

La regulación de la auditoría en el Proyecto de Real Decreto de desarrollo de la LOPD

Mar Martínez

Dimecres, 20 de juny 2007

1. INTRODUCCIÓN

El Ministerio de Justicia ha iniciado el trámite de información pública del Proyecto de Real Decreto 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. Una vez sea aprobado, este texto establecerá, entre otras previsiones, las medidas de seguridad que deberán aplicarse a los tratamientos de datos de carácter personal, **automatizados o no**, en desarrollo del artículo 9 de la citada Ley Orgánica (en adelante, LOPD).

Cuando se apruebe y entre en vigor, este Real Decreto derogará, entre otras normas, el vigente Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad para ficheros automatizados que contengan datos de carácter personal (en adelante, RD 994/99), que hasta ahora ha desarrollado reglamentariamente el principio de seguridad establecido por la LOPD).

Por todo ello, cualquier modificación en el marco jurídico aplicable a la protección de datos personales, como es el caso del futuro Real Decreto, implica un impacto importante en la aplicación de la gestión de las auditorías previstas en el actual Art. 17 de RD 994/99.

En consecuencia, teniendo en cuenta el avanzado estado de desarrollo del futuro texto, se ha considerado oportuno realizar un resumen de aquellas cuestiones que pudieran incidir en la gestión de las auditorías, todo ello teniendo en cuenta las previsiones que contiene el texto hecho público por el Ministerio de Justicia en su versión de fecha 30 de abril de 2007.

En la exposición de motivos se cita el Título VIII, que regula el principio de seguridad, como un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluído distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 motor de la aplicación de auditorías permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la

regulación. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del **documento de seguridad**. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y **no automatizados**.

2. ALCANCE Y OBJETIVOS

Se pretende que este artículo de la ponencia impartida en la Agencia Catalana de Protección de Datos el pasado día 20 de junio, contenga los aspectos más importantes que se desprenden del análisis del Proyecto de Real Decreto por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, el Proyecto), en relación con los tratamientos de datos personales realizados en el ámbito de la LOPD y con especial incidencia en lo relativo al principio de seguridad previsto en su Art. 9. Se ha prestado, asimismo, particular atención en identificar los aspectos que podrían suponer un cambio con respecto a lo dispuesto por el vigente RD 994/99.

3. CONSIDERACIONES GENERALES

- Este artículo se realiza y refiere al texto del PROYECTO DE REAL DECRETO 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, hecho público por la Secretaria General Técnica del Ministerio de Justicia en su versión de 30 de abril de 2007.
- El Proyecto de Real Decreto integra en un único texto :
 - El Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de regulación del Tratamiento automatizado de los datos de carácter Personal;
 - El Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos personales, aprobado por Real Decreto 994/1999, de 11 de junio, excepto los artículos 4.4, 17, 18, 19 y 20 que seguirán siendo de aplicación a los ficheros automatizados que existieran en la fecha de entrada en vigor del presente Real Decreto cuando los mismos estuvieran incluidos en el anterior Art. 4.4. Estos preceptos quedan derogados en el plazo de un año desde la entrada en vigor del presente Real Decreto.

- Competencias sancionadoras de la Agencia Española de Protección de Datos atribuidas en la Ley 34/2002, de 11 de julio de Servicios de la sociedad de la información y de comercio electrónico y de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

4. ESTRUCTURA DEL REGLAMENTO

Títulos I – Disposiciones generales

Fija el objeto y ámbito de aplicación, definiciones y cómputos de plazos.

Título II – Principios de protección de datos

Principios de calidad, consentimiento, deber de información y encargado del tratamiento.

