



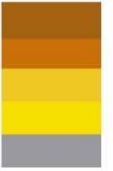
La seguridad digital del futuro, hoy

* [Normativa vigente en materia de Protección de
Datos Personales – Nuevos Retos]

Tudela, 8 de Abril de 2008



Ley Orgánica 15/1999



➤ Objeto de la LOPD

- Ficheros públicos

- Ficheros privados

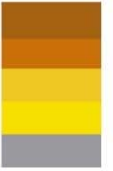
Que contengan datos de carácter personal.

Ley Orgánica 15/1999



- Excepciones a la aplicación de la LOPD
 - ✓ Ficheros utilizados para actividades personales o domésticas.
 - ✓ Ficheros sometidos a normativa sobre protección de materias clasificadas
 - ✓ Ficheros para la investigación del terrorismo y de delincuencia organizada

Ley Orgánica 15/1999



- Conceptos básicos:
 - ✓ Datos de carácter personal.
 - ✓ Fichero.
 - ✓ Tratamiento de datos.
 - ✓ Responsable del fichero o tratamiento.
 - ✓ Afectado o interesado.
 - ✓ Procedimiento de disociación.
 - ✓ Encargado del tratamiento.
 - ✓ Consentimiento del interesado.
 - ✓ Cesión o comunicación de datos.
 - ✓ Fuentes accesibles al público.

Ley Orgánica 15/1999



PROCEDIMIENTO A SEGUIR EN UNA ORGANIZACIÓN PARA CUMPLIR CON LA NORMATIVA VIGENTE

Detección de las bases de datos o ficheros.



Diagnóstico de situación de los mismos.



Plan de implantación o subsanación de las deficiencias.



Elaboración del Documento de Seguridad.



Auditoria bienal.

Ley Orgánica 15/1999



- Principales ficheros existentes en cualquier organización
 - ✓ Personal
 - ✓ Contabilidad
 - ✓ Marketing
 - ✓ Seguridad
 - ✓ Servicio Médico

Ley Orgánica 15/1999



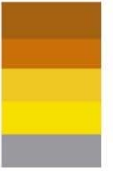
■ Personal

- ✓ Fichero cuya finalidad es la gestión de las relaciones de la empresa con:
 - Los empleados
 - Personal en prácticas / becarios
 - Candidatos

■ Contabilidad

- ✓ Fichero cuya finalidad es la gestión de:
 - Clientes
 - Proveedores
 - Acreedores

Ley Orgánica 15/1999



■ Marketing

- ✓ Fichero cuya finalidad es la gestión de la actividad comercial y promocional de la organización, dirigida a:
 - Clientes
 - Potenciales clientes
 - Datos extraídos de fuentes accesibles al público.

■ Seguridad

- ✓ Fichero cuya finalidad es la gestión de la seguridad en el edificio / instalaciones de la organización:
 - Control de visitas
 - Videovigilancia

■ Servicio Médico

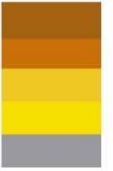
- ✓ Fichero cuya finalidad es la gestión del servicio médico de la organización:
 - Revisiones médicas de los empleados
 - Accidentes laborales de los empleados

Ley Orgánica 15/1999



- Principios básicos del tratamiento:
 - ✓ Deber de Información.
 - ✓ Consentimiento del afectado.
 - ✓ Calidad de los datos.
 - ✓ Seguridad de los datos.
 - ✓ Deber de secreto.
 - ✓ Derechos de las personal
 - Acceso
 - Rectificación
 - Oposición
 - Cancelación
 - ✓ Flujo de datos
 - Cesiones
 - Tratamiento por cuenta de terceros.

Ley Orgánica 15/1999



■ Deber de información – Artículo 5 LOPD

- ✓ Carácter Previo.
- ✓ Modo:
 - Expreso
 - Preciso
 - Inequívoco
- ✓ A cerca de:
 - Existencia de un fichero, finalidad y destinatarios de los datos.
 - Carácter obligatorio o facultativo de las respuestas.
 - Consecuencias de la obtención de los datos.
 - Consecuencias de la negativa a suministrarlos.
 - Ejercicio de derechos.
 - Identidad y dirección del responsable del fichero

Ley Orgánica 15/1999



- Consentimiento del afectado – Artículo 6 LOPD
 - ✓ Ha de ser inequívoco e informado
 - ✓ Tipos de consentimiento:
 - Expreso
 - Tácito
 - ✓ Excepciones:
 - Funciones propias de la administración.
 - Partes de una relación contractual o precontractual.
 - Interés vital del interesado.
 - Fuentes accesibles al público.

