

## ***Medidas de seguridad.***

### **Aplicación de las medidas de seguridad a los ficheros y tratamientos de datos personales. Especial atención al Reglamento de Medidas de Seguridad**

Ricard Martínez Martínez

1. Una aproximación extrajurídica a la seguridad. 1.1 El estado de la técnica. 1.2. Usuarios reticentes: el deber de secreto. 1.3 costes y mitos? 1. 3. Los costes de la seguridad. 2. Seguridad ¿Por qué? 3. Las medidas de seguridad. 3.1 Niveles de seguridad. 3.2 Algunas novedades significativas. 3.2.a) Exenciones en los niveles de seguridad. 3.2.b) Ficheros segregados. 3.2.c) Prestaciones de servicios 3.2.d) Organización del personal 3.2.e) Redes de comunicaciones. 3.2.f) Dispositivos portátiles. 3.3 Esquema de medidas de seguridad. 3.3.a). El alcance de la seguridad. 3.3.b) La importancia estratégica del documento de seguridad. 3.3.b) Algunos conceptos complicados. 3.3 c) La formación de los usuarios. 3.3d) El responsable de seguridad. 3.3.e) Algunas políticas de seguridad. 3.3.f) La seguridad en ficheros no automatizados. 4. El diseño de la seguridad: la auditoria. 5. Consideraciones finales.

#### ***1. Una aproximación extrajurídica a la seguridad.***

La aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) ofrece al jurista una oportunidad única de lo que podríamos definir como una aproximación “problemática” a la aplicación del Derecho<sup>1</sup>.

En protección de datos el operador jurídico, sea o no profesional del Derecho, se enfrenta a la necesidad de conocer los hechos con todo detalle, de identificar el origen de los datos, el uso que se hace de ellos, las personas o departamentos que tratan los datos, los eventuales destinatarios de la información... En una palabra, no puede aplicarse la norma sin esquematizar previamente el flujo de datos y contar con un mapa de la realidad lo más fidedigno posible. Si se permite la exageración, aquí no

---

<sup>1</sup> De hecho, la aplicación de las normas sobre protección de datos se vive en la práctica como algo que «presenta dificultades o que causa problemas». Sin embargo, nada más alejado de lo que se pretende transmitir con la primera afirmación. Se emplea aquí el término problema en el sentido que le atribuye la RAE como «planteamiento de una situación cuya respuesta desconocida debe obtenerse a través de métodos científicos». Ciertamente, se está muy lejos de afirmar que el método de interpretación y aplicación del Derecho sea exactamente el mismo que el empleado por las ciencias empíricas y no se trata aquí de reproducir aquí el eterno debate sobre la existencia de una “Ciencia del Derecho”.

sirve la vieja, y a veces mal entendida, técnica de la subsunción cuando esta se concibe como pura aplicación mecánica de la norma forzando, si hace falta, la realidad de los hechos. Aquí resulta indispensable tener un cabal entendimiento de la realidad material sobre la que se aplica la LOPD y, a la par, un profundo conocimiento del sector jurídico sobre el que se aplica la Ley debido al carácter instrumental y/o transversal del derecho fundamental a la protección de datos.

Esta afirmación adquiere mayor valor, si cabe, cuando se refiere a la aplicación de las medidas de seguridad previstas por 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 adelante RDLOPD.

### **1.1 El estado de la técnica.**

La primera apreciación a la que se enfrentará cualquier profesional que opere con la aplicación de las normas sobre protección de datos ante los problemas de seguridad podría resumirse con una sola palabra: “imposible”. Como más adelante se examinará la primera percepción que se tiene del RDLOPD, como por otra parte ocurre con la propia Ley Orgánica, es una sensación de impotencia. El responsable percibe la seguridad como un conjunto de obligaciones leoninas, exageradas e inalcanzables.

Nada más lejos de la realidad. Según la Ley de Moore el número de transistores en un chip se duplica cada 18 meses y con ello la capacidad de los sistemas para tratar y almacenar información con un mantenimiento prácticamente constante de los costes de producción y adquisición. En este sentido, cualquier usuario de productos informáticos puede constatar que las generaciones de ordenadores se suceden a un ritmo de 9 a 12 meses.

Esta evolución tecnológica debe ser entendida desde una doble perspectiva:

- El aumento de la velocidad y capacidad de proceso, el cada vez mayor espacio para el almacenamiento de información y las prestaciones que nos ofrece la “Galaxia Internet” incrementan el uso de las tecnologías de la información y las comunicaciones y, paralelamente, los riesgos que comportan.
- Ahora bien, los cambios no se producen únicamente en el plano del hardware. También evoluciona el software tanto en los sistemas operativos como en el conjunto de aplicaciones y gestores de bases de datos relacionados con los tratamientos. Y otro tanto sucede con programas complementarios como antivirus, cortafuegos, gestores de correo electrónico o detectores de spyware y/o malware.

Por tanto, en muchas ocasiones los problemas no derivarán tanto de la propia naturaleza del tratamiento como del estado de actualización de los equipos y del software que los trata. Aquí se constata ciertamente un problema cultural de naturaleza extrajurídica. ¿Realmente es consciente el responsable del fichero de la importancia que para su negocio posee una adecuada inversión en hardware y software? Con independencia de la respuesta a esta pregunta, más propia de un estudio sociológico que jurídico, lo cierto es que la mayor parte de exigencias vinculadas a la seguridad resultan resolubles con la mayor parte de productos existentes en el mercado y con la aplicación del más elemental sentido común.

## **1.2. Usuarios reticentes: el deber de secreto.**

El siguiente elemento a considerar en esta aproximación no jurídica a la seguridad tiene mucho que ver con la percepción subjetiva del usuario que vendrá obligado a velar por la seguridad, a diseñar la misma o, simplemente a cumplir con ciertas reglas básicas de conducta.

En este sentido, el usuario concibe el RDLOPD como una obligación adicional “excesiva”: Así, desde el responsable del fichero, pasando por los profesionales de la informática al último usuario del sistema viven la seguridad como una pesada carga. Generalmente, debe tenerse en cuenta que no se interiorizan los beneficios que la aplicación de las medidas de seguridad proporciona. No se percibe la seguridad como un conjunto de actuaciones que tenderán a mejorar las condiciones del trabajo, la calidad de la información y, sobre todo, no se alcanza a comprender que la implementación de medidas de seguridad creará un contexto en el que sea posible atribuir la responsabilidad de modo individual.

Sin, embargo desde el punto de vista del usuario de los sistemas de información resulta evidente que la obligación de garantizar la seguridad en la medida en que tiene por objeto garantizar el deber de confidencialidad no es sino una de las manifestaciones del deber de secreto del artículo 10 LOPD. Como es conocido éste dispone:

«Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

El deber de secreto no es otra cosa que una manifestación específica y reforzada del secreto profesional que incumbe al personal de cualquier

organización respecto de la información a la que accede. En tal sentido, en la mayor parte de profesiones existe este deber, si bien en algunas se acentúa habida cuenta del ejercicio de funciones públicas, del acceso a información médica<sup>2</sup> o sanitaria, e incluso de la prestación de servicios de naturaleza religiosa. Aquí, sin embargo, este deber de secreto se acentúa por cuanto su papel se ordena a la protección de un derecho fundamental. Este hecho, la protección de la información personal objeto de tratamiento, justifica por sí sólo que cualquier usuario que mantenga relación con un fichero o tratamiento venga vinculado por el deber de secreto.

Se trata, por tanto, de un deber que se proyecta respecto de todos los que intervengan en cualquier fase del tratamiento. Ello incluye, a todo el personal que materialmente acceda a las aplicaciones o a los resultados derivados de su funcionamiento, e incluso a aquellos que no accedan directamente a la base de datos pero sí materialmente a las explotaciones de datos que a partir de éstas se obtengan.

Por último, una interpretación integrada del deber de secreto con el principio de seguridad induce a considerar que el deber de secreto alcanza a cualquier información cuyo conocimiento por terceros pudiera poner en riesgo el sistema de información. En este sentido, la revelación de un usuario y una contraseña que permita acceder a una aplicación que trata datos no sólo infringiría la seguridad sino también el deber de secreto. Es más, suele existir personal informático cuya tarea no comporta el acceso a

---

<sup>2</sup> Existen profesionales, como los sanitarios, para los que la satisfacción del deber de secreto resulta particularmente exigente. Véase 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. Esta norma y alguno de sus desarrollos autonómicos contienen criterios respecto del tratamiento informático de la información clínica.

datos personales pero la revelación de cuyos conocimientos podría poner en peligro la información contenida en un sistema de información<sup>3</sup>.

Del mismo modo, existen usuarios que no acceden al recurso informático pero acceden a datos personales y vienen vinculados por el deber de secreto. Piénsese a título de ejemplo en aquellos casos en los que un informe, un etiquetado, o una explotación de datos para ser sometida a un análisis concreto no es protegida o simplemente puesta a disposición de terceros.

Aún así, el artículo 10 LOPD debe entenderse como un reforzamiento específico del deber de secreto más que como una obligación añadida. En tal sentido, el natural entendimiento de los principios de buena fe y de diligencia profesional comporta de suyo el que cualquier sujeto que tenga algún tipo de relación con datos de carácter personal venga obligado por este deber. En cualquier caso, la particular naturaleza del derecho fundamental a la protección de datos obligaba de algún modo a contemplar dicho deber expresamente.

En otro orden de cosas, y por último, debe destacarse que no siempre existe una conciencia en los responsables de alto nivel sobre la prioridad de las necesidades derivadas de la aplicación del RDLOPD. Y, desde una perspectiva centrada en la realidad práctica resulta fundamental obtener su implicación. Como posteriormente se analiza, resulta esencial que la dirección de una organización sea plenamente consciente de los beneficios que incorpora un compromiso con la seguridad.

Por otra parte, existe un conjunto de valores cuya interiorización resulta estratégica por parte de todos y cada uno de los usuarios relacionados con un sistema de información:

---

<sup>3</sup> Véanse las resoluciones que se adjuntan en los materiales.

- La información y los sistemas que la soportan constituyen activos valiosos e importantes para la Organización. Por tanto, el normal desenvolvimiento de las tareas depende de la seguridad tanto como de otros factores.
- La seguridad permite depositar la suficiente confianza sobre la capacidad de la información y de los sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la organización.
- La seguridad proporciona confianza tanto interna, para los propios gestores, como externa para el cliente o administrado.
- La seguridad es presupuesto para la eficiencia en el manejo de la información y, lógicamente, para la de los procesos decisorios basados en la información personal y en el uso de las tecnologías de la información y las comunicaciones.
- No existe ningún proceso vinculado a la búsqueda de calidad y excelencia que no requiera un adecuado cumplimiento de la LOPD y el RDLOPD.
- La seguridad constituye un presupuesto más para la garantía del derecho fundamental a la protección de datos.

Transmitir este conjunto de valores y hacerlo de un modo positivo puede resultar esencial para una adecuada implementación del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

### **1. 3. Los costes de la seguridad.**

Otro de los elementos disuasorios para una adecuada implementación de la seguridad reside en que las organizaciones,

especialmente en el entorno de las PYMES, conciben la seguridad como algo extraordinariamente costoso. Y ello se debe a diversas razones que no siempre les son imputables.

En primer lugar, existe un desconocimiento absoluto de las propias medidas de seguridad de modo que únicamente se viene a saber que es algo que debe hacerse, que es obligatorio y que pueden imponerse graves sanciones si no se cumple. Sin embargo, en la mayoría de los casos las medidas del RDLOPD responden al sentido común y a la más elemental traslación de las conductas de seguridad del mundo físico al virtual.

No es ajena a esta realidad la existencia de prácticas profesionales caracterizadas por trasladar al usuario una jerga absolutamente incomprensible con el objetivo de “colocar” un determinado servicio. Ciertamente, se trata de prácticas que en términos porcentuales son mínimas. Sin embargo, cualquier conocedor del mundo de la protección de datos sabe que la prestación de servicios cuando se basa en mantener al responsable del fichero en la ignorancia o en el puro miedo a la sanción sin ningún valor añadido, o en la pura dependencia del consultor. Esto sin contar los casos en los que con su labor no inyectan cultura LOPD en la organización o cuando se basan en un mantenimiento “ficticio” de un documento de seguridad acaban por generar un profundo rechazo.