Título III – Derechos ARCO

Derechos de las personas (acceso, rectificación, cancelación y oposición)

Título IV – Disposiciones aplicables a ficheros titularidad privada

Solvencia patrimonial y crédito; actividades de publicidad y prospección comercial

Título V – Obligaciones previas al tratamiento

Disposiciones creación ficheros

Notificación e inscripción. Colaboración Autoridades Autonómicas

Título VI – Transferencias internacionales

Disposiciones generales, trasferencias a países con niveles adecuados y no adecuado

Título VII – Códigos tipo

Consideraciones sobre los códigos tipo

Título VIII – Medidas de seguridad en el tratamiento

Reformulación del RMS, incluyendo ficheros y tratamientos no automatizados (capítulo III)

Título IX – Procedimientos tramitados por la AEPD

Tutela de los derechos ARCO, potestad sancionadora, inscripción de ficheros y códigos tipo, transferencias internacionales y otros.

5. RESUMEN NUEVAS OBLIGACIONES SEGURIDAD

A continuación, se especifican los aspectos que podrían incidir en los Responsables de Ficheros una vez que el Proyecto entrase en vigor.

A) MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

Se definen las medidas de seguridad a aplicar a tratamientos no automatizados, de gran incidencia en la Administración Pública (expedientes administrativos, inspección, expedientes policiales, historias clínicas, procedimientos judiciales, etc.).

- Elaboración de Documentos de Seguridad (DS) para los tratamientos no automatizados, del mismo modo que en la actualidad se hace para los tratamientos automatizados; Con el nuevo texto será posible tener un único documento de seguridad que incluya cualquier tipo de organización de la información (manual, informatizada o mixta)
- Elaboración, implantación y difusión de procedimientos de:
 - Tratamiento y acceso a la documentación, y custodia de la misma
 - Notificación y gestión de incidencias
- Asignación de autorizaciones y responsabilidades: por ejemplo, en relación con:
 - La aprobación o negación de acceso a los documentos
 - El mantenimiento del registro de incidencias
 - Nombramiento de responsables de seguridad
- Gestión de todos los mecanismos que limiten accesos no autorizados: archivadores o armarios con llave, reubicación de la documentación en zonas de acceso restringido o que estén bajo vigilancia permanente (requerido para datos de nivel alto), etc.;
- Gestión de procedimientos de destrucción de documentos, e inventario de las instalaciones de mecanismos al efecto: trituradoras de papel, contratación de servicios especializados, etc.;
- Ejecución de auditorías bianuales obligatorias (como se viene haciendo para ficheros automatizados), para datos de nivel medio o alto

- Para datos de nivel alto (entre los que se incluye la información sobre la salud de personas), deben identificarse los accesos realizados a los documentos, para lo cual puede ser recomendable implantar un libro de control de accesos a la documentación. Este podría ser a su vez informatizado.

B) SE ESTABLECEN NUEVAS PREVISIONES EN RELACION CON LA FIGURA DE ENCARGADO DE TRATAMIENTO:

- Gestión y control por parte del Responsable de las garantías que debe reunir el encargado (terceras empresas con acceso a datos personales) del tratamiento.
- Se gestionará la solicitud para obtener autorización para realizar transferencias internacionales de datos (lo que se requiere cuando un suministrador pretende prestar servicios desde determinados países);
- Incluir estos compromisos del cumplimiento de los requisitos aplicables, haciendo constar la existencia de encargados en el Documento de Seguridad;

C) SE DEFINEN NUEVOS CONCEPTOS:

Se define el concepto de “Persona identificable” a semejanza con la definición utilizada en la Directiva 95/46/CE. A su vez se define “Dato disociado” como aquél que no permite la identificación de un afectado o interesado.

D) SE DEBERÁ ACREDITAR EL CUMPLIMIENTO DEL DEBER DE INFORMACIÓN

Para poder cumplir con esta previsión se deberá poder gestionar las evidencias conservando el soporte en el que conste el cumplimiento del deber de información. Estas nuevas obligaciones requerirán la gestión e inventario de conservación de carteles, impresos, formularios, grabaciones / locuciones, etc., lo que podrá realizarse por medios informáticos.

- Asimismo, aunque ya existía un criterio unánime en relación con la conservación de la prueba respecto del principio de consentimiento (cuando sea exigible), se aventura el texto actual a recomendar, en particular, la utilización de una tecnología, en este caso el escaneado de la documentación en soporte papel, siempre y cuando

“se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales “.

