DIPUTACIÓN DE ALMERÍA

Proteccion de Datos Personales LOPD y adecuacion a RGPD UE

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA Y RPC

Servicio de Organizacion y Seguridad
Manuel Soler Hernandez
msolerhe@dipalme.org
17 de Noviembre de 2017

OBJETIVO DE LA PONENCIA

Explicar como se gestiona en la Diputacion de Almeria y en la RPC el cumplimiento de la LOPD (Ley 15/1999), y que se esta haciendo o se debe hacer para su adaptacion al nuevo RGPD (UE) 2016/679.

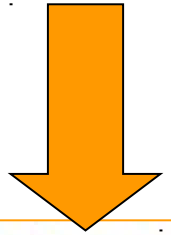
En los aspectos mas importantes de la protección de datos personales.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

1- CONCEPTOS GENERALES DE LOPD Y RGPD - UE

(1.0) PROTECCION DE DATOS PERSONALES

Toda persona física tiene derecho a la protección de los datos de carácter personal que la conciernen y este derecho le atribuye la facultad de controlar sus datos



LAS EMPRESAS Y ORGANISMOS PÚBLICOS TRATAN DATOS DE CARÁCTER PERSONAL Y ESTÁN OBLIGADOS A GARANTIZAR EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS.

(1.1) ENTORNO NORMATIVO ACTUAL

Hasta Mayo de 2018:

- **LOPD** (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)
- **RLOPD** (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal)

A partir de Mayo de 2018

- **RGPD (UE)** (REGL AMENTOS REGL AMENTO (UE) 2016/679 DEL PARL AMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016)

Normativa relacionada:

- **LSSI** (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico)
- **ENS** (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica)
- **LTBG** (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.)
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

(1.2) OBJETO

LOPD:

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

RGPD -UE

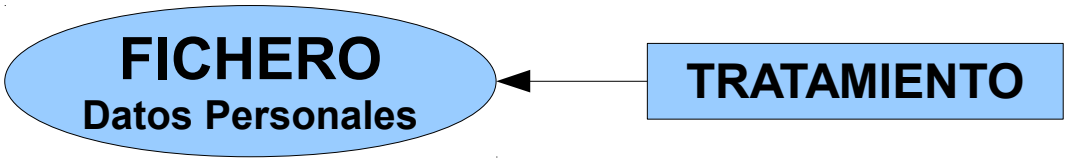
.. establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos

..protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

(1.3) AMBITO

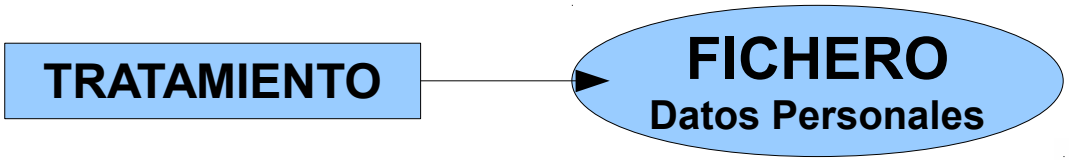
LOPD:

será de aplicación a los datos de carácter personal registrados en soporte físico (FICHERO), que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.



RGPD -UE

se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.



(1.4) DEFINICIONES (RGPD -UE)

«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); ……

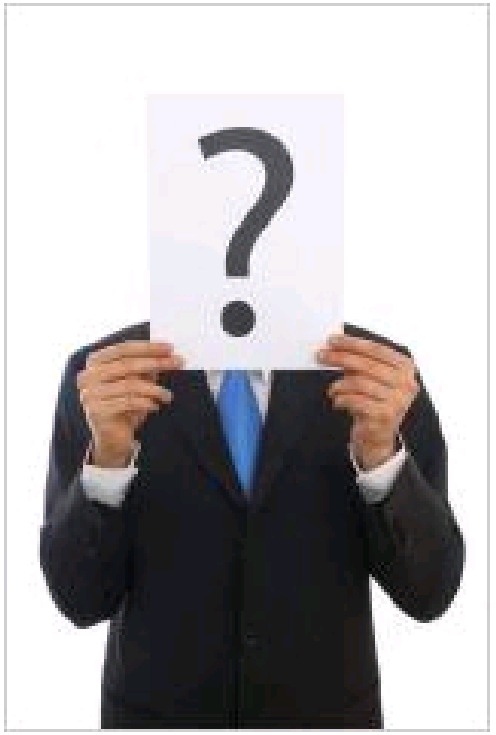
«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

«fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

(1.4.a) LOPD - DEFINICIONES

PERSONAS FÍSICAS IDENTIFICADAS O IDENTIFICABLES

Para comprender mejor el concepto de "datos de carácter personal" intentaremos explicar a que se refiere la Ley Orgánica de Protección de Datos cuando habla de "...*información concerniente a personas físicas identificadas o identificables*":



- **Información concerniente a una persona identificada.** Se considera que una información hace referencia a una persona física identificada cuando nos indica directamente a que persona se refiere sin necesidad de que tengamos que realizar ningún tipo de averiguación posterior. Un claro ejemplo de ello lo tenemos en el Documento Nacional de Identidad (DNI), que está considerado como dato de carácter personal porque la información que contiene identifica perfectamente a una persona física determinada.
- **Información concerniente a una persona identificable.** Se considera que una información hace referencia a una persona física cuando a priori no nos indica a que persona se refiere pero nos aporta información suficiente para poder llegar a averiguar su identidad. El ejemplo más claro lo tenemos en el ADN, que sabemos que contiene información genética concerniente a una persona concreta pero no sabremos de quien se trata hasta que no lo sometamos al procedimiento adecuado. El reglamento que desarrolla la Lopd (Real Decreto 1720/2007) considera como "persona identificable" a "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados*"

(1.4.b) Ejemplos

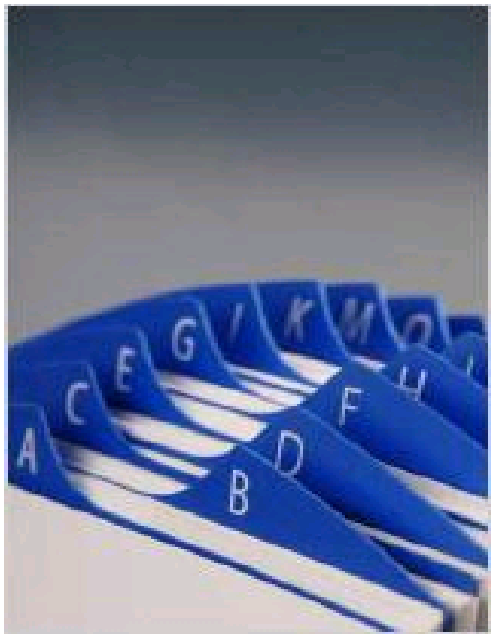
Algunos ejemplos de datos con los que se pueden Identificar a las Personas

Datos	Identificada	Identificable
Nombre y Apellidos		
NIF		
ADN		
Matricula Vehiculo		
Huella digital		
Email		
FOTO		

La combinacion de varios datos Identificables hace mas facil la identificacion de la persona

(1.4.c) LOPD - DEFINICIONES

CATEGORIAS DE DATOS DE CARÁCTER PERSONAL



- **Datos especialmente protegidos:** Ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y vida sexual.
- **Datos de carácter identificativo:** Nif/dni, dirección, imagen, voz, Nº Seguridad Social/mutualidad, teléfono, marcas físicas, nombre y apellidos, firma/huella, firma electrónica, tarjeta sanitaria.
- **Datos relativos a las características personales:** datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.
- **Datos relativos a las circunstancias sociales:** Características de alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.
- **Datos Académicos y profesionales:** Formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.
- **Detalles de empleo:** Profesión, puestos de trabajo, datos no económicos de nomina, historial del trabajador.
- **Datos que aportan Información comercial:** Actividades y negocios, licencias comerciales, subscripciones a publicaciones o medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- **Datos económicos, financieros y de seguros:** Ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, datos deducciones impositivas/impuestos, seguros, hipotecas, subsidios, beneficios, historial de créditos, tarjetas de crédito.
- **Datos relativos a transacciones de bienes y servicios:** Bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones/indemnizaciones.

(1.4.d) LOPD - DEFINICIONES

FICHEROS AUTOMATIZADOS

- **Ficheros automatizados.** Con el termino fichero automatizado la normativa sobre protección de datos se refiere a todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados (definición del autor). Están claramente incluidos dentro de este concepto los ficheros de datos personales que almacenan la información en **soportes informáticos** (bases de datos, archivos, carpetas etc.) y que se encuentran organizados de manera que se puede acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.

(1.4.e) LOPD - DEFINICIONES

FICHEROS NO AUTOMATIZADOS

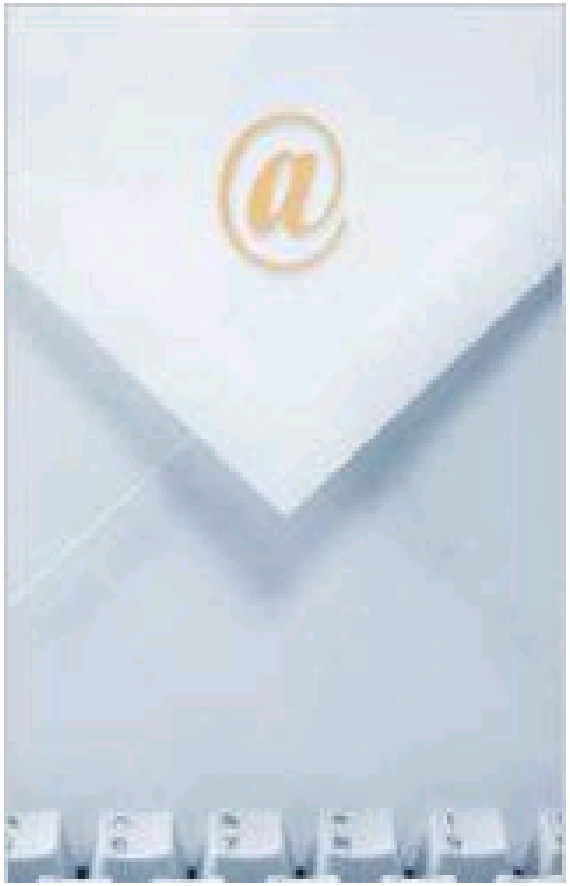
- **Ficheros no automatizados**. Los ficheros no automatizados están definidos legalmente como *"todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"* (artículo 5.1.n Real Decreto 1720/20007). El mejor ejemplo de un fichero no automatizado lo tenemos en los archivadores existentes en la mayoría de las organizaciones en los que se almacenan **expedientes de documentos** organizados por grupos de personas (empleados, clientes, proveedores etc.) y estructurados de manera que se pueda localizar cada expediente utilizando criterios identificativos determinados (búsqueda alfabética por nombre o apellidos, etc.).

(1.4.f) LOPD - DEFINICIONES

AGRUPACON DE FICHEROS O TRTAMIENTO POR FINALIDAD

AGRUPACIÓN DE FICHEROS POR SU FINALIDAD

Aunque físicamente los datos de carácter personal se encuentren almacenados en distintos tipos de ficheros e incluso aunque geográficamente se encuentren ubicados en distintas instalaciones, **todos los ficheros físicos existentes en una organización determinada (automatizados y no automatizados) que hayan sido creados con la misma finalidad se agrupan en un solo fichero jurídico que es el que hay que notificar a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.**



(1.4.g) LOPD - DEFINICIONES

EJEMPLO: AGRUPACON DE FICHEROS POR FINALIDAD

Para comprender mejor esta idea vamos a analizar cómo suelen tratar las empresas los datos personales de sus clientes; de manera general, los datos de los clientes se encuentran almacenados un software de facturación, en varios archivos informáticos (hojas de cálculo, archivos de texto...) y también en varias carpetas y archivadores que contienen la documentación de los clientes en formato papel (fichas, facturas etc.). Pues bien, aunque físicamente existe un fichero automatizado (formado por todos los archivos y aplicaciones informáticas) y un fichero no automatizado (formado por todas las carpetas y archivadores ordenados alfabéticamente por nombre y apellidos) jurídicamente se trata de un solo fichero de carácter "mixto" (automatizado y no automatizado) que ha sido creado con la finalidad de gestionar las relaciones comerciales entre la empresa y sus clientes.