Por otra parte, en muchas ocasiones el responsable del fichero no ha invertido en software para el tratamiento y acude a programas muy básicos que no siempre reúnen las especificaciones de seguridad que corresponden al nivel del fichero. Así, difícilmente podrá gestionarse desde el punto de vista del RDLOPD un fichero que contenga datos de salud si no se adquiere software específico. En otras ocasiones, cada vez menos, son los propios responsables del diseño y comercialización del

software quienes no lo han implementado convenientemente. De ahí que el responsable del fichero también considere entre los costes que deberá soportar los propios de la adquisición de nuevos programas.

Sin embargo el responsable no tiene en cuenta los aspectos positivos de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y del RDLOPD. Por ello, en seguridad resulta altamente conveniente explicitar los valores positivos con la finalidad de obtener una implicación de la organización. En este sentido la implementación de las medidas de seguridad:

- Proporciona un conocimiento cabal de los riesgos y vulnerabilidades y también, en muchas ocasiones permite identificar los modos en los que se tratan los datos, suprimir tratamientos innecesarios o centralizar aquellos que lo requieran. Esto puede traducirse en un incremento de la eficiencia y de la productividad e incluso en un ahorro en costes de personal, en entornos corporativos de gran tamaño cuando se localizan cuellos de botella en la gestión de la información.
- Contribuye a garantizar la corrección de las decisiones de la organización ya que se basan en información confiable y no manipulada.
- Ofrece confianza al titular de los datos: su perfil informativo será el adecuado y no variará arbitrariamente.
- Garantiza el funcionamiento normal de la organización.
- Permite restaurar los sistemas ante cualquier evento imprevisto y facilita la respuesta en todos los casos incluso ante las catástrofes.

En la práctica la seguridad afecta a todas las formas de información y sus soportes así como a cualquier método usado para transmitir conocimiento, datos e ideas. Debe tenerse en cuenta que tanto la información y los sistemas que la soportan constituyen activos valiosos e importantes para la Organización. La implementación de medidas de seguridad permite depositar la suficiente confianza sobre la capacidad de dicha información y de los sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la Organización. Por lo tanto, resulta evidente que la aplicación del RDLOPD no sólo puede concebirse desde una perspectiva de costes ya que se trata de algo valioso en si mismo.

## **2. Seguridad ¿Por qué?**

En todo lo expresado hasta aquí subyace el título que da lugar a este epígrafe. En realidad este tipo de pregunta se plantea sobre el conjunto de las cuestiones relacionadas con la protección de datos. Constantemente los medios de comunicación constatan el bajo nivel de aplicación de la LOPD en términos porcentuales. Por más que las cifras que se proporcionan puedan alejarse de la realidad, lo cierto es que cualquier operador jurídico que desarrolle su tarea en este ámbito constata día a día el bajo nivel de sensibilidad de los responsables de los ficheros.

Todo ello obliga a una labor pedagógica que explique al responsable el porqué de la LOPD y, en lo que atañe a este módulo, el porqué de la seguridad. Y la respuesta a este interrogante es doble.

En primer lugar, existe un argumento sencillo y evidente aunque por alguna extraña razón invisible para los responsables de los ficheros. Vivimos en una sociedad cuyo valor principal comienza a ser la información y el conocimiento. En muchos sectores de producción, y sin

ninguna duda en el conjunto de la Administración, la información y el conocimiento poseen un valor estratégico.

No es concebible un funcionamiento normal del Estado Social sin el manejo de ingentes cantidades de información personal. Del mismo modo actos cotidianos como tomar un tren, llamar por teléfono o hacer la compra resultarían de todo punto imposibles sin el auxilio de las tecnologías de la información y las comunicaciones. Curiosamente, no se parece ser consciente de ello.

Nadie pone en duda todas las acciones de la industria y los gobiernos dedicadas a garantizar la estabilidad monetaria, el correcto y seguro desenvolvimiento del proceso productivo o a asegurar el control sobre materias primas y bienes de equipo esenciales.

Pues bien la seguridad, aunque venga de la mano del RDLOPD resulta fundamental para garantizar el adecuado funcionamiento de todos los sistemas, traten o no datos de carácter personal. Además, resulta esencial en cualquier proceso de gestión que requiera uso de tecnologías de la información y, en la práctica, se proyecta sobre el modo de ordenar la actividad de las organizaciones. El objetivo primario de la seguridad es proteger recursos valiosos: información, hardware y software. Es un instrumento que garantiza el funcionamiento de la organización. Todo ello, amén, de los beneficios que se apuntaron en el epígrafe anterior.

Sin embargo, los responsables de los ficheros acaban siendo más receptivos a otro planteamiento. Deben adoptarse medidas de seguridad en cualquier caso ya que es una obligación legal impuesta por el art. 9 de la Ley Orgánica 15/1999 y desarrollada por el Real Decreto 994/1999.

### **3. Las medidas de seguridad.**

El artículo 9 de la Ley Orgánica 15/1999 se ocupa de fijar las condiciones básicas de seguridad que deben reunir los tratamientos<sup>4</sup>. Estas medidas han sido desarrolladas por el Título VIII del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. Como se expondrá a continuación el nuevo Reglamento de desarrollo de la Ley Orgánica innova parcialmente el sistema en el ámbito de los ficheros automatizados con cambios significativos. Pero, y esta seguramente sea la gran novedad, por primera vez, aporta criterios aplicables a los ficheros no automatizados.

El objetivo de las medidas de seguridad es garantizar la confidencialidad, la integridad y la disponibilidad de la información con la finalidad de garantizar el derecho fundamental a la protección de datos. Debe subrayarse que cada uno de los objetivos de la seguridad constituye el corolario lógico del conjunto de principios y reglas contenidos en la LOPD.

En primer lugar, la confidencialidad deriva del propio objeto de la norma, que no es otro que garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

---

<sup>4</sup> Este dispone:

«Artículo 9. 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 garantice la seguridad de los datos de carácter personal y evite 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.

Por otra parte, la integridad responde a las exigencias del principio de calidad de los datos que supone que estos sean veraces, adecuados y puestos al día y cuya consecuencia lógica comporta el protegerlos frente a alteraciones indebidas. Así mismo, actúa como exigencia imprescindible para garantizar la prueba de las vulneraciones de la Ley y garantizar los derechos de los ciudadanos.

Finalmente, la disponibilidad responde a las necesidades de gestión que comporta cualquier sistema de información y a la vez es presupuesto necesario para el ejercicio de los derechos de acceso, rectificación y cancelación.

### **3.1 Niveles de seguridad.**

El art. 81 del RDLOPD establece los niveles de seguridad que se aplicarán a los ficheros en función de la tipología de datos que contengan. El precepto identifica tres niveles, -básico, medio y alto-, para cada uno de los cuales fija las medidas a adoptar. Debe señalarse que los distintos niveles de seguridad son acumulativos y por tanto cada nivel incorpora las medidas dispuestas para el inmediatamente inferior. Se trata de un precepto de contenido complejo que se esquematiza para su mejor comprensión.

---

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».

NIVELES DE SEGURIDAD	
Básico	Todos los ficheros o tratamientos
Medio	<ul style="list-style-type: none"> <li>- Los relativos a la comisión de infracciones administrativas o penales.</li> <li>- Solvencia patrimonial y crédito.</li> <li>- Ficheros de Administraciones Tributarias que se relacionen con el ejercicio de sus potestades tributarias.</li> <li>- Ficheros de entidades financieras para finalidades relacionadas con la prestación de servicios financieros.</li> <li>- Ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social en relación con el ejercicio de sus competencias.</li> <li>- Ficheros de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.</li> <li>- Aquéllos 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.</li> </ul>
Medio reforzado	A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto correspondiente al establecimiento de un registro de accesos.
Alto	<ul style="list-style-type: none"> <li>- Ficheros con datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.</li> <li>- Ficheros que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.</li> <li>- Aquéllos que contengan datos derivados de actos de violencia de género.</li> </ul>
Podrán aplicar el básico	<ul style="list-style-type: none"> <li>- Los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando: <ul style="list-style-type: none"> <li>a) 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.</li> <li>b) 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.</li> </ul> </li> <li>- Los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.</li> </ul>
Ficheros segregados	<p>Cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al 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, y que esto se haga constar en el documento de seguridad<sup>5</sup>.</p>

<sup>5</sup> El tenor literal del precepto es el que sigue:

« Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

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

En principio, el nivel básico de seguridad se aplicará a todos los ficheros. El nivel medio corresponderá a los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y datos sobre solvencia patrimonial y crédito. Debe precisarse que el sentido del concepto

---

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

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

e) Aquéllos 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.

f) Aquéllos 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.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenidas en el artículo 103 de este Reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) 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.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoría se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este Título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al 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, y que esto se haga constar en el documento de seguridad».

“servicios financieros” que según la Agencia Española de Protección de Datos hace referencia a:

«la intermediación monetaria, las actividades relacionadas con la Banca Central, Bancos, Cajas y Cooperativas, las actividades de arrendamiento financiero, las llevadas a cabo por Sociedades de crédito hipotecario, entidades de financiación, Sociedades mediadoras en el mercado de dinero y el Instituto de Crédito Oficial (ICO), así como las efectuadas por Instituciones de inversión colectiva de carácter financiero, Sociedades y fondos de capital riesgo y otras sociedades de inversión en activos financieros. También son servicios financieros los relacionados con la Administración de mercados financieros, y las actividades llevadas a cabo por Sociedades de valores, sociedades de garantía recíproca y de reafianzamiento, sociedades de tasación, casas de cambio, fondos de garantía de depósito y sus sociedades gestoras.

Por este mismo motivo la Clasificación Nacional de Actividades Económicas, a la que anteriormente se ha hecho mención incluye dentro de los servicios de intermediación financiera los relacionados con seguros de vida (incluso si se realizan por entidades de previsión social), los planes de pensiones y, dentro del epígrafe referido a "seguros no vida", los seguros de daños y el reaseguro. Asimismo se consideran actividades de intermediación financiera las efectuadas por agentes y corredores de seguros e intermediarios de seguros»<sup>6</sup>.

Por otra parte por “Hacienda Pública” cabe entender exclusivamente a los ficheros titularidad de la Hacienda Pública y los ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria ya sea la Agencia Estatal de la Administración Tributaria, los correspondientes a las Comunidades Autónomas en materia de Tributos cedidos o aquellos padrones fiscales, correspondientes a los tributos locales, de los que son responsables las Haciendas Locales, así como las Administraciones Públicas que tengan por objeto la exacción de algún recurso de naturaleza tributaria<sup>7</sup>.

El nuevo Reglamento introduce algunos cambios significativos al atribuir la condición de ficheros de nivel medio a los de las Entidades

---

<sup>6</sup> Véase el informe de la AEPD sobre «Aplicación de niveles de seguridad y alcance de la referencia a servicios financieros - Año 1999».

Disponible en <https://www.agpd.es/index.php?idSeccion=212>.

<sup>7</sup> Véase el informe de la AEPD sobre el «Sentido de la expresión datos relativos a Hacienda Pública - Año 1999», disponible en <https://www.agpd.es/index.php?idSeccion=213>.

Gestoras y Servicios Comunes de la Seguridad Social en relación con el ejercicio de sus competencias y a aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. Evidentemente se trata de ficheros que suelen incorporar datos muy relevantes de la trayectoria profesional de los ciudadanos, lo que justificaría plenamente esta decisión. Por otra parte, no debe considerarse esta calificación como una exclusión respecto de aquellos casos en los que los ficheros incorporen datos de salud o filiación sindical que, salvo que se den ciertas condiciones que a continuación se expondrán, tendrían un nivel alto.

Por otra parte, pasan a ser de nivel medio, -ya que antes sólo aplicaban algunas de las mismas, «aquellos que contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo». Esta locución contiene un concepto jurídico indeterminado que convendrá concretar en cada caso. La Agencia ha ofrecido un cierto criterio en su Informe 160/2004 sobre «Nivel de seguridad de ficheros con datos de localización»<sup>8</sup>. Estos datos son los que se obtienen mediante el seguimiento de la ubicación concreta de los teléfonos móviles con la finalidad de ofrecer servicios a sus titulares como los de localización de direcciones, servicios útiles (gasolineras, restaurantes, oferta de ocio en la zona etc.), publicidad segmentada por razón de proximidad a la ubicación del usuario o ayuda en caso de urgencia. Al respecto señala la AEPD:

«En este supuesto, suponiendo que el tratamiento de los datos cumpla con los requisitos que se han señalado anteriormente, dicho tratamiento permitiría conocer la localización del afectado en cada momento concreto o en los supuestos en que dicha localización fuera sometida a tratamiento, lo que supondrá un conocimiento suficiente del comportamiento del usuario de la

---

<sup>8</sup> Disponible en <https://www.agpd.es/index.php?idSeccion=491>.

terminal sometida a localización, en caso de que dicho usuario fuera suficientemente identificable.

