Foro, Nueva época, núm. 8/2008: 193-220 ISSN:1698-5583

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

Fernando FALCÓN Y TELLA
Profesor Contratado Doctor de Filosofía del Derecho
Facultad de Derecho. Universidad Complutense de Madrid
ffalte@hotmail.com

RESUMEN

A lo largo del presente artículo se analiza el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, examinando las medidas de seguridad aplicables a cada nivel —básico, medio y alto— tanto en ficheros y tratamientos automatizados como manuales.

Palabras clave: medidas de seguridad, ficheros, datos, niveles de seguridad —básico, medio y alto—.

ABSTRACT

In this paper the author analyses the Title VIII of the R.D. 1720/2007, December 21st, which containing the development rules of the Organic Law 15/1999, December 13th, on Personal Data Protection (Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal), *with the aim of study the security measures applied to each —basic, intermediate and high— level in files or in automated or manual treatments.*

Keywords: security measures, files, data, security levels —basic, intermediate and high—.

ZUSAMMENFASSUNG

Im Verlauf des vorliegenden Artikels wird der VIII. Titel des Spanischen Gesetzes Nr. 1720/2007, vom 21. Dezember untersucht. Untersucht wird die Ausführungsbestimmung zur Anwendung des Spanischen Organgesetz 15/1999, vom 13. Dezember (Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal) *zum Schutz personengebundener Daten, wobei die Sicherheitsvorkehrungen, die auf der jeweiligen Sicherheitsstufe —niedrig, mittel, hoch— sowohl bei automatisierten als auch bei manuellen Datenverarbeitungsprozessen angewendet werden, im Mittelpunkt der Betrachtung stehen.*

Schlüsselwörter: Sicherheitsmaßnahmen, Datenbestände, Sicherheitsstufen (niedrig, mittel, hoch).

1. INTRODUCCIÓN

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —LOPD— vino a derogar, como es sabido, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal —LORTAD—[1]. La LOPD introduce como novedades más importantes, entre otras muchas, las siguientes[2]: la ampliación del concepto de dato personal a la imagen y soni-

[1] Lo que inicialmente iba a ser una mera reforma de la LORTAD con el objeto de trasladar a nuestro ordenamiento jurídico el contenido de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, terminó convirtiéndose en un nuevo texto normativo que vino a derogar la LORTAD. La LOPD se publicó el día 14 de diciembre de 1999 y entró en vigor el día 14 de enero de 2000. Véase sobre el tema: P. GUTIÉRREZ SÁNCHEZ, «Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)», en *Actualidad Informática Aranzadi,* núm. 28, julio de 1998, pp. 1 y ss.; E. SUÑÉ LLINÁS, *Tratado de Derecho Informático,* vol. I, *Introducción y protección de datos personales,* Madrid, Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid-Instituto Español de Informática y Derecho, 2000, pp. 103 y ss.; A. TÉLLEZ AGUILERA, *Nuevas tecnologías. Intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999,* Madrid, Edisofer, 2001, pp. 107 y ss., y M. Á. DÁVARA RODRÍGUEZ, *Manual de Derecho Informático,* 10.ª ed., Navarra, Aranzadi, 2008, pp. 62 y ss.

[2] Véase A. TÉLLEZ AGUILERA, *Nuevas tecnologías..., op. cit.,* p. 108. Sobre las principales novedades introducidas por la LOPD resultan sumamente interesantes los trabajos de J. M. FERNÁNDEZ LÓPEZ, «La nueva Ley de Protección de Datos de carácter personal de 13

do[3], la conciliación de los principios de protección de datos personales con la libertad de expresión, el reconocimiento del derecho de oposición a que los datos sean objeto de tratamiento, la aparición de la figura del encargado del tratamiento[4] o la especial protección de los datos sindicales[5].

La LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos de carácter personal, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente su derecho al honor e intimidad personal y familiar, dando cumplimiento al mandato constitucional[6]. Es de aplicación —como señala su art. 2.1— a todos «los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado», si bien a lo largo de su articulado es posible encontrar algunas deficiencias técnicas que parecen no tener presente la considerable ampliación del ámbito de aplicación contemplado en la Ley[7].

---

de diciembre de 1999. Su porqué y sus principales novedades», en *Actualidad Informática Aranzadi,* núm. 34, enero de 2000, pp. 1 y ss., y J. M.ª Álvarez-Cienfuegos Suárez, «Notas a la nueva regulación de la protección de datos de carácter personal», en *La Ley,* núm. 5.036, 17 de abril de 2000, pp. 1 y ss.

[3] Si bien la LORTAD no hacía referencia a estos conceptos, el art. 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollaban determinados aspectos de la LORTAD, ya aludía a la hora de definir los datos de carácter personal a «la información fotográfica, acústica o de cualquier otro tipo».

[4] Según establece el propio art. 3.*g)* LOPD, el «encargado del tratamiento» es «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trae datos personales por cuenta del responsable del tratamiento». El art. 5.1.*i)* del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, profundiza algo más en la definición, al señalar que es «la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio», pudiendo ser también encargados del tratamiento «los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados».

[5] Véase nota 32.

[6] El art. 18 de la Constitución garantiza en su apartado primero «el derecho al honor, a la intimidad personal y familiar y a la propia imagen», para terminar señalando en el apartado cuarto que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

[7] Por ejemplo, en el art. 26.3 LOPD se habla de ficheros «automatizados» a la hora de señalar que se deben comunicar a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad de los mismos cuando, en realidad, en virtud de la ampliación del objeto de la Ley, debería de hablarse de cualquier fichero que contenga datos de carácter personal registrados en soporte físico que sea susceptible de tratamiento, esté o no automatizado. Además carece de una Exposición de Motivos que explique la razón de su existencia.

El Título II de la LOPD consagra —en ocasiones de forma poco afortunada—[8] los principios básicos que rigen en materia de protección de datos de carácter personal, que pueden agruparse en dos categorías: en primer lugar, los principios relativos a la calidad de los datos y a su tratamiento; y, en segundo término, los principios relativos a la seguridad, que son los que a lo largo de estas líneas se pretende analizar en profundidad, teniendo además en cuenta que este segundo grupo de principios ha sufrido recientemente un cambio en su regulación reglamentaria.

2. EL ART. 9 DE LA LOPD

La LOPD es extremadamente genérica a la hora de establecer el régimen jurídico en materia de seguridad de datos de carácter personal. En efecto, su art. 9 se limita a establecer la obligación de aplicar las medidas técnicas y organizativas necesarias para la protección de los datos de carácter personal. Dicho precepto dice literalmente:

> «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 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[9].
>
> 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 art. 7 de esta Ley»[10].