El fichero de nuestro ejemplo será notificado a la Agencia Española de Protección de Datos como un **"fichero mixto"** al que vamos a identificar como **"fichero de clientes"** y cuya finalidad, tal y como está tipificada en el » **formulario de notificación de ficheros (NOTA)** , será la de **"Gestión de Clientes, contable, fiscal y administrativa"**.

(1.4.h) LOPD – DATOS EXCLUIDOS DE LOPD

DATOS EXCLUIDOS DE LA APLICACIÓN DE LA LOPD

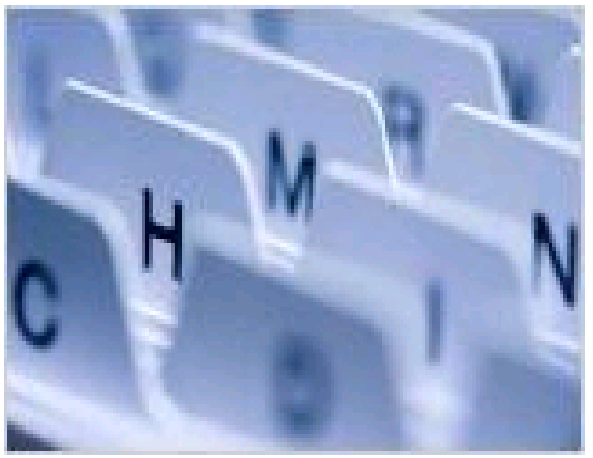
¿A qué datos NO se aplica la Lopd? | artículo 2 Real Decreto 1720/2007. Existen determinados datos de carácter personal que, a pesar de hacer referencia a una persona física determinada, se encuentran excluidos del ámbito de aplicación de la Lopd , dichos datos son los siguientes:

- **Datos referidos a personas jurídicas y las personas de contacto.** La Lopd no se aplica a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
- **Datos relativos a empresarios individuales.** La Lopd no se aplica a los tratamientos de datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.
- **Datos relativos a personas fallecidas.** La Lopd no se aplica a los tratamientos de datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos

(11.4.i) LOPD – FICHEROS EXCLUIDOS

FICHEROS EXCLUIDOS DE LA APLICACIÓN DE LA LOPD

¿A qué ficheros NO se aplica la Lopd? |artículo 2.2 Lopd. El régimen de protección de los datos de carácter personal establecido en la Ley Orgánica de Protección de Datos no será de aplicación a los siguientes ficheros:



- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares).
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

(1.4.j)) RESPONSABLE Y ENCARGADO DE TRATAMIENTO

(RGPD-UE) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; …..

(RGPD-UE) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

(1.5) PRINCIPIOS LOPD

El tratamiento de datos personales debe realizarse conforme a los siguientes principios:

- Calidad de los datos
- Derecho de información
- Consentimiento del afectado
- Datos especialmente protegidos
- Datos relativos a la salud.
- Seguridad de los datos.
- Deber de secreto
- Comunicación de datos
- Acceso a los datos por cuenta de terceros

(1.6) PRINCIPIOS – RGPD-UE (NOVEDADES)

- **Principio de transparencia** en el tratamiento vinculado al tratamiento leal y lícito (información accesible y comprensible)

- **Principio de minimización** Vinculación a "necesidad". proporcionalidad cuantitativa y cualitativa."Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios"

- **Principios de seguridad y confidencialidad**: La seguridad como principio y como obligación.

- **Principio de responsabilidad proactiva o "accountability"**: El responsable del tratamiento será responsable de cumplir los principios Proteccion de Datos Personales y capaz de demostrarlo («responsabilidad proactiva»).

(1.7) DATOS ESPECIALMENTE PROTEGIDOS

(LOPD)- Artículo 7. Datos especialmente protegidos:
…..datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, saludo vida sexual.

(RGPD-UE) Articulo 9 Tratamiento de categorías especiales de datos personales :
datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

(1.8) LEGITIMACIÓN PARA TRATAMIENTO

Todo tratamiento de datos necesita apoyarse en una base que lo legitime. Y estas son:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- **Interés público o ejercicio de poderes públicos.**
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Hay que Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos

(1.9) DERECHOS DE LAS PERSONAS

LOPD:

- Informacion
- Acceso
- Rectificación
- Cancelación
- Oposición

RGPD – UE: (Novedades)

- **Supresion (Olvido)**
- **Limitación del tratamiento**
- **Portabilidad de los datos**

(1.10) SEGURIDAD DE LOS DATOS

LOPD (Art 9) y RLOPD:

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

RGPD – UE (Art 24):

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

- **(Art 25) Protección de datos desde el diseño y por defecto**

(1.11) SEGURIDAD DE LOS DATOS

RLOPD:

Artículo 95. Responsable de seguridad.

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

RGPD – UE (Art 37):

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

(1.11) IMPLANTAR SISTEMA DE GESTION

Para cumplir con la normativa de proteccion de datos personales, es necesario **implantar un sistema de gestion de seguridad de los datos personales (medidas técnicas y organizativas)** que garantice los derechos y libertades de las personas físicas

(1.12) IMPLANTAR SISTEMA DE GESTION

Segun nueva RGDP-UE, hay que plantearse:

- Que Tratamiento de Datos Personales se realiza en la organización
- Que riesgos asumo que puedan violar los derechos y libertades de las personas.
- Riesgo de las nuevas tecnologias (servidores, portatiles, pen drives, correo electronico, redes sociales, big data, cloud,…)

Y Realizar las siguientes acciones:

- Analisis de riesgos
- Establecer Medidas de Seguridad
- Y seguimiento y medicion del sistema implantado

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

2- ¿COMO SE ORGANIZA LA GESTION LOPD EN DIPUTACION?

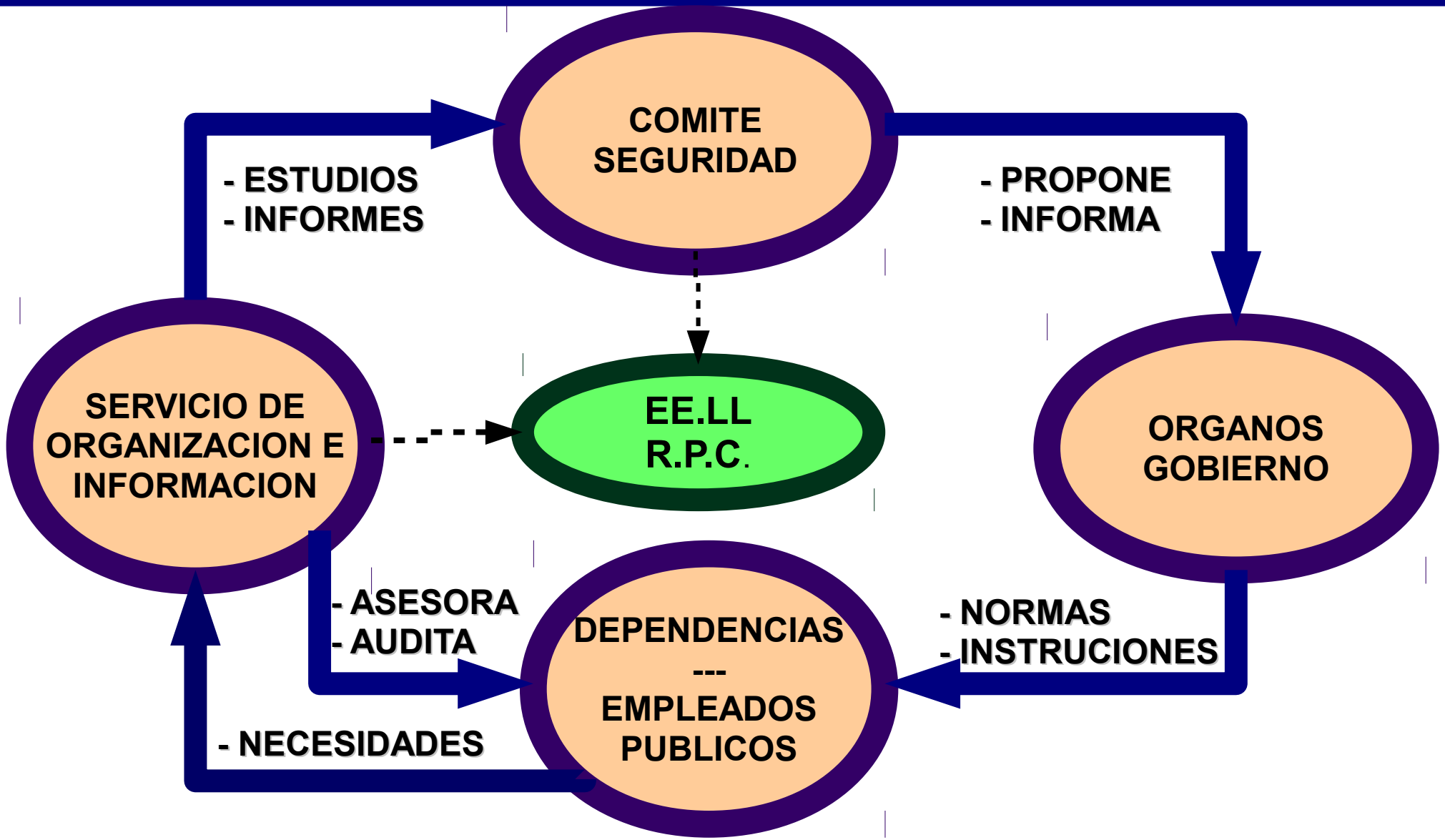
(2.0) GESTION LOPD PROCESO CONTINUO

DIPUTACION TRATA DATOS PERSONALES Y POR TANTO ES RESPONSABLE DE SU TRATAMIENTO

LA GESTION DE LA LOPD SE TIENE QUE IMPLANTAR COMO UN PROCESO CONTINUO:

- **Planificar**
- **Hacer**
- **Auditar**
- **Actualizar**

(2.1) ORG.GESTION LOPD EN DIPUTACION



El procedimiento de contestacion sobre Derechos ARCO los COORDINA la Seccion de Regimen Interior.
Y se debe cambiar para que los haga el Servicio Organizacion e Informacion

(2.2) COMITE DE SEGURIDAD

FUNCIONES:

- **Coordinar las actividades y controles** de seguridad de la información, **protección de datos** y portal de transparencia establecidos en la Diputación de Almería y entidades adheridas al Convenio Marco RPC y **velar por el cumplimiento de la normativa vigente interna y externa en materia de protección de datos,** seguridad y transparencia.

- **Proponer a los Organos de Gobierno** la política de seguridad de la información de esta Administración, así como otros **documentos que definan las distintas actuaciones a desarrollar dentro del marco legislativo que regula** el Esquema Nacional de Seguridad, **protección de datos (LOPD)** y transparencia (Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno).

(2.3) SERVICIO ORGANIZACION E INFORMACION

FUNCIONES:

- Supervisar la ejecucion y mantenimiento de la gestion de la LOPD
- Asesorar a las dependencias y empleados publicos en la gestion de la LOPD.
- Auditar y comprobar la gestion de la LOPD en las dependencias.
- Realizacion de notas informativas a los empleados publicos sobre cumplimiento de la LOPD
- Dinamizar y concienciar sobre la gestion y cumplimiento de LOPD
- Informar sobre las solicitudes de derecho ARCO
- Realizar los informes sobre Alta, Modificacion y baja de ficheros en la AEPD.
- Coordinar la colaboracion con la AEPD

EL Jefe del Servicio sera el Responsable de la Seguridad de la Informacion de la Diputacion.

(2.4) DEPENDENCIAS Y EMPLEADOS PUBLICOS

FUNCIONES:

- Velar por el Complimientos de las normas y directrices e proteccion de datos que apruebe la organización.
- Informar sobre los nuevos ficheros de tratamiento de datos personales que se implanten en la dependencia.
- Colaborar en la gestion de proteccion de datos según las directrices de la organización.
- Comprobar y hacer cumplir las directrices de seguridad en su dependencia.

- Los responsables maximos de las Dependencias seran Responsables Delegados de Seguridad.
- Los Usuarios deben cumplir el deber de secreto y cumplir con las directivas de seguridad.

(2.5) ORGANOS DE GOBIERNO

FUNCIONES:

- Aprobar el tratamiento de ficheros y sus finalidades.
- Aprobar los procedimientos y normas sobre proteccion de datos personales.

- El Presidente de la Diputacion es el Responsable (Alcaldes de Aytos) maximo de la Gestion de la Proteccion de Datos Personales.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3- IMPLANTACION

LOPD Y RGPD-UE

(3.1) QUE SUPONE LA GESTION DE LA LOPD

A) Inscripción de los ficheros en el Registro General de la AEPD.

