

CURSO SUPERIOR EN CORPORATE COMPLIANCE. I EDICIÓN

Módulo X . PROTECCION DE DATOS DE CARÁCTER PERSONAL



Normativa actual en LOPD, internacional,
europea y española. Ámbito de aplicación.

Ponente: Manuel Peña Zafra

Abogado. Economista.

Miembro de Responsia Compliance, S.L. y Vicepresidente del
Grupo de Prevención de Blanqueo de Capitales del Colegio de
Abogados de Granada

LEY ORGANICA 15/1999, DE PROTECCION DE DATOS DE CARÁCTER PERSONAL

◆ RÉGIMEN JURÍDICO

◆ **Constitución Española** de 27 de diciembre de 1978:

◆ **Art. 10**, reconoce el derecho a la dignidad de la persona.

◆ **Art. 18**, apartado 4º:

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."



Derecho fundamental a la protección de datos de carácter personal.



Autónomo e independiente. (STC 292/2000)

◆ RÉGIMEN JURÍDICO

➤ **Reglamento 2016/679 CE (28 de mayo 2016)**

➤ **Directiva 95/46/CE**, relativa a la protección personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DEROGADA

➤ **Directiva 2002/58/CE**, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

LOPD, Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

RD. 1720/2007, 21 de diciembre, que desarrolla la Ley 15/1999.



◆ RÉGIMEN JURÍDICO

➤ **NOVEDADES INTRODUCIDAS POR EL RD 1720/2007.**



(Desarrollar la Ley 15/1999, y aclarar los aspectos oscuros y de difícil interpretación de la misma). **MAS IMPORTANTES:**

RD/LOP

⇒ FICHERO AUTOMATIZADO, COMO EN SOPORTE **PAPEL.**

⇒ EXCLUYE DE SU APLICACIÓN A LAS PERSONAS **FALLECIDAS.**

⇒ COMPUTO DE PLAZOS, **DIAS HABILES.**

⇒ CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE MENORES DE EDAD. (**>14 AÑOS**)

⇒ “NUMERUS CLAUSUS” AL CONCEPTO DE **FUENTES ACCESIBLES AL PUBLICO.**

LEY ORGANICA 15/1999, DE PROTECCION DE DATOS DE CARÁCTER PERSONAL

➤ **NOVEDADES INTRODUCIDAS POR EL RD 1720/2007.**

RD/LOP

(Desarrollar la Ley 15/1999, y aclarar los aspectos oscuros y de difícil interpretación de la misma). **MAS IMPORTANTES:**

⇒ **DERECHO DE OPOSICION**, suple las lagunas actuales.

⇒ **MEDIDAS DE SEGURIDAD**. (Contemplando específicamente los no automatizados).

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016.

➤ NOVEDADES INTRODUCIDAS POR EL REGLAMENTO 2016/679 CE.



(ES APLICABLE A PARTIR DE 25 DE MAYO DE 2018),
pero entrada en vigor el 28 de mayo de 2016.

⇒ **CONSENTIMIENTO EXPLICITO PARA EL TRATAMIENTO**, pieza fundamental del sistema

⇒ **PROTECCION ESPECIFICA DE LOS NIÑO HASTA LOS 16 AÑOS**

⇒ **MEDIDAS DE SEGURIDAD**.(Contemplando específicamente los no automatizados).

Bien jurídico protegido

- DERECHO DE AUTODETERMINACIÓN INFORMATIVA
- HABEAS DATA
- LIBERTAD INFORMATICA
- DERECHO A LA PROTECCIÓN DE DATOS
 - *Control que a cada individuo le corresponde sobre la información que personalmente le concierne, sea íntima o no, para **impedir** que otros puedan conocerla y/o utilizarla de forma que les perjudique.*

LEY ORGANICA 15/1999, DE PROTECCION DE DATOS DE CARÁCTER PERSONAL

OBJETO

Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y derechos fundamentales de las personas físicas, y especialmente de su **honor e intimidad**.

AMBITO

Datos de carácter personal registrados en cualquier tipo de soporte que los haga susceptibles de tratamiento. Las empresas y organismos públicos tratan DCP y están obligados a garantizar su protección

OBLIGACIONES

La LOPD establece las obligaciones que los responsables de los ficheros y los encargados de los tratamientos han de cumplir para garantizar la observancia del derecho a la protección de datos de carácter personal.

