llevarse a cabo actividades de monitorización y revisión que permitan identificar acciones preventivas y correctivas orientadas al cumplimiento y a la mejora global de los diferentes procesos en los que se vean involucrados datos de carácter personal.

8.2. Auditoría de las medidas de protección

El artículo 24.1, en su última frase, se refiere a la revisión de las medidas de protección adoptadas en relación con los tratamientos: «Dichas medidas se revisarán y actualizarán cuando sea necesario».

La revisión de las medidas comúnmente se concreta en la ejecución de procesos de auditoría sobre las medidas implantadas, es decir, de verificación de que las medidas están implantadas tal y como se definió en su momento, y de la verificación de si estas cumplen adecuadamente con la función de protección que originó su implantación.

En el RGPD no hay una mención expresa a que esa revisión deba llevarse a cabo siempre sobre la base de procesos formales de auditoría; puede llevarse a cabo de la manera que se considere más oportuna, aunque evidentemente la aplicación de técnicas de auditoría generalmente resultará lo más apropiado.

De hecho, en la primera versión del Reglamento, a partir de la propuesta de 25 de enero de 2012 de la Comisión Europea, en su artículo 22 («Obligaciones del responsable del tratamiento»), se hacía referencia a que el responsable del tratamiento debía implantar mecanismos para «verificar la eficacia» de las medidas implantadas y que, siempre que no fuera desproporcionado, esas verificaciones debían ser «llevadas a cabo por auditores independientes internos o externos». Esa referencia tan directa a la auditoría como obligación desaparece del texto definitivamente aprobado en mayo de 2016.

El RLOPD, en su artículo 96, sí que obliga, a partir del nivel medio de seguridad, a llevar a cabo una auditoría de protección de datos, como mínimo cada dos años, de manera ordinaria, con el objeto de verificar el cumplimiento de lo previsto en el RLOPD en cuanto a las medidas de seguridad (título VIII).

También se prevé que se lleve a cabo tal auditoría con carácter extraordinario cuando cambios sustanciales en el tratamiento pudieran dar lugar a la ineficacia de las medidas de seguridad implantadas.

Se hace referencia a la existencia de un informe de auditoría que debe dictaminar sobre la adecuación de las medidas de seguridad a lo previsto en la LOPD y en el RLOPD, identificando las deficiencias y proponiendo medidas correctoras o adicionales, y todo ello sustentado en datos, hechos y observaciones; en definitiva, en evidencias o pruebas de auditoría.

Ese informe de auditoría es analizado por el responsable se seguridad, que debe trasladar las conclusiones al responsable del tratamiento, a fin de que este tome las decisiones que correspondan atendiendo al contenido del informe de auditoría, para que los tratamientos se lleven a cabo en las debidas condiciones de seguridad. Esos informes de auditoría quedan a disposición de la autoridad de control.

Como podemos observar, y ya hemos mencionado, el RLOPD entra en detalles sobre cómo cumplir con la obligación de auditoría o revisión que no vamos a encontrar en el RGPD.

Aunque en el RGPD no se haga una referencia directa a la auditoría como mecanismo de revisión, lo cierto es que sí que encontraremos algunos preceptos que tienen en cuenta que se trata de una herramienta que va ser comúnmente utilizada.

Por ejemplo, en el artículo 28 («Encargado del tratamiento»), al concretar las estipulaciones que, como mínimo, deben recogerse en el contrato o acto jurídico que regule las relaciones de servicio entre responsable y encargado de tratamiento, se hace referencia, en su letra «h», al compromiso contractual del encargado de poner a disposición del responsable la información necesaria para «permitir o contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable».

Del mismo modo, en el artículo 39 del RGPD («Funciones del delegado de protección de datos»), se prevé que el delegado de protección de datos supervise el cumplimiento de lo dispuesto en «las auditorías correspondientes».

También, al regular en el artículo 47 las normas corporativas vinculantes, se menciona, entre los contenidos mínimos a especificar:

> «j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán **auditorías de protección de datos** y métodos para garantizar acciones correctivas para proteger los derechos del interesado». La auditoría, como instrumento de verificación del cumplimiento, da respuesta también al principio de responsabilidad proactiva, por lo que el conjunto del proceso de auditoría deberá documentarse adecuadamente y quedar a disposición de las autoridades de control.