En este sentido, hay que hacer la consideración que para poder afirmar que existe esa garantía, sería necesario implantar mecanismos de firma digital y cifrado del resultado del escaneado. La implantación de estos mecanismos puede suponer nuevas inversiones para los responsables y mas teniendo en cuenta que esta previsión aplica a los ficheros desde su nivel básico.

Estos últimos son mecanismos de seguridad que no se están aplicando, de forma generalizada, en la práctica del escaneado. En la actualidad, la forma mas común informatizada de almacenar y conservar las evidencias para posteriormente poder acreditar el derecho de información y consentimiento, es aquella que utiliza las técnicas de escaneado convencional sin aplicar mecanismos de seguridad al resultado obtenido, lo que implica, que no se pueda garantizar la seguridad jurídica de los documentos obtenidos en relación con su integridad como se exige con el nuevo texto del reglamento.

F) SE PODRÁ NOTIFICAR EN UN MISMO FICHERO TRATAMIENTOS AUTOMATIZADOS JUNTO A OTROS NO AUTOMATIZADOS

Se establece de forma reglamentaria la previsión que ya en este momento se acepta con el modelo simplificado de declaración de ficheros de la Agencia Española de Protección de Datos. De esta forma queda perfectamente establecida la obligación de notificar los tratamientos manuales a los efectos de su inscripción en los Registros de las autoridades de protección de datos.

En este sentido, se podría haber utilizado el reglamento para lo contrario, es decir, excepcionar de obligación formal de notificar los ficheros manuales a aquellos responsables que ya tuvieran inscritos sus datos identificativos para ficheros informatizados, toda vez que en ningún caso, con esta previsión se estaría mermando o reduciendo ninguno de los derechos de los ciudadanos. Recordemos que en muchos países de nuestro entorno, y de conformidad con la Directiva, los Estados miembros podrán excepcionar de la obligación formal de notificar su ficheros a las autoridades correspondientes. Asimismo, habría que tener en consideración que el propio texto de la LOPD en su artículo 26 *Notificación e inscripción Registral* en varios de sus apartados utiliza únicamente el término “fichero informatizado”.

G) ASPECTOS RELATIVOS A LA TRAMITACIÓN DE DISPOSICIONES DE CREACIÓN, MODIFICACIÓN O SUPRESIÓN DE FICHEROS RESPECTO DE LA ENTRADA EN VIGOR Y LOS PLAZOS ESTABLECIDOS EN EL PERIODO TRANSITORIO

PERIODO TRANSITORIO FICHEROS DE TITULARIDAD PÚBLICA

El Proyecto plantea un plazo transitorio para la adecuación de los ficheros preexistentes, indicando que dicho plazo solamente resultaría aplicable a los tratamientos inscritos antes de la fecha de entrada en vigor. Esta previsión es muy clara para los ficheros de titularidad privada. Pero en el caso de los ficheros de titularidad pública antes de su notificación es obligatoria la tramitación de un acuerdo de creación del fichero. Como es bien conocido por todos, estos trámites tienen unos plazos y fases en su tramitación que en algunos Organismos puede llegar a varios meses.

Por lo tanto, sería necesario establecer alguna previsión singular para aquellas disposiciones que crearan ficheros y a la entrada en vigor del Reglamento se encontraran en alguna fase de la tramitación del correspondiente procedimiento de creación del fichero.

Disposiciones Transitorias.

Segunda. Plazos de implantación de las medidas de seguridad.

3. Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente Reglamento deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Por ello, **sería deseable que el plazo transitorio se hiciera extensible para el caso de las Administraciones Públicas a los ficheros que, en el momento de aprobación del Proyecto, estén en fase de tramitación**, ya que la obligación de aplicar a los mismos el nuevo Reglamento desde el primer momento podría implicar la necesidad de suspender el trámite de creación con objeto de proceder a su adaptación. Ello podría significar que en ciertos casos se retrasaría la puesta en marcha de prestación de nuevos servicios a los ciudadanos.