◆ ¿Quién es el responsable?

- Es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los DCP.

◆ ¿Quién es el encargado?

- Es la persona física o jurídica, pública o privada, u órgano administrativo que sólo o conjuntamente con otros, trate DCP por cuenta del responsable del fichero como consecuencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio (contrato).

**Ambos pueden ser sancionados
de acuerdo a la LOPD**

• **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables.

• **Fichero:** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

• **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

NOTA: una persona facilita sus datos cuando, abre una cuenta en el banco, se matricula en un curso, cuando se apunta al gimnasio, cuando pide hora para una consulta médica, cuando busca trabajo, cuando navega por Internet, cuando damos el nº de teléfono, la dirección e-mail, una fotografía, etc.

- **Cesión o comunicación de Datos:** Tratamiento de datos que supone su revelación a una persona distinta del interesado .
- **Dato disociado:** Aquel que no permite la identificación de un afectado o interesado .
- **Persona identificable:** toda persona cuya identidad pueda determinarse, directa o indirectamente mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural y social.
No se considera identificable si dicha identificación requiere plazos o actividades desproporcionadas.
- **Cancelación:** procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implica el **Bloqueo** de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de Administraciones Públicas, Jueces y Tribunales.

◆ CONCEPTOS UE

- **Limitación del Tratamiento:** el marcado de los datos de carácter personal conservados con la finalidad de limitar su tratamiento.
- **Elaboración de Perfiles:** consiste en utilizar datos personales para evaluar determinados aspectos personales.
- **Seudonimización:** tratamiento mientras el cual ya no puede atribuirse aun interesado sin utilizar información adicional, siempre que esta este por separado y este sujeta a medidas técnicas y organizativas...
- **Violación de la seguridad de los datos personales.** Toda violación de seguridad que ocasione la destrucción, perdida o alteración de accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.
- **Datos genéticos:** DP relativos a características heredadas o adquiridas que proporciona una información única sobre la fisiología o la salud de esa persona (muestra biológica) .





◆ CONCEPTOS UE

• **Datos biométricos:** DP obtenidos a través de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales.

• **Elaboración de Perfiles:** Consiste en utilizar datos personales para evaluar determinados aspectos personales, Ej. Imágenes faciales o datos dactiloscópicos

• **Normas corporativas vinculantes:** Las políticas PD asumida por representante de un grupo empresarial a un país o mas terceros.



◆ ¿SUJETOS QUE INTERVIENEN?


- **AFECTADO O TITULAR DE LOS DATOS** (art. 3 e) LOPD
- **ENCARGADO TRATAMIENTO** (art. 3 g) LOPD
- **RESPONSABLE DEL FICHERO** (art. 3 d) LOPD
- **CORRESPONSABLE DE TRATAMIENTO**(Art. 26 UE)
- **REPRESENTANTE** (Art. 27 UE)
- **RESPONSABLE DE SEGURIDAD**(NIVEL MEDIO Y ALTO)
- **DELEGADO DE PROTECCION DE DATOS**(Art. 37 UE)
- **USUARIOS**.(Normalmente empleados)




◆ DATOS ESPECIALMENTE PROTEGIDOS

La Constitución Española establece: “ *Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*”