8.3. Revisión de los riesgos

Teniendo en cuenta que en la gestión de riesgos deben sustentarse todas las decisiones relacionadas con los tratamientos, particularmente las que tienen que ver con la seguridad de estos, la evaluación de los riesgos debe ser revisada, ya sea de manera ordinaria o extraordinaria. Esta revisión debe llevarse a cabo a fin de verificar si los riesgos que se tuvieron en cuenta en su momento siguen estando bajo control, o si han aparecido nuevos riesgos, que podrían afectar a los derechos y libertades de las personas afectadas por los tratamientos.

Por supuesto, nada obsta para que esa revisión de los riesgos se lleve a cabo dentro del propio proceso de auditoría.

Como ya se ha hecho referencia, el RGPD orienta el cumplimiento a la gestión continuada de la protección de datos; por ello, una vez evaluados y tratados los riesgos, no podemos olvidarnos de ellos sin más, puesto que de manea inherente las operaciones de tratamiento de datos personales suponen riesgos para las personas.

Al tratar los riesgos se ha modificado su probabilidad y su gravedad, intentado minimizarlos y mantenerlos bajo control; por tanto, siguen latentes, de manera que si por alguna circunstancia las medidas adoptadas en razón de la valoración de los riegos no fueran eficaces, estos podrían producir sus efectos negativos.

Por consiguiente, el tratamiento y sus riesgos van a requerir ser revisados de manera periódica, para verificar que efectivamente los riesgos se mantienen en un nivel aceptable.

En este sentido, deben contemplarse dos tipos de revisiones, las de tipo ordinario, para las cuales debería fijarse un plazo adecuado de tiempo para su ejecución, por ejemplo dos años, según el caso. En caso de estar ante un tratamiento de muy alto riesgo, las revisiones anuales tampoco serían descartables; concretar ese periodo de revisión también supone una decisión que debe ser tomada por parte del responsable a partir del riesgo.

En el caso de las revisiones ordinarias, estaríamos ante un proceso muy similar al que ya se llevó a cabo cuando se evaluaron los riesgos por primera vez, centrándonos en verificar que no han aparecido nuevos riesgos y que, respecto de los ya conocidos, se mantienen en el mismo nivel, constatando que las medidas implantadas siguen siendo adecuadas.

Otra cosa sería el supuesto de revisiones extraordinarias, que deberían llevarse a cabo cuando las operaciones de tratamiento se modifiquen sustancialmente, ya sea por la introducción de nuevas tecnologías, nuevos modelos de negocio, nuevos datos, nuevos afectados, etc.

En ese caso, debería llevarse a cabo una evaluación de riesgos más completa, a fin de actualizar la evaluación inicial, en razón de cambios relevantes en las condiciones de tratamiento.

También constituye una evidencia alineada con el principio de responsabilidad proactiva tener implantados unos procesos de revisión que estén adecuadamente documentados.

9. Conexión entre la seguridad del tratamiento y la evaluación de impacto sobre los datos personales

El RGPD incorpora una nueva obligación para los responsables de tratamientos, la de llevar a cabo una evaluación del impacto que las operaciones de tratamiento pueden tener sobre la protección de los datos personales (en adelante, EIPD), cuando esas operaciones puedan poner en riesgo, de una manera relevante, los derechos y libertades de las personas, por tanto, una obligación estrechamente vinculada a la gestión de los riesgos.

Las EIPD no dejan de ser la versión europea de las evaluaciones de impacto sobre la privacidad, conocidas por sus siglas en inglés PIA (Privacy Impact Assessment), que ya tienen un cierto recorrido en el ámbito de la privacidad y la protección de los datos personales, especialmente en el mundo anglosajón.