---

[8] La regulación contenida en el Título II LOPD es poco afortunada en cuanto a sistemática se refiere —como acertadamente ha puesto de manifiesto A. TÉLLEZ AGUILERA, *Nuevas tecnologías..., op. cit.,* p. 127—, puesto que: por un lado, se incluyen preceptos que configuran auténticos derechos y que, en consecuencia, deberían estar en el título siguiente, y por otro lado, regula aspectos, como el consentimiento del afectado o la cesión de datos, que, dada su indudable trascendencia, merecerían un tratamiento autónomo.

[9] En esta línea el art. 44.3.*b)* LOPD establece como infracción grave sancionable con multa de hasta 300.506 euros la de «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».

[10] El art. 7 LOPD establece un régimen mayor de protección a los datos de carác-

La parquedad de dicho precepto obliga a plantearse lo que ha de entenderse por «medidas técnicas y de organización adecuadas para garantizar la seguridad de los datos personales»[11]. Para poder dar una respuesta adecuada a dicha cuestión era necesario hasta hace poco tiempo acudir al desarrollo reglamentario de la norma, al Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Dicho Real Decreto, aunque es anterior a la aprobación de la LOPD, en virtud de lo establecido en la disposición transitoria tercera de la LOPD continuó en vigor en todo aquello en que no se opusiera a la misma, articulando un sistema que planteaba un buen número de problemas de aplicación práctica a las pequeñas empresas, autónomos y profesionales liberales[12].

El Real Decreto 994/1999 determinaba las medidas de índole técnica y organizativa que garantizaban la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos que garantiza el art. 18.4 de la Constitución frente a su alteración, pérdida, tratamiento o acceso no autorizado. Las medidas de seguridad que establecía dicho Reglamento se configuraban como las básicas de seguridad que tenían que cumplir todos los ficheros que contuvieran datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigían un grado de protección mayor. Dicho Reglamento establecía la exigencia por parte del responsable del fichero[13]

---

ter personal que considera dignos de una especial protección. Dichos datos personales son aquellos que revelen ideología, afiliación sindical, religión y creencias, los referidos al origen racial y a la vida sexual, los relativos a la salud y los relativos a la comisión de infracciones penales o administrativas.

[11] Parece razonable pensar que las medidas de seguridad adecuadas dependerán necesariamente de los avances tecnológicos, puesto que ni pueden ser exigibles protecciones técnicamente inviables, ni tiene sentido proteger los datos personales frente a amenazas técnicamente irrealizables. Véase J. L. Cueva Calabia, «La LORTAD y la seguridad de los sistemas automatizados de datos personales», en *Actualidad Informática Aranzadi,* núm. 13, octubre de 1994, p. 8.

[12] Véase F. Ramos Suárez, «Nuevo Reglamento de seguridad para la protección de ficheros automatizados con datos de carácter personal: ¿obstáculo o ayuda al desarrollo de la empresa española?», en *Revista Electrónica de Derecho Informático,* núm. 14, septiembre de 1999. En este mismo sentido se manifiesta F. Jurado Ubeda, «Las Pymes ante la nueva Ley de Protección de Datos Personales», en VVAA, *Nueva Ley de Protección de Datos de Carácter Personal y reglamento de medidas de seguridad informática,* Madrid, 2000, p. 69.

[13] Según establece el art. 3.*d)* LOPD, el «responsable del fichero o tratamiento» es «la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que

de elaborar e implantar la normativa de seguridad prevista en el mismo mediante un documento —el denominado documento de seguridad— de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. A su vez, clasificaba las medidas de seguridad exigibles en tres niveles: básico, medio y alto. Dichos niveles se establecían atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, teniendo cada uno de ellos la condición de mínimo exigible, de forma que el Reglamento establecía el nivel mínimo de protección que debía tener cada tipo de fichero, no existiendo ningún obstáculo para que el responsable del fichero adoptase un nivel de seguridad mayor.

3. EL REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE, POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En fecha reciente la normativa en materia de seguridad de datos de carácter personal ha cambiado con el Real Decreto 1720/2007, de 21 de diciembre[14], por el que se aprueba el Reglamento de desarrollo de la Ley

decida sobre la finalidad, contenido y uso del tratamiento». El art. 5.1.*q)* del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, profundiza algo más en la definición, al señalar que es «la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que, solo o conjuntamente con otros, decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente», pudiendo ser también responsables del fichero o del tratamiento «los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados».

[14] El 21 de diciembre de 2007 se aprobó el Real Decreto 1720/2007, que fue publicado en el *Boletín Oficial del Estado* núm. 17, de 19 de enero de 2008, y entró en vigor a los tres meses de su publicación, esto es, el día 19 de abril de 2008. En relación a la implantación de las medidas de seguridad en los ficheros automatizados preexistentes al Reglamento el plazo es —como señala la disposición transitoria segunda— de un año desde su entrada en vigor —19 de abril de 2009—. No obstante, existen dos excepciones a la regla general: la primera, referente a las medidas de seguridad de nivel alto de los ficheros que contengan datos derivados de actos de violencia de género; y la segunda, relativa a las medidas de seguridad de nivel alto para los datos de tráfico y localización en ficheros de operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas. En estos dos casos, el plazo es de dieciocho meses desde la entrada en vigor del Reglamento —19 de octubre de 2009—. En relación a los fiche-

Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que deroga el Real Decreto 994/1999.

El Real Decreto 1720/2007 —que viene a ser el desarrollo reglamentario completo de la LOPD— establece en el Título VIII las medidas de seguridad que han de adoptarse en el tratamiento de datos de carácter personal. La finalidad perseguida es garantizar que nadie no autorizado pueda acceder a los datos y evitar la alteración o pérdida de los mismos. Como reconoce la propia Exposición de Motivos del Reglamento, a lo largo del Título VIII se regula un aspecto esencial en materia de protección de datos, como es el de su seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión. Y es que la seguridad en este campo obligaba a una reglamentación particularmente rigurosa. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían tenido los responsables de los ficheros e identificar los puntos fuertes y débiles de la regulación. Por otra, se venía reclamando la adaptación de la normativa en diferentes puntos y aspectos[15].

En este sentido, el Real Decreto 1720/2007 —en adelante, el Reglamento— intenta ser, como señala su propia Exposición de Motivos, particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponde adoptar en cada caso y en la revisión

---

ros no automatizados o manuales los plazos son los siguientes: un año desde la entrada en vigor para aquellos que requieren solamente las medidas de seguridad de nivel básico —19 de abril de 2009—; dieciocho meses para los ficheros que exigen un nivel medio de seguridad —19 de octubre de 2009—, y dos años desde la entrada en vigor del Reglamento para aquellos ficheros que deben adoptar las medidas de seguridad calificadas como de nivel alto —19 de abril de 2010—. Lógicamente, los ficheros —tanto automatizados como no automatizados— creados con posteridad a la entrada en vigor del Reglamento, esto es, el día 19 de abril de 2008, deberán tener implantadas, desde el momento de su creación, la totalidad de las medidas de seguridad reguladas en el mismo.