Todo ello implicará que el supuesto deberá considerarse subsumido en el artículo 4.4 del Reglamento de Medidas de Seguridad, debiendo implantarse las medidas a las que el mismo se refiere, (...)»<sup>9</sup>.

En un plano intermedio se sitúan los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización. En este caso se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto correspondiente al establecimiento de un registro de accesos. Esta medida adicional viene justificada por al menos dos tipos de razones. Por una parte se trata de datos que, como se vio en el informe anteriormente citado ofrecen información personal relevante desde el punto de vista de los perfiles de personalidad. Pero además se trata de información de interés policial al amparo de las obligaciones que impone a los operadores la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. En efecto estos deben conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación. Además deben ceder estos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

---

<sup>9</sup> Lo mismo ocurrirá cuando se trate, por ejemplo, de un fichero o tratamiento que contenga datos curriculares cuando éstos incluyan información muy detallada sobre el sujeto, por ejemplo, cuando se incluyan sus aficiones o un perfil de estudios muy concreto y también lo serían por ejemplo los tratamientos ordenados a obtener perfiles de comprador. El mismo nivel podría tener un fichero utilizado para la selección de personal.

Por último, siguen siendo de nivel alto los ficheros que contengan datos especialmente protegidos, -datos de ideología, religión, creencias, origen racial, salud o vida sexual-, así como los que contengan datos recabados para fines policiales sin consentimiento de los titulares. A ellos se unen aquéllos ficheros que contengan datos derivados de actos de violencia de género. Se trata de datos personales que afectan a un ámbito muy íntimo de la información personal lo que justifica su especial consideración.

### **3.2 Algunas novedades significativas.**

En las Disposiciones Generales del Capítulo I del Título VIII del nuevo Reglamento se introducen novedades cuya repercusión será a buen seguro muy importante.

#### *3.2.a) Exenciones en los niveles de seguridad.*

En este ámbito históricamente ha planteado dudas la atribución del nivel alto a tratamientos que incluyen el porcentaje de discapacidad o referencias del tipo “discapacitado si/no” o “en situación de incapacidad laboral si/no”. En su momento, la Agencia Española de Protección de Datos consideró que un dato relativo al grado de minusvalía debe ser considerado como de nivel alto<sup>10</sup> No obstante, aunque este planteamiento resulte esencialmente válido, el nuevo reglamento introduce varias innovaciones que se plantean como excepción a la regla general.

En este sentido el artículo 81.5 permite la implantación de las medidas de seguridad de nivel básico en el caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación cuando se den las siguientes circunstancias:

- «a) 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.
- b) 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».

Por otra parte el párrafo sexto del precepto dispone que:

«También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente 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 tres casos tienen en común un elemento esencial que relaciona el tratamiento con la finalidad del mismo. En el primer caso, no se tratan los datos de ideología, afiliación sindical, religión o creencias con la finalidad de establecer un perfil ideológico de un sujeto, simplemente se trataría de realizar una transferencia dineraria. El ejemplo, arquetípico de este primer supuesto sería el de la detracción de la cuota sindical. Es evidente que la exigencia de un nivel alto de seguridad en estos casos, como más adelante se verá al describir las medidas que incluye, complica extraordinariamente sistemas de información cuyos tratamientos buscan un resultado bastante más sencillo que la obtención de perfiles ideológicos: la gestión de personal<sup>11</sup>.

En el caso de los ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad se pretende no someter al responsable del fichero a una aplicación preventiva del nivel de seguridad alto que no guarde relación con las finalidades y usos del fichero. Existen multitud de ejemplos en el ámbito público y privado en el que la presentación de un documento por parte del titular de los datos, -como una petición o

---

<sup>10</sup> Véase su informe sobre «Especialidades relativas a los ficheros de nóminas - Año 1999», disponible en <https://www.agpd.es/index.php?idSeccion=214>.

instancia, un impreso, una sugerencia o reclamación, un currículum etc.-, puede incluir datos especialmente protegidos que, sin embargos, ni han sido requeridos ni resultan necesarios al responsable. Sin esta excepción, la mayor parte de sistemas de información deberían necesariamente aplicar un nivel alto de seguridad por razones estrictamente preventivas resultando esta última a todas luces una consecuencia claramente desproporcionada.

Por último, en el párrafo sexto se contempla una excepción que guarda directa relación con la del párrafo quinto letra a) del artículo 81. Su razón es prácticamente idéntica, el responsable del fichero se ve compelido a tratar un dato de salud que sólo revela una información del tipo “discapacitado si-no”, inválido si-no o porcentaje de discapacidad, pero en ningún caso describe discapacidad o enfermedad alguna. Pero además, el responsable trata un dato personal de esta naturaleza porque se lo impone como deber público sin ninguna finalidad relacionada con la salud del titular de los datos. Se trata de cuestiones como el cálculo y la práctica de las retenciones en el Impuesto de la Renta de las Personas Físicas o la atribución de beneficios y ayudas sociales como la matrícula gratuita en los estudios universitarios. Por tanto supuestos en los que el objeto que persigue el responsable no es el del conocimiento de un determinado estado de salud sino la simple comprobación de un dato objetivo para el cumplimiento de un deber público.

### *3.2.b) Ficheros segregados.*

Otra de las nuevas aportaciones del artículo 81 nuevo Reglamento de desarrollo de la LOPD se encuentra en su párrafo octavo. Este precepto trata de atender a la realidad de los sistemas permitiendo a los

---

<sup>11</sup> Cuestión distinta es que se produjese un uso para finalidad distinta. STC 11/1998....

responsables de los ficheros dimensionar la seguridad para cada uno de los recursos.

«8. A los efectos de facilitar el cumplimiento de lo dispuesto en este Título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al 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, y que esto se haga constar en el documento de seguridad».

Se trata de permitir que el responsable pueda dimensionar la seguridad en función de los sistemas afectados. Así, por ejemplo, cuando en un sistema de información complejo se gestionen datos de nivel alto en un recurso específico y concreto bastaría con programar sobre el las correspondientes medidas.

### *3.2.c) Prestaciones de servicios*

Otro de los elementos destacados del Reglamento deriva de la fijación de un completo estatuto del encargado del tratamiento. La regulación del mismo se contempla en el Capítulo Tercero del Título II y se completa por el artículo 82 en materia de seguridad. No debe olvidarse que el párrafo segundo del artículo 12 LOPD exige la existencia de un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido. Este contrato deberá contemplar de modo concreto las medidas de seguridad que el encargado del tratamiento está obligado a implementar. Ha sido tradicional no entender que la simple referencia o reproducción del artículo 12 LOPD no suponía su cumplimiento, el contrato debía tener un contenido material, debía incluir “instrucciones” específicas para el encargado. De aquí que el artículo 82 obligue a reconocer las circunstancias concretas en las que se realiza la prestación del encargado, -en los locales del encargado, con acceso remoto y simple acceso en modo consulta a los datos, o en los propios locales del

encargado-, y a fijar las obligaciones del encargado en función de esta circunstancia. Lógicamente no pueden ser las mismas cuando se tiene un simple acceso a los datos, como un usuario más del sistema de información, que cuando se almacenan datos en soportes propios. En este último caso, el encargado deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

Además el Reglamento precisa con mucho detalle el contenido de este documento de seguridad en los párrafos quinto y sexto del artículo 88 obligando a identificar los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

Por último en el párrafo sexto se ha atendido a una realidad muy extendida en el ámbito de la pequeña empresa, del pequeño comercio y del empresario individual o autónomo. Es muy común que este tipo de responsables acudan a un tercero al que encomiendan la llevanza de la gestión de personal y de la gestión contable y fiscal de sus empresas con el resultado práctico de que el encargado gestiona los datos personales con motivo de su prestación y el responsable, en la práctica, no aloja ningún dato en su entorno físico o informático. De ahí que el Reglamento ordene anotar tal extremo en el documento de seguridad y permita delegar en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Esta delegación debe recogerse de modo expreso en el contrato celebrado al amparo del artículo 12 de la LOPD. Señala la norma que «en tal caso, se atenderá al

documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este Reglamento». Se trata de evitar situaciones absurdas en las que el documento de seguridad del responsable no pudiera ser otra cosa que copia casi literal del original del encargado.

Por otra parte, las prestaciones de servicios susceptibles de poner en riesgo los sistemas de información no sólo son aquellas que comportan acceso a datos. Un ejemplo evidente de ello son los servicios de limpieza. El desarrollo de estas prestaciones se produce en horarios en los que las instalaciones no se encuentran ocupadas y podría permitir prácticas como el desechado inadecuado de determinados soportes, -fotocopias o documentos-, el acceso a documentos no sujetos a custodia, o la desactivación de sistemas como el aire acondicionado que pueden ser críticos para la estabilidad del hardware. Por ello el artículo 83 se refiere a las prestaciones de servicios sin acceso a datos personales.

«El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio».

Este precepto debería entenderse en sentido amplio y abarcar al conjunto de acciones que puedan comprometer la seguridad de los datos por afectar no sólo a su contenido sino a la seguridad de las instalaciones y soportes que los contengan.

### *3.2.d) Organización del personal*

El articulado del Título VIII del Reglamento viene a reconocer una realidad ineludible, la gestión de la seguridad es compleja y no se produce casi nunca un modelo rígido de gestión. En este sentido, el responsable no

decide todo ya que en muchas ocasiones el director-gerente, el administrador o el funcionario público que posee facultades para decidir no incorpora el bagaje de conocimientos adecuado. De hecho, ni siquiera la seguridad es responsabilidad de una única persona ya que existen sistemas de información que requieren de personas a su cargo, o en determinados ámbitos es necesario especializar al personal, analistas, programadores, gestores de aplicaciones, gestores de redes, gestores de incidencias etc.-, y por ello existe más de un responsable de seguridad.

Por ello el artículo 84 contempla la posibilidad de delegar las autorizaciones del responsable del fichero o tratamiento incluyéndolas en el documento de seguridad donde deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. Por otra parte el artículo 88.4.a) contempla para nivel medio la existencia de uno o varios responsables de seguridad que deberá recoger el documento de seguridad y que completa el artículo 95 señalando que «esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados».

### *3.2.e) Redes de comunicaciones.*

El Reglamento presta cierta atención a las redes de de comunicaciones. Así debe destacarse que aunque el artículo 85 prácticamente reitera el contenido del antiguo artículo 5 del Real Decreto 994/1999, contiene dos importantes precisiones. En primer lugar, establece la necesidad de garantizar la seguridad los accesos a datos de carácter personal a través de redes de comunicaciones, subrayando «sean o no públicas» y remitiéndose a los criterios de fijación de los niveles de seguridad del artículo 80 del reglamento. Por tanto, el control para el

acceso a través de cualquier red se articulará de acuerdo con el nivel básico, medio o alto del fichero y además se articulará tanto cuando para el mismo se usen redes públicas como en redes internas, intranets o de área local.

Pero no es esta la única previsión novedosa. Al regular las medidas de nivel alto el artículo 104 RDLOPD, además de mantener al antigua exigencia de cifrado o mecanismo equivalente, introduce el concepto de red inalámbrica. Por tanto, no se trata sólo de cifrar datos cuando circulen a través de redes públicas sino también a cuando lo hagan través de redes wireless, bluetooth etc.

En tal sentido, es importante tener en cuenta que existen determinados contextos, -como por ejemplo en el ámbito educativo o en espacios de municipales de promoción del acceso a Internet-, en los que no existiendo una red pública en sentido estricto se produce un uso de la red interna por usuarios invitados que no forman parte de la organización. Parece razonable ir más allá de una política de mínimos e implementar las medidas del artículo 104 RDLOPD.