Las EIPD deben situarse en el contexto de las medidas o acciones preventivas, es decir, se trata de un proceso de evaluación que debe realizarse antes de iniciar las operaciones de tratamiento de los datos personales; en este sentido, conecta con el concepto de privacidad en el diseño (*privacy by design*), que en el RGPD se identifica como «protección de datos desde el diseño». Eso implica que, tanto en el momento de definir las diferentes operaciones de tratamiento como al determinar los medios que van a ser utilizados para tratar los datos personales, van a tenerse en cuenta, en esa toma de decisiones, los principios, derechos y obligaciones recogidos por la normativa que vaya a ser de aplicación al conjunto de tratamientos de datos personales que se pretenden llevar a cabo. Todo ello desde la necesidad de gestionar los riesgos que pueden suponer las operaciones de tratamiento para los derechos y libertades fundamentales.

La diferencia respecto de la obligación de evaluar riesgos e implantar medidas de seguridad en los tratamientos es que esta última es una obligación que aplica con carácter general a todos los tratamientos, en tanto que las EIPD están orientadas a tratamientos que aún no existen y que por tanto se están proyectando. Además, como se verá, no es una obligación que alcance a todos los tratamientos de datos personales.

Las EIPD es otro de los instrumentos útiles en relación con el principio de «responsabilidad proactiva», puesto que facilita no solo el cumplimiento sino la capacidad de demostrarlo; por tanto, permiten «construir y demostrar el cumplimiento».

Las EIPD están orientadas a asegurar preventivamente que, cuando las operaciones de tratamiento puedan entrañar riesgos especialmente relevantes (alto riesgo), se prevea tomar medidas para reducir, en la medida de lo posible, que

esas operaciones de tratamiento puedan dañar o perjudicar a las personas, o afectar negativamente a sus derechos y libertades, impidiendo o limitando su ejercicio, o contenido.

En este sentido, y como diferencia con la seguridad de los tratamientos, en la evaluación de impacto no solo se tiene en cuenta la seguridad. El alcance es mayor, ya que esos riesgos y las medidas que puedan llegar a definirse para mitigarlos podrán referirse a otras cuestiones no relacionadas con la seguridad de los tratamientos: el tiempo de conservación de los datos, la designación del responsable de protección de datos, la gestión del consentimiento, las transferencias internacionales, etc., por citar tan solo algunos ejemplos.

Tal y como ha expresado el Grupo de Trabajo del Artículo 29, la evaluación de impacto es un proceso diseñado para describir el tratamiento, evaluar su necesidad y proporcionalidad, y ayudar a gestionar los riesgos que pueden resultar para los derechos y libertades, evaluando tales riesgos y determinando las medidas más adecuadas para abordarlos.

El RGPD, en su Considerando 84, recoge que «a fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas», el responsable del tratamiento deberá realizar una evaluación de impacto relativa a los datos personales para evaluar, en especial, «el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo».

El resultado de la evaluación necesariamente deberá tenerse en cuenta al tomar las decisiones relacionadas con el cumplimiento de lo previsto en el RGPD, lo que incluye la capacidad de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con lo previsto en el Reglamento (como ya se ha avanzado, atendiendo al principio de responsabilidad proactiva o demostrable).

Una cuestión importante es que, si del resultado de la evaluación se llega a la conclusión de que las operaciones de tratamiento implican un alto riesgo, que no puede ser mitigado (gestionado), a partir de la tecnología disponible, o bien por los costes o dificultades de implantación de las medidas necesarias para reducir los riesgos, el responsable del tratamiento deberá consultar a la autoridad de protección de datos competente (autoridad de supervisión) sobre cómo proceder. Por descontado, esa consulta debe llevarse a cabo antes de iniciar las operaciones de tratamiento que generan esos riesgos.

En relación con los supuestos en que debe llevarse a cabo la EIPD, en tanto entrañen un alto riesgo, el Considerando 91 del RGPD se refiere a que deben aplicarse, en particular, a las operaciones que supongan un tratamiento de datos a gran escala, es decir, que tienen por objeto el procesamiento de una can-

tidad considerable de datos personales, ya sea en el ámbito regional, nacional o supranacional, y que por tanto podrían afectar a un gran número de personas, o bien cuando se utilizan nuevas tecnologías también a gran escala.

También deberá llevarse a cabo cuando se traten datos sensibles, o bien cuando se utilicen tecnologías emergentes; en particular, cuando hagan más difícil para las personas afectadas ejercer sus derechos.