[15] El Real Decreto 1720/2207 nace con la vocación de desarrollar no sólo los mandatos contenidos en la LOPD, sino también aquellos otros que en estos años de vigencia de la LOPD la práctica ha demostrado que precisan de una mayor regulación reglamentaria. Abarca el ámbito tutelado anteriormente por el Real Decreto 1332/1994, de 20 de junio, y el Real Decreto 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar los criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otro lado, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, obligaba también a desarrollar los procedimientos para el ejercicio de la potestad sancionadora por la Agencia. Sobre el Real Decreto 1720/2007 resulta sumamente interesante y clarificador el reciente estudio de M. Á. Dávara Rodríguez, *Análisis del Real Decreto 1720/2007: el Reglamento de la LOPD,* Madrid, DaFeMa, 2008.

de las mismas cuando sea necesario. A su vez, intenta ordenar con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, pretende regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica.

El principio de seguridad en materia de protección de datos de carácter personal exige, a nivel práctico, que el responsable de un fichero o tratamiento y el encargado del tratamiento puedan conocer los riesgos existentes y establecer los medios necesarios para que no se produzca un tratamiento ilegal, no consentido o efectuado de forma irregular de los datos. Asimismo, resulta importante garantizar no solamente la confidencialidad sobre las medidas a establecer en equipos, programas o sistemas de información, sino también sobre el mantenimiento del secreto de aquellas personas que operan con datos o que tengan acceso a los mismos «para poder prevenir el mal uso de los datos, o para evitar el desvío de la información, malintencionadamente o no, hacia sitios no previstos, así como para garantizar su integridad»[16].

Intentando dar respuesta a estos problemas el Título VIII del Reglamento regula a lo largo de cuatro capítulos las medidas de seguridad a adoptar. El primero de los mismos contiene una serie de disposiciones generales en materia de seguridad, ya sean ficheros automatizados o no automatizados. El Capítulo II se ocupa por completo de una cuestión tan específica y discutida como el documento de seguridad. El Capítulo III establece las medidas de seguridad aplicables a ficheros y tratamientos automatizados. Finalmente, el Capítulo IV regula las medidas de seguridad que han de respetar los ficheros y tratamientos no automatizados o manuales.

A lo largo del presente artículo se intenta analizar, siguiendo el propio esquema utilizado en el Reglamento, la normativa común a todo tipo de ficheros y las medidas de seguridad aplicables tanto a ficheros y tratamientos automatizados como a ficheros y tratamientos no automatizados.

3.1. Disposiciones comunes a todo tipo de ficheros

La primera previsión contenida en el Reglamento es la relativa al alcance de las medidas de seguridad contempladas en el Reglamento, que se circunscribe a los responsables de los ficheros o tratamientos y a los encar-

[16] M. Á. Dávara Rodríguez, *Manual..., op. cit.,* p. 83.

gados del tratamiento, con independencia de si los tratamientos son automatizados o manuales.

Se establece con carácter general la obligatoriedad de que todas y cada una de las limitaciones al acceso a los datos de carácter personal estén recogidas en el documento de seguridad, distinguiéndose entre las limitaciones al personal propio y al ajeno —teniéndose en cuenta en este segundo caso además si el encargado del tratamiento presta los servicios en los locales del responsable del fichero o tratamiento o en sus propios locales—.

También se ocupa el Reglamento de establecer algunas garantías mínimas en el caso de que los datos personales se almacenen en dispositivos portátiles o sean tratados fuera de los locales del responsable del fichero o tratamiento. En tales casos será preciso que haya una autorización previa del responsable del fichero o tratamiento[17] y que se respete el nivel de seguridad correspondiente al tipo de fichero tratado, tema al que paso a referirme a continuación.

3.1.1. *Los niveles de seguridad*

El Reglamento mantiene los tres niveles de seguridad referidos anteriormente —básico, medio y alto—[18], que tienen la condición de «mínimos exigibles»[19], por lo que una vez que un fichero cumpla el nivel de seguridad exigido reglamentariamente no hay impedimento alguno para que el responsable del fichero adopte un nivel de seguridad superior con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos[20]. Además, con el objeto de facilitar el cumplimiento de las previ-

---

[17] La autorización constará en el documento de seguridad y se establecerá para un usuario o para un perfil de usuarios, determinándose un periodo de validez para la misma, tal y como exige el art. 86.1 del Reglamento.

[18] Téngase en cuenta además que, según establece el art. 85 del Reglamento, «las medidas de seguridad exigibles a los accesos de datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local».

[19] Art. 81.7 del Reglamento.

[20] Como señala J. L. Cueva Calabia, «La LORTAD y la seguridad...», *op. cit.,* p. 7, mediante la *confidencialidad* un sistema seguro sólo permitirá el conocimiento de la información a aquellos usuarios que estén autorizados para ello; en virtud de la *integridad* un sistema seguro es aquel que impide que la información en él contenida o por él procesada pueda ser alterada de forma indebida, errónea o no autorizada, o que pueda perderse, y gracias a la *disponibilidad* la información y el sistema deben poder ser utilizados por los usuarios autorizados a ello en cualquier momento.

siones normativas en materia de seguridad cuando en un sistema de información[21] existan ficheros o tratamientos que en función de su finalidad, uso o de la naturaleza de los datos que contengan requieran la adopción de medidas de seguridad diferentes a las del sistema principal «podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos»[22].

En el caso de que existan ficheros temporales[23] o copias de documentos[24] —tanto informatizadas como manuales— que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares se exige, como no podía ser de otra manera, que los mismos sean destruidos totalmente una vez que dejen de ser necesarios para tal fin y que hasta ese momento cumplan el nivel de seguridad que les corresponda conforme a los criterios generales que a continuación se señalan.

A. El nivel básico de seguridad

Tendrán el nivel básico de seguridad todos los ficheros o tratamientos de datos de carácter personal que no estén obligados a tener un nivel de seguridad medio o alto, esto es, todos los ficheros o tratamientos deberán adoptar las medidas de nivel básico.

B. El nivel medio de seguridad

El art. 81.2 del Reglamento enumera una serie de ficheros o tratamientos que deben contar, además de con las medidas de seguridad de nivel básico, con las medidas de seguridad de nivel medio. Dichos ficheros o tratamientos son los siguientes:

---

[21] Se entiende por «sistema de información» el conjunto de ficheros, tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal.

[22] Posibilidad prevista en el art. 81.8 del Reglamento, que exige que tal circunstancia se haga constar en el documento de seguridad.

[23] Los «ficheros temporales» son, como señala el propio art. 5.2.*m)* del Reglamento, «aquellos ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento».