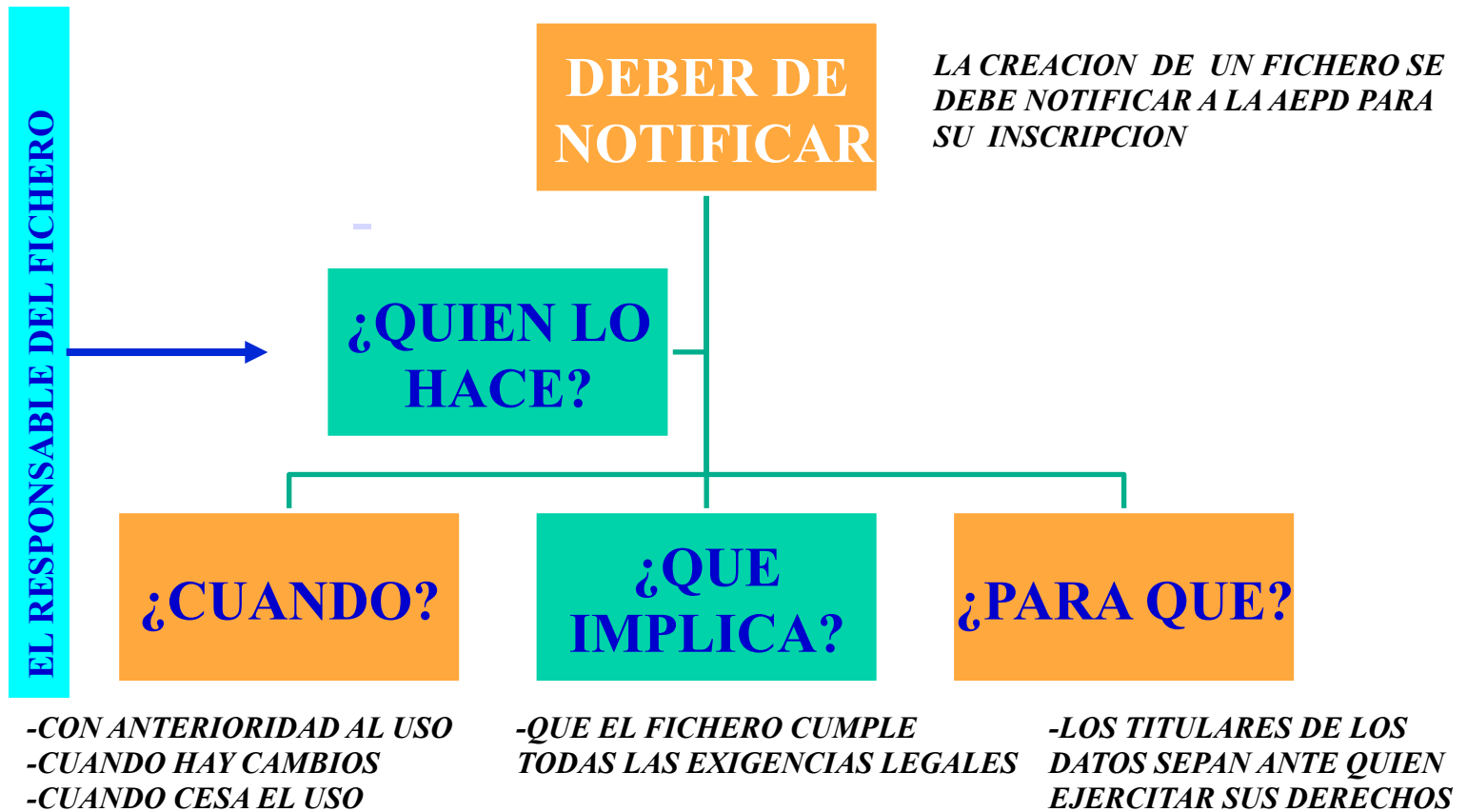
Se necesita consentimiento **expreso y por escrito** del interesado para el tratamiento de datos que revelen:

- 
- Ideología
 - Afiliación sindical
 - Religión
 - Creencias

Se necesita consentimiento **expreso** o que lo disponga una ley para recavar, tratar o ceder datos relativos a:

- 
- Origen racial
 - Salud
 - Vida sexual

◆ NOTIFICACION DE FICHEROS



Orden ECC/2503/2014, de 29 de diciembre, por la que se crea el fichero de datos de carácter personal denominado «Fichero de Titularidades Financieras».

Artículo 1. Objeto.

Se crea el fichero con datos de carácter personal, denominado «Fichero de Titularidades Financieras», con las características que se indican en el anexo y en los términos y condiciones fijados en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Artículo 2. Responsable del fichero.

El responsable del fichero es la Secretaria de Estado de Economía y Apoyo a la Empresa, actuando como encargado del tratamiento por cuenta de está el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, según lo establecido en el artículo 43 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en el artículo 50.2 del Reglamento de desarrollo, aprobado por Real Decreto 304/2014, de 5 de mayo.