### *3.2.f) Trabajo fuera de los locales y dispositivos portátiles.*

El Real Decreto 994/1999, era particularmente rígido e impreciso en materia de lo que denominaba «ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero». La rigidez e imprecisión se debía a que únicamente se regulaba la existencia de una autorización expresa del responsable y la garantía de la seguridad sin mayor detalle. En este sentido, no se contemplaba la existencia del encargado, de hecho cabría plantearse hasta que punto el propio encargo constituía un supuesto de trabajo fuera de los locales, ni se tenía en cuenta la habitualidad en la realización de estos trabajos.

La nueva regulación en cambio, en su artículo 86 se refiere al régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento. Parece contemplar además cierta flexibilidad para la autorización previa. Así señala la autorización a la que se refiere «podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas». Por tanto, sin perjuicio de las autorizaciones concretas que se requieran cuando se trata de trabajos cíclicos y generales pueden preverse autorizaciones que los contemplen. Debe recordarse que, como más arriba se señaló, el responsable puede delegar autorizaciones lo cual resta rigidez al sistema pudiendo acercar el proceso decisional a los gestores más cercanos a los sistemas de información.

Por otra parte, resultaba coherente aplicar estos principios a los dispositivos portátiles ya que por su propia naturaleza suponen la posibilidad de desarrollar tratamientos fuera de los locales. No debe olvidarse que los dispositivos portátiles son en si mismo soportes y ya desde nivel básico (artículo 92) existirá un registro de soportes en que se anotará la salida debiendo existir, como se había señalado una autorización previa. Más adelante el artículo 101 del Reglamento, contempla una medida específica para los ficheros o tratamientos de nivel alto obligando a cifrar «los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero».

### 3.3 Esquema de medidas de seguridad.

El Reglamento de medidas de seguridad contempla una amplia panoplia de medidas de seguridad. Alguno de estos aspectos ha sido objeto de consideración detallada en el epígrafe anterior. La disponibilidad limitada de espacio no permite entrar a considerar de modo exhaustivo cada una de las medidas, y especialmente resultaría arriesgado hacerlo desde una perspectiva técnica. Si que puede ofrecerse un esquema:

MEDIDAS ADICIONALES A TODOS LOS NIVELES		
Acceso a datos a través de redes de comunicaciones	Las medidas de seguridad exigibles a los accesos a 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.	
Trabajo fuera de los locales o uso de dispositivos portátiles	<ul style="list-style-type: none"> <li>- Autorización previa del responsable del fichero o tratamiento:               <ul style="list-style-type: none"> <li>a) tendrá que constar en el documento de seguridad</li> <li>b) podrá establecerse para un usuario o para un perfil de usuarios</li> <li>c) se determinará un periodo de validez para las mismas.</li> </ul> </li> <li>- Deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.</li> </ul>	
Ficheros temporales o copias de trabajo de documentos creados exclusivamente para la realización de trabajos temporales o auxiliares.	<ul style="list-style-type: none"> <li>- Deberán cumplir el nivel de seguridad que les corresponda.</li> <li>- Será borrados o destruidos una vez que haya dejado de ser necesario para los fines que motivaron su creación.</li> </ul>	
Delegación de autorizaciones.	<ul style="list-style-type: none"> <li>- Cabe la delegación de las autorizaciones que se atribuyen al responsable del fichero.</li> <li>- En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación.</li> <li>- Esta designación no supone una delegación de la responsabilidad que corresponde al responsable del fichero</li> </ul>	
Prestaciones de servicios sin acceso a datos personales	<ul style="list-style-type: none"> <li>- Adoptar las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.</li> <li>- Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.</li> </ul>	
Encargado del tratamiento.	Locales del Responsable	Deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
	Acceso remoto con prohibición de copiar datos	Deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
	Locales del encargado	Deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.
	General	El encargado del tratamiento estará sometido a las medidas de seguridad contempladas en el Reglamento.

<b>DOCUMENTO DE SEGURIDAD</b>	
<b>CONTENIDO</b>	
Medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.	
<b>Tipos de documento</b>	<ul style="list-style-type: none"> <li>- Único y comprensivo de todos los ficheros o tratamientos.</li> <li>- Individualizado para cada fichero o tratamiento.</li> <li>- Agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable.</li> </ul>
<b>Contenido mínimo</b>	<ul style="list-style-type: none"> <li>a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.</li> <li>b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.</li> <li>c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.</li> <li>d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.</li> <li>e) Procedimiento de notificación, gestión y respuesta ante las incidencias.</li> <li>f) Procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.</li> <li>g) Medidas que sea 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.</li> </ul>
<b>Contenido en niveles medio y alto</b>	<ul style="list-style-type: none"> <li>a) Identificación del responsable o responsables de seguridad.</li> <li>b) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento<sup>12</sup>.</li> </ul>
<b>ACTUALIZACIÓN</b>	
<b>Mantenimiento</b>	Deberá mantenerse en todo momento actualizado.
<b>Revisión</b>	Será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados <sup>13</sup> .
<b>DOCUMENTO DEL ENCARGADO</b>	
<b>Contenido</b>	<ul style="list-style-type: none"> <li>- Identificación de ficheros o tratamientos que se traten en concepto de encargado.</li> <li>- Referencia al contrato o documento que regule las condiciones del encargo.</li> <li>- Identificación del responsable.</li> <li>- Período de vigencia del encargo.</li> </ul>
<b>Datos ubicados de modo exclusivo en soportes del encargado</b>	<ul style="list-style-type: none"> <li>- El responsable deberá anotarlos en su documento de seguridad.</li> <li>- Si afecta a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios.</li> <li>- La delegación se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 LOPD, con especificación de los ficheros o tratamientos afectados.</li> </ul>

<sup>12</sup> La norma no indica cuales deban ser los controles periódicos, ni sus plazos, aunque recoge expresamente una auditoria interna o externa bienal (nivel medio en todo tipo de ficheros) y controles mensuales del registro de accesos del nivel alto de los ficheros automatizados. Es evidente que pueden y deben establecerse controles sobre aspectos estratégicos como las altas y bajas de usuarios, -y las políticas vinculadas a la identificación y autenticación de los mismos como la realización de cambios cíclicos de contraseña-, la gestión y resolución de las incidencias, las copias de respaldo y/o los cambios en el software, hardware o en las instalaciones. Por otra parte, podría plantearse políticas de control sobre el acceso de personal externo autorizado.

En la práctica, y con el texto del Reglamento nada impide en absoluto practicar controles periódicos sobre cada una de las medidas que prevé.

<sup>13</sup> En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

## Ficheros automatizados

Nivel Básico		
<b>Funciones y obligaciones del personal</b>	<ul style="list-style-type: none"> <li>- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el documento de seguridad.</li> <li>- Definir las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.</li> <li>- Formación e información del personal para que conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento</li> </ul>	
<b>Usuarios y control de accesos</b>	<ul style="list-style-type: none"> <li>- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones.</li> <li>- Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.</li> <li>- Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.</li> <li>- Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el documento de seguridad, conforme a los criterios establecidos por el responsable del fichero.</li> <li>- El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.</li> </ul>	
<b>Identificación y autenticación</b>	<ul style="list-style-type: none"> <li>- Adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.</li> <li>- Establecer mecanismos para la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.</li> <li>- Si se usan contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.</li> <li>- El documento de seguridad establecerá la un cambio periódico de contraseñas nunca superior a un año. Mientras estén vigentes, se almacenarán de forma ininteligible.</li> </ul>	
<b>Registro de incidencias</b>	<ul style="list-style-type: none"> <li>- Establecer un procedimiento de notificación y gestión de las incidencias</li> <li>- Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas</li> </ul>	
<b>Gestión de soportes y documentos.</b>	<b>Etiquetado</b>	<ul style="list-style-type: none"> <li>- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.</li> <li>- No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.</li> <li>- Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considere especialmente sensibles.</li> </ul>
	<b>Registro de salida</b>	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
	<b>Traslado</b>	En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
	<b>Destrucción</b>	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
<b>Copias de respaldo y recuperación.</b>	<b>Copia de respaldo</b>	<ul style="list-style-type: none"> <li>- Copia como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.</li> <li>- Fijar procedimientos para la recuperación de los datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.</li> <li>- En ficheros parcialmente automatizados si existe documentación que permite la reconstrucción se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.</li> </ul>
	<b>Control periódico</b>	Control periódico semestral de la definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
	<b>Pruebas con datos reales</b>	Prohibición de pruebas con datos reales anteriores a la implantación o modificación de los sistemas de información salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Deberá haberse realizado una copia de seguridad.

<b>Nivel Medio</b>		
<b>Responsable de seguridad</b>	<b>Designación</b>	En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.
	<b>Tipos de designación</b>	<ul style="list-style-type: none"> <li>- Única para todos los ficheros o tratamientos de datos de carácter personal</li> <li>- Diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.</li> </ul>
<b>Auditoria.</b>	<b>Periodicidad</b>	Al menos cada dos años se realizará una auditoria interna o externa que verifique el cumplimiento las medidas de seguridad del Reglamento.
	<b>Auditoria Extraordinaria</b>	<ul style="list-style-type: none"> <li>- Deberá realizarse siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.</li> <li>- Esta auditoria inicia el cómputo de dos años.</li> </ul>
	<b>Informe de auditoria</b>	<ul style="list-style-type: none"> <li>- Deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.</li> <li>- Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.</li> <li>- Los informes de auditoria serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas</li> </ul>
<b>Gestión de soportes y documentos.</b>	<b>Registro de entrada</b>	Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, 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 que deberá estar debidamente autorizada.
	<b>Registro de Salida</b>	Se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, 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 entrega que deberá estar debidamente autorizada.
<b>Identificación y autenticación.</b>		El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
<b>Control de acceso físico</b>		Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
<b>Registro de incidencias: recuperación de datos</b>		<ul style="list-style-type: none"> <li>- El registro deberán consignar además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.</li> <li>- Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.</li> </ul>

<b>Nivel Alto</b>		
<b>Gestión de soportes</b>	Etiquetado “críptico”	La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
	Distribución	2. La distribución de los soportes se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
	Portátiles	<ul style="list-style-type: none"> <li>- 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.</li> <li>- Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea 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.</li> </ul>
<b>Copias de respaldo y recuperación.</b>		Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas correspondiente, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.
<b>Registro de accesos</b>	Funcionamiento	<ol style="list-style-type: none"> <li>1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.</li> <li>2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.</li> <li>3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.</li> <li>4. El período mínimo de conservación de los datos registrados será de dos años.</li> <li>5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.</li> </ol>
	Excepción	<p>No será necesario el registro de accesos definido en este artículo en caso de que concurren las siguientes circunstancias:</p> <ol style="list-style-type: none"> <li>a) Que el responsable del fichero o del tratamiento sea una persona física.</li> <li>b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.</li> </ol> <p>La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.</p>
<b>Telecomunicaciones</b>		La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## Ficheros no automatizados

Nivel Básico													
<b>Funciones y obligaciones del personal</b>	<ul style="list-style-type: none"> <li>- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el documento de seguridad.</li> <li>- Definir las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.</li> <li>- Formación e información del personal para que conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento</li> </ul>												
<b>Usuarios y control de accesos</b>	<ul style="list-style-type: none"> <li>- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones.</li> <li>- Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.</li> <li>- Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.</li> <li>- Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el documento de seguridad, conforme a los criterios establecidos por el responsable del fichero.</li> <li>- El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.</li> </ul>												
<b>Registro de incidencias</b>	<ul style="list-style-type: none"> <li>- Establecer un procedimiento de notificación y gestión de las incidencias</li> <li>- Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas</li> </ul>												
<b>Gestión de soportes y documentos.</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; vertical-align: top;">Etiquetado</td> <td> <ul style="list-style-type: none"> <li>- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.</li> <li>- No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.</li> <li>- Podrán etiquetarse críticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.</li> </ul> </td> </tr> <tr> <td style="vertical-align: top;">Registro de salida</td> <td>La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.</td> </tr> <tr> <td style="vertical-align: top;">Traslado</td> <td>En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.</td> </tr> <tr> <td style="vertical-align: top;">Destrucción</td> <td>Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.</td> </tr> <tr> <td style="vertical-align: top;">Custodia de los soportes</td> <td>Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas</td> </tr> <tr> <td style="vertical-align: top;">Dispositivos de almacenamiento</td> <td>Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.</td> </tr> </table>	Etiquetado	<ul style="list-style-type: none"> <li>- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.</li> <li>- No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.</li> <li>- Podrán etiquetarse críticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.</li> </ul>	Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.	Traslado	En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.	Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.	Custodia de los soportes	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas	Dispositivos de almacenamiento	Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.
Etiquetado	<ul style="list-style-type: none"> <li>- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.</li> <li>- No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.</li> <li>- Podrán etiquetarse críticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.</li> </ul>												
Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.												
Traslado	En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.												
Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.												
Custodia de los soportes	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas												
Dispositivos de almacenamiento	Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.												
<b>Criterios de archivo.</b>	<p>El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán 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.</p> <p>En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.</p>												

Nivel Medio		
Responsable de seguridad	Designación	En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.
	Tipos de designación	- Única para todos los ficheros o tratamientos de datos de carácter personal - Diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
Auditoria		Los ficheros no automatizados de este nivel se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de las medidas de seguridad.