[24] La referencia expresa a las copias de documentos contenida en el art. 87 del Reglamento supone una ampliación del objeto de protección, puesto que la anterior normativa sólo hacía referencia a los ficheros temporales.

Los relativos a la comisión de infracciones administrativas o penales.

Teniendo en cuenta que el art. 7.5 de la LOPD establece que estos datos «sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras», parece razonable que el Reglamento entienda que es suficiente su mantenimiento en el nivel de seguridad medio y no los incluya en el nivel alto[25].

Cuestión distinta es el nivel de seguridad que debe exigirse a los libros de los Registros de la Propiedad, Mercantiles y de Bienes Muebles contenidos en soportes informáticos. Tradicionalmente, los libros de los Registros se llevaban en soporte papel, si bien en los últimos años se ha procedido —al menos en gran medida— a la informatización de todos los libros de los Registros[26]. Por ello resulta necesario plantearse qué nivel de seguridad ha de aplicarse a los ficheros registrales. Teniendo en cuenta que dichos ficheros pueden contener algunos datos relativos a la comisión de infracciones administrativas o penales resulta obligatorio aplicar el nivel medio de protección. No obstante, debido a la importancia real de los datos contenidos «sería conveniente ir al nivel máximo de seguridad disponible con la tecnología actualmente existente»[27].

Aquellos cuyo funcionamiento se rija por el art. 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

El art. 29 de la LOPD se ocupa de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito, estable-

---

[25] Véase, en este sentido, A. Téllez Aguilera, *Nuevas tecnologías..., op. cit.,* p. 140.

[26] Tras la reforma del año 2005 se ha dado una nueva redacción al art. 238 de la Ley Hipotecaria, insertando dos nuevos párrafos y estableciendo que «los libros de los Registros de la Propiedad, Mercantiles y de Bienes Muebles deberán llevarse por medios informáticos que permitan en todo momento el acceso telemático a su contenido. El Registro dispondrá de un sistema de sellado temporal que dejará constancia del momento en que el soporte papel se trasladó a soporte informático». El alcance de este precepto no resultaba claro, puesto que podía interpretarse como la obligación de llevanza simultánea de los libros del Registro en soporte papel e informático o bien como la opción por el soporte exclusivo informático. No obstante, los Registros han optado en la práctica por la primera interpretación, que parece la correcta teniendo en cuenta además «no sólo el sentido común, sino una interpretación sistemática de la Ley e, incluso, las enmiendas presentadas y las declaraciones parlamentarias habidas durante la tramitación», como señala E. Guichot, *Publicidad registral y derecho a la privacidad. Una necesaria conciliación,* Madrid, Colegio de Registradores de la Propiedad y Mercantiles de España, 2006, p. 99.

[27] E. Guichot, *Publicidad registral..., op. cit.,* p. 100.

ciendo que «sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento».

Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

Dicha previsión si bien no resulta una novedad presenta una redacción más clara que en la anterior normativa, que permitía dudar sobre el alcance de este tipo de ficheros[28], que —al igual que sucedía con *los relativos a la comisión de infracción administrativas o penales*— dada su titularidad pública parece justificado que no se hayan incluido dentro del nivel de seguridad alto.

Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

En este punto el Reglamento ha introducido la obligatoriedad de que se trate de una entidad financiera[29], si bien no hay ninguna precisión sobre lo que se debe entender por «servicios financieros», aunque parece conveniente dar una interpretación extensiva al término.

Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

Supone una verdadera novedad —posiblemente la única en este apartado— frente a la anterior normativa, que no contenía ninguna previsión en este sentido.

---

[28] El art. 4.2 del derogado Real Decreto 994/1999, de 11 de junio, contenía una mención excesivamente genérica, puesto que se refería a «los ficheros de la Hacienda Pública», lo que podía hacer pensar que se estuviesen incluyendo los ficheros de empresas que contuvieran datos de carácter personal relativos a la Hacienda Pública, como podían ser datos sobre las nóminas y retenciones de IRPF de sus trabajadores, aunque finalmente se interpretó que el nivel medio de seguridad sólo se exigiría cuando el responsable del fichero fuera una Administración Pública titular de competencias en materia tributaria.

[29] El art. 4.2 del derogado Real Decreto 994/1999, de 11 de junio, hacía referencia a «los ficheros que contengan datos de carácter personal relativos a servicios financieros».

Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Es otra de las «novedades» previstas en el Reglamento, si bien en este caso no se puede hablar de novedad en sentido estricto, puesto que los ficheros que contenían datos personales suficientes que permitieran obtener una evaluación de la personalidad del individuo debían adoptar algunas de las medidas de seguridad del nivel medio[30].

Mención aparte merece el reforzado régimen aplicable a *los ficheros o tratamientos de datos de tráfico y localización de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas*[31]. El Reglamento establece que en estos casos se aplicarán todas las medidas de seguridad del nivel básico y medio y además la medida de seguridad del nivel alto correspondiente al registro de accesos, contenida en el art. 103 del Reglamento.

C. El nivel alto de seguridad

Además de las medidas de seguridad de nivel básico y medio, las medidas de seguridad de nivel alto se aplicarán —como señala el art. 81.3 del Reglamento— en los siguientes ficheros o tratamientos de datos de carácter personal:

---

[30] El art. 4.4 del derogado Real Decreto 994/1999, de 11 de junio, establecía un nivel intermedio de protección para este tipo de ficheros, puesto que exigía además del nivel básico algunas medidas de seguridad del nivel medio, en concreto las que contenían los arts. 17 —auditoría—, 18 —identificación y autenticación—, 19 —control de acceso físico— y 20 —gestión de soportes—. Dicho nivel intermedio o combinado de protección ha sido suprimido en el vigente Reglamento, puesto que los «ficheros o tratamientos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos» deberán adoptar todas las medidas previstas en el nivel medio de seguridad.

[31] Los ficheros o tratamientos de estos datos se regirán además por su normativa específica, el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Los que se refieran a datos de ideología, afiliación sindical[32]*, religión, creencias, origen racial, salud*[33] *o vida sexual.*

No obstante, hay algunas excepciones a la regla general. La primera de las mismas se refiere a los ficheros y tratamientos de datos de ideología, afiliación sindical, religión creencias, origen racial, salud o vida sexual. En efecto, en dichos ficheros o tratamientos bastará adoptar las medidas de seguridad de nivel básico cuando «los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros» o cuando «se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad»[34]. La segunda excepción se refiere únicamente a los ficheros o tratamientos que contengan datos relativos a la salud, que podrán adoptar las medidas de seguridad del nivel básico, si bien limitándose exclusivamente —como señala el art. 81.6 del Reglamento— a los datos relativos «al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos».

Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas[35].

Aquellos que contengan datos derivados de actos de violencia de género.