Primero. Identificación del fichero, indicando su denominación, así como la descripción de su finalidad y usos previstos.

a) Identificación del fichero: Fichero de Titularidades Financieras.

b) Finalidad y usos previstos: Prevenir e impedir el blanqueo de capitales y la financiación del terrorismo.

Segundo. Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos, y su procedencia.

a) Colectivo: Titulares, titulares reales, representantes o autorizados y cualesquiera otras personas con poderes de disposición en cuentas corrientes, cuentas de ahorro, cuentas de valores o depósitos a plazo, con independencia de su denominación comercial.

b) Procedimiento de recogida: Transmisión electrónica de datos vía Editrán, desde las entidades de crédito en España al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias a través de su representante ante el Servicio Ejecutivo.



Tercero. Estructura básica del fichero y el sistema de tratamiento utilizado en su organización.

- a) Estructura: Datos identificativos de los titulares, titulares reales, representantes o autorizados y cualesquiera otras personas con poderes de disposición (nombre y apellidos o denominación social; tipo y número de documento identificativo (número de identificación fiscal español; otros documentos fehacientes de identificación); fecha de nacimiento o de constitución; país de nacionalidad; país emisor del documento identificativo; país de residencia declarada; condición en que intervienen y fecha de inicio y, en su caso, fin de la intervención; tipo y numeración de la cuenta o el depósito y fecha de apertura y, en su caso, cancelación.
- b) Sistema de tratamiento: Automatizado.

Cuarto. Comunicaciones de los datos previstas.

Las comunicaciones de los datos se realizarán a Jueces de Instrucción, Ministerio Fiscal, Fuerzas y Cuerpos de Seguridad, Centro Nacional de Inteligencia, Agencia Estatal de Administración Tributaria y Servicio Ejecutivo de la Comisión.

Quinto. Transferencias internacionales previstas a terceros países.

El Servicio Ejecutivo de la Comisión, en su calidad de encargado del tratamiento por cuenta de la Secretaría de Estado de Economía y Apoyo a la Empresa, no tiene previsto realizar transferencias internacionales.

Sexto. Órganos responsables del fichero y su tratamiento.

- a) Responsable del fichero: Secretaría de Estado de Economía y Apoyo a la Empresa.
- b) Encargado del tratamiento: Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

◆ EL NUEVO REGLAMENTO EUROPEO DE PROTECCION DE DATOS. 679/2016

Novedades:

Nuevos derechos de los ciudadanos: derecho al olvido y derecho a la portabilidad de los datos de un usuario de un sistema de tratamiento electrónico a otro.

La creación de la figura del Delegado de Protección de Datos (DPO ? Data Protection Officer).

Obligación de realizar Análisis de Riesgos y Evaluaciones de Impacto para determinar el cumplimiento normativo.

La obligación de registrar documentalmente las operaciones de tratamiento, tanto por parte de los Responsables de Fichero como por los Encargados de Tratamiento.

LEY ORGANICA 15/1999, DE PROTECCION DE DATOS DE CARÁCTER PERSONAL

◆ EL NUEVO REGLAMENTO EUROPEO DE PROTECCION DE DATOS

Nuevas notificaciones a la Autoridad de Control: brechas de seguridad y autorización previa para determinados tipos de tratamiento.

Nuevas obligaciones de información al interesado, mediante un sistema de iconos armonizado para todos los países de la UE.

Incremento de la cuantía de las sanciones.

Aplicación del concepto "**Ventanilla Única**" (One-stop-shop), para que los ciudadanos interesados puedan efectuar trámites, aunque estos afecten a autoridades en la materia de otros estados miembros.

Establecimiento de obligaciones para nuevas categorías especiales de datos.

Nuevos principios en relación a las obligaciones de información: transparencia y minimización.

CURSO SUPERIOR EN CORPORATE COMPLIANCE. I EDICIÓN

Módulo XI . PROTECCION DE DATOS DE CARÁCTER PERSONAL



Principios de Protección de datos y derechos de las personas.

Ponente: Antonio J. Salcedo Martín

Abogado.

Miembro de Responsia Compliance, S.L. y Secretario del Grupo de Prevención de Blanqueo de Capitales y cumplimiento normativo del Colegio de Abogados de Granada

CURSO SUPERIOR EN CORPORATE COMPLIANCE. I EDICIÓN

Módulo XI . PROTECCION DE DATOS DE CARÁCTER PERSONAL



Tipos de Ficheros. Medida de seguridad en el tratamiento de datos de carácter personal. Documento de seguridad.