En este mismo sentido, sería recomendable **acelerar cuanto sea posible la creación de los ficheros de datos personales que estén previstas para los próximos meses**, a fin de que la adecuación de los ficheros correspondientes pueda beneficiarse del plazo transitorio otorgado por el nuevo Reglamento.

G) GESTIÓN DE DELEGACIONES

Verificación con alertas de la posibilidad de que el responsable de tratamiento delegue en las personas que estime oportunas la concesión de autorizaciones, en los supuestos que se indica la obligación de recabar autorización por parte de dicho responsable. En ese caso, sería necesario hacer constar en el Documento de Seguridad quiénes son las personas en quienes se delega.

6. NUEVAS DEFINICIONES

- ✓ **Documentación:** todo escrito, señal, gráfico, sonido, dibujo, película, fotografía, cinta magnética, cinta mecanográfica, cassette, disco, CD-Rom, DVD, dispositivos externos de almacenamiento u otro medio físico en el que se haya registrado información.
- ✓ **Ficheros temporales:** 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.
- ✓ **Perfil de usuario:** accesos autorizados a un grupo de usuarios.
- ✓ **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
- ✓ **Transmisión de documentos:** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
- ✓ **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos. **Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.**

7. NIVELES DE SEGURIDAD

- Se mantienen los 3 niveles de seguridad:
 - **BASICO**
 - **MEDIO**
 - **ALTO**

- En general, **se mantienen todas las medidas exigidas anteriormente**, pasando algunas a exigirse en un nivel inferior o excepcionando ciertas medidas de nivel alto, **se añaden nuevas** medidas de seguridad.
- Se incluyen medidas de seguridad específicas para los **ficheros no automatizados** (capítulo IV del Título VIII)

NIVEL MEDIO incluyen:

- ✓ Los relativos a la comisión de infracciones administrativas o penales.
- ✓ Los relativos a solvencia patrimonial y el crédito (art. 29 Ley 15/1999).
- ✓ Aquellos de los que sean responsables:
 - Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.
 - Las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
 - Las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias en materia de recaudación. (NEW)
- ✓ 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.

- **NIVEL ALTO incluyen:**

- ✓ Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- ✓ Datos recabados para fines policiales sin consentimiento de las personas afectadas.
- ✓ Datos derivados de actos de violencia de género.(NEW)
- ✓ Aquéllos 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. (NEW)

NUEVO

- Se excluyen de **NIVEL ALTO** y pasan a **BÁSICO**:
 - ✓ Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando:
 - a) 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 accesorio se contengan aquellos datos sin guardar relación con su finalidad.
 - ✓ Relativos a la salud, sobre el grado de discapacidad o declaración de la dicha condición, con motivo del cumplimiento de deberes públicos.
 - ✓ Cuando en un SI existan ficheros o tratamiento que requieran la aplicación de mas de un nivel de seguridad podrán segregarse las medidas a aplicar (esta circunstancia deberá quedar reflejada en el DS)

8. ENCARGADO DE TRATAMIENTO (art. 80) (NUEVO)

- ✓ Cuando se preste servicios **en los locales del responsable** será necesario un compromiso de confidencial del personal bajo la autoridad del encargado de tratamiento. Asimismo se hará constar las circunstancias del servicio en el DS del responsable
- ✓ Cuando el **acceso sea remoto** (se prohibirá que el encargado incorpore los datos a su sistema). Deberá constar este hecho en el DS y el personal con acceso externo deberá cumplir, además de las medidas recogidas en el documento del encargado, las medidas de seguridad complementarias del Responsable.
- ✓ Si el servicio fuera prestado **en los propios locales del ET** deberá elaborar un DS o completar el existente, identificando el fichero y el responsable e incorporará las medidas de seguridad particulares para cada fichero
- ✓ Si existiera prestación de servicios **sin acceso a datos personales**, el responsable adoptará las medidas adecuadas para limitar el acceso a los datos, soportes o recursos. Deberá constar en el contrato la prohibición de tal acceso y la obligación del secreto en caso de conocer datos con motivo de la prestación del servicio