Se configura como otra de las novedades introducida en el Reglamento, cuya justificación resulta comprensible, teniendo además en cuenta los avances que se están intentando llevar a cabo en esta materia.

---

[32] Resulta interesante recordar que el art. 4.3 del derogado Real Decreto 994/1999 no hacía ninguna referencia a los datos de afiliación sindical, máxime si se tiene en cuenta que el art. 7.2 LOPD los considera datos especialmente protegidos. Tan sólo una razón de orden cronológico de ambas disposiciones explicaba tal omisión, si bien la doctrina entendía que los ficheros que contuvieran datos de afiliación sindical debían adoptar el nivel de seguridad alto, teniendo en cuenta además la jurisprudencia del Tribunal Constitucional, que en la STC 94/1998, de 4 de mayo, equipara el dato de afiliación sindical al de la ideología, afirmando que se trata de un dato digno de especial protección. Véase, en este sentido, A. Téllez Aguilera, *Nuevas tecnologías..., op. cit.,* p. 146. También se mostraba favorable a la inclusión de los datos de afiliación sindical entre los que requerían medidas de seguridad de nivel alto, si bien encontraba obstáculos insalvables para solventar la cuestión por la vía interpretativa, E. Suñe Llinas, *Tratado de Derecho Informático..., op. cit.,* pp. 214 y 215.

[33] Respecto a los datos relativos a la salud, conviene tener en cuenta su normativa específica, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

[34] Art. 81.5 del Reglamento.

[35] Ya incluidos en el art. 4.3 del derogado Real Decreto 994/1999, de 11 de junio.

3.1.2. *El documento de seguridad*

El responsable del fichero o tratamiento elaborará el denominado *documento de seguridad,* que tendrá el carácter de documento interno de la organización y recogerá, como es lógico, las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. El documento de seguridad deberá mantenerse en todo momento actualizado[36] y será de obligado cumplimiento para el personal con acceso a los sistemas de información. Podrá ser único para todos los ficheros o tratamientos o individualizado para cada fichero o tratamiento. Incluso, podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado o atendiendo a otros criterios organizativos[37].

Este documento deberá contener, como mínimo, los siguientes aspectos:

— Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
— Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento.
— Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
— Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
— Procedimiento de notificación, gestión y respuesta ante las incidencias[38].
— Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados[39].

Añadiendo el Reglamento un nuevo extremo, no previsto en la anterior normativa, que debe contener el documento de seguridad[40]:

---

[36] El documento de seguridad será revisado siempre que se produzcan cambios relevantes que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

[37] Frente al debate existente sobre si era necesario tener un único documento de seguridad o un documento de seguridad por cada fichero o tratamiento o, incluso, un documento de seguridad por cada nivel de seguridad, el Reglamento admite múltiples posibilidades. Véase M. Á. Dávara Rodríguez, *Análisis del Real Decreto..., op. cit.,* p. 113.

[38] La «incidencia» se define en el Reglamento como «cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos».

[39] Este extremo ya figuraba en la anterior reglamentación de la materia, si bien ahora se indica que es exigible solamente a los ficheros y tratamientos automatizados.

[40] No obstante, el Proyecto de Real de Decreto, de fecha 10 de septiembre de 2007, pre-

— Las medidas que sean necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Cuando se trate de ficheros o tratamientos a los que les son aplicables las medidas de seguridad de nivel medio o alto, el documento de seguridad deberá contener dos extremos más: en primer término, *la identificación del responsable de seguridad;* y, en segundo lugar, *los controles periódicos que se deban realizar para verificar el cumplimiento de lo establecido en el documento de seguridad*.

3.2. Medidas de seguridad aplicables a ficheros y tratamientos automatizados

El capítulo III del Título VIII del Reglamento establece las medidas de seguridad que han de cumplir los ficheros y tratamientos automatizados y se divide en tres secciones, una para cada uno de los tres niveles de seguridad existentes.

3.2.1. *Medidas de seguridad de nivel básico*

Son los arts. 89 a 94 del Reglamento los que regulan el nivel de seguridad básico, estableciendo las exigencias que el mismo supone. Dichas exigencias —que paso a señalar a continuación, intentando destacar las que resultan novedosas— son las siguientes:

A) Funciones y obligaciones de los usuarios con acceso a los datos

Las funciones y obligaciones de cada uno de los usuarios[41] o perfiles de usuarios[42] con acceso a los datos personales y a los sistemas de infor-

---

veía otro extremo, ya que incluía en el art. 88 un apartado más —letra *h)*— referido a «las medidas de seguridad adoptadas respecto de los ficheros o tratamientos no automatizados», que finalmente fue suprimido en el Reglamento aprobado.

[41] El art. 5.2.*p)* del Reglamento define «usuario» como el «sujeto o proceso autorizado para acceder a datos o recursos», añadiendo que «tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuarios físico».

[42] Téngase en cuenta la novedad que supone no referirse únicamente al «usuario», sino

mación estarán —indica el Reglamento— claramente definidas en el documento de seguridad. Asimismo, en el mismo se establecerán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento. En cualquier caso, la finalidad perseguida es que todos los usuarios conozcan todas las normas de seguridad que afecten a su trabajo, así como las consecuencias derivadas de su incumplimiento.

B) Registro de incidencias

Se debe articular un procedimiento de notificación y gestión de las incidencias que tengan lugar, esto es, de aquellas anomalías que afecten o pudieran afectar a los datos de carácter personal. Dicho procedimiento contendrá necesariamente un registro en que se harán constar una serie de extremos: el tipo de incidencia, el momento en que se ha producido o detectado, la persona que notifica la incidencia y a quién le es comunicada la misma, los efectos derivados de la incidencia y —lo cual supone una novedad— las medidas correctoras aplicadas.

C) Control de acceso

Los usuarios sólo tendrán acceso a aquellos datos o recursos[43] que necesiten para desarrollar sus funciones. El responsable del fichero tendrá tres obligaciones básicas: en primer lugar, establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados; en segundo lugar, fijará los criterios conforme a los cuales el personal autorizado en el documento de seguridad podrá conceder, modificar o anular el acceso autorizado sobre los recursos; y, en tercer lugar, deberá encargarse de que exista una relación actualizada de usuarios y perfiles de usuario en la que se establezca los accesos autorizados para cada uno de ellos. Resulta novedosa la equiparación en materia de seguri-

a un «perfil de usuario», esto es, «accesos autorizados a un grupo de usuarios», puesto que en la práctica los responsables de los ficheros o los tratamientos y, en su caso, los encargados del tratamiento no identifican al usuario con una persona física concreta, sino con aquellas personas que desempeñan las funciones propias de un puesto o de determinadas responsabilidades laborales.