Ponente: Manuel Peña Zafra

Abogado. Economista.

Miembro de Responsia Compliance, S.L. y Vicepresidente del Grupo de Prevención de Blanqueo de Capitales del Colegio de Abogados de Granada

SEGURIDAD DE LOS DATOS

- 1. El responsable del fichero**, y, en su caso, el **encargado del tratamiento** deberán **adoptar las medidas de índole técnica y organizativas** necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- 2.** No se registrarán datos de carácter personal en ficheros que **no reúnan** las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
- 3. Reglamentariamente** se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

◆ NIVELES DE SEGURIDAD

“Se deben de adoptar las medidas de índole técnica que garanticen la seguridad de los DCP y eviten su alteración, Perdida, tratamiento o acceso no autorizado” (Art 9 de la LOPD)

Se aplican tanto a los ficheros como a los tratamientos

Se deben aplicar tanto por el **responsable del fichero** como por el **encargado del tratamiento**.



ACUMULATIVOS



BÁSICO

MEDIO

ALTO

Niveles

◆ NIVELES DE SEGURIDAD

BASICO

- ✚ Control de acceso: SI
- ✚ Registro de Incidencias: SI
- ✚ Gestión de soportes y documentos SI
- ✚ Copias de respaldo: SEMANAL

- IDENTIFICACION Y AUTENTICACION



Periodicidad:
< 1 AÑO



◆ NIVEL MEDIO

BASICO :



- Responsable de Seguridad.
- Auditoria.

• IDENTIFICACION Y AUTENTICACION



3 intentos erróneos



LEY ORGANICA 15/1999, DE PROTECCION DE DATOS DE CARÁCTER PERSONAL



◆ NIVEL ALTO

MEDIO :



- SOPORTES CIFRADOS.
- TELECOMUNICACIONES

- TELECOMUNICACIONES
- SOPORTES CIFRADOS

- IDENTIFICACION Y AUTENTICACION



Registro de Accesos





◆ Aplicación de los niveles de seguridad

Nivel básico. Cualquier otro fichero que contenga datos de carácter personal.

También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.





◆ Aplicación de los niveles de seguridad

Nivel medio. Ficheros o tratamientos con datos

- De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
- Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.(relacionado art.13 LOPD, impugnación de valoraciones)
- De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.



Nivel medio. Ficheros o tratamientos con datos:

- Relativos a la comisión de infracciones administrativas o penales.
- Que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito).
- De Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias.
- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.
- De Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias.

continuación.



◆ Aplicación de los niveles de seguridad

Nivel alto. Ficheros o tratamientos con datos:

- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
- Recabados con fines policiales sin consentimiento de las personas afectadas.
- Derivados de actos de violencia de género.



1. El responsable del fichero o tratamiento elaborará **un documento de seguridad que recogerá las 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.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.





- 1.- **Ámbito de aplicación del documento**
- 2.- **Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.**
- 3.- **Procedimiento general de información al personal.**
- 4.- **Funciones y obligaciones del personal.**
- 5.- **Procedimiento de notificación, gestión y respuesta ante las incidencias.**
- 6.- **Procedimientos de realización de copias de respaldo y de recuperación**
- 7.- **Procedimiento de revisión.**
- 8.- **Consecuencias del incumplimiento del Documento de Seguridad.**

El documento de seguridad deberá mantenerse en todo momento **actualizado** y 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



◆ Seguridad del Tratamiento. UE(2016/279)

•El Responsable y el Encargado del tratamiento.

- Aplicaran medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al **RIESGO**:
 - ◆ La seudonimización y el cifrado de datos personales
 - ◆ La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes en los sistemas.
 - ◆ La capacidad de restaura la disponibilidad y el acceso de forma rápida en caso de accidente físico o técnico.
 - ◆ Un proceso de verificación, evaluación y valoración regulares de la eficacia del medidas técnica y organizativas para garantizar el tratamiento.

•El responsable y el encargado del tratamiento.