B) Calidad de los datos

C) Cláusulas de protección de datos (consentimiento e informacion), **formularios para la recogida de datos** y ejercicio de derechos ARCO.

D) El **deber de secreto.** Confidencialidad.

E) Redacción del **documento de seguridad** con toda la normativa necesaria.

F) Adopción de **medidas de seguridad.**

G) Solicitar el **Tratamiento internacional** de datos.

H) Realizar **Contratos para tratamientos por terceros y cesiones** o comunicaciones de datos.

I) Nombrar a **Responsable de seguridad.**

J) Auditoría cada dos años (Ficheros nivel de seguridad en los datos medio o Alto).

K) Difusion y **Formacion al Personal**

L) Se hace necesario el **Apoyo a la EELL de la provincia.**

(3.2) FASES DE IMPLANTACION DE LA LOPD

(3.2) QUE SUPONE LA GESTION DEL RGPD-UE

El RGPD-UE obliga al responsable del tratamiento a:

A) Análisis de riesgo
B) Registro de actividades de tratamiento
C) Protección de Datos desde el Diseño
D) Medidas de seguridad
E) Notificación de “violaciones de seguridad de los datos”
F) Evaluación de impacto sobre la Protección de Datos
G) Delegado de Protección de Datos
H) Cooperar con las Autoridades de Control

(3.3) IMPACTO DE RGPD-UE EN AAPP

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

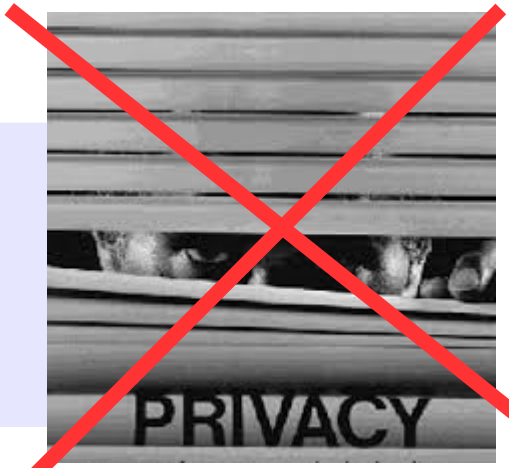
1.Necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos que llevan a cabo
2.Si el tratamiento es en base el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal.
3.Consentimiento expreso que exige que sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa
4.Necesidad de adecuar la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD (arts. 13 y 14).
5.Necesidad de establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos
6.Necesidad de establecer procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD
7.Necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD
8.Necesidad de adecuar los contratos de encargo que actualmente se tengan suscritos a las previsiones del RGPD.
9.Necesidad de hacer un análisis de riesgo
10.Necesidad de establecer un Registro de Actividades de Tratamiento tanto para Responsable como para Encargado
11.Necesidad de revisar las medidas de seguridad
12.Notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados
13.Necesidad de valorar si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo
14.Necesidad de designar un Delegado de Protección de Datos (DPD).
15. Necesidad de adaptar los instrumentos de transferencia internacional de datos personales a las previsiones del RGPD

(3.4) ¿COMO SE CUMPLE?

DATOS PERSONALES

Aplicar Medidas de Seguridad

Garantizar los derechos y libertades de las personas físicas



(3.5) COMO SE DEFINEN LAS MEDIDAS A APLICAR

LOPD (Art 9) y RLOPD:

Para aplicar medidas de seguridad hay que catalogar los ficheros en:

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal.

NIVEL MEDIO. Ficheros o tratamientos con datos: Tributarios, Relativos a la comisión de infracciones administrativas o penales, financieros, Seguridad Social, de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, de los operadores de comunicaciones electrónicas.

NIVEL ALTO. Ficheros o tratamientos con datos: de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, recabados con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género.

(3.5) COMO SE DEFINEN LAS MEDIDAS A APLICAR

- **RGPD – UE (Art 24):** Se debe realizar un **Análisis de Riesgos** y se aplicaran entre otras las siguientes medidas Tecnicas y Organizativas a utilizar, según los riesgos:
  - seudonimización y el cifrado de datos personales;
  - capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
  - capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
  - un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

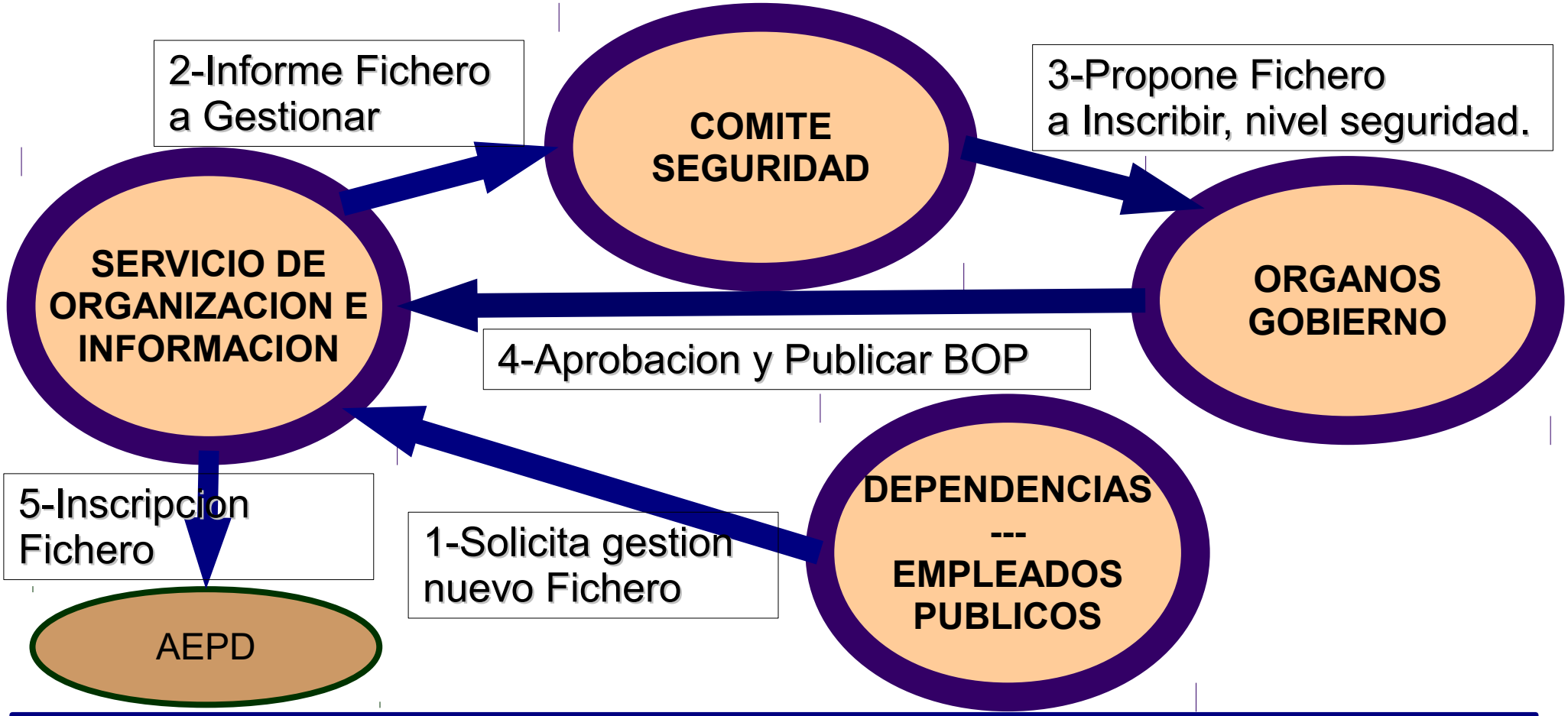
GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.A- (LOPD) INSCRIPCION DE FICHEROS EN LA AEPD

(RGPD-UE) REGISTRO DE ACTIVIDADESDE TRATAMIENTO

(3.A.1) - INSCRIPCION DE FICHEROS EN AEPD

LOPD - Artículo 26. Notificación e inscripción registral.
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.



El nuevo RGPD (UE) – hay que mantener un Registro de Actividades de Tratamiento de datos Personales

(3.A.2) INSCRIPCION FICHERO AEPD

LOPD (Art.20) Indica como deben crearse los ficheros de titularidad publica, se debe de indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

(3.A.3) REGISTRO DE ACTIVIDADES TRATAMIENTOS

RGPD-UE (Art.30) Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener:

a) Datos del responsable y, en su caso, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, ……

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, …..

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

(3.A.4) EJEMPLOS DE FICHERO Y REG.ACT.TRAMIENTO

LOPD

Fichero de Actividades Deportivas de Ayuntamiento de Pulpi
<VER>

LOS FICHEROS CREADOS E INSCRITOS EN AEPD, NO SUELEN MODIFICARSE A NO SER QUE CAMBIEN LA FINALIDAD O LA MODALIDAD DE TRATAMIENTO, O EL NIVEL DE SEGURIDAD APLICADO.

<MAS BUROCRATICO>

RGPD-UE

Registro de actividad del Tratamiento de Actividades Deportivas de Ayuntamiento de Pulpi
<VER>

EL REGISTRO DE TRATAMIENTO TIENE MAS CAMBIO DEBIDO A QUE HAY QUE INDICAR EL TRATAMIENTO QUE SE REALIZA Y DONDE SE LLEVA ACABO DICHO TRATAMIENTO.

<MAS AGIL>

(3.A.5) REGISTRO DE ACTIVIDADES TRATAMIENTOS

RGPD-UE (Art.30) Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga: :

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.B- CALIDAD DE LOS DATOS

(3.B.1) CALIDAD DE LOS DATOS

LOPD

El responsable del fichero debe cumplir con los principios de la calidad de los datos:

- Transparencia en la recogida de los datos.
- Finalidad del tratamiento
- Proporcionalidad de los datos
- Uso de los datos
- Exactitud de los datos
- Cancelacion de los datos
- Almacenamiento de los datos

RGPD (UE)

El nuevo RGPD obliga a los responsables de fichero a la responsabilidad activa, que implica entre otras las siguientes medidas:

- Protección de datos desde el diseño
- Minimizacion
- Proteccion de datos por defecto
- Evaluacion de impacto.

El nuevo RGPD refuerza los principios de la calidad de los datos, y obliga a la proteccion desde el diseño

(3.B.2) EJEMPLO DE TRATAMIENTO

¿CÓMO HAS CONOCIDO NUESTRO FESTIVAL?

FICAL
FESTIVAL INTERNACIONAL DE CINE DE ALMERÍA

Si deseas recibir información puntual de todas las actividades culturales de la Diputación de Almería, rellena la siguiente ficha:

APELLIDOS _____

NOMBRE _____

TLF _____

CORREO ELECTRÓNICO _____

DIRECCIÓN _____

PROVINCIA _____

LOCALIDAD _____

CP _____

FECHA DE NACIMIENTO _____

PROFESIÓN _____

De acuerdo con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, autorizo a la Diputación de Almería al tratamiento de los datos personales recogidos en el presente formulario. Le informamos que Los datos de carácter personal que nos facilite quedarán registrados en un fichero titularidad de la DIPUTACIÓN PROVINCIAL DE ALMERÍA, con la finalidad de ENCUESTA FICAL. Le comunicamos que puede ejercitar los derechos de acceso, rectificación y cancelación de sus datos comunicándolo por escrito a la Sección de Régimen Interior de la DIPUTACIÓN PROVINCIAL DE ALMERÍA, en la dirección: C/ Navarro Rodrigo 17, 04001, Almería, adjuntando copia de documento que acredite su identidad.

DIPUTACIÓN DE ALMERÍA

XVI FESTIVAL INTERNACIONAL DE CINE DE ALMERÍA

CICLO 'ALMERÍA, TIERRA DE CORTOS'

Sesión 1: Martes 19 de septiembre de 2017 - 20,30 h.

- ☐ **Indalopatía**, de Jaime García. 2016. Ficción. 9 minutos.
- ☐ **Gracias**, de Pedro Flores. 2015. Ficción. 14 minutos.
- ☐ **Tras la piel**, de Antonio Ufarte. 2016. Ficción. 18 minutos.
- ☐ **1936, cronicas de la guerra** , de Andreu Fullana Arias. 2016. Ficción. 12 minutos.
- ☐ **Masacre medieval**, de Víctor Díaz Pardo.2016. Ficción. 3'30 minutos.
- ☐ **San Cristán**, deJosé Carlos Castaño Muñoz. 2016. Documental. 8 minutos.
- ☐ **Dignidad El Puche**, de Pol Andreu Sansano, Ariadna G. García. 2016. Documental. 27 minutos.