[43] Por «recurso» entiende el Reglamento «cualquier parte componente de un sistema de información».

dad entre el personal ajeno al responsable del fichero que tenga acceso a los recursos —en el caso de que existiera— y el personal propio[44].

D) Gestión de soportes y documentos

Se establece con carácter general la obligación —siempre que sea posible—[45] de que los soportes y documentos[46] que contengan datos personales permitan identificar el tipo de información que contienen[47] y ser inventariados. A dichos soportes y documentos sólo podrá acceder el personal autorizado en el documento de seguridad[48].

El Reglamento introduce algunas reglas con el objeto de que los soportes y documentos informáticos que contengan datos de carácter personal no sean sustraídos, perdidos o accedidos de forma indebida siempre que los mismos salgan de los locales habilitados a tal fin[49]. En este sentido, se exige para la salida de soportes y documentos informáticos que sea autorizada por el responsable del fichero, a no ser que dicha salida se encontrase debidamente autorizada en el documento de seguridad. También hay algu-

---

[44] El apartado 5 del art. 91 del Reglamento señala que todo el personal «deberá estar sometido a las mismas condiciones y obligaciones de seguridad».

[45] Será posible siempre que las características físicas del soporte no imposibiliten el cumplimiento de esta obligación, dejando en ese caso —como dice el art. 92.1— «constancia motivada de ello en el documento de seguridad».

[46] El Reglamento se refiere expresamente a la gestión de documentos y no sólo a la gestión de soportes, entendiendo por «documento» —como señala el art. 5.2.*f)*— «todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada», y por «soporte» —como dice el art. 5.2.*ñ)*— el «objeto físico que almacena o contiene datos o documentos u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos».

[47] La identificación de los soportes que contengan datos especialmente sensibles «se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permita» a los usuarios autorizados identificar su contenido, dificultándose así su identificación para las demás personas.

[48] Se elimina la obligatoriedad de almacenar los soportes informáticos en un lugar con acceso restringido al personal autorizado, pero los soportes y documentos sólo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

[49] En mi opinión la posibilidad de salida de soportes y documentos que contengan datos de carácter personal mediante correo electrónico o como archivos adjuntos al correo electrónico —expresamente prevista en el Reglamento— puede plantear en ocasiones algunos problemas técnicos a la hora de garantizar la seguridad de los datos. Por tanto, resulta conveniente que se adopten las medidas de seguridad necesarias y suficientes que garanticen totalmente, mediante el cifrado de los soportes y documentos u otras técnicas, que no se produzcan accesos indebidos.

na previsión específica en materia de seguridad para el caso de destrucción o borrado de datos personales contenidos en soportes, de forma que sea imposible su recuperación posterior.

E) Identificación y autenticación

El responsable del fichero o tratamiento es a quien corresponde adoptar las medidas que garanticen la correcta identificación[50] y autenticación[51] de los usuarios, algo que requerirá el establecimiento de un mecanismo que permita la identificación inequívoca y personalizada de los usuarios que intenten acceder al sistema y la comprobación de que dicho usuario está autorizado. Uno de los mecanismos más usados en la práctica es la utilización de una contraseña[52].

Las contraseñas tienen que cumplir una serie de requisitos. En primer lugar, deben ser confidenciales e íntegras, para lo cual se arbitrará un procedimiento de asignación, distribución y almacenamiento de contraseñas[53]. En segundo término, se cambiarán con la periodicidad que se determine en el documento de seguridad, que en ningún caso —y esta previsión constituye una novedad— será superior a un año.

F) Copias de respaldo y recuperación

La anterior normativa exigía, de forma genérica, que el responsable del fichero fuera el encargado de verificar la definición y la correcta aplicación de los procedimientos de realización de copias de respaldo[54] y de recuperación de los datos. El Reglamento mantiene dicha obligación y establece que dicha verificación se llevará a cabo cada seis meses.

---

[50] Por «identificación» entiende el Reglamento el «procedimiento de reconocimiento de la identidad de un usuario».

[51] La «autenticación» es, según se define en el Reglamento, el «procedimiento de comprobación de la identidad de un usuario».

[52] La definición de «contraseña» contenida en el art. 5.2.*c)* del Reglamento es la siguiente: «información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso».

[53] Mientras la contraseña esté vigente se almacenará encriptada, esto es, de «forma ininteligible», como precisa el último apartado del art. 94 del Reglamento.

[54] El actual Reglamento se refiere literalmente a «verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo», que son las copias «de los datos de un fichero automatizado en un soporte que posibilite su recuperación», según señala su art. 5.2.*e)*.

Se mantienen prácticamente inalteradas dos de las previsiones contenidas en la anterior reglamentación: por un lado, se deberán realizar copias de respaldo, al menos semanalmente, salvo que no se hubiera producido ninguna actualización de los datos; por otro, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, si bien el segundo apartado del art. 94.1 añade que «en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados», siempre que la existencia de documentación permita la reconstrucción, «se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad».

Se introduce «una nueva regla» en orden a la realización de pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos personales, no permitiéndose que dichas pruebas se lleven a cabo con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote la realización de la prueba en el documento de seguridad. No obstante, si está previsto efectuar pruebas con datos reales se deberá realizar, como es lógico, una copia de seguridad con carácter previo. En realidad, aunque he señalado que se trataba de una «novedad», dicha regla se encontraba ya contenida en el viejo Reglamento, pero ubicaba dentro del capítulo dedicado a las medidas de seguridad de nivel medio. Pese a ello, algún autor entendía —de forma acertada en mi opinión— que dada la dicción del precepto, cuya «prohibición cede ante la adopción de las medidas de seguridad correspondientes al tipo de fichero en cuestión, se trata de una medida de seguridad referida a todo tipo de ficheros que contienen datos personales y, por tanto, incluida dentro del nivel básico»[55]. En cualquier caso —y debido a su ubicación actual— con el nuevo Reglamento ya no hace falta interpretar que se trata de una medida de seguridad de nivel básico.

3.2.2. *Medidas de seguridad de nivel medio*

En el caso de ficheros o tratamientos que exigen un nivel de seguridad medio se deberán adoptar, además de lo dispuesto y ya visto para el nivel básico, las siguientes medidas de seguridad:

---

[55] A. Téllez Aguilera, *Nuevas tecnologías.., op. cit.,* p. 139.

A) Responsable de seguridad

La figura del responsable de seguridad no es una novedad y en ningún caso su existencia supone una exoneración de la responsabilidad del responsable del fichero o del encargado del tratamiento. Las funciones del responsable de seguridad, que debe ser una persona física[56], son las de coordinar y controlar las medidas de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados.

B) Auditoría

Se mantiene la exigencia de llevar a cabo una auditoría interna o externa, al menos cada dos años, sobre los sistemas de información e instalaciones de tratamiento y almacenamiento de datos. Se introduce la obligación de realizar una auditoría extraordinaria[57], siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad adoptadas para verificar la adaptación, adecuación y eficacia de las mismas.