Nivel Alto		
Almacenamiento de la información	Armarios o archivadores	Deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
	Excepción	Si, atendidas las características de los locales no fuera posible disponer de áreas cerradas el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.
Copia o reproducción	Realización	Únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
	Destrucción	Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
Acceso a la documentación.	Acceso	El acceso a la documentación se limitará exclusivamente al personal autorizado.
	Identificación	Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
	Usuarios no registrados	Deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.
Traslado de documentación		Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Conviene no obstante apuntar algunos conceptos importantes sobre los que debe hacerse hincapié.

### 3.3.a). El alcance de la seguridad.

Debe subrayarse que la seguridad de los sistemas de información que contengan datos personales se proyecta más allá del ámbito de la informática. En primer lugar, la seguridad se desplegará en el medio físico garantizando el control sobre los entornos en los que se encuentre la información. Para ello se tendrá en cuenta no sólo el control de acceso de las personas, previniendo frente a intrusiones no autorizadas o riesgo de

robo. También deberán desarrollarse planes de contingencia frente a situaciones catastróficas como incendios e inundaciones.

En segundo lugar, debe tenerse en cuenta que la seguridad se erige en un objetivo de toda la organización abarcando todos y cada uno de los miembros de su personal. Es un parámetro que debe tenerse en cuenta al diseñar el entorno organizativo y comporta el establecimiento de un conjunto de obligaciones para todo el personal relacionado con los tratamientos en cualquiera de sus ámbitos. En este sentido alcanzará en todo caso a aquellos que de un modo u otro posean acceso a la información pero también a quienes no teniéndola puedan comprometer la seguridad de los sistemas. Así, una mala práctica del responsable de controlar la seguridad de los accesos o una práctica de riesgo en el almacenamiento de productos de limpieza o en el uso de algunos de ellos podría afectar también a la integridad de los sistemas en su dimensión física o lógica.

Por último, en el ámbito informático la seguridad se articulará en todos y cada uno de los niveles relacionados con el tratamiento, ya sea el de la propia aplicación, el sistema operativo sobre el que se ejecute o el entorno de red local. Por otra parte, resultará esencial tener en cuenta a equipos como, portátiles, PDA, tablet PC, Pendrive y memorias externas, entre otros, que por su movilidad o portabilidad, pueden salir fuera de los locales y estar sujetos a riesgos adicionales. Y otro tanto sucede con los soportes de grabación.

En suma se trata de proteger el sistema fijando criterios racionales de utilización para los usuarios internos protegiéndolo a la vez contra las agresiones externas o internas de todo tipo<sup>14</sup>.

*3.2.b) La importancia estratégica del documento de seguridad.*

Como se ha visto las concretas medidas que se adopten en aplicación del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (RDLOPD) deberán documentarse.

Al margen de la constancia formal de las medidas adoptadas en cumplimiento del RDLOPD, y por tanto de su necesaria exhibición cuando así lo soliciten los funcionarios de inspección de la Agencia Española de Protección de Datos, el documento de seguridad cumple con otras funciones.

En primer lugar, la documentación de la seguridad constituye el punto de partida necesario para la formación del personal, con independencia de las medidas adicionales que se puedan adoptar. En efecto, el Reglamento no sólo prevé la necesidad de definir y documentar claramente las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal, además obliga al responsable del fichero a adoptar «necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento» (artículo 89.2 RDLOPD).

---

<sup>14</sup> Véase VV. AA. *Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada*. AENOR, Madrid, 2004 y MAGERIT. Versión 1.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, disponible en <http://www.csi.map.es/csi/pg5m20.htm>.

Por otra parte, hay que tener en cuenta la funcionalidad de distintos aspectos del documento. En el mismo existirán de distintos registros dedicados a ejercer un control sobre los recursos, -copias de seguridad, inventarios de soportes que contengan datos, entrada, salida y/o destrucción de soportes que contengan datos que se incorporan o salen del fichero-, sobre el funcionamiento del sistema, -como el registro de accesos en ficheros de nivel alto o los registros de incidencias-, o sobre la evaluación global de las medidas adoptadas mediante la documentación de los informes de auditoría realizados. Asimismo, el documento contendrá la descripción del entorno físico y lógico de los sistemas de información. Todos estos elementos serán esenciales a lo largo de la vida de los tratamientos en la medida en que, por una parte, el documento de seguridad es el resultado del análisis de riesgos previo que conduce a implementar las medidas previstas por el RDLOPD, y por otra, constituye fiel prueba de la propia evolución del sistema y documento de base para modificar e incluir nuevas medidas.

En este sentido, resulta capital una concreta previsión del artículo 88 RDLOPD. Este precepto, como el antiguo artículo 8.3 RMS, obliga a mantener el documento actualizado en todo momento y a revisarlo siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. Y precisa que «un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas».

Debe subrayarse que la exigencia de disponer de un documento de seguridad no es meramente formal y su ausencia constituye una infracción grave<sup>15</sup>.

### *3.3.b) Algunos conceptos complicados.*

Existen algunos conceptos en el RDLOPD cuyo sentido debe precisarse en la medida que puedan resultar oscuros para el responsable del fichero.

En primer lugar, la primera definición del art. 5.2 RDLOPD reza así:

«Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal».

Este concepto tiene una enorme trascendencia desde el punto de vista de la protección de datos personales y no aparece en las definiciones del artículo 3 LOPD. En efecto, en ellas se nos describe que es un fichero y que es un tratamiento:

«b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

Como es sabido, la definición de tratamiento es mucho más dinámica y en la práctica toda la aplicación de la Ley Orgánica pivota

---

<sup>15</sup> Como se indica en la Resolución R/00285/2005:

«En el presente caso, ha quedado acreditado que Administraciones “P.M” carecía, a fecha 26/01/2004, del preceptivo Documento de Seguridad regulado en el artículo 9 de la LOPD, en relación con el artículo 8 y siguientes del citado Reglamento de Seguridad. Sin embargo, disponía de ficheros automatizados con datos de carácter personal de sus administrados.

El incumplimiento del artículo 8 del citado Reglamento supone una infracción por parte de Administraciones “P.M” del artículo 9 de la LOPD, tipificado como grave en el artículo 44.3.h) de dicha norma».

Dictada en el procedimiento N° PS/00152/2004.

sobre ese concepto. Sin embargo, la idea de sistema de información es profundamente fecunda y un referente de primer orden no ya para la seguridad sino para la inscripción de los ficheros y la aplicación de las propias medidas de seguridad.

En la realidad se produce lo que podríamos designar de un modo un tanto artificioso como “inscripción de ficheros jurídicos”. En la práctica, no se da una relación de 1 a 1 entre los ficheros lógicos, esto es los ficheros informáticos realmente existentes y los ficheros inscritos. Si un responsable gestiona su relación con los clientes y proveedores mediante un software comercial del tipo Contaplus, una hoja de cálculo y un fichero con una relación nominal con cualquier tipo de extensión (.mdb, .doc, .pdf), se inscribe un único fichero ante el RGPD. Y ello sin profundizar en sistemas complejos donde se realice minería de datos y se use un datawarehouse.

Sin embargo, la realidad es mucho más rica que la foto fija descrita en el formulario de inscripción ante el Registro General de Protección de Datos ya que éste se basa en una pura descripción de categorías. Cuando se descende a la necesidad de describir la realidad en un documento de seguridad, de identificar los usuarios y sus perfiles, de aplicar medidas de seguridad concreta va a ser la idea de sistema de información la que nos va a permitir dotar de unidad a las políticas de seguridad dentro del sistema, a fijar políticas globales y, a la par, a descender hasta el fichero lógico concreto al que afectan.

El segundo concepto del artículo 5.2 RDLOPD al que conviene prestar atención, es el de usuario que se define como «sujeto o proceso autorizado para acceder a datos o recursos». De hecho, conviene centrarse en dos elementos que pueden tener trascendencia, no sólo sobre la

seguridad *strictu sensu*, sino sobre otro aspecto estudiado en este curso: “el encargado del tratamiento”.

Que un usuario sea un sujeto no nos ofrece duda alguna pero ¿que significa que un usuario sea un proceso? ¿Por qué es relevante esta noción? Existen sistemas, como por ejemplo las propias soluciones para el datawarehousing en los que las consultas a la base de datos no las realiza directamente el usuario sino un programa, un proceso, que actúa como intermediario. De ahí la importancia de documentar la existencia de ese “usuario-proceso”. Por poner otro ejemplo muy común en el entorno universitario. En la Universidad española se ha generalizado, de la mano del patrocinio bancario, la instalación de kioscos virtuales desde los que los estudiantes pueden verificar directamente su expediente académico. Eso significa que las bases de datos de gestión académica reciben múltiples llamadas de procesos que activa directamente el titular de los datos. Ese titular de los datos no es un usuario del sistema en términos de seguridad. A nadie se le puede ocurrir utilizando un sano criterio dar de alta a 30000 sujetos en el documento de seguridad de la Universidad de Murcia, facilitarles sus obligaciones de seguridad y obligarles asumir una responsabilidad a todas luces excesiva. Lo que realmente actúa como usuario del sistema es el proceso que sirve la consulta al kiosco y esto es lo que debe documentarse.

Por todo ello el Reglamento precisa que «tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico».

El otro elemento a tener en cuenta en la definición es el hecho de que usuario no sólo es quien accede a datos sino también quien accede a “recursos”. Por tanto no se exige un acceso material a los datos. El técnico

del servicio externo de mantenimiento informático que realiza una ampliación en la memoria de un ordenador de una PYME que aloje un fichero y que después realiza la comprobación arrancando el sistema puede que no acceda a un solo dato. No obstante, accede a los recursos físicos que lo contienen y arranca el sistema operativo sobre el que funciona. Recuérdese que el RDLOPD define un recurso como « cualquier parte componente de un sistema de información»

Por tanto, materialmente puede ser responsable de un borrado accidental de la base de datos aunque no acceda a un solo byte de información. El ejemplo, además no es en absoluto inocente y debe tenerse muy en cuenta ya que cuando ese usuario que accede a recursos pertenezca a la organización de un tercero que preste un servicio ineludiblemente deberá celebrarse un contrato al amparo del art. 12 LOPD.

Otro de los conceptos que suele plantear dudas tanto a los responsables de los ficheros como a los usuarios de sistemas de información es el de incidencia. Esta se define como «cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos». Por tanto, se trata de un concepto muy indeterminado que deberá ser ponderado en cada caso concreto. En este sentido, y a título de ejemplo, pueden citarse multitud de supuestos que pueden calificarse como tales:

- Un robo en el centro de proceso de datos.
- Un incendio o inundación.
- El olvido de una contraseña seguido de un bloqueo del acceso.

- La pérdida de las llaves que permiten el acceso a un entorno físico controlado.
- Errores en la llevanza de los registros de altas y bajas de usuarios, de entradas y/o salidas de soportes etc.
- Un ataque externo, un virus informático etc.
- Las averías en los equipos.
- Incluso, llevados al extremo, constituye una incidencia el que un ordenador aparezca con una sesión abierta al principio de la jornada cuando no existe la seguridad de si durante la noche alguien pudo acceder a el y la información que contenga.

Ante estas situaciones es conveniente que las organizaciones diseñen procedimientos para gestión de las incidencias y motiven de modo especial a los usuarios para que las notifiquen.