Ley Orgánica 15/1999



- Calidad de los datos – Artículo 4 LOPD
 - ✓ Los datos tratados deben ser:
 - Adecuados, pertinentes y no excesivos
 - Exactos y puestos al día
 - ✓ Datos innecesarios o no pertinentes:
 - Cancelación / bloqueo
 - ✓ Datos inexactos:
 - Rectificación.

Ley Orgánica 15/1999



- Seguridad de los datos – Artículo 9 LOPD
 - ✓ Medidas técnicas y organizativas que garanticen:
 - Seguridad de los datos.
 - Eviten su alteración no autorizada.
 - Pérdida.
 - Tratamiento.
 - Acceso no autorizado.

Ley Orgánica 15/1999



- Deber de secreto – Artículo 10 LOPD
 - ✓ Afectados
 - Responsable del fichero.
 - Personas que tratan los datos (personal de la organización).

 - ✓ Obligaciones.
 - Secreto profesional.
 - Debe de guarda de los datos.
 - Formalización de contratos de confidencialidad.

 - ✓ Responsabilidades.
 - Posibles sanciones laborales.
 - Responsabilidad penal (Art. 197, 199 Código Penal).

Ley Orgánica 15/1999



■ Flujo de Datos

✓ Cesión de datos

- ❑ La normativa establece la posibilidad de comunicar datos a terceros, estableciendo una serie de limitaciones y obligaciones a cumplir, tanto por el cesionario como por el cedente:
- ❑ Toda cesión deberá realizarse previo consentimiento del afectado.
- ❑ Excepciones Art. 11.2:
 - Cesión autorizada por Ley.
 - Datos recogidos de fuentes accesibles al público.
 - Cuando el tratamiento responda a una libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
 - Cuando la cesión tenga por destinatario al Defensor del Pueblo, Ministerio Fiscal o los Jueces y tribunales o el Tribunal de Cuentas.
 - La cesión se realice entre Administraciones Públicas.
 - La cesión de datos de salud sea necesario para solucionar una urgencia o realizar estudios epidemiológicos.
- ❑ El cedente debe informar en la primera cesión al afectado acerca de la finalidad del fichero, la naturaleza de los datos cedidos, nombre y dirección del cesionario.

Ley Orgánica 15/1999



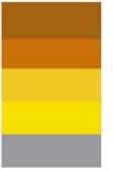
■ Flujo de Datos

✓ Acceso a datos por cuenta de terceros

En el artículo 12 se establece la forma en la cual se debe regular el tratamiento de los datos por parte de un tercero, siempre y cuando el tratamiento sea necesario para prestar un servicio:

- Se debe formalizar un contrato entre el Responsable del Fichero y el Encargado del Tratamiento, donde se debe regular:
 - Seguir las instrucciones del Responsable del Fichero.
 - No utilizar los datos para un fin distinto.
 - No comunicar los datos a terceros.
 - Destruir o devolver los datos una vez se haya finalizado la relación contractual.
 - Establecer las medidas de seguridad que el Encargado debe cumplir para el correcto y seguir tratamiento de los datos.

Ley Orgánica 15/1999

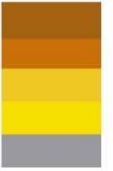


■ Flujo de Datos

✓ Transferencia Internacional de datos

- No se considerarán transferencias internacionales de datos las transferencias realizadas a países pertenecientes al Espacio Económico Europeo.
- Se debe solicitar la autorización al Director de la Agencia Española de Protección de Datos.
- Existen excepciones recogidas en el artículo 34 de la LOPD.

Ley Orgánica 15/1999



■ Ejercicio de Derechos

- ✓ Derecho de Acceso
- ✓ Derecho de Rectificación
- ✓ Derecho de Cancelación
- ✓ Derecho de Oposición

REAL DECRETO 1720/2007 - NOVEDADES



■ Información y Consentimiento para el tratamiento de los datos:

El nuevo RLOPD limita la posibilidad de solicitar el consentimiento para más de una finalidad diferente. Debiéndose identificar cada finalidad diferente y dar la posibilidad al afectado a negarse a alguna de ellas.