Puntúa cada cortometraje de 1 a 10, siendo 10 la máxima puntuación

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.C- FORMULARIOS DE RECOGIDA DE DATOS PERSONALES

(3.C.1) FORMULARIOS DE REGOGIDA DE DATOS

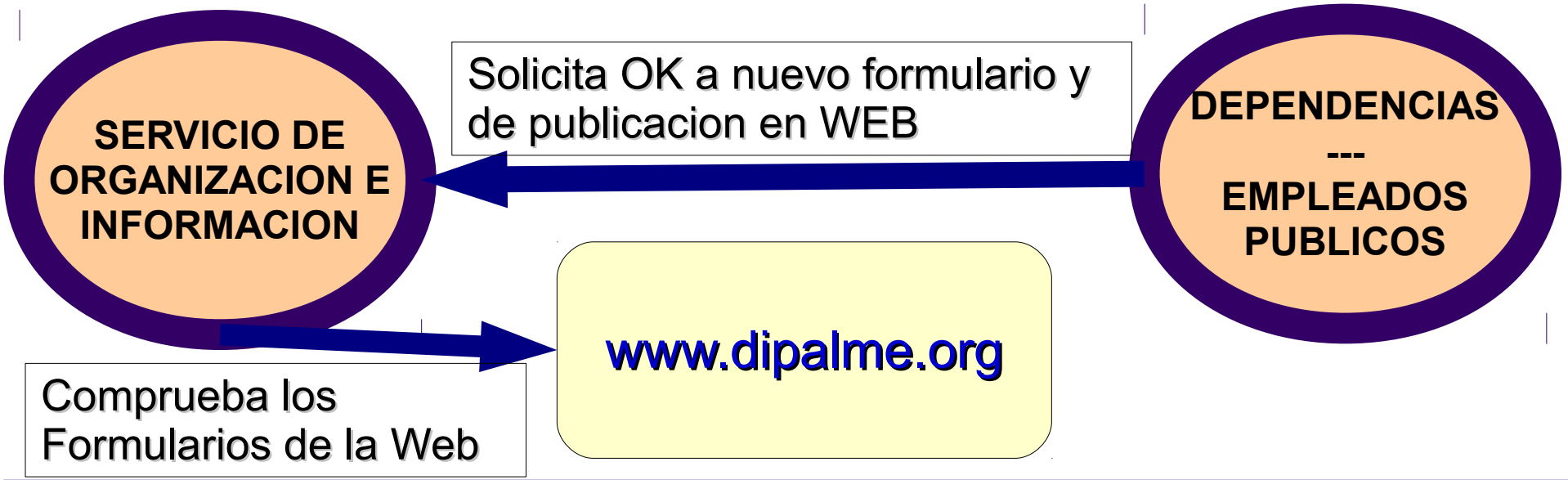
Para poder recoger datos personales, se tiene que informar de para qué se quieren esos datos, cómo se van a utilizar, si se van a comunicar a terceros y hay que habilitar un medio para que los interesados se pongan en contacto para que pueden ejercitar sus derecho ARCO.

Los Formularios deben dejar claro:

- **El Consentimiento de los interesados**
- **Que se informa según exige la LOPD**
- **Sobre la cesión o comunicación a terceros.**
- **Como ejercer los derechos ARCO**

(3.C.2)GESTION FORMULARIOS EN DIPUTACION

El Servicio de Organizacion e Informacion, supervisa la imagen institucional y realiza la revision de la confeccion de los formularios. Y realiza la comprobaciones de publicacion de los formularios en le Web www.dipalme.org



ES MUY IMPORTANTE CONSEGUIR LA SUPERVISION DEL 100% DE LOS FORMULARIOS EN PAPEL Y WEB, PARA CUMPLIR CON LA LOPD.
Existe aun formularios que no son supervisados y no cumplen con la LOPD

Para la entrada del nuevo RGPD (UE) tenemos que revisar el procedimiento sobre revision de formularios.

(3.C.2) CONSENTIMIENTO DEL INTERESADO

LOPD

Artículo 6. Consentimiento del afectado.
1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento

Se incluye en los formularios de recogida de informacion

RGPD (UE)

El RGPD mantendrá los mismos principios del consentimiento que establece la LOPD, exigiendo un consentimiento libre, informado, específico e inequívoco. Sin embargo, como novedad respecto de la LOPD, indica que para poder considerar que el consentimiento es inequívoco, deberá existir una declaración del interesado o una acción positiva que manifieste su conformidad. El silencio, las casillas ya marcadas o la inacción no constituirán prueba de consentimiento

Revision de formularios de recogida de informacion

(3.C.3) EJEMPLO DE CONSENTIMIENTO

Que cumple con la LOPD

En virtud de lo dispuesto en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que mediante la cumplimentación del presente formulario sus datos personales quedarán incorporados a los ficheros titularidad de (nombre de la Compañía), y serán tratados con la finalidad de (indicar la finalidad de la recogida de datos), así como para mantenerle informado, incluso por medios electrónicos, sobre cuestiones relativas a la actividad de la compañía y sus servicios. Si no desea que tratemos sus datos para estas finalidades por favor le rogamos señale la casilla correspondiente con una cruz. Usted puede ejercer, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal mediante correo electrónico dirigido a [poner tu correo aquí @] o bien mediante un escrito dirigido a [indicar tu dirección postal].

Para cumplir con el RGPD (UE)

…. **Si ~~no~~ desea que tratemos sus datos para estas finalidades por favor le rogamos señale la casilla correspondiente con una cruz.....**

Tenemos que revisar todos los formularios. (Recordemos que la Administracion, es raro que tenga que pedir consentimiento, ya que suele haber una norma que le habilite para el tratamiento).
Ojo CON LOS DATOS DE Menores.

(3.C.4) DEBER DE INFORMACION

LOPD

Nuestra legislación actual establece la obligación de informar en todo proceso de recogida de datos personales sobre la existencia de un fichero o tratamiento de datos de carácter personal, la identidad del responsable del tratamiento, la finalidad de la recogida de los datos y de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos ARCO de acceso, rectificación, cancelación y oposición.

Se incluye en los formularios de recogida de informacion y Carteles de Informacion

RGPD (UE)

El Reglamento establece la **obligación de informar sobre nuevos aspectos**. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, el período de conservación de los mismos y que los interesados podrán dirigir sus reclamaciones a las Autoridades de protección de datos, si consideran que hay un problema con la forma en que están manejando sus datos.

Revision de formularios de recogida de informacion y carteles

(3.C.5) COMO INFORMA DIPUTACION - LOPD

- En los formularios de recogida de información en Papel.
- En los formularios web de recogida de información
- En la web en el Aviso Legal y en la Política de Privacidad.
- En carteles publicitarios visibles en paredes y tablones.
- En pedestales de metacrilato en puntos de Información y Registro
- En Pantallas y Televisores de Información
- En los Centros telefónicos de información (Ej: Servicio Admon.Tributaria)

La Diputacion tiene muchas Dependencias y Centros en toda la Provincia, lo que dificulta la revision.
Hay que realizar un revision profunda de cara a al entrada en vigor del RGPD (UE).

(3.C.5)LOPD – EJEMPLO DE COMO INFORMAR

En cumplimiento de lo dispuesto en el Art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal , el Servicio de Administración Tributaria (SAT) de la Diputación de Almería le informa que sus datos personales, que han sido recogidos por el SAT o facilitados por Vd han sido incorporados para su tratamiento en un fichero automatizado.

Así mismo se le informa que la recogida y tratamiento de dichos datos tienen como finalidad la gestión de los procedimientos tributarios y recaudatorios que establece la Ley General Tributaria (58/2003 de 17 de diciembre) , Reglamento General de Recaudación (RD 939/2005 de 29 de Julio) y demás normas aplicables.

Le comunicamos que puede ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos comunicándolo por escrito a la Sección de Régimen Interior de la DIPUTACIÓN PROVINCIAL DE ALMERÍA, en la dirección: c/ Navarro Rodrigo 17, 04001, Almería, adjuntando copia de documento que acredite su identidad.

(3.C.6) COMO INFORMAR SEGUN RGPD(UE)

Los procedimientos de recogida de información pueden ser muy variados y, en consecuencia, los modos de informar a las personas interesadas deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos. Por ejemplo, algunas de las nuevas formas de recogida de datos y, en consecuencia, a través de los cuales hay que informar, pueden ser:

- ✓ Formularios en papel,
- ✓ Navegación o formularios Web,
- ✓ Datos de actividad personal
- ✓ Entrevista telefónica
- ✓ Registro de aplicaciones móviles
- ✓ Datos de sensores (IoT)

La Diputacion tiene que revisar los distintos sistemas de recogida de datos de los que dispone, para informar adecuadamente. (Ejemplo. Sistemas GPS en vehiculos)

(3.C.7) INFORMAR POR CAPAS- RGPD(UE)

Para hacer compatible la mayor exigencia de información que introduce el RGPD y la concisión y comprensión en la forma de presentarla, desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas o niveles.

- **Una primera capa con información Basica**
- **Una segunda capa con Información Detallada.**

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A. +info…
Finalidad	Gestionar el envío de información y prospección comercial +info…
Legitimación	Consentimiento del interesado +info…
Destinatarios	Otras empresas del grupo Warren&Brandeis, Inc. Encargados de Tratamiento fuera de la UE, acogido a "Privacy Shield" +info…
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional +info…
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos/info/

<VER GUIA>

(3.C.8) CESION DE DATOS PERSONALES

Para poder llevar a cabo una cesión de datos personales o comunicación de datos, de conformidad con la normativa, es necesario obtener el **consentimiento del titular de los datos**. El afectado por la cesión de los datos, debe ser informado y consentir expresamente la comunicación de los datos, para ello es necesario que sepa a quién se van a ceder y con qué finalidad. en este sentido, el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal regula la obtención y características del consentimiento del titular de los datos.

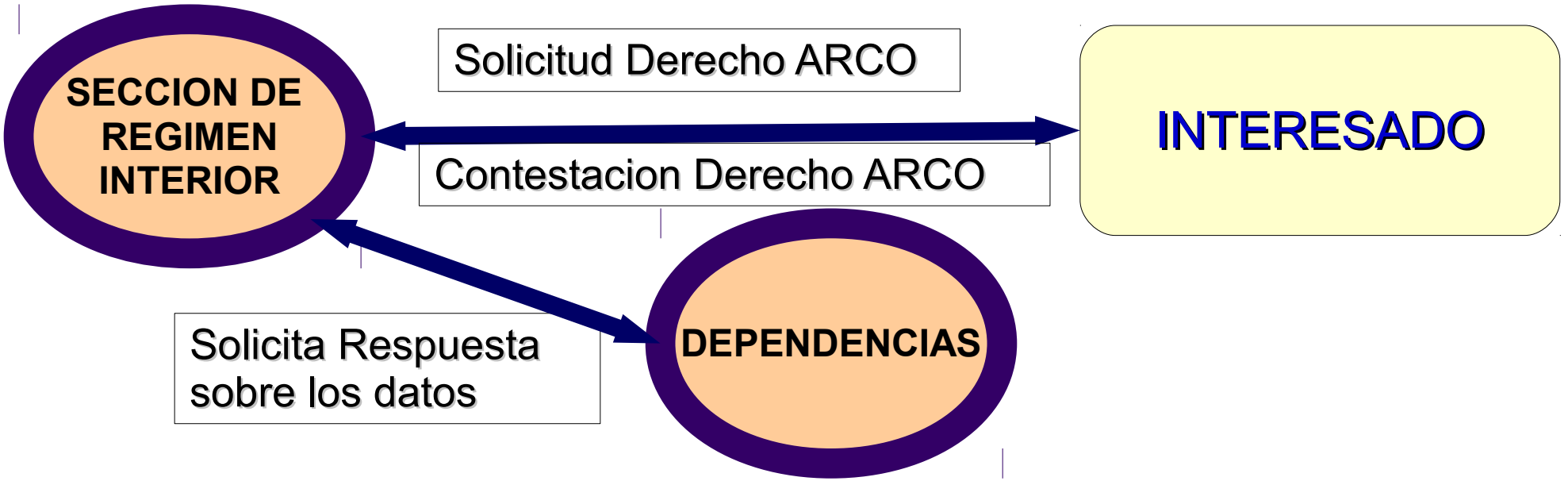
En la Diputacion la mayoria de ocasiones la cesion de datos personales viene regulado por las leyes, por lo que no se tiene que pedir consentimiento, pero si hay que informar.