Por ejemplo, se hace referencia expresa a que será necesario proceder a realizar la evaluación de impacto cuando se lleve a cabo el control de áreas de acceso público a gran escala, especialmente cuando se utilizan dispositivos óptico-electrónicos (típicamente sistemas de videovigilancia).

Respecto de los encargados de tratamiento, se considera que estos deberán cooperar con el responsable del tratamiento, a los efectos de garantizar el cumplimiento de las medidas que resulten de la evaluación de impacto de protección de datos. Esa colaboración se extiende a aquellos casos en que deba llevarse a cabo una consulta previa a la autoridad de supervisión competente, por tanto una colaboración equivalente al tipo de implicación que estos deben tener en relación con las medidas de seguridad, si bien en el caso de las EIPD la obligación de llevarlas a cabo solo alcanza a los responsables de tratamiento.

Que solo sea obligación de los responsables tiene todo el sentido, ya que las EIPD se aplican a tratamientos respecto de los cuales todavía deben tomarse decisiones (en fase de diseño), por lo que el tratamiento aún no existe. En consecuencia, quien decide que un conjunto de operaciones de tratamiento exista solo puede ser el responsable del tratamiento; recordemos que como principio general el encargado debe limitarse a llevar a cabo las operaciones de tratamiento siguiendo las instrucciones del responsable.

La EIPD tiene como objetivo «gestionar los riesgos» para los derechos y libertades de las personas físicas, sobre la base de tres procesos:

- establecimiento de las características: «teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo»;

- evaluación de los riesgos: «valorar la particular gravedad y probabilidad del alto riesgo»;

- tratamiento de los riesgos: «mitigar el riesgo» y «garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento».

En definitiva, EIPD y seguridad de los tratamientos son conceptos que están estrechamente vinculados, especialmente por su objetivo: gestionar los riesgos para los derechos y libertades.

9.1. La seguridad de los tratamientos en las evaluaciones de impacto

La falta de adopción de medidas de seguridad adecuadas en los tratamientos constituye en sí misma una importante fuente de riesgo potencial para los derechos y libertades; por tanto, a la hora de llevar a cabo la evaluación de impacto, habrá que tener en cuenta también los riesgos derivados de los potenciales incidentes de seguridad.

El RGPD plantea la necesidad de que las medidas de seguridad concretas a aplicar se adapten al riesgo y a las circunstancias que rodean a los tratamientos, lo que modifica sustancialmente el modelo actual (el del título VIII del RLOPD). En este, como ya sabemos, para determinar las medidas de seguridad, en la práctica solo se tiene en cuenta el tipo de datos; ahora las medidas de seguridad a adoptar deberán adaptarse a cada caso concreto.

Por lo que respecta a la gestión de los riesgos en relación con la seguridad de los tratamientos, en el contexto de la ejecución de una EIPD, habrá que tener en cuenta los riesgos desde la misma perspectiva que hemos aplicado para la gestión de riesgos de seguridad, es decir, evaluar qué efectos negativos se pueden derivar para las personas como consecuencia de:

- la destrucción de datos personales
- la pérdida de datos personales
- la alteración de datos personales (accidental o malintencionada)
- la comunicación no autorizada de datos personales
- el acceso no autorizado a los datos personales

Como podemos observar, no hay diferencias entre uno y otro planteamiento en cuanto a la gestión de riesgos, ya que los potenciales escenarios de riesgo que puedan darse en el contexto de unas determinadas operaciones de tratamiento se van a evaluar y gestionar del mismo modo, con la diferencia de que, en un caso, se hace en la fase de diseño (el tratamiento aún no se está llevando a cabo), reservándose para situaciones de alto riesgo, mientras que en la gestión de riesgos genérica las operaciones de tratamiento ya existen y se aplica a todos los tratamientos, aunque representen un mínimo riesgo.

No debemos olvidar que cualquier tratamiento implica de manera inherente riesgos para los derechos y libertades de las personas; la cuestión es valorar adecuadamente ese nivel de riesgo y mantenerlo bajo control, aplicando medidas técnicas u organizativas.