✓ Carga de la Prueba:

- ❑ Obligación del Responsable del Fichero de acreditar y probar el cumplimiento del deber de información y obtención del consentimiento del afectado.
- ❑ Obligación de conservar el soporte en el que conste el cumplimiento del deber de informar mientras persista el tratamiento de los datos del afectado.
 - El nuevo RLOPD establece la posibilidad de utilizar medios informáticos o telemáticos, siempre y cuando la inalterabilidad del soporte original (Ej. Escaneo y cifrado del documento).
- ❑ Recomendable articular en dicho soporte la recogida del consentimiento, aprovechando la documentación a efectos de prueba.

REAL DECRETO 1720/2007 - NOVEDADES



■ Información y Consentimiento para el tratamiento de los datos:

El nuevo RLOPD establece un procedimiento específico para la recogida del consentimiento:

- ✓ Cuando no se cuente con el consentimiento (y/o no se haya cumplido con el deber de información) o sea necesario un nuevo consentimiento para una finalidad diferente:
 - Se deberá proceder a comunicar al afectado cumpliendo el deber de confidencialidad:
 - Cuando se trate de responsables que presten al afectado un servicio que genere información o facturación periódica, la comunicación puede llevarse a cabo de forma conjunta a esta información o facturación, siempre y cuando se realice de forma claramente visible.
 - Concesión al afectado de un plazo de 30 días para manifestar su negativa la tratamiento:
 - En caso de no pronunciarse se entiende que consiente el tratamiento de sus datos.
 - Se recoge la obligación de facilitar un medio sencillo y gratuito para manifestar su negativa al tratamiento (en particular, envío prefranqueado, teléfono gratuito o servicios de atención al cliente).

REAL DECRETO 1720/2007 - NOVEDADES



■ Información y Consentimiento para el tratamiento de los datos:

El nuevo RLOPD establece un procedimiento específico para la recogida del consentimiento:

- Concesión al afectado de un plazo de 30 días para manifestar su negativa la tratamiento (Cont.):
 - Necesidad de que el responsable del fichero pueda conocer si la comunicación ha sido objeto de devolución, en cuyo caso no se podría proceder al tratamiento de los datos referidos a este afectado.
 - Problema de prueba, salvo que se utilicen las comunicaciones periódicas para información o facturación.
 - Limitación temporal para el uso del procedimiento. No será posible solicitar nuevamente el consentimiento por este procedimiento respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar desde la fecha de la anterior solicitud.

REAL DECRETO 1720/2007 - NOVEDADES



■ Información y Consentimiento para el tratamiento de los datos:

✓ Supuestos especiales:

- ❑ Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la finalidad inicial de la relación
- ❑ Interpretación restrictiva del concepto “finalidad relacionada”.
 - Exclusión de finalidades comerciales (información sobre productos y servicios de la propia empresa o de sociedades del Grupo).
- ❑ Debe permitirse al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.
 - Se entiende particularmente cumplido el citado deber, si se permite al afectado la marcación de una casilla.
 - » Claramente visible.
 - » Que no se encuentre previamente marcada.

REAL DECRETO 1720/2007 - NOVEDADES

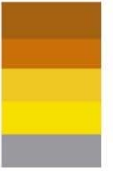


■ Información y Consentimiento para el tratamiento de los datos:

✓ Tratamiento de datos de menores de edad:

- ❑ La información dirigida a menores de edad deberá expresarse en un lenguaje fácilmente comprensible.
- ❑ Diferenciación en función de la edad del menor:
 - Mayores de 14 años: consentimiento personal.
 - Menores de 14 años: consentimiento de los padres o titulares de la patria potestad.
- ❑ No puede recabarse del menor información relativa a los demás miembros del grupo familiar, sin el consentimiento de los titulares de dichos datos, salvo los estrictamente necesarios para recabar la autorización al tratamiento de los padres o tutores y exclusivamente con dicha finalidad.
- ❑ Se establece la necesidad de articular procedimiento que garanticen que se ha comprobado la edad del menor y la autenticidad del consentimiento prestado por el familiar.

REAL DECRETO 1720/2007 - NOVEDADES



- Información y Consentimiento para el tratamiento de los datos:
 - ✓ Operaciones mercantiles de reestructuración societaria:
 - Comprende tanto las que suponen sucesión universal como las que no.
 - No se considera que existe una cesión de datos.
 - No obstante, se mantiene la obligación de dar cumplimiento al deber de información establecido en el artículo 5 de la LOPD.