En el Servicio Admon Tributaria a veces se tienen que comunicar datos de Tributos a Interesados no Titulares, y se comunican sin los datos del Titular.

Revision de formularios de recogida de informacion y carteles, si se informa sobre la cesiond ella informacion. Para la nueva entrada del RPD (UE)

(3.C.9) DERECHOS ARCO

La Seccion de Regimen Interior es quien COORDINA resolucion de las Solicitudes del Derecho ARCO, según el actual procediemto existente.



Se debe cambiar el Procedimiento para que resuelva el Servicio de Organizacion e Informacion, y por tanto revisar los Formularios y todos los sistemas de informacion.

(3.C.10) DERECHOS ARCO SEGUN RGPD (UE)

LOPD	RGPD (UE)
•Derecho de acceso •Derecho de rectificación •Derecho de oposición •Derecho de cancelación.	•Derecho a la transparencia de la información •Derecho de supresión (derecho al olvido) •Derecho de limitación •Derecho de portabilidad.

se establece la obligación para el responsable del tratamiento de proporcionar medios para que las solicitudes de ejercicio de derechos se presenten por medios electrónicos, en particular cuando los datos personales se hayan recabado a través de estos medios

Comenzar a implementar procedimientos de información (leyendas legales incluidas en los procesos de recogida de datos de carácter personal) los nuevos derechos que asisten a los interesados.

(3.C.11) CLAUSULAS DE FORMULARIOS

LOPD

Modelos de clausulas

<Ver Documento>

Ejemplo de formulario WEB

Ejemplo de Formulario con Consentimiento inequivoco

VER FORMULARIOS DE DIPUTACION

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.D- DEBER DE SECRETO. CONFIDENCIALIDAD.

(3.D.1) DEBER DE SECRETO

Articulo 10 LOPD: El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Para cumplir el deber de secreto, el Responsable del Fichero debe al menos:

- Informar al personal del deber de Secreto.
- Adoptar las medidas necesarios para la confidencialidad de los datos.

Para cumplir con el deber de secreto, entre sus medidas la Diputacion:

- **Hace firma unas clausulas de confidencialidad a todos los empleados**
- **Se hace firma a todos los Usuarios de la RPC confidencilidad.**
- **Se definen las funciones de cada puesto de trabajo**
- **Para acceso a las aplicaciones a cada usuarios se le asigna un perfil de acorde a sus funicones.**

No estaría de mas implantar sistemas para realizar recordatorios a empleados y usuarios del deber de secreto (sobre confidencialidad).

El RGPD (UE), no introduce grandes cambios en este aspecto.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.E- DOCUMENTO DE SEGURIDAD

(3.E.1) DOCUMENTO DE SEGURIDAD

Actualmente el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD) establece la obligación de aplicar diferentes medidas de seguridad, en función del nivel básico, medio o alto de los datos tratados. Dichas medidas se concretan y describen en el Documento de Seguridad.

La Diputación de Almeria, dispone de un Documento de seguridad, tal y como exige la LOPD. Pero:

- **La mayoría del Personal lo desconoce.**
- **No esta actualizado, ni es mantenido correctamente.**
- **Gran parte de los procedimiento y protocolos se estan cumpliendo, pero existe desconocimiento de que se realizan por exigencias de la LOPD**

El Documento de Seguridad debe ser un documento de referencia para todo el personal de la Diputación en lo referente a la Seguridad del tratamiento de datos personales.
Debe conocerlo todo el personal. Hay que informarle y formarle.

(3.E.2) DOCUMENTO SEGURIDAD EN RGPD-UE

El RGPD ya no distingue entre ficheros de nivel básico, medio o alto, sino que especifica que las medidas de seguridad se aplicarán teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas. La nueva legislación habla de "*medidas técnicas y organizativas apropiadas*" para garantizar un nivel de seguridad adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse.

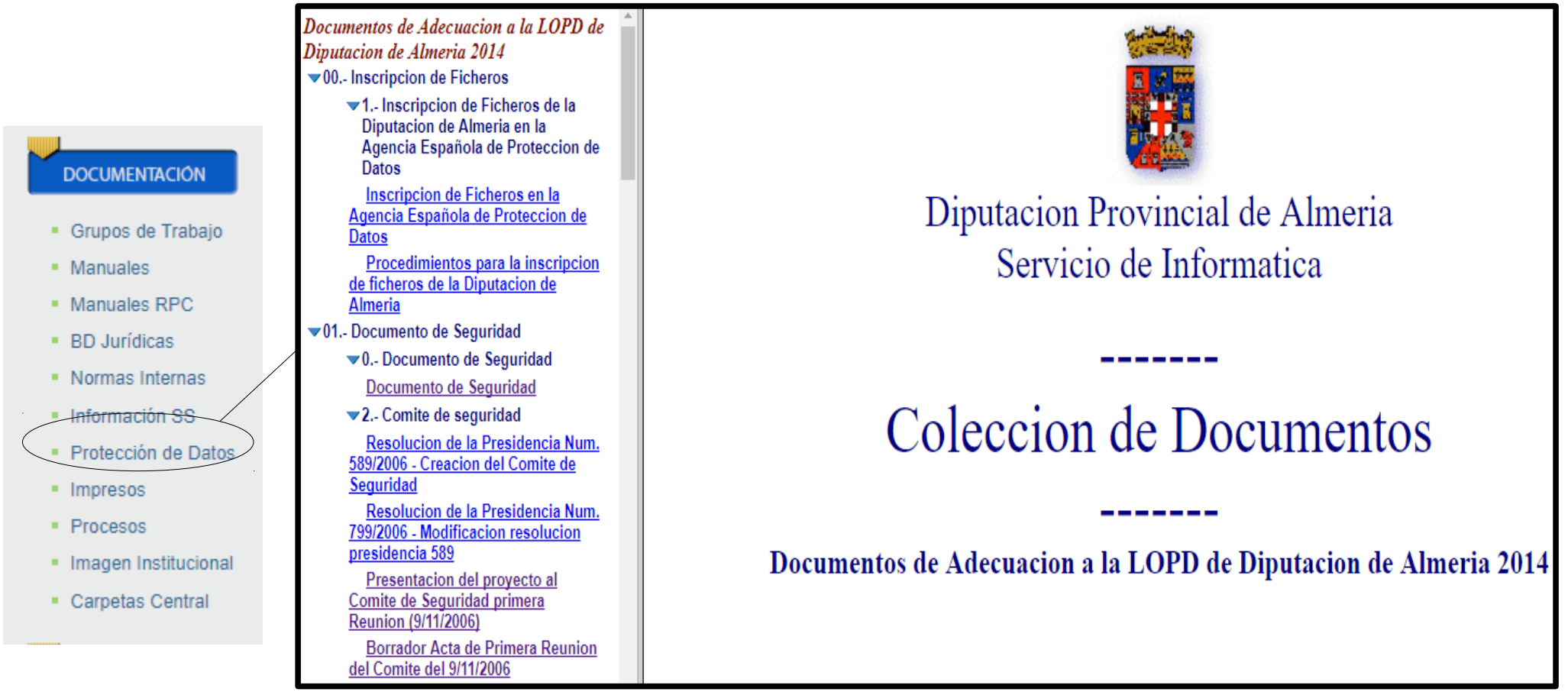
El Documento de Seguridad, cobrara mas relevancia con el nuevo RGPD, ya que sera en el donde hay que describir LAS MEDIDAS TECNICAS Y ORGANIZATIVAS que se aplicaran en la Organización

En la Diputación es necesario plantearse el modelo de documento a implantar:

- Documento de Seguridad único para toda la Diputación
- Documento de Seguridad por Dependencia.

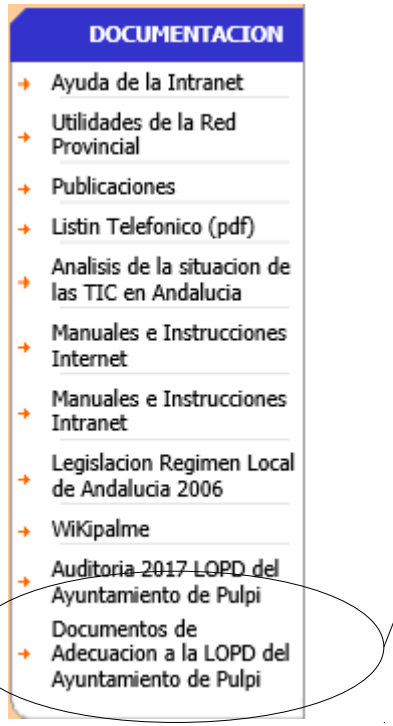
(3.E.3) DOCUMENTO SEGURIDAD DIPUTACION

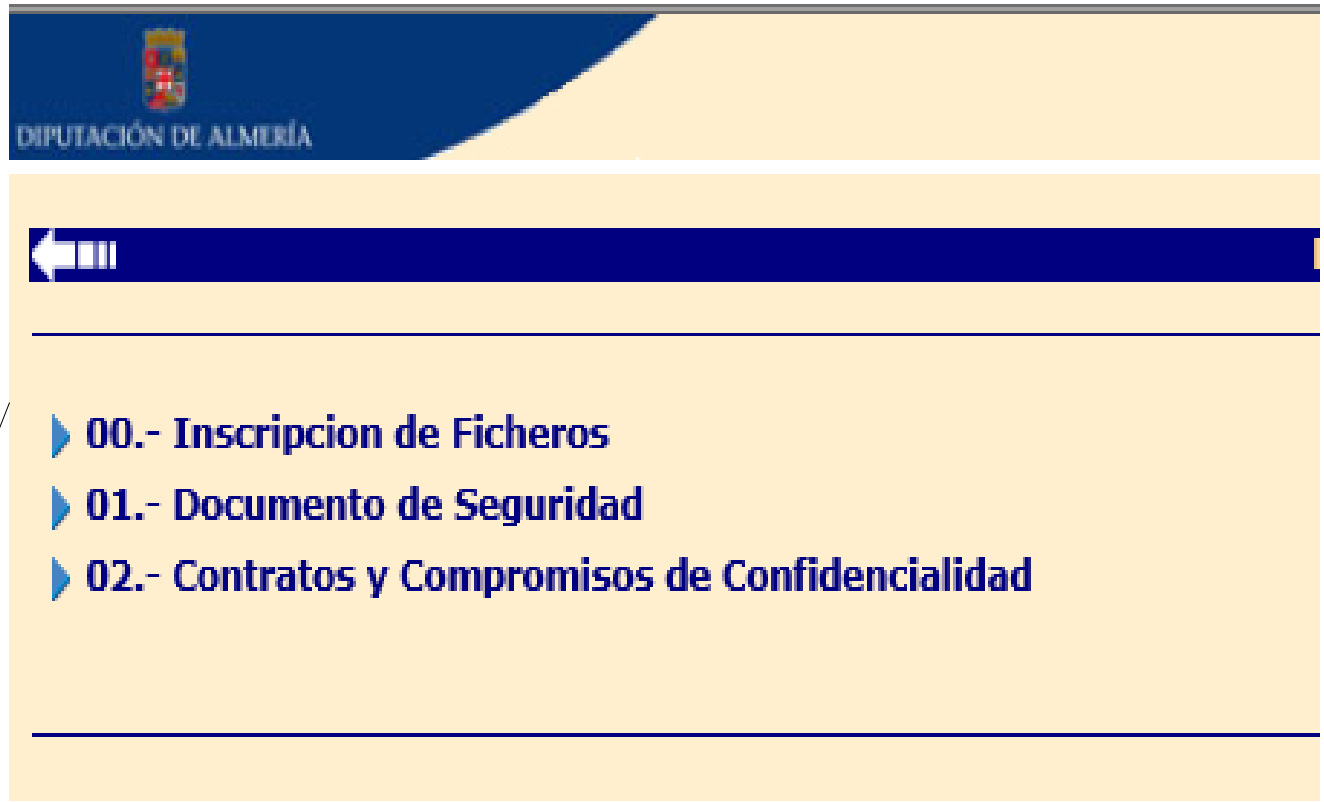
Desde la Intranet de la Diputacion se puede acceder al contenido deldocumento de Seguridad



(3.E.4) DOCUMENTO SEGURIDAD AYTOS

Desde la Intranet del Ayuntamiento se puede acceder al contenido deldocumento de Seguridad





GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.F- MEDIDAS DE SEGURIDAD

(3.F.1) MEDIDAS DE SEGURIDAD

Las medidas de seguridad se implantaran para evitar la pérdida de los datos o el acceso a estos por parte de terceros no autorizados.