El informe de la auditoría deberá contener los siguientes extremos: en primer lugar, dictaminar la adecuación de las medidas de seguridad a la normativa vigente; en segundo término, identificar las deficiencias y proponer las medidas correctoras o complementarias necesarias; y, finalmente, incluir los datos, hechos y observaciones en que se basen los dictámenes

[56] Parece lógico entender que el responsable de seguridad no pueda ser una persona jurídica, puesto que el Reglamento —igual sucedía en la anterior reglamentación— configura al responsable de seguridad como una función o puesto de trabajo, a efectos de facilitar el cumplimiento de las medidas de seguridad mediante la exigencia de que exista una persona que se responsabilice dentro de la empresa de la aplicación, coordinación, control y seguimiento de las medidas de seguridad. No obstante, no parece necesario que el responsable de seguridad sea un empleado del responsable del tratamiento, por lo que lo podría ser un tercero contratado para tales fines. Véase J. APARICIO SALOM y J. FERNÁNDEZ-SAMANIEGO, «Reglamento de medidas de seguridad. Preguntas y respuestas», en *Nueva Ley de Protección de Datos de Carácter Personal y reglamento de medidas de seguridad informática,* Madrid, 2000, p. 49.

[57] La auditoría extraordinaria iniciará el cómputo del plazo de dos años previsto con carácter general.

alcanzados y las recomendaciones propuestas. El responsable de seguridad analizará el informe[58] y elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas pertinentes.

C) Gestión de soportes y documentos

Deberá establecerse un sistema de registro de entrada de soportes y un sistema de registro de salida que permitan conocer el tipo de documento o soporte, la fecha y hora, el emisor o el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción o la entrega.

D) Identificación y autenticación

En el caso de ficheros o tratamientos automatizados que requieran el nivel medio de protección el responsable del fichero o tratamiento establecerá —como señala de forma escueta el art. 98 del Reglamento— «un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información».

E) Control de acceso físico

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se encuentren instalados los equipos físicos que den soporte a los sistemas de información. Dicha medida es, a mi juicio, un tanto desproporcionada y en algunos casos de muy difícil y costosa aplicación práctica, puesto que se exige una separación física de los equipos que dan soporte a los sistemas de información con un control de acceso a los usuarios autorizados, no estando permitido que los equipos estén ubicados en zonas comunes a las que tengan acceso otras personas[59].

---

[58] El informe quedará —como señala el art. 96.3— «a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas».

[59] En idéntica línea, A. Téllez Aguilera, *Nuevas tecnologías..., op. cit.,* p. 145, apunta

F) Registro de incidencias

En el Registro de incidencias, además de lo previsto para el nivel básico, deberán consignarse también los procedimientos realizados de recuperación de los datos de carácter personal, reflejando la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación. Para la ejecución de los procedimientos de recuperación de los datos será necesaria la autorización del responsable del fichero, aunque ya no se exige que la autorización sea escrita.

3.2.3. *Medidas de seguridad de nivel alto*

Todos los ficheros o tratamientos de datos de carácter personal que requieren la adopción de medidas de seguridad de nivel alto deberán cumplir, además de las medidas de seguridad de tipo básico y medio a las que me he referido en las líneas precedentes, los siguientes extremos:

A) Gestión y distribución de soportes

El Reglamento presenta como novedad importante la obligación de identificación de los soportes que contengan datos de carácter personal mediante sistemas de etiquetado que permitan a los usuarios con acceso autorizado identificar su contenido y que dificulten la identificación para cualquier otra persona no autorizada.

Si fuera necesario distribuir estos soportes se hará cifrando los datos de carácter personal o utilizando otro mecanismo que garantice que la información no sea accesible o manipulada durante su transporte. Igualmente, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero[60].

---

las dificultades prácticas que planteaba la anterior normativa, que exigía que exclusivamente el personal autorizado en el documento de seguridad pudiera tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

[60] No obstante, se evitará —en la medida en que sea posible— el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. Y para el caso de

B) Copias de respaldo y recuperación

Se mantiene la obligación de conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en el que se encuentren los equipos informáticos que los tratan, cumpliendo en todo caso las medidas de seguridad contenidas en el Reglamento y quedando garantizada la integridad de la información de manera que sea posible su recuperación.

C) Registro de accesos

Se creará un registro de accesos en el que «de cada intento de acceso»[61] se guardarán, como mínimo, la identificación del usuario, la fecha y hora, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado[62]. El periodo mínimo de conservación de los datos registrados se mantiene invariable en dos años[63].

El responsable de seguridad tendrá una doble función: por un lado, controlará los mecanismos que permiten el registro de accesos y evitará la desactivación o manipulación de los mismos; y, por otro, revisará al menos una vez al mes la información registrada y elaborará un informe.

D) Telecomunicaciones

Añade el Reglamento, como última novedad significativa, que la transmisión de datos de carácter personal que requieran un nivel alto de protección se realizará cifrando dichos datos o bien utilizando cualquier otro mecanis-

---

que fuera estrictamente necesario «se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos», como señala el apartado 3 del art. 101 del Reglamento.

[61] Téngase en cuenta que ya no se habla de «cada acceso», sino de «cada intento de acceso», lo cual me parece mucho más correcto.

[62] Se exceptúa la obligatoriedad de establecer un Registro de accesos cuando el responsable del fichero o del tratamiento sea una persona física y garantice que sólo él tiene acceso y trata los datos de carácter personal, circunstancia que se hará constar en el documento de seguridad. Y es que en este caso, lógicamente, no tiene mucho sentido mantener la exigencia.

[63] Periodo algo largo que puede ocasionar, a mi juicio, ciertas dificultades de aplicación práctica.

mo que garantice que la información no sea inteligible ni manipulada por terceras personas, ya sea a través de redes públicas —exigencia ya contemplada— o por redes inalámbricas de comunicaciones electrónicas.

3.3. Medidas de seguridad aplicables a ficheros y tratamientos no automatizados

El Capítulo IV del Título VIII del Reglamento establece por primera vez medidas de seguridad aplicables a los tratamientos y ficheros manuales, lo cual supone una novedad frente a la anterior normativa, que se refería exclusivamente a medidas de seguridad en ficheros automatizados. Las medidas de seguridad exigibles a ficheros y tratamientos no automatizados se clasifican también en tres niveles.