REAL DECRETO 1720/2007 - NOVEDADES

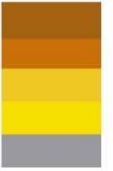


■ Flujo de Datos:

✓ Cesión de datos:

- ❑ El nuevo reglamento establece la posibilidad de indicar únicamente los sectores de actividad de las organizaciones a las cuales se les van a ceder los datos.
- ❑ El cesionario tendrá la obligación de informar al afectado en los primeros tres meses desde que recibió los datos, acerca de los datos recabados, su nombre, dirección y finalidad del tratamiento.

REAL DECRETO 1720/2007 - NOVEDADES



■ Flujo de Datos:

- ✓ Acceso a datos por cuenta de terceros:
 - Se permite la subcontratación (Art. 21 RLOPD) de servicios siempre y cuando:
 - El responsable del fichero autorice la subcontratación.
 - No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:
 - » Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.
 - » Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
 - » Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
 - » Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior. En este caso, el subcontratista será considerado encargado del tratamiento.

REAL DECRETO 1720/2007 - NOVEDADES



■ Flujo de Datos:

- ✓ Acceso a datos por cuenta de terceros:
 - Conservación de los datos por el Encargado del Tratamiento:
 - Obligación de destruir o devolver al responsable del fichero los documentos una vez finalizada la relación contractual, así como cualquier soporte o documento en que consten datos de carácter personal.
 - **Excepción:** existencia de una previsión legal que exija su conservación.
 - En este caso debe procederse a la devolución de los mismos, garantizado el responsable del fichero dicha.
 - Adicionalmente, el encargado del tratamiento conservará debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del fichero.

REAL DECRETO 1720/2007 - NOVEDADES

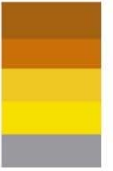


■ Flujo de Datos:

✓ Transferencia Internacional de Datos

- No cabe transferencia internacional (por subcontratación) del encargado del tratamiento ubicado fuera de España.
- No se regula el contenido del contrato a celebrar entre exportador e importador en el que consten garantías de respeto a la protección de la vida privada de los afectados y sus derechos y libertades.
 - Subsistencia del contenido regulado en la Instrucción de la AEPD 1/2000.
 - Autorización a grupos multinacionales de empresas en base a normas internas vinculantes (Binding Corporate Rules).

Ley Orgánica 15/1999



■ Niveles de seguridad

✓ Básico

- Todos los ficheros que contengan datos de carácter personal.
- Los ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social que tengan relación con sus competencias y las mutuas de accidentes de trabajo y de enfermedades profesionales de la Seguridad Social.
- 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.
- 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.
- 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.

✓ Medio

- Ficheros que contengan datos personales sobre características o personalidad de los afectados, que permitan deducir su comportamiento.

Ley Orgánica 15/1999



■ Niveles de seguridad

✓ Medio

- Ficheros que contengan datos personales sobre características o personalidad de los afectados, que permitan deducir su comportamiento.
- Infracciones administrativas o penales.
- Hacienda Pública.
- Servicios financieros.
- Datos de solvencia patrimonial y crédito.

✓ Alto

- Ficheros que contengan datos personales sobre características o personalidad de los afectados, que permitan deducir su comportamiento.
- Ideología.
- Religión.
- Creencias.
- Origen Racial.
- Salud o vida sexual.
- Fines policiales (sin consentimiento del afectado).

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

✓ Funciones y obligaciones del personal:

- ❑ Funciones y obligaciones de cada una de las personas con acceso a los datos y los sistemas claramente definidas y documentadas en el documento de seguridad.
- ❑ Diferenciación dentro de estas funciones las correspondientes al Responsable del Fichero, Responsable de Seguridad, la persona de sistemas y a los usuarios de los datos.
- ❑ El Responsable del Fichero deberá dar a conocer a todo el personal las normas establecidas y las consecuencias del incumplimiento.
- ❑ Se definirán funciones y obligaciones de cada uno de los usuarios o perfiles de usuario con acceso a los datos y a los sistemas en el documento de seguridad.
- ❑ Se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

- ✓ Registro de Incidencias (cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal):
 - ❑ Procedimiento de notificación y gestión de incidencias. Tipo de incidencias, fecha y hora del incidente, persona que notifica, persona que recibe la notificación y efectos derivados.
 - ❑ Procedimiento conocido y utilizado por todo el personal.
 - ❑ Debe incluir conceptos de las medidas correctoras aplicadas.
 - ❑ El control de acceso afectará a los recursos y no solo a ficheros incluyendo Documentos y a los Ficheros no automatizados. Art.105.1 b - Novedad