9. ENCARGADO DE TRATAMIENTO (NUEVO)

- ✓ El Responsable del tratamiento deberá velar por que el Encargado reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento (Art.17.2)
- ✓ El encargado no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél. (Art. 17.3)

10. DELEGACIÓN DE AUTORIZACIONES

- ✓ Las autorizaciones previstas en el Título VIII atribuidas al responsable del fichero o tratamiento **podrán ser delegadas** en las personas designadas al efecto
- ✓ En el DS deberán constar las **personas habilitadas para otorgar** estas autorizaciones así como aquellas en las que recae dicha delegación.
- ✓ **En ningún caso esta designación supone una delegación de la responsabilidad** que corresponde al responsable del fichero

11. DOCUMENTO DE SEGURIDAD

- ✓ único y comprensivo de todos los ficheros o tratamientos
- ✓ individualizado por fichero o tratamiento
- ✓ Podrán elaborarse distintos DS según el sistema de tratamiento **utilizado para su organización (manual, mixto o automáticos)**
- ✓ O bien atendiendo a criterios organizativos del responsable

Documento de Seguridad NIVEL BASICO (Nuevo)

- Medidas a adoptar para el transporte de soportes y documentos.
- Funciones de control o autorizaciones delegadas.
- Medidas de seguridad para ficheros o tratamientos no automatizados.
- Tratamientos por cuenta de terceros.
- Autorización de los tratamientos fuera de los locales o almacenados en dispositivos portátiles para usuarios/perfiles y por un periodo de validez.
- Medidas a adoptar en caso de reutilización o desecho de soportes. **Anteriormente se exigían a partir del Nivel Medio.**

Documento de Seguridad NIVEL MEDIO (Nuevo)

- ✓ Cuando exista un tratamiento de datos por cuenta de terceros deberá identificarse los ficheros o tratamientos que se traten con referencia expresa al contrato o documento que regule las condiciones del encargo, la identificación del *responsable (sic.)* y periodo de vigencia del encargo
- ✓ Cuando el fichero se incorpore y trate de modo exclusivo en los sistemas del encargado, el responsable deberá anotar en su DS. Podrá delegarse en el encargado la llevanza del documento de seguridad (salvo lo relativo a las funciones propias o medidas relativas a recursos propios). Este hecho se indicará de modo expreso en el contrato Art. 12 LOPD

12. Funciones y Obligaciones del Personal (Nuevo)

- También se definirán las funciones de control o autorizaciones delegadas

13. Identificación y Autenticación (Nuevo)

- Mecanismos basados en certificados digitales
- Reconocimiento de datos biométricos
- Criterios de accesos.
- Procedimientos de asignación y gestión de contraseñas

- Periodicidad máximo sin cambiar **un año**
- Almacenamiento ininteligible de contraseñas activas
- Mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. **Anteriormente se exigía a partir del nivel medio.**
- Límite de intentos reiterados de acceso no autorizado. **Anteriormente se exigía a partir del nivel medio.**
- El personal ajeno al responsable estará sujeto a las mismas obligaciones que el personal propio

14. Gestión de Soportes (Nuevo)

Gestión de soportes Nivel Básico

- Se exceptúan cuando las características físicas de los soportes imposibiliten su cumplimiento
- Se consideran salidas los adjuntos en correos electrónicos
- En el traslado de la *documentación* se adoptarán las medidas para evitar la sustracción
- Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. **Anteriormente se exigía a partir del nivel medio.**
- Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. **Anteriormente se exigía a partir del nivel medio.**

Gestión de Soportes Nivel Alto

- Sistema de etiquetado que dificulte la identificación del contenido para personas no autorizadas.
- Otros mecanismos que garanticen que la información no sea accesible (*antes inteligible*)
- Cifrado de dispositivos portátiles fuera de las instalaciones. En los casos de dispositivos que no permitan cifrados se hará constar motivadamente en el DS