10. Régimen sancionador, indemnizaciones y seguridad del tratamiento

La seguridad de los tratamientos constituye una obligación establecida en el RGPD, a partir de uno de los principios recogidos en su artículo 5 («integridad y confidencialidad»), que obliga a responsables y encargados de tratamientos a adoptar las medidas de seguridad adecuadas a los riesgos que presenten las operaciones de tratamiento.

Si no se adoptan medidas o, aun adoptándolas, estas no han resultado eficaces para proteger los datos personales, estaríamos ante un incumplimiento de las disposiciones del RGPD que podría acabar en una declaración de infracción del reglamento.

Los incumplimientos podrán ser sancionados por las autoridades de protección de datos en el ejercicio de las funciones que tienen atribuidas para salvaguardar el derecho fundamental a la protección de los datos de carácter personal.

Entraremos en mayor detalle sobre el régimen sancionador, tanto de la LOPD como del RGPD. Antes conviene hacer mención a otro tipo de consecuencias que puede tener el incumplimiento de las disposiciones del RGPD relacionadas con la seguridad de los tratamientos.

Concretamente, en el Considerando 146 se parte de la base de que el responsable o el encargado del tratamiento deberán indemnizar por los daños y perjuicios que pueda sufrir una persona cuyos datos hayan sido tratados infringiendo el RGPD; obviamente, si se demuestra que estos no son responsables de tales daños y perjuicios, quedarán exentos de responsabilidad.

De tal modo que el artículo 82 del RGPD («Derecho a indemnización y responsabilidad») establece que, cuando una persona sufra «daños y perjuicios materiales o inmateriales como consecuencia de una infracción» del RGPD, tendrá derecho a recibir una indemnización por los daños y perjuicios sufridos.

Por tanto, el responsable del tratamiento responderá por los daños y perjuicios causados por las operaciones de tratamiento que no cumplan con las disposiciones del RGPD.

En el caso de los encargados de tratamiento, estos deberán responder si no cumplen con las obligaciones previstas para ellos en el RGPD o si actúan sin seguir las instrucciones proporcionadas por el responsable del tratamiento.

El derecho a indemnización se regula también en la normativa aún vigente, si bien se ubican en el título III, dedicado a los «derechos de las personas», concretamente en el artículo 19 de la LOPD.

La regulación de esa posibilidad de indemnización de la LOPD es equivalente a lo previsto en el RGPD. Si se causan daños y perjuicios por incumplimiento de la ley, la persona afectada tiene derecho a ser indemnizada por el responsable o por el encargado del tratamiento, según sea el caso.

La persona afectada deberá acudir a los órganos de la jurisdicción ordinaria para reclamar por daños y perjuicios, cuyo origen sea el tratamiento de sus datos de carácter personal llevado a cabo incumpliendo lo previsto en la legislación.

10.1. Infracciones relacionadas con la seguridad de los tratamientos en la LOPD

El artículo 44 de la LOPD califica como infracción grave «mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen».

Como ya hemos visto, la determinación de las medidas de seguridad que deben adoptarse se recoge en el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, concretamente en su título VIII, dedicado a las «medidas de seguridad en el tratamiento de los datos de carácter personal».

Por tanto, si no se han implantado las medidas de seguridad adecuadas, es decir, las previstas en el RLOPD en función del tipo de datos objeto de tratamiento, o estas no funcionan adecuadamente, los datos no se estarán tratando en las debidas condiciones de seguridad, y podría declararse la infracción por parte de la autoridad de control competente sobre la base del inicio de un expediente sancionador, que habitualmente va precedido por una fase de investigación previa, o inspección.

En general, los expedientes sancionadores tienen su origen en reclamaciones o denuncias de las personas afectadas por los tratamientos.

Hay otros tipos infractores que, en algún caso, podrían estar conectados con las medidas de seguridad, como por ejemplo «la vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal», previsto en el artículo 10 de la LOPD, es decir, a veces la falta de medidas de seguridad puede desembocar en unas consecuencias que podrían estar también tipificadas como infracciones.