LOPD

El Reglamento de LOPD establece las medidas de seguridad según el nivel de los ficheros:

- Basico
- Medio
- Alto

RGPD (UE)

La nueva legislación habla de "*medidas técnicas y organizativas apropiadas*" para garantizar un nivel de seguridad adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse.

El RGPD (EU) cambia el planteamiento de los criterios para que tipo de medidas aplicar, pero los tipos y sistemas de medidas que se deben de aplicar son las que se están aplicando ahora. SI ESTABLECE QUE HAY QUE REALIZAR ANALISIS DE RIESGOS (igual que ENS)

(3.F.2) LOPD – RESUMEN MEDIDAS DE SEGURIDAD

Lopd | seguridad en ficheros automatizados

Aviso. El contenido de esta web tiene un carácter meramente informativo, podría estar incompleto y carece de validez jurídica alguna. El uso que se haga del contenido de esta web es responsabilidad exclusiva del usuario.

INTRODUCCIÓN

Las medidas de seguridad aplicables en los » **ficheros automatizados** se encuentran reguladas en los artículos 89 a 104 del reglamento que desarrolla la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007) y son las siguientes:

	Medidas de seguridad	Nivel Basico	Nivel Medio	Nivel Alto
1	» Funciones y obligaciones del personal	Si	Si	Si
2	» Registro de incidencias	Si	Si	Si
3	» Control de acceso	Si	Si	Si
4	» Gestión de soportes y documentos	Si	Si	Si
5	» Identificación y autenticación	Si	Si	Si
6	» Copias de respaldo y recuperación	Si	Si	Si
7	» Responsable de seguridad	------	Si	Si
8	» Auditoria	------	Si	Si
9	» Gestión de soportes y documentos	------	Si	Si
10	» Identificación y autenticación	------	Si	Si
11	» Control de acceso físico	------	Si	Si
12	» Registro de incidencias	------	Si	Si
13	» Gestión y distribución de soportes	------	------	Si
14	» Copias de respaldo y recuperación	------	------	Si
15	» Registro de accesos	------	------	Si
16	» Telecomunicaciones	------	------	Si

Acceder a la pagina con la fuente de la informacion

(3.F.3) LOPD – RESUMEN MEDIDAS DE SEGURIDAD

Lopd | seguridad en ficheros no automatizados

Aviso. El contenido de esta web tiene un carácter meramente informativo, podría estar incompleto y carece de validez jurídica alguna. El uso que se haga del contenido de esta web es responsabilidad exclusiva del usuario.

INTRODUCCIÓN

Las medidas de seguridad aplicables en los » **ficheros no automatizados** se encuentran reguladas en los artículos 105 a 114 del reglamento que desarrolla la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007) y son las siguientes:

	Medidas de seguridad	Nivel Basico	Nivel Medio	Nivel Alto
1	» Funciones y obligaciones del personal	Si	Si	Si
2	» Registro de incidencias	Si	Si	Si
3	» Control de acceso	Si	Si	Si
4	» Gestión de soportes y documentos	Si	Si	Si
5	» Criterios de archivo	Si	Si	Si
6	» Dispositivos de almacenamiento	Si	Si	Si
7	» Custodia de los soportes	Si	Si	Si
8	» Responsable de seguridad	------	Si	Si
9	» Auditoria	------	Si	Si
10	» Almacenamiento de la información	------	------	Si
11	» Copia o reproducción	------	------	Si
12	» Acceso a la documentación	------	------	Si
13	» Traslado de la documentación	------	------	Si

Acceder a la pagina fuente de la informcion

(3.F.4) ¿QUE MEDIDAS APLICA DIPUTACION?

Para ver el cumplimiento de las Medidas de seguridad en general, vamos a clasificarlas las medidas que se aplicaran en los siguientes ámbitos:

- **MEDIDAS DOCUMENTALES**
- **MEDIDAS DE SEGURIDAD INFORMATICA**
- **MEDIDAS DE SEGURIDAD FISICA**
- **MEDIDAS SEGURIDAD ORGANIZATIVA**

(3.F.5) ¿QUE MEDIDAS APLICA DIPUTACION?

MEDIDAS DOCUMENTALES: son aquellas que se recogen por escrito para acreditar el cumplimiento de la LOPD

- Dar de alta los ficheros ante la Agencia Española de Protección de Datos. SI
- Elaborar el documento de seguridad. SI
- Contratos consentimiento con el afectado (recogida de datos) NO
- Los contratos con los encargados del tratamiento (prestación de servicios). SI

MEDIDAS DE SEGURIDAD INFORMATICA

- Gestión y control de Usuarios. SI (problema en cambio y baja)
- Cambios de Contraseñas. SI
- Los controles de acceso a los datos. SI (pero no todos accesos y cambios)
- La utilización de contraseñas únicas e intransferibles (cambio periódico). SI
- La realización de copias de seguridad de los datos.SI (servidores informatica)
- Encriptado de la Información NO
- Borrado de ficheros temporales. SI (solo servidor central de Datos)
- Borrado de datos innecesarios. SI
- Firma Electrónica de documentos. SI (se esta empezando)
- Control de equipos portatiles, moviles, tables, etc. NO
- Bloqueo de Pcs. SI (pero no por todo el personal)
- Seguridad Sistemas (Cortafuegos, Antivirus....). SI

(3.F.6) ¿QUE MEDIDAS APLICA DIPUTACION?

MEDIDAS DE SEGURIDAD FISICAS:

- El acceso a archivos con llave, código o huella (dato biométrico). SI (poco uso)
- Archivadores con llaves. SI (se desconoce el uso)
- Trituracion de documentos. SI
- La contenedores para la destrucción. NO
- Mesas despejadas. NO

MEDIDAS DE SEGURIDAD ORGANIZATIVA:

- Informar y Formar al personal sobre LOPD. SI (informar poco)
- El registro de incidencias respecto a los datos. NO
- Protocolo de destrucción de soportes y equipos. NO
- Inventarios y etiquetado de soportes. NO
- Procedimiento entrada y salida, cesion de información a terceros NO
- Procedimiento envios telematicos NO. (Editran, DipalBox)
- Acceso a Internet. SI (Pero sin aprobacion de Norma)
- Procedimiento uso de Email. NO
- Protocolo traslado documentos papel. NO
- Las auditorias obligatorias cada dos años. SI (ultima hace 4 años)

TENEMOS QUE MEJORAR MUCHO, SOBRE TODO EN EL DISEÑO PROCEDIMIENTOS Y FORMACION E INFORMACION A LOS EMPLEADOS.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.F bis- OBLIGACIONES CON LA SEGURIDAD

FUNCIONES Y OBLIGACIONES

Figuras implicadas en el cumplimiento de las Obligaciones de Seguridad la LOPD:

-Responsable del Fichero y Tratamiento

-Encargado del Tratamiento

-Responsable de Seguridad

-Responsables Delegados

-Comite de Seguridad

-Usuario Administradores de los Sistemas

-Usuarios y/o Empleados

FUNCIONES Y OBLIGACIONES USUARIOS

Usuario es todo el personal autorizado que accede a los datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo.

Todos los usuarios tienen la obligación de colaborar con el Responsable del Fichero para velar por el cumplimiento de la legislación vigente sobre Protección de Datos de Carácter Personal.

Los usuarios deben respetar los procedimientos definidos para gestionar la seguridad de la información que se detallan a continuación.

FUNCIONES Y OBLIGACIONES USUARIOS

OBLIGACIONES GENERALES

• Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos de carácter personal, está obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el Responsable del Fichero.

• La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta leve, grave o muy grave, conforme a lo previsto en el artículo 44 de la LOPD, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.

• Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.

• Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.

• Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos. Para ello se informará al Responsable del Fichero, Responsable de Seguridad o Encargado del tratamiento y se recogerá siempre en solicitud escrita.

OBLIGACIONES GENERALES SOBRE DEBER INFORMAR

- Facilitar el derecho de informacion a los titulares de los datos personales, que se traten, según los requisitos previstos en la normativa vigente.

- Velar por el cumplimiento de la obligacion de informacion sobre los datos personales, en la confeccion y uso de formularios de recogida y modificacion de datos.

- Valar por el uso adecuado delos carteles para cumplir con la obligacion de informar sobre tratamiento de datos persoanles.

CESION Y COMUNICACIÓN DE DATOS

-Recuerde que la cesión o comunicación de datos personales se pueden realizar:

-Con el consentimiento de propietario de los datos.

-Cuando exista una Ley o norma que lo habilite.

-Cuando se ceda a otra Administración para la misma finalidad para la que se recogieron.

- Cuando que se haga para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario

- No se pueden comunicar a una persona distinta del propietario si no tenemos su consentimiento o el tercero acredita dicho consentimiento. (Representante o Administrador)

PUESTOS DE TRABAJO (Credenciales y Contraseñas)

- Cada usuario tiene que tener credenciales personales para acceso a puesto de trabajo y sistemas. No se utilizaran credenciales genéricas.
- Cada usuario deberá custodiar de forma confidencial las contraseñas de los códigos de usuarios que se le asigne.
- Si tiene sospechas de que la conocen terceros deberá cambiarla
- En el primer acceso al sistema deber cambiarla.
- La longitud de la contraseña debe ser mínimo de 8 caracteres, y debe contener letras y números, no debe coincidir con el código de usuario.
- Deberá cambiar la contraseña al menos cada 6 meses.

PUESTOS DE TRABAJO (Uso de puesto)

- Los Usuarios utilizaran el puesto de trabajo debe ser utilizado solo para los trabajos y tratamiento de información dentro sus funciones.

- El uso personal solo se realizara si existen garantias de que no afecten a la seguridad y previa autorizacion del responsable.

- La ubicación del puesto de trabajo se realizara de forma que se garantice la confidencialidad siempre que se trate datos personales.

- Durante la ausencia del usuario el equipo de trabajo debera estar apagado o bloqueado (uilizar bloqueo de pantalla o suspension)

- No se debe cambiar la configuración del puesto si la previa autorizacion de los adminsitradores.

-Los antivirus, antispam, etc.. no se manipularan, respetando las configuraciones de los administradores.

IMPRESIÓN

- La impresión de documentos con datos personales se realizara garantizando la confidencialidad.
- Se utilizaran preferentemente impresoras que no impriman si la presencia del usuario, y que borren los trabajos si nadie demanda la impresión (sistema de impresión con identificación usuario).
- Solo se imprimira lo que sea estrictamente necesario.
- Se debe imprimir reestabilizando al maximo el papel.
- Se utilizaran las marcas de agua para indicar si el documento, es borrador, confidencial, etc..
- Las impresoras individuales seran utilizadas solo para casos muy especificos y con autorizacion.
- Se deben evitar las impresiones en la nube, quedando prohibidas para datos personales.
- Se comprobara que no queden documentos en las bandejas de salida.
- Se deben Impresoras con Identificacion de Usuarios

ALMACENAMIENTO DE INFORMACION

-Se evitara guardar información en los Puestos de trabajo, si no se garantiza la confidencialidad, integridad y disponibilidad. (Si no se realizan copias de seguridad con garantias).

-Para guardar la información se utilizaran los sistemas de almacenamientos en red que tengan garantizadas los controles de acceso y la gestión de copias de seguridad.

-La utilización y generación de documentos de trabajo se almacenaran en espacios de almacenamiento temporales y se borraran una vez no sean necesarios.

-Se vaciara la papelera de reciclaje del puesto de trabajo diariamente.

USO DE PORTATILES, TABLES, MOVILES, ETC..

-Se evitara el uso de Portatiles, Tables, Moviles, etc..

-Para el caso que sea estrictamente necesario Se borraran los datos des estos dispositivos una vez que no sean necesarios.

-Se deberá de garantizar el nivel de seguridad correspondiente.

-Para tratar información con datos personales fuera de las instalaciones del Responsable del fichero se debe disponer de los correspondientes permisos y se de garantizar el nivel de seguridad.

-Se debe borrar la informacion que se utilice en estos equipos cuando se dejen de utilizar.

CONTROL DE ACCESOS

- Los usuarios accederán solo a lo sistemas de información que estén autorizados y con los previligios correspondientes a las funciones a desarrollar.

-Deberán se solicitar de sus responsables aquellos permisos de acceso que le sean necesario para el desempeño de sus funciones.