3.3.1. *Medidas de seguridad de nivel básico*

A los ficheros y tratamientos no automatizados les serán de aplicación las mismas previsiones que a los ficheros y tratamientos automatizados en lo relativo a alcance, niveles de seguridad, encargado del tratamiento, prestaciones de servicios sin acceso a datos personales, delegación de autorizaciones, régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento, copias de trabajo de documentos y documento de seguridad. Además, los ficheros y tratamientos no automatizados que exigen un nivel básico de seguridad deberán cumplir las medidas de seguridad de nivel básico enumeradas a lo largo de las precedentes páginas para ficheros y tratamientos automatizados en lo referente a funciones y obligaciones del personal, registro de incidencias, control de acceso y gestión de soportes[64].

[64] Por tanto, sólo se excluyen en el nivel básico de seguridad de los ficheros manuales las medidas de seguridad de nivel básico previstas para los ficheros y tratamientos automatizados en materia de identificación y autenticación —art. 93— y copias de respaldo y recuperación —art. 94—. Dicha exclusión parece natural, puesto que —como señala M. Á. Dávara Rodríguez, *Análisis del Real Decreto..., op. cit.,* p. 128— «difícil resultaría aplicar la identificación y autenticación similar a la informatizada en un procedimiento manual para el acceso de documentos, aunque no podemos descartar, y así habrá que hacerlo, la identificación y autenticación manual para acceso a los documentos no automatizados. Lo mismo se podría decir sobre las copias de respaldo y recuperación que, en un soporte manual, parece no tener mayor sentido debido a la dificultad de realización».

Otras medidas de seguridad de nivel básico aplicables a los ficheros y tratamientos no automatizados son las relativas a criterios de archivo, dispositivos de almacenamiento y custodia de los soportes, de las que paso a dar cuenta a continuación.

El archivo de soportes y documentos se llevará a cabo teniendo en cuenta los criterios previstos en su respectiva normativa. Solamente en el que caso de que no existiera, será el responsable del fichero el encargado de fijar los criterios y procedimientos de actuación a seguir para el archivo[65].

Los armarios, archivadores, cajones o cualquier otro dispositivo de almacenamiento de los documentos que contengan datos personales deberán disponer de determinados mecanismos que impidan su apertura[66]. Siempre que los documentos no estén archivados en los dispositivos de almacenamiento, por estar siendo utilizados en un proceso de revisión o tramitación, la persona que esté a cargo de la misma deberá custodiarlos, evitando su acceso por persona no autorizada.

3.3.2. *Medidas de seguridad de nivel medio*

Además de las medidas de seguridad de nivel básico, los ficheros y tratamientos no automatizados que requieran un nivel medio de protección deberán cumplir dos exigencias más: en primer lugar, se designará uno o varios responsables de seguridad con las mismas funciones previstas que en el caso de ficheros y tratamientos automatizados; y, en segundo término, los ficheros se someterán a una auditoría interna o externa, al menos cada dos años[67].

---

[65] En cualquier caso se deberá «garantizar la correcta conservación de los documentos, la localización y consulta de la información, y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación», según señala el art. 106 del Reglamento.

[66] El responsable del fichero manual adoptará medidas que impidan el acceso de personas no autorizadas si las características físicas de los dispositivos de almacenamiento no permitan adoptar esta medida.

[67] Parece lógico que, dado el carácter no automatizado o manual de los ficheros y tratamientos, el nivel medio de seguridad no establezca tantas exigencias en orden a la gestión de soportes y documentos, identificación y autenticación, control de acceso físico o registro de incidencias, como exigía el nivel medio de seguridad para los ficheros y tratamientos automatizados.

3.3.3. *Medidas de seguridad de nivel alto*

Finalmente, los arts. 111 a 114 del Reglamento contienen algunas exigencias más en el caso de los ficheros no automatizados que requieren un nivel alto de seguridad, relativas al almacenamiento de la información, la generación de copias o reproducción de los documentos y al acceso y traslado de la documentación.

Los armarios, archivadores y demás dispositivos de almacenamiento de los ficheros deberán encontrarse en áreas de acceso protegido mediante puertas con sistema de apertura mediante llave o dispositivo equivalente. Dichas áreas deberán permanecer cerradas, siempre que no se necesite acceder a los ficheros manuales[68].

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad[69], debiendo procederse a la destrucción de las copias o reproducciones desechadas de forma que no sea posible su recuperación posterior.

En materia de acceso y traslado de documentación el Reglamento es, en mi opinión, demasiado genérico e impreciso. En primer lugar, se señala que «el acceso a la documentación se limitará exclusivamente al personal autorizado» y que «se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios». Por tanto, parece deducirse que en el caso de documentos que sólo puedan ser utilizados por un único usuario no hará falta identificar los accesos realizados. Algo poco razonable, puesto que al tratarse del nivel alto de seguridad resultaría adecuado arbitrar mecanismos que, aun en el caso de ser un único usuario el autorizado en el documento de seguridad, impidieran un acceso injustificado a los datos de

---

[68] No obstante, se faculta al responsable del fichero o tratamiento para adoptar medidas alternativas que deberán constar, debidamente motivadas, en el documento de seguridad para aquellos casos en los que las características de los locales imposibilitaran la existencia de áreas de acceso protegido. Algo que, a mi juicio, resulta razonable, puesto que, aunque la calidad y calificación de los datos tratados sean iguales, no pueden exigirse las mismas medidas, en orden a tener áreas especialmente protegidas, a un médico que dispone de una pequeña consulta privada en su domicilio que a un facultativo que tiene su consulta en un gran hospital.

[69] Nótese que el Reglamento no obliga a realizar copias de respaldo o de seguridad, sino que establece una exigencia para el caso de que se realizaran, como acertadamente ha puesto de relieve M. Á. Dávara Rodríguez, *Análisis del Real Decreto..., op. cit.,* p. 130.

carácter personal contenidos en los ficheros manuales. En segundo término, se establece que si tuvieran que acceder a los documentos otras personas deberá quedar registrado el acceso en la forma establecida al efecto en el documento de seguridad[70].

Finalmente —y también, en mi opinión, de forma excesivamente genérica— se establece la necesidad de adoptar medidas encaminadas a impedir el acceso o manipulación de la información en el caso de que se produzca un traslado físico de la documentación, aunque sin arbitrar ninguna medida concreta. Y es que no resulta tarea fácil, puesto que la mayor parte de las medidas en las que pueda pensar el lector de las presentes líneas —que espero, no obstante, hayan servido para clarificar algo la materia— más que impedir la manipulación de la información permiten tan sólo ver si ésta se ha producido[71].

[70] El art. 113.3 del Reglamento no precisa los extremos sobre los que debe quedar constancia, dejando plena libertad para que el documento de seguridad establezca el procedimiento.

[71] Véase, en esta misma línea, M. Á. DÁVARA RODRÍGUEZ, *Análisis del Real Decreto..., op. cit.,* p. 132, que considera, en cualquier caso, una buena medida «redactar una leyenda de responsabilidad y confidencialidad sobre esta materia, en la que se instruyese al que transporta la documentación».