El artículo 10 establece que el responsable, y quienes pueden intervenir en el tratamiento de los datos personales, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos; se trata de una obligación que permanece incluso después de que ya no exista relación con el responsable del tratamiento (se trata también de una infracción grave).

«Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros». Conviene recordar que, en el caso de tratamientos sujetos a la responsabilidad de las Administraciones públicas, no se imponen sanciones económicas, estableciendo la resolución sancionadora las medidas que deben implantarse para corregir la situación de infracción; la autoridad de control, en su caso, también puede proponer el inicio de actuaciones disciplinarias.

De manera excepcional, la autoridad de control podrá, según la naturaleza de los hechos constitutivos de infracción, y si concurren ciertas circunstancias (las del artículo 45.5 de la LOPD), no acordar la apertura del procedimiento sancionador, procediendo a apercibir al infractor para que, en un plazo determinado, el responsable acredite la adopción de las medidas correctoras adecuadas.

Para aplicar la figura del apercibimiento será necesario que se trate de unos hechos que constituirían «infracción leve o grave» y «que el infractor no haya sido sancionado o apercibido con anterioridad»; nótese que deben concurrir ambas circunstancias.

Ya hemos hecho referencia al anteproyecto de Ley orgánica de protección de datos que, en relación con las infracciones, deberá introducir el régimen sancionador previsto en el RGPD atendiendo, en particular, al principio de tipicidad de las infracciones administrativas que se deriva del artículo 25.1 de la Constitución.

10.2. Infracciones relacionadas con la seguridad de los tratamientos en el RGPD

El RGPD también prevé el derecho de las personas afectadas por los tratamientos a presentar una reclamación ante una autoridad de control, si considera que el tratamiento que se está haciendo de sus datos personales infringe el reglamento (art. 77.1).

La infracción de lo previsto en los artículos 32, 33 y 34 del RGPD (como hemos visto, directamente relacionados con la seguridad de los tratamientos) podrá sancionarse con una «multa administrativa» de hasta 10.000.000 de euros, o bien con una cuantía equivalente, como máximo, al 2 % del volumen de negocio total anual global del ejercicio financiero anterior del responsable o encargado del tratamiento (se aplicará la cuantía mayor).

Se pueden imponer también otro tipo de sanciones que no impliquen una multa.

Lo cierto es que el RGPD no identifica unos tipos infractores concretos (hechos constitutivos de posible infracción), puesto que se limita a hacer referencia a la infracción de preceptos específicos del RGPD (artículos), sin describir las conductas que implican tal incumplimiento, de lo que se deriva una evidente falta de atención al principio de tipicidad.

El PLOPD incluye, en su título VIII, el régimen sancionador que presumiblemente será aplicable en el ordenamiento jurídico español cuando se incumpla con lo previsto en el RGPD. Hay que tener en cuenta que se trata de un proyecto de ley que deberá seguir el pertinente procedimiento legislativo, y que durante él mismo puede sufrir modificaciones. En consecuencia, lo que se expresa a continuación es solo con carácter orientativo.

En el artículo 70 del PLOPD se identifican a aquellos que pueden ser responsables de cometer infracciones en relación con los tratamientos de datos de carácter personal y que, por tanto, estarán sujetos al régimen sancionador, excluyendo de su aplicación al delegado de protección de datos.

El artículo 72 del proyecto de LOPD considera infracción muy grave, vinculada directamente a la seguridad de los tratamientos, llevar a cabo tratamientos de datos personales vulnerando los principios y garantías previstos en el artículo 5 del RGPD (entre ellos, recordemos que está el principio de «integridad y confidencialidad», que se concreta en que los datos personales sean tratados garantizando su seguridad).