El último elemento que requiere de una cierta interpretación es la referencia a los ficheros temporales. Si se interroga a un informático sobre que es un fichero temporal, en su respuesta indicará que los ficheros temporales son generados por los sistemas operativos para guardar datos intermedios o de ayuda. También indicará que una vez deja de funcionar la aplicación, el fichero suele borrarse automáticamente. Así, desde este punto de vista el fichero paralelo que genera Word, por razones de seguridad y para tener una copia recuperable ante un incidente, la apertura de un archivo desde un correo electrónico, -antes de decidir si se conservará o no-, o la información que un programa lanza a la impresora constituye técnicamente un fichero temporal. La vida de éste puede ser absolutamente efímera, a veces de unos cuanto segundos.

El Reglamento define los ficheros temporales como «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».

Posteriormente el artículo señala:

«Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación».

Por tanto, puede decirse que en el plano de las definiciones el Reglamento recoge la definición técnica que se acaba de exponer junto con una noción de naturaleza funcional que se refiere a ficheros de “uso temporal”. Se trata de aquellos datos que por cualquier razón se integran en un fichero ajeno a la base de datos de modo previo o posterior a su incorporación a la misma. Así, existirá un fichero temporal cuando una aplicación no permite realizar determinadas acciones como imprimir etiquetas y se exportan a otra los datos necesarios para ello o cuando los datos, antes de ser cargados a la base de datos, y para evitar su introducción manual se incluyen un archivo del tipo txt que aplicaciones como Acces son capaces de importar automáticamente.

Pero en el artículo 87 sólo se fijan obligaciones de seguridad para el segundo caso. Los ficheros temporales así concebidos en realidad pertenecen al sistema de información y resulta fundamental realizar respecto de ellos al menos cinco acciones:

- Documentar el procedimiento en virtud del cual se autoriza su creación con indicación clara de las finalidades y las personas autorizadas para ello.
- Reflejar su existencia en el documento de seguridad con las indicaciones precisas que permitan atribuir la responsabilidad que proceda en su caso.
- Indicar sucintamente los criterios y medidas de seguridad que deban seguirse en su gestión.
- Fijar con claridad el lapso temporal de la existencia del fichero temporal junto con el procedimiento para decidir su mantenimiento por un segundo período cuando sea estrictamente necesario.
- Establecer el método para su destrucción que en todo caso garantizará que la información resulte absolutamente irrecuperable.

### *3.3 c) La formación de los usuarios.*

Como se indicó más arriba la documentación de la seguridad constituye el punto de partida necesario para la formación del personal, con independencia de las medidas adicionales que se puedan adoptar. El RDLOPD obliga al responsable del fichero a adoptar «medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento». (artículo 89.2 RDLOPD).

Ahora bien, esta puesta en conocimiento se resuelve en muchas ocasiones con una simple notificación escrita al personal al que se solicita

un acuse de recibo mediante la oportuna firma. Esta metodología, por muy correcta que resulte desde el punto de vista del cumplimiento formal del Reglamento, puede resultar poco acertada.

Mucho más adecuado puede ser el cumplimiento de esta obligación “de forma comprensible” a través de procesos de formación que pueden alcanzar un elevado grado de excelencia si van acompañados de sencillos manuales personalizados. La formación bien entendida es un proceso dialéctico del que se derivan múltiples ventajas:

- Garantiza un conocimiento profundo de las funciones y obligaciones de seguridad ya que la formación constituye un proceso que permite interactuar con el usuario, aclarar sus dudas, profundizar en cuestiones estratégicas...
- Permite subrayar la importancia de la seguridad para la organización y para el propio usuario promoviendo su compromiso activo con las políticas de seguridad.
- Facilita la activación de las políticas organizativas de un modo dinámico en el que incluso la presencia de los distintos usuarios acentúa la sensación de equipo y permite al usuario contemplar esta realidad como parte de un diseño global subrayando la importancia de su propio papel.
- Cuando resulta necesario facilita la especialización de los gestores.
- Contribuye a la gestación de una cultura LOPD en la organización y, cuando se realiza adecuadamente, a la asunción de un compromiso ético con la seguridad por cuanto con ello no sólo contribuye al funcionamiento adecuado de la organización sino

también, y en último extremo, a la tutela de los derechos fundamentales de los ciudadanos.

No debe olvidarse que la formación en seguridad es un proceso que al igual que la propia seguridad se retroalimenta. Por ello, resulta muy relevante disponer de alguna fuente de información, por ejemplo en el web institucional, que permita al usuario consultar dudas, problemas experiencias y que, en caso de necesidad alerte sobre novedades, precauciones etc.

Por último, no puede obviarse en el proceso el informar sobre la existencia de un régimen sancionador, ya que además viene normativamente exigido. Las infracciones a la seguridad no sólo tienen lo que podríamos denominar “consecuencias LOPD”, el usuario debe ser informado de las consecuencias disciplinarias internas que de su incumplimiento puedan derivarse además de la eventual responsabilidad civil que pudiera existir. Sin embargo, resulta fundamental subrayar que salvo en casos extremos este capítulo jamás puede constituir el eje central de un proceso de formación ya que lo único que puede conseguirse con ello es temor o rechazo.

#### *3.3.d) El responsable de seguridad.*

Otro de los elementos a considerar en este breve recorrido por algunos aspectos del RDLOPD es el del responsable de seguridad. Más arriba se señalaron dos aspectos muy relevantes en el nuevo Reglamento. En primer lugar, la posibilidad que se atribuye al responsable para delegar autorizaciones.

Por otra parte, se indicó que el artículo 88.4.a) contempla para nivel medio la existencia de uno o varios responsables de seguridad que deberá recoger el documento de seguridad y que completa el artículo 95

señalando que «esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados».

Esta figura se define como «la persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables». El artículo 95 RDLOPD, en el capítulo que regula las medidas de nivel medio, indica:

«Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este Reglamento».

El propio precepto se encarga de precisar que no resulta necesario que se trate de un único individuo. Una interpretación lógica conduce a subrayar que las concretas funciones atribuidas a cada responsable serán las que decida el responsable del fichero. Esto supone que puedan existir responsables con una asignación funcional de tipo vertical o piramidal, esto es, a quienes se atribuya una función de coordinación general de la seguridad de toda la organización. También pueden existir delegaciones de tipo horizontal o transversal de modo que se atribuya una responsabilidad sectorizada sobre elementos como redes y comunicaciones, sistemas o incidencias. Por último, cabría también una delegación de responsabilidad que se proyectara sobre un fichero o ficheros concretos en función de la estructura organizativa, funcional, física, geográfica etc. de la organización. Obviamente, una o varias de estas figuras bajo la denominación de “responsable de seguridad” podrían

convivir en una misma entidad. Lo que resulta en todo caso, de obligado cumplimiento es la documentación de sus funciones y obligaciones.

Por otra parte, la realidad del mundo empresarial conduce a la existencia de PYMES que no cuentan con personal especializado, entidades que recurren a servicios de empresas externas y/o que alojan sus aplicaciones y/o sistemas mediante soluciones de hosting o housing. A partir de la regulación normativa pueden extraerse soluciones aplicables a este tipo de supuestos:

- Del RDLOPD no se deduce en ningún caso el que el responsable del fichero y el responsable de seguridad no puedan ser materialmente hablando la misma persona física. En las personas jurídicas no se dará esta dualidad ya que responsable del fichero normalmente lo será la entidad. No obstante en el caso del comerciante, el empresario individual, el profesional y el autónomo podría ocurrir perfectamente que un mismo sujeto desempeñase ambas funciones.
- En ningún caso se deduce del RDLOPD la exigencia de que el responsable de seguridad deba tener un perfil profesional determinado aunque el más elemental sentido común aconseje residenciar tales funciones en el personal informático cuando exista.
- Podría atribuirse esta función a un tercero que preste este tipo de servicio con lo que procedería celebrar un contrato de tratamiento de datos por cuenta de terceros al amparo del art. 12 LOPD.

- Conviene reflexionar sobre la importancia de esta figura en la medida en la que su existencia puede ser recomendable incluso en organizaciones que sólo utilicen datos de nivel básico cuando el tamaño de la entidad y/o la importancia estratégica de la información aconsejen disponer de alguien que coordine la seguridad y garantice su adecuado funcionamiento.

### *3.3.e) Algunas políticas de seguridad.*

En este breve repaso por aspectos específicos relacionados con la seguridad se destacarán aspectos relativos a los flujos internos de información, el uso de Internet y las políticas relativas a la destrucción de soportes.

En primer lugar, debe tenerse en cuenta que al fijar las políticas de seguridad no siempre se tienen en cuenta los flujos internos a la organización. Como ya se señaló al exponer los ficheros temporales resulta esencial ejercer un verdadero control material sobre la información que se trata en una organización. En ocasiones, y debido al tamaño algunos centros de proceso de datos cuentan con unidades que elaboran y sirven explotaciones de datos a los departamentos que las requieren. Esto supone que la información del fichero se traslada a otro soporte, ya sea físico o lógico, no sujeto a los controles propios del sistema de información. Por tanto, resulta aconsejable fijar políticas que racionalicen estas explotaciones internas de datos y los envíos de datos entre personas y/o departamentos de la organización. En este sentido, puede resultar altamente aconsejable mantener un registro de este tipo de uso de los datos ya que contribuirá a mantener un control riguroso sobre los flujos internos de datos, a racionalizar estos flujos y a implementar cuando proceda la correspondiente seguridad. No debe olvidarse que el tratamiento de datos

se rige por el principio de finalidad y un recurso de este tipo también permite fijar con precisión que departamento puede acceder a los datos y para que usos concretos se encuentra autorizado.

En tercer lugar, el uso de internet constituye un elemento relevante a destacar. En un módulo anterior se estudió el conjunto de problemas que se asocian a la articulación de controles sobre el tráfico de las comunicaciones y el uso de recursos como navegadores y correo electrónico. Si existe algún bien jurídico que justifique el establecimiento de reglas y controles, aunque no necesariamente invasivos, este no es otro que la seguridad.

Debe tenerse en cuenta que el uso de internet puede estar en el origen de importantes fallos de seguridad. Así, la ejecución inadvertida de un virus o de archivos que incorporen spyware o malware puede poner en peligro el adecuado funcionamiento de los sistemas de información. Debe tenerse en cuenta que en muchas ocasiones la instalación de software de libre distribución incorpora como “precio” a su pretendida gratuidad la apertura de puertos, el acceso a información sobre contenidos y hábitos de los usuarios e incluso el uso de recursos de la máquina para tareas de computación distribuida. Por otra parte, el uso de programas peer to peer puede producir como consecuencia la apertura de carpetas con información estratégica a cualquier usuario en todo el planeta. Aunque lo cierto, es que ni siquiera es necesario buscar ejemplos sofisticados. Si, por ejemplo, en una administración de tamaño medio alto la mayor parte de los usuarios intercambian de modo indiscriminado los típicos mensajes de correo electrónico que incorporan un archivo powerpoint adjunto con alguna imagen o sonido idílicos, aparte del consabido riesgo de los virus, pueden imponer tal carga de trabajo a los servidores que acaben por

saturar y ralentizar la capacidad de proceso de los mismos constituyendo esto en si mismo un evidente riesgo para la seguridad.

Por todo ello, conviene implementar medidas técnicas como el empleo de antivirus y firewall, pero también establecer reglas de comportamiento para los usuarios. Por ello resultará esencial identificar las reglas de uso del correo electrónico de la organización y establecer reglas o prohibiciones en relación con:

- El uso de internet para tareas no relacionadas directamente con las funciones asignadas.
- La introducción de contenidos en la red corporativa y/o ordenador personal.
- El envío de correos masivos empleando la dirección de correo electrónico corporativa.
- La instalación de software no autorizado.

Por último, como colofón a este breve repaso a medidas de seguridad que pueden poseer una importancia específica cabe referirse al desechado y la reutilización de soportes, aunque sólo sea por tratarse de uno de los supuestos que ha dado lugar a la imposición de sanciones por infracción del deber de seguridad.

La gestión de soportes que contengan datos de carácter personal cubre todo el periodo de vida de los mismos incluida su reutilización. Por tanto, a lo largo del ciclo útil de cualquier soporte deberemos tener en cuenta tres etapas:

- Creación del soporte. Éste aloja datos y se anota en el correspondiente registro según se trate de un soporte integrado en el sistema o de un soporte que vaya a salir del mismo con destino

a un tercero ya sea con motivo de una comunicación de datos o de un encargo del tratamiento.