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

✓ Control de Acceso:

- Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones.
- Mecanismos que eviten el acceso a datos o recursos con derechos de acceso distintos.
- Concesión de permisos sólo por el personal autorizado.
- El control de acceso afectará a los recursos y no solo a ficheros incluyendo Documentos y a los Ficheros no automatizados. Art.105.1c- Novedad

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

✓ Gestión de soportes y documentos

- Etiquetado de soportes (CD, DVD, etc.) de forma que se identifique el tipo de información que contiene.
- Inventario.
- Almacenamiento con acceso restringido.
- Salida de soportes incluidos correos electrónicos fuera de los locales de ubicación del fichero autorizadas por el responsable del fichero. Art.92.2- **Novedad**
- Las personas que manejan los soportes deben estar debidamente autorizadas y constar en el documento de seguridad. Art.92.1 **Novedad**
- Se hace extensible además de a los soportes, a la gestión de documentos Art.105.1 d **Novedad**
- Se establecen excepciones al etiquetado e inventariado si las características físicas del soporte lo imposibilita, debiendo quedar reflejado en el documento de seguridad. Art. 92.1 **Novedad**
- Salidas autorizadas y reflejadas en el documento de seguridad.
- En el traslado de documentación se adoptarán medidas para evitar la pérdida, sustracción o acceso indebido. Art. 92.3 **Novedad**
- Normas para la eliminación y destrucción segura de documentos o soportes con el fin de evitar la recuperación posterior. Art.92.4 **Novedad**
- El control de acceso afectará a los recursos y no solo a ficheros incluyendo Documentos y a los Ficheros no automatizados. Art.105.1 d **Novedad**

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

✓ Identificación y autenticación

- Acceso controlado por procedimientos de identificación y autenticación.
- Existencia de procedimientos que permitan obtener la relación actualizada de usuarios con acceso a los sistemas y recursos autorizados.
- Procedimiento de asignación, distribución y almacenamiento de contraseñas que asegure confidencialidad e integridad.
- Periodicidad de cambio de contraseñas establecido en el documento de seguridad.
- El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema y verificación de que está autorizado.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Obligaciones comunes

✓ Copias de respaldo y recuperación

- Verificar la definición y aplicación de los procedimientos de copias y recuperación.
- Entorno de pruebas sin datos reales salvo que se garantice el nivel de seguridad.
- Copias de respaldo, al menos con una periodicidad semanal.
- Verificación prevista y de recuperación de los datos al menos cada 6 meses. Art 94.3
- Si está previsto realizar pruebas con datos reales se deberá hacer copia de seguridad con anterioridad. Art 94.4-Novedad.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Básico

Ficheros no automatizados

- ✓ **Criterios de archivo**
 - ❑ Acorde con la legislación o normativa que le sea de aplicación, incluida la vigente en materia de protección de datos.
 - ❑ Documentos localizables y localizados, ya que deben facilitar el ejercicio de derechos ARCO de los afectados.
- ✓ **Dispositivos de almacenamiento**
 - ❑ Los dispositivos de almacenamiento de los documentos deberán disponer de mecanismos que obstaculicen su apertura .Art. 107
 - ❑ Cuando las características físicas de las organizaciones que no puedan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.
- ✓ **Custodia de soportes**
 - ❑ En el proceso de tramitación o tránsito, personal al cuidado de los datos. Art.108

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Medio

Obligaciones Comunes

✓ Responsable de seguridad

- Deberá nombrarse un Responsable de Seguridad (o varios) y su nombre constará en el documento de seguridad.