- Al **EVALUAR** la adecuación del nivel de seguridad, se tendrá en cuenta particularmente los riesgos que presente el tratamiento de datos:
 - ❑ Consecuencia de destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma o la comunicación de accesos no autorizados.

•El responsable y el encargado del tratamiento.

- La adhesión a un código de conducta aprobado o a un mecanismo de certificación, podrá servir para demostrar el cumplimiento.

•El responsable y el encargado del tratamiento.

- Tomaran medidas que garanticen que las personas autorizadas solo puedan tratar los DP siguiendo sus instrucciones del responsable.

Violaciones de Seguridad

- La debe notificar el responsable a la autoridad de control, en el plazo de no más. de 72 horas. Más tarde con motivos de la dilación.

•La notificación contemplará como mínimo:

- Descripción de la naturaleza de la violación.
- Nombre y datos del Delegado de Protección de Datos.
- Descripción de las posible consecuencias de la violación.
- Medidas adoptadas o propuestas para remediar o mitigar la violación.

•El responsable documentara:

- Cualquier violación.
- Los hechos relacionados con ella.
- Los efectos producidos.
- Las Medidas correctivas adoptadas.

◆ LEGISLACION EN MATERIA DE PREVENCIÓN DE BLANQUEO DE CAPITALS

-LEY 10/2010, DE PREVENCIÓN DE BLANQUEO DE CAPITALS Y FINANCIACIÓN DEL TERRORISMO

-Resolución de 10/08/2012, Secretaria General del Tesoro y Política Financiera.(Jurisdicciones que establecen requisitos equivalentes la Legislación Española).

-Real Decreto 304/2014, se aprueba el Reglamento de la Ley 10/2010.

- DIRECTIVA (UE) 2015/849, DE PREVENCIÓN DE LA UTILIZACIÓN DEL SISTEMA FINANCIERO PARA EL BLANQUEO DE CAPITALS Y FINANCIACIÓN DEL TERRORISMO, DE 20 DE MAYO DE 2015. DEROGA 2006/70/CE (3ª Directiva)



◆ RELACION CON OTRAS LEYES

◆ Vinculación con la Ley 10/2010 PBC

-Artículo 15. Tratamiento de datos de personas con responsabilidad pública.

-Artículo 32. Protección de datos de carácter personal.

-Artículo 43. Fichero de Titularidades Financieras.

◆ Vinculación con la Ley 10/2010 PBC // RD 304/2014

Artículo 53. *Protección de datos. (Titularidades financieras)*

Artículo 60. *Utilización de datos y nivel de seguridad en los tratamientos de carácter personal.*

Artículo 61. *Ficheros comunes para el cumplimiento de las obligaciones en materia de prevención.*





◆ Vinculación con la Ley 10/2010 PBC

Artículo 32. Protección de datos de carácter personal.

1. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de las disposiciones de esta Ley se someterán a lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo.

2. **No se requerirá el consentimiento** del interesado para el tratamiento de datos que resulte necesario para el cumplimiento de las obligaciones de información a que se refiere el Capítulo III.

Tampoco será necesario el mencionado consentimiento para las comunicaciones de datos previstas en el citado Capítulo y, en particular, para las previstas en el artículo 24.2.

3. En virtud de lo dispuesto en el artículo 24.1, y en relación con las obligaciones a las que se refiere el apartado anterior, **no será de aplicación al tratamiento de datos la obligación de información** prevista en el artículo 5 de la Ley Orgánica 15/1999.

Asimismo, **no serán de aplicación a los ficheros y tratamientos** a los que se refiere este precepto las normas contenidas en la citada Ley Orgánica referidas al ejercicio de **los derechos de acceso, rectificación, cancelación y oposición**. En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

Lo dispuesto en el presente apartado será igualmente aplicable a los ficheros creados y gestionados por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley.

4. Los órganos centralizados de prevención a los que se refiere el artículo 27 tendrán la condición de encargados del tratamiento a los efectos previstos en la normativa de protección de datos de carácter personal.

5. Serán de aplicación a los ficheros a los que se refiere este artículo **las medidas de seguridad de nivel alto** previstas en la normativa de protección de datos de carácter personal.