-Deberán de solicitar de sus responsables que se les anule los permisos y privilegios que no le sean necesarios.

-Se detectan cualquier anomalía en los premisos y privilegios deberán comunicarlas a sus superiores.

GESTION DE DOCUMENTOS CON DATOS PROTEGIDOS

- Los documentos o ficheros que generen los usuarios y que tengan datos personales se deben almacenar en dispositivos que garanticen su confidencialidad (sistemas de almacenamiento de red con los correspondientes controles de acceso), y en caso de duda codificados.

- El envió por email de este tipo de documentos deberá de ser en los casos estrictamente necesarios y codificando la información de los datos protegidos.

- También se deberá utilizar la disociación de la información cuando se vea peligrar la confidencialidad.

USO DE CORREO ELECTRONICO (I)

-No se deben utilizar cuentas de Email no corporativos para el envio en mensajes relacionados con las funciones del puesto. Ojo con las transferencia internacional de datos.

-No se debe usar el Correo personal en las instalaciones con los equipos de la empresa sin las debidas medidas de seguridad.

-Borrar todo mensaje del que se tenga dudas de su remitente o de su contenido.

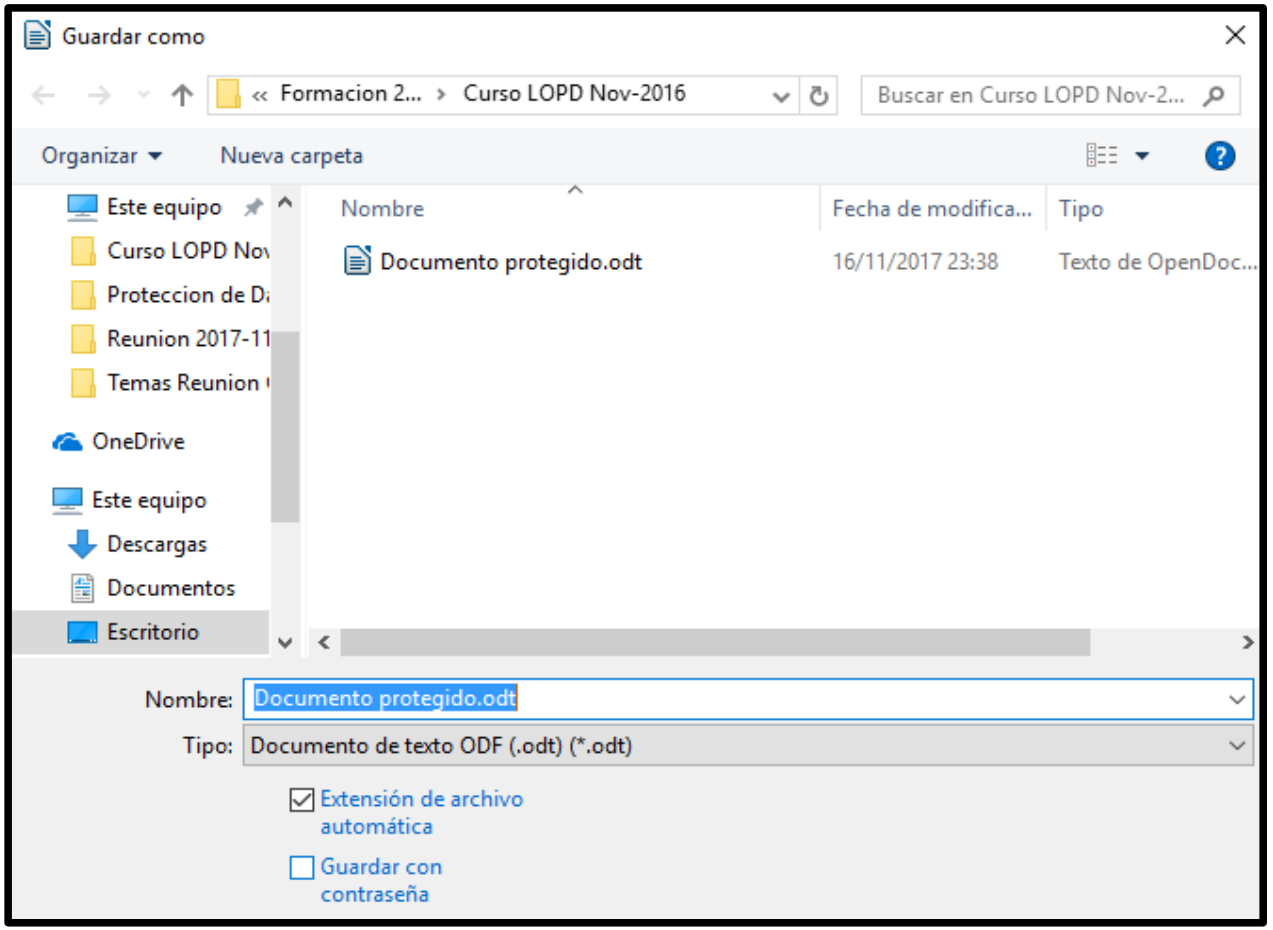
-Para el envió de información con datos personales protegidos fuera de las instalaciones de la organización se debe enviar codificada.

-Solo se puede comunicar datos personales si se van a utilizar para la misma finalidad con la que están declarados.

- Se debe utilizar el Email Departamental para envios oficiales.

Proteger documentos con contraseñas

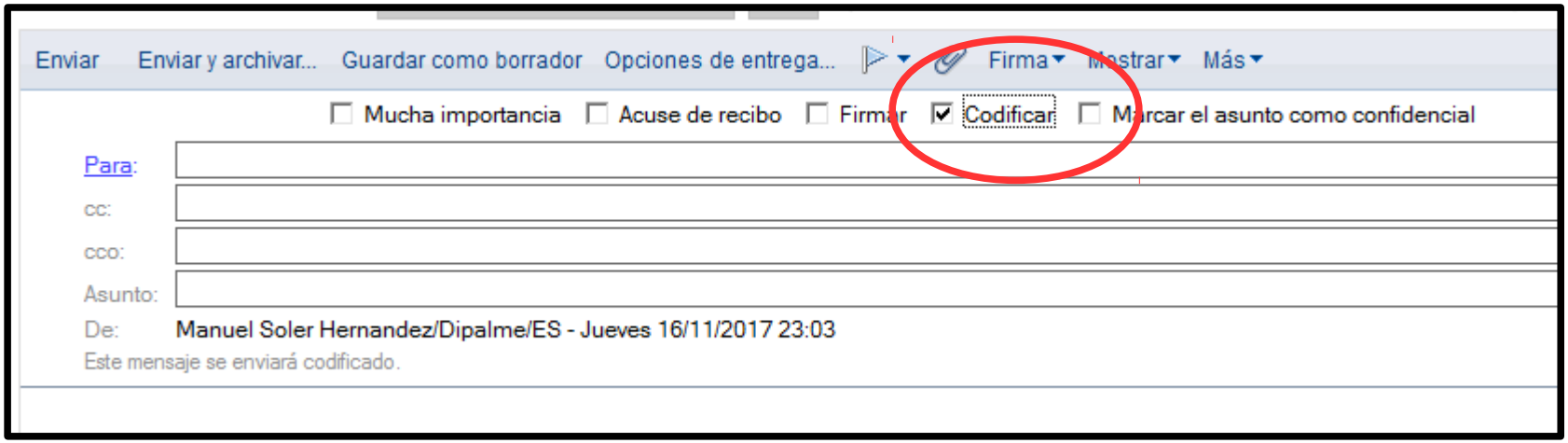
- Con las distintas herramientas ofimaticas, word, excel, openoffice, libreoffice, etc. se puede proteger



USO DE CORREO ELECTRONICO (II)

- Codificar los correos electrónicos

  -Cuando los destinatarios de los Email sean, usuarios y email departamentales, se puede realizar la codificacion de los email de forma que si se abre por otro usuario no pueda leer el contenido.

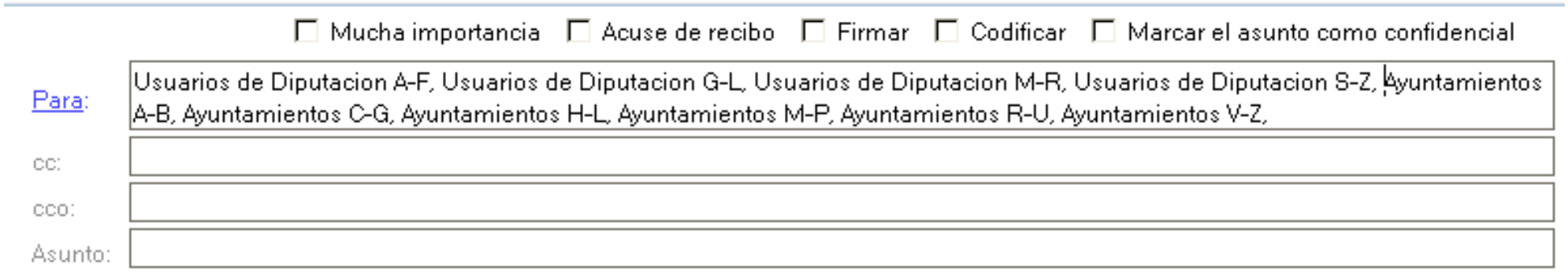


USO DE CORREO ELECTRONICO (II)

- Siempre. que se utiliza el Email, se están tratado datos personales, al menos la dirección de mail. Por eso:

  -Debe borrar de forma periódica los Email que no necesite. (Articulo 4.5 Calidad de los datos)

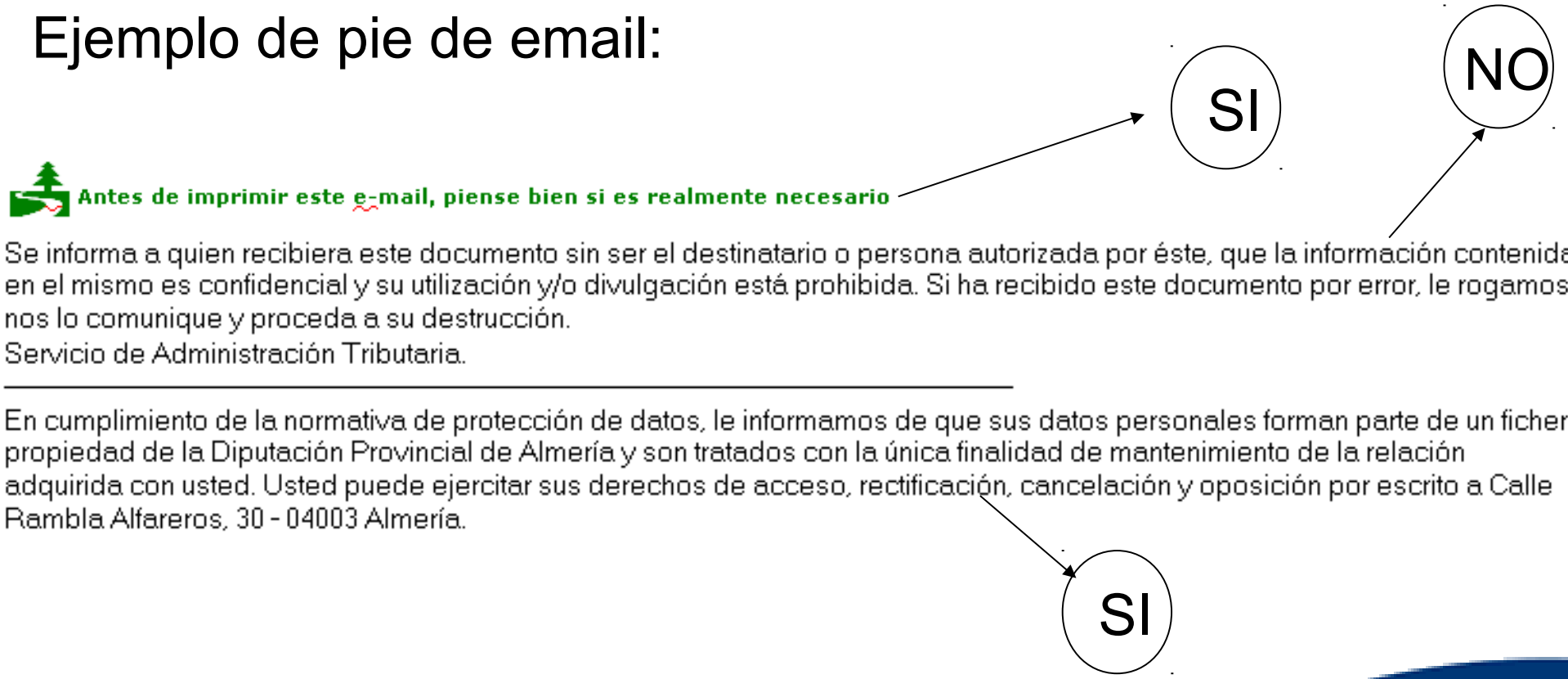
  -Debe tener cuidado de no difundir los Email, utilizando el campo CCO cuando envía email masivos, con listas de distribución (Ver ejemplo).