Por su parte, el artículo 73 considera como infracciones graves, vinculadas directamente a la seguridad de los tratamientos, las siguientes conductas:

- el tratamiento de datos de carácter personal «sin llevar a cabo una previa valoración de los riesgos»;

- no adoptar las medidas técnicas y organizativas adecuadas para integrar las garantías necesarias para cumplir con los requisitos de protección de los datos recogidos en el RGPD (no se hace referencia directa a medidas de seguridad, pero quedarían incluidas en esta definición, un tanto amplia, de cumplimiento de los requisitos que deben tenerse en cuenta para llevar a cabo tratamientos de datos de carácter personal según el RGPD, aunque desde la perspectiva de dotar de mayor seguridad jurídica al texto tal vez sería conveniente una referencia más clara);

- el incumplimiento, por parte del encargado del tratamiento, del deber de notificar al responsable una violación de la seguridad de los datos;

- que el responsable del tratamiento no notifique una violación de la seguridad de los datos a la autoridad de control;

- que el responsable del tratamiento no comunique una violación de la seguridad de los datos a los afectados, cuando haya sido requerido para ello por la autoridad de control.

Y el artículo 74 considera como infracciones leves, vinculadas directamente a la seguridad de los tratamientos, las siguientes conductas:

- notificar de manera incompleta o defectuosa la información que debe acompañar a una notificación de violación de la seguridad de los datos;

- no documentar las violaciones de la seguridad de los datos;

- no comunicar a las personas afectadas que se ha producido una violación de la seguridad de los datos, cuando el incidente pueda suponer un alto riesgo para los derechos y libertades.

Finalmente, cabe decir que se establece, en el artículo 77, un régimen especial para ciertas categorías de responsables o encargados de tratamiento. Este precepto, básicamente, reproduce lo que la LOPD prevé en el caso de las Administraciones públicas, en tanto que esas categorías de responsables y encargados no serán objeto de multa administrativa si llevan a cabo alguna de las conductas consideradas como infracción, siendo objeto de apercibimiento, junto con el requerimiento de adoptar las medidas necesarias para corregir la situación.

Resumen

Sin duda, el RGPD supone un cambio sustancial en lo que respecta a la seguridad de los tratamientos: la necesidad de identificar, analizar y valorar los riesgos, a los efectos de seleccionar las medidas de seguridad técnicas y organizativas más adecuadas, implica que responsables y encargados de tratamientos deben asumir una responsabilidad directa sobre cómo proteger los datos.

Por tanto, las medidas a adoptar para asegurar los tratamientos van a ser el resultado de gestionar los riesgos que puedan implicar las operaciones de tratamiento, teniendo en cuenta los diversos factores que pueden concurrir en esas operaciones, es decir, «personalizando» qué medidas resultan más eficaces en cada caso.

Un planteamiento que resulta más eficiente, aportando una mejora evidente respecto de la situación actual, donde en la práctica solo se tiene en cuenta el tipo de datos tratados, para a continuación escoger unas medidas de seguridad «preseleccionadas» por el legislador.

Ese nuevo escenario, si bien aporta flexibilidad, en cuanto a cómo cumplir con la normativa, no es menos cierto que también supone una dificultad añadida para responsables y encargados de tratamiento. Con el nuevo marco legal no solo se trata de implantar adecuadamente las medidas de seguridad, sino que deberán seleccionarse también de una manera adecuada. Por lo tanto, la calidad de la evaluación de riesgos va a ser esencial para cumplir acertadamente con la obligación de implantar medidas de seguridad en las operaciones de tratamiento.

Este cometido puede resultar especialmente complejo para los responsables y encargados de tratamiento con menos recursos, o sin una «cultura» previa de la gestión de riesgos. En consecuencia, deberán buscarse mecanismos que permitan que ese tipo de responsables y encargados de tratamiento puedan llevar a cabo la evaluación de riesgos de una manera sencilla y adaptada a sus posibilidades y circunstancias.

En general, el RGPD debería dar como resultado unas medidas de seguridad más ajustadas a las circunstancias específicas de cada tratamiento, lo que debería redundar en una mejor protección de los tratamientos y, en consecuencia, una mayor salvaguarda del derecho fundamental a la protección de los datos de carácter personal.

Ciertamente los cambios son relevantes, y en los primeros momentos de su plena aplicación se van a plantear situaciones que podrán ser objeto de diversa interpretación. Por ello, la opinión y la actividad de las autoridades de control

va a ser esencial para ir clarificando aquellos aspectos de la seguridad de los tratamientos que, si bien no se puede afirmar que sean confusos en cuanto a su definición, sí que pueden resultar complejos en cuanto a su aplicación.