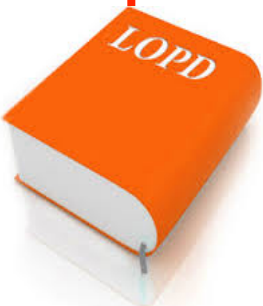


-Artículo 60. Utilización de datos y nivel de seguridad en los tratamientos de carácter personal.

-1. Los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida establecidas en la Ley 10/2010 de 28 de abril y este reglamento no podrán ser utilizados para fines distintos de los relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo **sin el consentimiento del interesado**, salvo que el tratamiento de dichos datos sea necesario para la gestión ordinaria de la relación de negocios.

-2. Los sujetos obligados aplicaran **medidas de seguridad de nivel alto a los tratamientos** llevados a cabo para el cumplimiento de las obligaciones de comunicación a las que se refiere el capítulo III de este Reglamento.

-3. Será exigible a los tratamientos efectuados en el cumplimiento del **deber de diligencia debida** el nivel de seguridad que corresponda conforme a lo previsto en la normativa vigente de protección de datos de carácter personal.



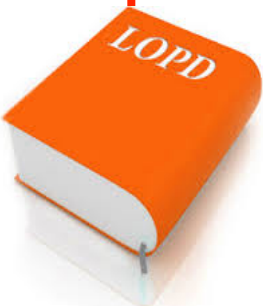
-Artículo 60. Utilización de datos y nivel de seguridad en los tratamientos de carácter personal.

NIVEL ALTO:

Dotar de unas medias de seguridad alta a un fichero no es nada fácil y cumplir con todos los requerimientos del mismo conlleva un coste excesivo y una formación extra, que no todos tienen.

Sirva a modo de ejemplo, teniendo en cuenta la acumulación de niveles de seguridad, los requerimientos de nivel alto:

MEDIDAS DE: **NIVEL BASICO + NIVEL MEDIO + NIVEL ALTO**



◆ Vinculación con la Ley 10/2010 PBC // RD 304/2014

NIVEL ALTO:

FICHEROS AUTOMATIZADOS:

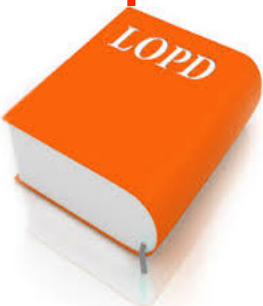
Identificación de soportes con etiquetado comprensible e identificado a los usuarios, y que dificulte su identificación al resto de personas.

La distribución de soportes, se realizara cifrando dichos datos o con otros mecanismos que permitan su no manipulación durante su transporte.
Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

Copias de respaldo y recuperación, en lugar diferente al que se encuentren los equipos informáticos que la tratan...

Registro de accesos, (solo personas jurídicas), periodo mínimo 2 años, donde se podrá tener acceso al menos identificar el usuario, fecha y hora que se realizo, el fichero accedido, el tipo de acceso y si se ha autorizado o denegado.

Telecomunicaciones, cifradas



◆ Vinculación con la Ley 10/2010 PBC // RD 304/2014

NIVEL ALTO:

FICHEROS NO AUTOMATIZADOS:

Almacenamiento de la información, los armarios y archivadores en áreas con puertas dotadas de sistemas de apertura mediante llave o dispositivo equivalente.

Copia o reproducción, solo mediante el control de la persona autorizada, y destrucción una vez utilizada.

El acceso solo personal autorizado.

Etc..





◆ La Cuarta Directiva” 2015/849, del Parlamento Europeo y del Consejo. (20 de mayo 2015)

Obliga a que por los sujetos obligados se facilite a los nuevos clientes la información requerida en el artículo 10 de la Directiva 95/46/CE, antes de entablar una relación de negocios, lo que supone ir en contra del artículo 15 y 32 de nuestra actual Ley y por lo tanto supone un cambio fundamental en la aplicación por el sujeto obligado de la misma.

Artículo 10. Información en caso de obtención de datos recabados del propio interesado.

"Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

- a) la identidad del responsable del tratamiento y, en su caso, de su representante;*
- b) los fines del tratamiento de que van a ser objeto los datos;*
- c) cualquier otra información tal como:*

- los destinatarios o las categorías de destinatarios de los datos,*
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder; la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información".*





FIN PRESENTACION



Échele el candado a su datos, y eduque en la LOPD a los que los tratan.