USO DE CORREO ELECTRONICO (III)

- ¿Cómo informar del tratamiento de Datos en los envios de Email y cumplir con el Articulo 5?

Ejemplo de pie de email:



ALMACENAMIENTO DE INFORMACION EN LA NUBE

-No utilizar Gamil u otro proveedor parecido de correo gratuito en la nube como correo oficiales de la organización.

-No se utilizaran sistemas de almacenamiento en la nube como Dropbox, Drive, etc. (ojo con Transferencias Internacionales).

-La Red Provincial de Comunicaciones dispone de un Sistema Seguro DipalBox.

-Se puede utilizar DipalBox para guardar información voluminosa codificada y/o protegida y enviar datos de codificación y/o contraseñas por email.

USO DE DIPALBOX PARA ENVIO DE INFORMACION

GESTION DE SOPORTES (I)

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Ejemplos de soportes: disquetes, cd-rom, dvd-rom, memoria usb, disco duro, etc.

Los Usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

- Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.

- Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con una etiqueta externa e inventariados.

GESTION DE SOPORTES (II)

• Los soportes que contengan datos de carácter personal, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.

• La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del Responsable del Fichero, deberá ser autorizada por el Responsable del Fichero o estar debidamente autorizada en el Documento de Seguridad.

• La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada por el responsable del fichero (o aquel en que se hubiera delegado), o encontrarse debidamente autorizada en el Documento de Seguridad.

GESTION DE SOPORTES (IIi)

• El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

• Cuando deban ser enviados datos personales fuera de las ubicaciones del Responsable del Fichero, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

RECOMENDACIONES PARA ARCHIVOEN PAPEL

- La referencias de los expedientes deberan ser codigos, de forma que no se pueda saber a priori que datos personales contienen.

- Se dipondra de listado con Informacion por Codigos y Apellidos, de forma que se relacionen de forma facil y localizable los expedientes archivados.

- Cuando los sistemas sean Mixtos, Electronicos y Papel, se buscara de forma electronica la referencia del expediente para su localizacion en el archivo en papel.

- Las zonas de archivo en papel debe estar protegida con llave a algon sistema de no permitir acceso a personal no autorizado.

- Los Archivadores deberan tener llaves, y se protegeran para no ser accedido por personal no autorizado.

- Se debe realizar un regisros de los expedientes que se sacan del archivo, por quien y para que.

2.3.1. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento.

- Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

DESTRUCCION Y REUTILIZACION DE SOPORTES

• Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

• Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable del Fichero.

DETRUCCION Y REUTILIZACION DE SOPORTES

• Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

• Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable del Fichero.

• Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable del Fichero para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

2.4. FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

• Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación.

LOPD – FUNCIONES Y OBLIGACIONES USUARIOS

2.5. DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

• En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

• Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Dichas medidas son:

• El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

• En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

2.5. DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

2.5.1. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

2.5. DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

2.5.1. DESTRUCCIÓN DE DOCUMENTACIÓN

• Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

• En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

• El Responsable del Fichero deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

2.6. GESTIÓN DE INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos de carácter personal en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

- Pérdida de información de algún fichero de datos de carácter personal.
- Modificación de datos personales por personal no autorizado o desconocido.
- Existencia de sistemas de información sin las debidas medidas de seguridad.

2.6. GESTIÓN DE INCIDENCIAS

- Los intentos de acceso no autorizados a ficheros de carácter personal.
- El conocimiento por terceros de la clave de acceso al sistema.
- El intento no autorizado de salida de un soporte.
- La existencia de soportes sin inventariar y que contengan datos personales.
- La destrucción total o parcial de un soporte que contenga datos de carácter personal.
- La caída del sistema de seguridad informática, que posibilite el acceso a datos personales por personas no autorizadas.
- El cambio de la ubicación física de ficheros con datos de carácter personal.
- Cualquier incidencia que pueda afectar a la confidencialidad, integridad y/o disponibilidad de los datos de carácter personal.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.G- TRATAMIENTO INTERNACIONAL DE DATOS

(3.G.1) TRATAMIENTO INTERNACIONAL DATOS

Una transferencia internacional de datos, es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (art. 5.1.s) RLOPD).

LOPD

Para realizar transferencias internacionales de datos, será necesaria la Autorización previa de la Directora de la Agencia Española de Protección de Datos, salvo que se ampare en alguno de los supuestos de excepción previstos en los apartados a) a j) del artículo 34 de la LOPD

RGPD (UE)

Se regula de forma muy similar a como se realiza en la LOPD.

OJO: Con el uso de aplicaciones en la NUBE, como Gmail, DropBox, Tuiter, FaceBook, etc... (se deben prohibir para datos personales).
Es necesario Informar al Personal sobre no utilizar estas herramientas.

(3.G.2) EJEMPLO DE TRATAMIENTO

Con el objeto de promocionar la pagina de FaceBook del Patronato de Turismo, se aprobecha la actuacionde David Bisbal en Huercla-Overa para rifar una jornada con el Cantante, de entre todos las entradas de ME GISTA de pagina de Turismos, para ello se solicita los siguientes datos:

http://www.techlegal.es/bases-legales-de-sorteos-y-concursos/

- Nombre y Apellidos
- NIF
- Email
- Movil
- Fecha de Nacimiento

Son proporcionados los datos para la Finalidad que se persigue con el tratamiento.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.H- CONTRTATO PARA TRATAMIENTO POR TERCEROS

(3.H.1) – CONTRATOS DE TRATAMIENTO DATOS

El artículo 12 de la LOPD impone a toda empresa, profesional y organización privada la celebración de un contrato de tratamiento de datos cuando el proveedor preste servicios que impliquen el acceso a datos personales.

RGPD (UE). Se regula de forma muy similar a como se realiza en la LOPD.

La Diputación de Almeria, en los pliegos de las Licitaciones, pone las clausulas sobre el tratamiento de datos personales.

Seria necesario que la Dependencia que gestiona la LOPD (Servicio de Organización e Información), emitiese informe sobre el cumplimiento de la LOPD en los pliegos de Contratación.

También es necesario contrastar que los empleados de las Empresas contratadas, saben y conocen las normas sobre Proteccion de Datos de la Diputacion, y que han firmado el deber de secreto.

EJEMPLO DE CLAUSULAS PARA CONTRATO CON TERCEROS

(3.H.2) – EJEMPLOCLAUSALAS PARA CONTRATO DE PRESTACIONES DE SERVICIO POR TERCEROS

3.3. El adjudicatario encargado del tratamiento estará sometido a las siguientes obligaciones con respecto de los datos de carácter personal:

- Actuará conforme a las instrucciones del SAT, responsable del fichero.
- Adoptará todas aquellas medidas de índole técnica y organizativa que resulten necesarias para garantizar la seguridad de los datos de carácter personal, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizados.
- No aplicará ni utilizará los datos con fines distintos a los de realización de los trabajos objeto del contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
- Estará obligado a guardar el secreto profesional respecto del mismo, aún después de finalizar sus relaciones contractuales.
- Una vez finalizados los trabajos objeto del contrato, el adjudicatario deberá devolver al SAT todos los documentos o soportes informáticos en que pudiera constar algún dato de carácter personal.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.I- RESPONSABLE DE SEGURIDAD – DELEGADO PROTECCION DE DATOS

(3.I.1) RESPONSABLE DE SEGURIDAD (LOPD)

Las empresas o cualquier otra entidad tendrá la obligación de nombrar a un responsable de seguridad cuando realice tratamientos de datos de carácter personal a partir del nivel medio, aunque es recomendable que se nombre en todo caso.

NOMBRAMIENTO: La designación podrá ser única para todos los ficheros o diferenciada según los sistemas de tratamientos utilizados, esta casuística deberá constar igualmente en el documento de seguridad.

FUNCIONES: La función principal es la de coordinar y controlar las medidas de seguridad definidas en el documento de seguridad, de esta función se derivan muchas otras, en su mayoría funciones que pueden ser delegadas por el propio responsable del fichero,

En la Diputación el Responsable del Fichero es el Jefe del Servicio de Organización e Información. Y se nombra Responsables Delegados en cada Dependencia que son los Responsables de las mismas. PERO EN LA PRACTICA NO FUNCIONA CORRECTAMENTE

(3.I.2) DELEGADO PROTECCION DATOS (RGPD)

RGPD (UE). Introduce la nueva figura del Data Protection Officer o Delegado de Protección de Datos, que asume nuevas y cualificadas competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos. ES OBLIGATORIO PARA LAS ADMON. PUBLICAS.

NOMBRAMIENTO: Tiene que ser una persona con la formación adecuada, y puede ser empelado de la propia organización, o contratar con personal externo mediante prestación de servicios.

MISION: velará porque se cumpla la normativa de protección de datos en las organizaciones y tendrá estrecha relación con las autoridades correspondientes a esta legislación. Gozara de total independencia.

ANTES DE MAYO DE 2018, LAS ADMONS PUBLICAS TIENEN QUE NOMBRAR U DELEGADO DE PROTECCION DE DATOS. DEBE TENER FORMACION JURIDICA EN PROTECION DE DATOS.

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.J- AUDITORIAS DE PROTECCION DE DATOS

(3.J.1) AUDITORIAS DE PROTECCION DE DATOS

LOPD

El artículo 96 de la LOPD, establece el informe de auditoría es obligatorio para todas las organizaciones que, por el tipo de datos que almacenan, tienen un nivel de seguridad medio o alto. Y sera bienal, puede ser interna o externa.

Las Auditorias son obligatoria

RGPD (UE)

-Obliga a las empresas a valorar los riesgos producidos por el uso de datos personales, así como a adoptar medidas de seguridad y procesos de verificación para cumplir con la normativa.
-Obliga a elaborar una evaluación de impacto cuando las actividades de tratamiento de datos impliquen un riesgo específico para los afectados por su naturaleza, alcance y fines.

Las Auditorias son esenciales

Cuanto menos formados en Proteccion de Datos Personales este el personal de Diputacion, mas se depende de auditorias externas. Ultlma auditoria hace 4 años

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.K- DIFUSION E FORMACION AL PERSONAL

(3.K.1) DIFUSION Y FORMACION

Cualquier empresa que trate datos de carácter personal esta obligada adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones , en lo relacionado con tratamiento de datos personales, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

LA Diputacion realiza Joranadas y cursos de Protecion de Datos Personales, pero son insuficientes.
La Difusion e informacion al personal sobre esta materia tambien es escasa y casi nula.

En 2016 se han realizado 3 acciones formativas de 1 dia, en el Plan Agrupado, para personal de Diputacion y EELL de la provincia, con una afluencia de alumnos de menos de 100.

HAY QUE REALIZAR MAS ESFUERZO EN FORMACION Y DIFUSION SOBRE PROTECCION DE DATOS PERSONALES

GESTION DE LA PROTECCION DE DATOS PERSONALES EN LA DIPUTACION DE ALMERIA

3.L- APOYO A LAS EE.LL. DE LA PROVINCIA

(3.L.1) APOYO A LAS EE.LL. DE LA PROVINCIA

El apoyo y la colaboracion de la Diputacion a las EE.LL. de la Provincia de Almeria para implantacion y mantenimiento de nuevas tecnologias se regula por el Convenio Marco de Gestion de la RPC. Siendo en particular para la Gestion en LOPD en:

- Colaboracion y subvencion en las Auditorias de LOPD
- Asesoramiento en la Gestion de la LOPD
- Resolucion de todo tipo de dudas y consulta.
- Atencion telefonico y en linea.
- Plazas para formacion dentro de Plan Agrupado.

Diputacion tiene que aumentar los recursos para apoyar a las EELL de la provincia en:

- **Cumplimiento del nuevo RGPD -UE**
- **Coordinar a los Delegados de Proteccion de Datos**

GRACIAS POR SU ATENCION

Servicio de Organizacion y Seguridad
Manuel Soler Hernandez
msolerhe@dipalme.org
16 de Noviembre de 2017