Fundación General UGR-Empresa

RESPONSIA Cumplimiento Legal

# CURSO SUPERIOR EN CORPORATE COMPLIANCE. II EDICIÓN

## Módulo XI . PROTECCION DE DATOS DE CARÁCTER PERSONAL

Fundación General UGR-Empresa

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

Fundación General UGR-Empresa

# 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

- BASICO
- 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**


- **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.

# Aplicación de los niveles de seguridad

***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.

# Documento de seguridad.(RD 1720/2007)

**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.

# Documento de seguridad.(RD 1720/2007)

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 resilencia 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 riegos que presente el tratamiento de datos:
  - Consecuencia de destrucción, perdida 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 mecanismos 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 PREVENCION DE BLANQUEO DE CAPITALES

**-LEY 10/2010, DE PREVENCION DE BLANQUEO DE CAPITALES Y FINANCIACION 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 PREVENCION DE LA UTILIZACION DEL SISTEMA FINANCIERO PARA EL BLANQUEO DE CAPITALES Y FINANCIACION DEL TERRORISMO, DE 20 DE MAYO DE 2015. DEROGA 2006/70/CE (3ª Directiva)**

Fundación General UGR-Empresa

# 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

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

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

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

RESPONSIA Cumplimiento Legal

Fundación General UGR-Empresa

## 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.

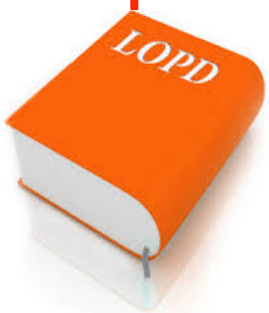
# Vinculación con la Ley 10/2010 PBC // RD 304/2014


**-Articulo 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.




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

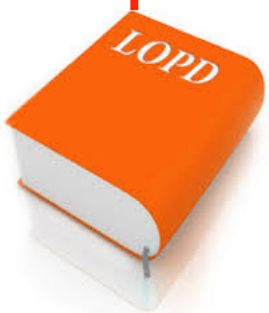

**-Articulo 60. Utilización de datos y nivel de seguridad en los tratamientos de carácter personal.**

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**




Fundación General UGR-Empresa

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

## NIVEL ALTO:

### FICHEROS AUTOMATIZADOS:

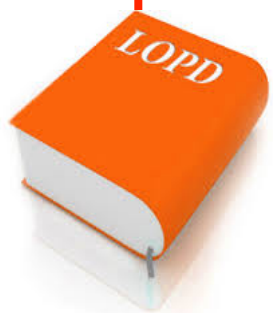
Identificación de soportes con etiquetado comprensible e identificado a los usuarios, y que dificulte su identificación al resto de personas.

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.*