- Reutilización del soporte. En este caso el soporte causará baja en el documento de seguridad y, sólo si se va a utilizar de nuevo para contener nuevos datos personales, podría causar una nueva alta.
- Destrucción del soporte. En este caso causará baja en el documento de seguridad.

Tanto en el caso de reutilización del soporte como en el de desechado existen un conjunto de obligaciones formales y materiales que deben ser tenidas en cuenta y documentadas.

Cuando con motivo de su reutilización un soporte deje de contener datos de carácter personal vinculados a un fichero procederá a anotarse su baja en el documento de seguridad. Dicha anotación deberá ser realizada por el responsable al que se le hayan asignado tales tareas. Cuando, el soporte vaya a ser utilizado de nuevo para incorporar datos sujetos a la LOPD deberá realizarse una anotación inventariando y etiquetando el soporte con un nuevo número o identificador de referencia con el fin de evitar confusiones.

En la reutilización de los soportes se garantizará el borrado físico completo del soporte de manera que resulte imposible la recuperación de los datos. Así por ejemplo:

- Los CD-RW y los DVD-RW se borrarán utilizando la instrucción del grabador que permite un borrado completo. Nunca se utilizará en estos casos el borrado rápido.

- Las unidades de disco duro se borrarán mediante procedimientos que garanticen completamente el borrado de los datos. Debe advertirse que la instrucción “borrar” o “enviar a la papelera” no borra físicamente los datos de un disco duro. Ni siquiera formatear un disco duro garantiza plenamente la destrucción de los datos. Por ello, se recomienda el uso de algún programa de destrucción segura de datos<sup>16</sup>.
- Los PEN-drive, agendas electrónicas, y otros soportes equivalentes, capaces de almacenar información deberán ser borrados de modo que los datos resulten inaccesibles de acuerdo con el método más adecuado en cada caso.
- No se aconseja en ningún caso la reutilización del soporte papel impreso a una cara ya que resulta ineficiente y peligroso desde el punto de vista de la seguridad, salvo el caso en el que la segunda impresión afecte a datos contenidos en el fichero y se garantice la seguridad de igual modo. Sin embargo, esta posibilidad debe ser tenida por excepcional ya que la coincidencia debería ser plena alcanzando incluso al hecho de que el propio usuario estuviera autorizado a acceder a los datos contenidos en el soporte reutilizado.

Del mismo modo, cuando por su propia naturaleza, o por haber agotado el ciclo de vida útil, un soporte deba ser desechado, y por tanto, destruido, conviene adoptar precauciones como las siguientes:

- Si el soporte va a ser destruido por un tercero es recomendable proceder a su borrado en los términos que se han indicado arriba.

---

<sup>16</sup> Existen programas freeware como Eraser o SDelete, o la utilidad cipher del sistema operativo XP.

- En todo caso debería garantizarse la destrucción física del soporte. Es fundamental tener en cuenta que el desensamblaje de un equipo no supone su destrucción: debe inutilizarse completamente cualquier parte del mismo que contenga información.
- En ningún caso el depósito de un soporte en un contenedor de basuras o reciclaje equivale a su destrucción, salvo claro está cuando éste sea el de la empresa contratada al efecto.
- Los soportes como papel, CD, DVD, cinta analógica, etc. deben ser físicamente destruidos de modo que la información que contiene resulte completamente irrecuperable.
- Los lugares de almacenamiento previo a la destrucción deberán disponer de controles de acceso físico limitado exclusivamente a usuarios autorizados o estar protegidos mediante cerradura o sistema que permita acceder sólo a éstos.
- La destrucción de un soporte debe anotarse en el documento de seguridad causando baja en el inventario cuando el soporte sea susceptible de ser inventariado.
- Cuando se acuda a un tercero se deberá celebrar un contrato de acceso a los datos por cuenta de terceros y aquél deberá certificar la efectiva destrucción de los soportes.

Este conjunto de recomendaciones resultan esenciales ya que las organizaciones en muchas ocasiones no contemplan esta etapa final en la vida de un soporte incurriendo en los correspondientes riesgos.

### *3.3.f) La seguridad en ficheros no automatizados.*

Una de las principales aportaciones del RDLOPD consiste en la regulación por el Capítulo IV del Título VIII de las «medidas de seguridad aplicables a los ficheros y tratamientos no automatizados». Hasta este momento no existían más criterios que los aportados por la Agencia Española de Protección de Datos en sus resoluciones confirmados en su caso por la jurisprudencia de la Audiencia Nacional.

En primer lugar, es evidente que la obligación de seguridad la fija con carácter general el artículo 9 LOPD. Como se ha subrayado en distintas ocasiones a lo largo de este curso el objeto de protección de la LOPD se proyecta sobre la información personal contenida en todo tipo de soportes. Así, la información contenida en soporte papel, en una fotografía etc. se puede digitalizar o fotocopiar, puede ser objeto de apropiación por terceros existiendo accesos indebidos, pueden cometerse errores en su destrucción que deriven en una infracción del deber de secreto o pueden sufrir daños irreparables a consecuencia de no disponer de medidas antiincendio o previsiones para evitar inundaciones.

Por tanto, resulta evidente que incluso antes del nuevo Reglamento podían diseñarse, adoptarse e implementarse, medidas de seguridad sobre los soportes no automatizados. En este sentido, la carencia de una norma expresa no era excusa teniendo en cuenta que vivimos en una sociedad que durante cientos de años ha aprendido a organizar, ordenar y asegurar bibliotecas y archivos documentales existiendo además profesiones específicas en esta materia. De hecho la técnica del RDLOPD es muy sencilla en este campo. Por una parte, enumera un conjunto de medidas análogas a las dispuestas para los soportes automatizados y por otro

recoge aspectos muy específicos y propios de los soportes no automatizados.

Anteriormente se ha ofrecido un esquema de medidas de seguridad por lo que aquí únicamente se subrayarán los aspectos más sobresalientes. En primer lugar, deben destacarse algunas definiciones contenidas en el artículo 5 RDLOPD. En primer lugar, se ofrecen criterios para clasificar los sistemas de información en relación con el tipo de tratamiento. En este sentido se define como sistema de tratamiento el «modo en que se organiza o utiliza un sistema de información». Desde este punto de vista existirán sistemas de información automatizados, no automatizados o parcialmente automatizados.

Por otra parte, se define como documento «todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada». Tanto los datos como los documentos pueden ser contenidos en un soporte entendiéndose por tal 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».

Finalmente se define la transmisión de documentos como «cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo». Este conjunto de definiciones, aportan los elementos básicos para abordar la realidad de los ficheros no automatizados.

Considerando las concretas medidas de seguridad dispuestas, deben destacarse en el nivel básico dos de ellas. En primer lugar, el artículo 106 obliga a establecer criterios de archivo que o bien se basan en la

legislación aplicable<sup>17</sup> o bien, en caso de no existir se fijarán por el responsable del fichero. Tales criterios, señala el reglamento «deberán 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». Por tanto se tratamiento de criterios orientados a garantizar la disponibilidad de la información.

Por otra parte, el artículo 107 RDLOPD regula los dispositivos de almacenamiento exigiendo únicamente que estos cuenten con mecanismos que obstaculicen su apertura. Por tanto, se está exigiendo disponer de armarios, archivadores o cajoneras que cuenten con cerradura. Pese a lo poco exigente de la disposición se permite no adoptar tal medida, estableciendo y documentando otras alternativas, cuando las características físicas de los dispositivos no la permitan.

Por último, y aunque sea una obviedad, el artículo 108 RDLOPD obliga a fijar políticas para la custodia de la información cuando la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento «por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo». Se traslada, como es lógico, un deber de custodia al usuario autorizado que la utilice el cual

---

<sup>17</sup> Véase Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. Ley 10/2001, de 13 de julio, de Archivos y Documentos de la Generalitat de Cataluña. Ley 6/1986, de 28 de noviembre, de Archivos de Aragón. Ley 3/1990, de 22 de febrero, de Patrimonio Documental y Archivos de Canarias. Ley 6/1990, de 11 de abril, de Archivos y Patrimonio Documental de la Región de Murcia. Ley 4/1993, de 21 de abril, de Archivos y Patrimonio documental de la Comunidad de Madrid. Ley 4/1994, de 24 de mayo, de Archivos y Patrimonio documental de La Rioja. Ley 3/2002, de 28 de junio, de Archivos de Cantabria. Ley 19/2002, de 24 de octubre, de Archivos Públicos de Castilla-La Mancha. Ley 7/2004, de 22 de diciembre, de modificación de la Ley 6/1991, de 19 de abril, de Archivos y del Patrimonio Documental de Castilla y León. Ley 3/2005, de 15 de junio, de la Generalitat, de Archivos. Ley 15/2006, del 17 de octubre, de archivos y patrimonio documental de las Illes Balears. Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos. Ley 2/2007, de 12 de abril, de archivos y patrimonio documental de Extremadura.

deberá «custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada».

En el nivel medio únicamente se contienen dos previsiones, el nombramiento de uno o varios responsables de seguridad y la realización de la correspondiente auditoria bianual interna o externa sobre el cumplimiento.

En el nivel alto, en primer lugar, se fijan políticas específicas ordenadas a proteger la información en el ámbito físico. Si en el nivel básico se planteaba poco más o menos la existencia de armarios o archivadores con cerraduras, aquí el artículo 111 prevé que estos contenedores se ubiquen en áreas de acceso restringido. No obstante, «si atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento», no fuera posible cumplir esta medida, «el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad».

En segundo lugar, el artículo 112 obliga a fijar políticas de copia o reproducción que garanticen que la misma se realizará bajo el control del personal autorizado en el documento de seguridad y que existirán instrucciones claras que garanticen la destrucción de las copias o reproducciones desechadas.

También, se fijan obligaciones en el traslado de la documentación, artículo 114, consistentes en adoptar medidas dirigidas a impedir el acceso o manipulación de la información en caso de su traslado físico.

La medida más compleja en este ámbito es la fijación por el artículo 113 de un control de acceso. En primer lugar, el acceso a la documentación se limitará exclusivamente al personal autorizado.

Además, se ordena establecer «mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios». Por otra parte, debe existir un procedimiento para el acceso por parte de personas que no sean usuarios autorizados por el documento de seguridad, -como personal externo (encargados del tratamiento), autoridades en procesos de inspección, personas legitimadas para la consulta de la información etc.-, y un registro de accesos.

Aunque el conjunto de medidas previstas en este precepto resulte el más complejo se encuentra plenamente justificado. Debe recordarse que la regulación, como más arriba se señaló, restringe la aplicación de medidas de nivel al alto en el caso de datos personales contenidos en soportes no automatizados a los casos en los que estrictamente se traten datos de nivel alto, excluyendo tal nivel cuando el tratamiento de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual se incidental o accesorio y no relacionada con la finalidad del fichero.

Por otra parte, la fijación de un control de accesos requiere del uso de un cierto sentido común y admite muy diversas posibilidades que van desde un procedimiento de retirada de documentación que se anote informáticamente hasta una simple plantilla en la carpeta de la documentación.

#### ***4. El diseño de la seguridad: la auditoría.***

La última cuestión de la que se va a ocupar este breve examen de las distintas cuestiones relacionadas con la aplicación de las medidas de seguridad del Reglamento es la de su diseño e implementación. Para una adecuada aplicación de la norma puede resultar útil facilitar una mínima noción de las prácticas habituales en esta materia.

En primer lugar, debe tenerse en cuenta que el responsable del fichero puede enfrentarse a esta tarea con una cierta sensación de impotencia ya que debe tener en cuenta los múltiples factores que inciden en la seguridad. Así, entre otros, debe considerar aspectos como;

- La localización geográfica de los usuarios.
- La topología de la red de comunicaciones.
- Las instalaciones o salas donde residen los equipos físicos.
- El equipamiento físico que soporta el sistema de información.
- La configuración del equipamiento lógico básico.
- El tipo y estructura de las bases de datos.
- La forma de almacenamiento de los datos.
- El número y complejidad de los procesos a realizar.
- La cultura corporativa de la organización.

Por todo ello, sin el soporte de la dirección, la implantación de las medidas de seguridad es imposible. En este sentido la primera tarea a emprender consiste en convencer al equipo directivo de la entidad de la necesidad de aplicar políticas de seguridad y, aunque en el común de los casos, el argumento último va a ser la existencia de un régimen sancionador, debe incidirse en el conjunto de beneficios que va a obtener la organización referidos más arriba. En este sentido, la realidad demuestra que la concienciación de la dirección, y junto con ella de todo el personal, es un elemento esencial para que las políticas de seguridad sean efectivas.