✓ Auditoría

- Los sistemas de información e instalaciones de tratamiento de datos se verán sometidos a una auditoría interna o externa, de los procedimientos e instrucciones vigentes en materia de seguridad de los datos, con el fin de verificar el cumplimiento del RLOPD.
- Periodicidad no superior a dos años.
- Informe de auditoría a disposición de la AEPD y deberá dictaminar sobre la adecuación de las medidas y controles, identificar sus deficiencias y proponer medidas correctoras. Deberá incluir evidencias que soporten dichos dictámenes.
- El informe es analizado por el Responsable de Seguridad que elevará las conclusiones al Responsable del Fichero para que este adopte las medidas correctoras adecuadas.
- Se deberá hacer una auditoría también cuando se hayan producido cambios sustanciales en los sistemas de información, iniciando así el cómputo de los dos años. **Novedad.**

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Medio

Obligaciones Comunes

✓ Gestión de soportes y documentos

- ❑ Se debe establecer un procedimiento de entrada y salida de soportes que contengan datos de carácter personal de nivel medio.
- ❑ Dicho registro deberá contener:
 - Tipo de soporte (CD, DVD, Cinta, etc.)
 - Fecha y hora de salida o entrada.
 - Emisor o destinatario.
 - El número del soporte.
 - Tipo de información que contiene.
 - Forman de envío.
 - Persona responsable de la recepción o de la entrega.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Medio

Obligaciones Comunes

- ✓ **Identificación y autenticación**
 - ❑ Exigencia que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
- ✓ **Control de acceso físico**
 - ❑ Sólo el personal autorizado en el documento de seguridad podrá acceder a los locales donde están los sistemas.
- ✓ **Registro de incidencias**
 - ❑ En el registro de incidencias deberán consignarse además, los procedimientos realizados de recuperación de datos indicando la persona que ejecuta el proceso, los datos restaurados y los que fueron necesarios grabar manualmente en la recuperación.
 - ❑ Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de datos.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Medio

Ficheros no automatizados

- ✓ Nombrar un responsable de seguridad para los datos no automatizados (el mismo que para los datos automatizados).
- ✓ Auditoría, siguiendo los requisitos establecidos anteriormente.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Alto

Obligaciones Comunes

✓ Gestión y distribución de soportes

- ❑ La identificación de los soportes será comprensible y con significado para el personal autorizado y no así para el resto. Art.101 Novedad
- ❑ Distribución de soportes con cifrado de datos o bien utilizando otras medidas que garanticen que la información no sea accesible o manipulada durante su transporte.
- ❑ Se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones bajo control del responsable del fichero. Art. 101.2 Novedad
- ❑ Deberá evitarse el tratamiento de datos en dispositivos portátiles que no permitan su cifrado. Si fuese inevitable se motivará suficientemente en el documento de seguridad y se adoptarán cuantas medidas fueran necesarias para paliar el riesgo. Art.101.3 Novedad

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Alto

Obligaciones Comunes

✓ Copias de respaldo y recuperación

- Copias de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los ficheros y cumpliendo las medidas de seguridad apropiadas.
- O utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación. Art 102. **Novedad**

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Alto

Obligaciones Comunes

✓ Registro de accesos

- De cada acceso se guardarán como mínimo, la identificación del usuario, fecha, hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado.
- Si ha sido autorizado será preciso guardar información del recurso accedido.
- Los mecanismos que permiten el registro de accesos estará bajo control directo del responsable de seguridad, sin que se permita la desactivación de los mismos.
- Periodo de 2 años de conservación mínima del registro.
- Una revisión periódica mensual del responsable de seguridad elaborando un informe de las revisiones realizadas y problemas detectados.
- No será necesario dicho registro en el caso de que concurran las siguientes circunstancias
Novedad:
 - Que el responsable del fichero o del tratamiento es una persona física.
 - Que el responsable del fichero o del tratamiento garantiza que únicamente él tiene acceso y trata los datos personales.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Alto

Obligaciones Comunes

✓ Telecomunicaciones

- La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará:
 - Cifrando los datos.
 - O bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

REAL DECRETO 1720/2007 – MEDIDAS DE SEGURIDAD



■ Nivel Alto

Ficheros no automatizados

- ✓ Almacenamiento de la información
 - ❑ Archivadores u armarios en áreas restringida con limitación de accesos.
- ✓ Copia o reproducción
 - ❑ Control del personal autorizado en el documento de seguridad.
 - ❑ Destrucción de copias evitando acceso y recuperación posterior.
- ✓ Acceso a la documentación
 - ❑ Limitación al personal autorizado
 - ❑ Establecer mecanismos de identificación de accesos a documentos utilizados por múltiples usuarios.
 - ❑ Accesos de personal no autorizado deberá quedar debidamente registrado de acuerdo con lo que se establezca en el documento de seguridad.
- ✓ Traslado de documentación
 - ❑ Medidas para impedir el acceso o manipulación durante el traslado.



La seguridad digital del futuro, hoy

* [Muchas gracias]