15. Copias de Respaldo (Nuevo)

- Verificación semestral de los procedimientos de copia y recuperación. **Nivel Básico**
- utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación **Nivel Alto**

16. Responsable de Seguridad

- La designación podrá ser única para todos los ficheros o diferenciada según los *sistemas de tratamiento* utilizados

17. Pruebas con Datos Reales

- Desaparece del texto “Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado”. Anteriormente aparecía en el Nivel Medio, deduciéndose de esta variación que en cualquier caso es necesario incluir medidas de seguridad cuando se este tratando datos personales. **No se hace mención como en el anterior reglamento**

18. Auditoria

- Al menos cada dos años, interna o externa que verifique el cumplimiento del presente Título
- Informe de auditoria adecuación de las medidas y **controles a la Ley** y desarrollo reglamentario **(Nuevo)**
- Deficiencias y propuestas correctoras.
- Análisis del responsable de seguridad y conclusiones al responsable del fichero,
- Adopción de las medidas correctoras adecuadas
- Con carácter extraordinario deberá realizarse dicha auditoria siempre que se realicen modificaciones que afecten en el cumplimiento de las medidas de seguridad .Esta auditoria inicia el cómputo de dos años **(Nuevo)**

19. REGISTRO DE ACCESOS

- Cuando se garantice que únicamente el responsable del fichero o del tratamiento tiene acceso y el Responsable sea una persona física, se exime de las obligaciones previstas a los efectos del registro de accesos. **(Nuevo)**

20. FICHEROS MANUALES (NUEVO)

OBLIGACIONES COMUNES

Aplica lo dispuesto para ficheros automatizados en lo relativo a:

- a) Niveles de seguridad
 - a) Alcance
 - b) Encargado del tratamiento.
 - c) Prestaciones de servicios sin accesos a datos personales.
 - d) Delegación de autorizaciones.
 - e) Régimen de trabajo fuera de los locales.
 - f) Copias de trabajo de documentos.
 - g) Documento de seguridad.
 - h) Funciones y obligaciones del personal.
 - i) Registro de incidencias.
 - j) Control de acceso.
 - k) Gestión de soportes.

NIVEL BÁSICO

- Criterios de Archivo
 - Archivado sujeto a los criterios previstos en su respectiva legislación.
Garantizar correcta conservación

(Si no existiera, el responsable del fichero establecerá los criterios)

- Debe posibilitar localización, consulta y derechos ARCO.

- Almacenamiento y custodia
 - Necesidad de mecanismos que obstaculicen el acceso a personas no autorizadas.
 - Deber de custodiar e impedir acceso a documentación mientras que esté en uso por la persona que esté a cargo.

NIVEL MEDIO

- Necesidad de la figura del Responsable de Seguridad
- Auditoría bianual que verifique el cumplimiento del *presente Título...*

NIVEL ALTO

- Almacenamiento
 - Armarios, archivadores, etc. deberán encontrarse en áreas cerradas. Si no fuera posible, se adoptarán medidas alternativas que se incluirán en el DS
- Copia o reproducción
 - Sólo bajo control del personal autorizado en el Documento de Seguridad. Deberán destruirse de forma segura cuando se desechen
- Acceso a la documentación
 - Exclusivamente por el personal autorizado
 - Mecanismos que permitan identificar los accesos realizados
 - Registro de accesos del personal no autorizado
- Traslado
 - Medidas que impidan acceso o manipulación en los traslados

21. DISPOSICIONES ADICIONALES

- Los productos de software que traten datos personales deberán indicar el nivel de seguridad (básico, medio, alto) que proporcionan.

- Plazos de implantación y adaptación:
 - Ficheros automatizados existentes 1 año, excepto para:
 - las de nivel alto referentes a violencia de género y tráfico de operadoras de telecomunicaciones, 18 meses.
 - Ficheros no automatizados existentes:
 - Básico: 1 año
 - Medio: 18 meses
 - Alto: 2 años
 - Ficheros creados con posterioridad a la entrada en vigor, cumplirán las medidas desde el momento de su creación.