Por ello existen un conjunto de ideas que deben transmitirse y que usualmente suelen proporcionar réditos importantes.

En primer lugar, debe subrayarse que la implementación de medidas de seguridad requiere ante todo el más elemental sentido común. La seguridad de la información en ningún caso tiene ni porque suponer una inversión desproporcionada o inasumible y ante todo debe basarse en criterios de coste y efectividad. Existen soluciones que pueden resolver el problema de una PYME perfectamente adaptadas a sus necesidades. Dicho de un modo sencillo, si bien un farmacéutico y un hospital tratan ficheros de nivel alto esto no significa que sus costes vayan a ser idénticos.

El analista que diseña e implementa la seguridad debe tener en cuenta la realidad material y ser consciente que no siempre existen soluciones universales, se trata siempre de un diseño ajustado, razonable y proporcional a las necesidades. Por otra parte, y en relación con la concienciación debe alertarse sobre el hecho de que la seguridad es un proceso que se retroalimenta con la experiencia y exige una reevaluación constante. Por tanto, el cumplimiento del RDLOPD no se agota con la redacción y aplicación del primer documento de seguridad, abarca todo el ciclo vital del sistema de información.

En segundo lugar, debe tenerse en cuenta que la implementación de medidas de seguridad no puede limitarse ni a una aplicación lineal de lo dispuesto por el RDLOPD ni proyectarse únicamente sobre los activos que contengan datos personales. La seguridad de los sistemas de información se orienta a proteger un bien valioso, la información, y se proyecta sobre ésta sea no un dato de carácter personal. Por ello, se requiere un enfoque

global que abarque las distintas áreas y a la vez integradora abarcando todos los factores humanos y tecnológicos afectados.

Normalmente el diseño de la seguridad de un sistema de información debe comenzar con un análisis de riesgos. Lo habitual es utilizar lo que se denomina el enfoque PDCA (Plan, Do, Check, Act) utilizado habitualmente en procesos de calidad. Este método se basa en cuatro etapas:

- Planificar las acciones.
- Implementar las políticas diseñadas en la fase de planificación
- Verificar la consecución de los objetivos propuestos.
- Aprovechar la información obtenida generando procesos de retroalimentación que sirvan para mejorar la planificación.

En la práctica, este enfoque, y cualquier otro método, requieren en una primera etapa la aplicación de un mínimo sentido común. En todos los métodos de implementación de la seguridad existen elementos comunes:

- Análisis de riesgos. Resulta evidente que la seguridad no puede consistir en una aplicación mecánica de los criterios normativos. Hay que conocer los riesgos y vulnerabilidades concretas de una organización para diseñar las medidas más adecuadas.
- La legalidad vigente constituye el marco de referencia, el objetivo mínimo a alcanzar. No obstante, existirán casos en los que los requerimientos de la organización sean superiores al mínimo normativo exigible.

- Debe partirse de un análisis del estado real de los sistemas no puede actuarse, como se acaba de indicar, desde una aproximación puramente teórica, desde una aplicación puramente lineal del RDLOPD.
- En relación con lo anterior, resulta indispensable disponer de un marco de referencia básico que permita identificar de modo sencillo y preliminar aspectos como:
  - ✘ La tipología de los datos y los niveles de seguridad que les correspondan.
  - ✘ Los requerimientos para el cumplimiento del RDLOPD.
  - ✘ Las medidas existentes.
  - ✘ Las medidas necesarias.
- La elección entre la aplicación de métodos estandarizados o el diseño de los propios de la organización va a depender de las necesidades y/o capacidades de la misma. No siempre las soluciones comerciales son las mejores. En ocasiones, cuando existan necesidades específicas deberán desarrollarse metodologías propias.
- Todos los métodos culminan con la definición de las políticas exigibles en todos los niveles:
  - ✘ Físico (catástrofes y seguridad en los accesos)
  - ✘ Personal (usuarios de los sistemas)
  - ✘ Informático (adquisición de aplicaciones, renovación de las existentes etc.)

- En cualquiera de las metodologías posibles la retroalimentación constituye un elemento esencial. La seguridad es un proceso dinámico que se enriquece con la experiencia. El registro de incidencias o la realización de las auditorías poseen un valor esencial más allá de las auditorías: renovar y mejorar constantemente la seguridad.

Por otra parte, el artículo 96 RDLOPD impone la obligación de auditar los sistemas de información con un nivel medio de seguridad, o superior, cada dos años. En concreto el precepto dispone:

«Artículo 96. Auditoría.

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente Título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas».

El nuevo Reglamento sólo ha planteado una novedad sustancial, la previsión de una auditoría extraordinaria cuando se produzcan cambios sustanciales que afecten a la seguridad.

En la práctica el inicio de las tareas de adaptación a la LOPD y al Reglamento de medidas de seguridad inicia con lo que en la jerga de los

consultores se denomina unas veces preauditoria, en otras ocasiones auditoria LOPD, y que en todo caso se acerca extraordinariamente a aquello que exige el RDLOPD. Por tanto, el cumplimiento de este precepto constituye siempre un adecuado punto de partida.

La extensión de estos materiales, impide entrar en mayores consideraciones sobre la naturaleza y las técnicas de la auditoria de protección de datos aunque se ofrecen en la bibliografía final algunas referencias interesantes al respecto.

En cualquier caso, se ha criticado la indefinición de los perfiles profesionales que deberían realizarla e incluso la posibilidad de realizar una auditoria interna. Baste aquí con subrayar que nada impide la fijación de mecanismos que garanticen la independencia cuando la auditoria es interna a condición de que el tamaño de la organización permita que el auditor no tenga ninguna relación con el sistema auditado, en especial cuando esta suponga responsabilidad con la propia seguridad.

Si bien es cierto que la auditoria externa genera costes, no lo es menos que en su desarrollo se produce lo que podríamos denominar como el «respeto a lo foráneo». Por otra parte, los auditores externos deberían incorporar un alto nivel de conocimientos y especialización así como un considerable bagaje experiencial. No obstante, ello no exime a la organización que contrata un auditor externo de la necesidad de disponer de puestos de trabajo en la materia o atribuir responsabilidades adicionales al personal.

Por otra parte, la auditoria interna puede comportar un cierto ahorro de costes, dinamizar la cultura interna en materia de protección de datos y fomentar la adquisición de Know How.

Se escoja uno u otro método, lo que parece indudable es la necesidad de auditar la seguridad de los sistemas con regularidad.

### **5. Consideraciones finales.**

Como se ha podido apreciar a lo largo de esta exposición el estudio del Reglamento de medidas de seguridad obliga a ir más allá de lo puramente jurídico. En este sentido, cualquier enfoque de esta materia obliga a los no juristas a transitar territorios ajenos al Derecho como el estado de la tecnología, a la adquisición de algunas nociones técnicas al menos a nivel básico y al conocimiento siquiera en un plano cultural de la existencia de estándares y metodologías aplicables.

Por otra parte, en la praxis aplicativa cotidiana no resulta infrecuente toparse con algunos mitos sobre la LOPD y la seguridad. El primero de ellos es la común afirmación de que en el reglamento las medidas de seguridad constituyen objetivos inalcanzables tal y como se plantean. En la misma línea se afirma que tales medidas resultan imposibles de implantar o que los usuarios son incapaces de aplicarlas debido a su dificultad técnica. Por otra parte, suele creerse que los costes que provocan son inasumibles o excesivos.

Sin embargo, y como se ha expuesto a lo largo de estos materiales muchas veces se logra un razonable nivel de seguridad simplemente aplicando el sentido común. Por otra parte, un correcto análisis de los riesgos acompañado de una adecuada ponderación de la relación coste-eficacia de las medidas a implementar suele facilitar la implementación de la seguridad. Hasta el punto que en la práctica el planteamiento debería ser el contrario ya que mayor inversión no equivale a mayor seguridad.

Por otra parte, se suele creer que si se aplica el RDLOPD, y también ocurre con la LOPD, el funcionamiento de la organización se verá

perjudicado o imposibilitado. Sin embargo, lo cierto es que la seguridad es instrumental a las necesidades de la organización a sus características, a sus vulnerabilidades. De hecho, va ser el soporte necesario para garantizar la continuidad y el funcionamiento normal de los procesos de gestión soportados por TIC. Además, y como se ha reiterado hasta la saciedad contribuye a ordenar los flujos de información y racionalizar el modo de obtenerla, tratarla, producirla y utilizarla.

Por último, no debe olvidarse que la seguridad no sólo constituye una obligación normativa sino que en general se proyecta como un requisito indispensable para el adecuado funcionamiento de las tecnologías de la información y las comunicaciones y elemento esencial para certificar su calidad.

## **Referencias.**

### **Bibliografía.**

ÁLVAREZ MARAÑÓN, GONZALO. *Seguridad informática para empresas y particulares*. Mc Graw Hill, Madrid, 2004.

FERNÁNDEZ-MEDINA PATÓN EDUARDO, MOYA QUILES ROBERTO, PIATTINI VELTHUIS, MARIO GERARDO. *Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada*. AENOR, Madrid, 2003.

MARZO PORTERA ANA, MACHO-QUEVEDO PÉREZ-VICTORIA ALEJANDRO. *La auditoria de de seguridad en la protección de datos de carácter personal*. Ediciones Experiencia, Barcelona, 2004.

VELASCO DOBAÑO J, VELASCO MASSIP, L. *Auditoria de la protección de datos*. Bosch, Barcelona, 2005.

### **Estándares y recomendaciones.**

Administración Pública Estatal, método MAGERIT de análisis y gestión de riesgos <http://www.map.es/csi>.

Arreglo sobre el reconocimiento de los Certificados de Criterios Comunes en el campo de la seguridad de las tecnologías de la información de 23 de mayo de 2000 (Comisión Europea EE. UU., Canadá) <http://www.commoncriteria.org>

Norma UNE 71502. Especificaciones para los sistemas de gestión de la seguridad de la información.

Norma UNE-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información.

Recomendación de la OCDE relativa a las directrices para la seguridad de sistemas y redes de información – hacia una cultura de seguridad. (Adoptada por el Consejo en su Sesión 1037 de 25 de Julio de 2002). [http://www.csi.map.es/csi/pdf/ocde\\_directrices\\_esp.pdf](http://www.csi.map.es/csi/pdf/ocde_directrices_esp.pdf).

### **Recursos.**

Agencia de Protección de Datos de la Comunidad de Madrid. Documento de seguridad de nivel básico.

[http://www.madrid.org/comun/org\\_apd/0,3575,97778857\\_52885713\\_110812884\\_12126735,00.html](http://www.madrid.org/comun/org_apd/0,3575,97778857_52885713_110812884_12126735,00.html)

Agencia de Protección de Datos de la Comunidad de Madrid. Documento de seguridad de nivel medio.

[http://www.madrid.org/comun/org\\_apd/0,3575,97778857\\_52885713\\_110812884\\_12126737,00.html](http://www.madrid.org/comun/org_apd/0,3575,97778857_52885713_110812884_12126737,00.html)

Agencia de Protección de Datos de la Comunidad de Madrid. Documento de seguridad de nivel alto.

[http://www.madrid.org/comun/org\\_apd/0,3575,97778857\\_52885713\\_110812884\\_12126739,00.html](http://www.madrid.org/comun/org_apd/0,3575,97778857_52885713_110812884_12126739,00.html)

Agencia Española de Protección de Datos. Guía documento de seguridad.  
<https://www.agpd.es/index.php?idSeccion=457>.

LANDWELL ABOGADOS. *Actos desleales de trabajadores usando sistemas informáticos e internet.*

[http://www.landwellglobal.com/es/esp/sp\\_downloads/inf\\_actos\\_desleales.pdf](http://www.landwellglobal.com/es/esp/sp_downloads/inf_actos_desleales.pdf).

Pricewaterhouse @ Coopers. 10 preguntas claves sobre seguridad.  
<http://www.pwc.com/extweb/service.nsf/docid/C44AFD37CFEA6DD985256EB00057D3A1>.

Red Temática Iberoamericana de Criptografía y Seguridad  
<http://www.criptored.upm.es/paginas/docencia.htm#gteoria>.