

Jornadas protección de datos, transparencia y esquema nacional de seguridad.

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

Servicio de Organización y Seguridad
Manuel Soler Hernandez
msolerhe@dipalme.org
6 de Octubre de 2017

OBJETIVO DE LA PONENCIA

Explicar como se gestiona en la Diputacion de Almeria 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 proteccion de datos personales.

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

1- INTRODUCCION

(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)** (REGLAMENTOS REGLAMENTO (UE) 2016/679 DEL PARLAMENTO 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) CONTROL DE SEGURIDAD EN DIPUTACION



- Los recursos dedicados al control de la seguridad física y del patrimonio son muy superiores que los destinados al de la seguridad de la Información.

- La información supone el mayor activo de la Diputación. Y con la Admon. Electrónica aumenta su importancia.

- Un porcentaje alto de esa información contiene datos personales



(1.3) GESTION LOPD PROCESO CONTINUO

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



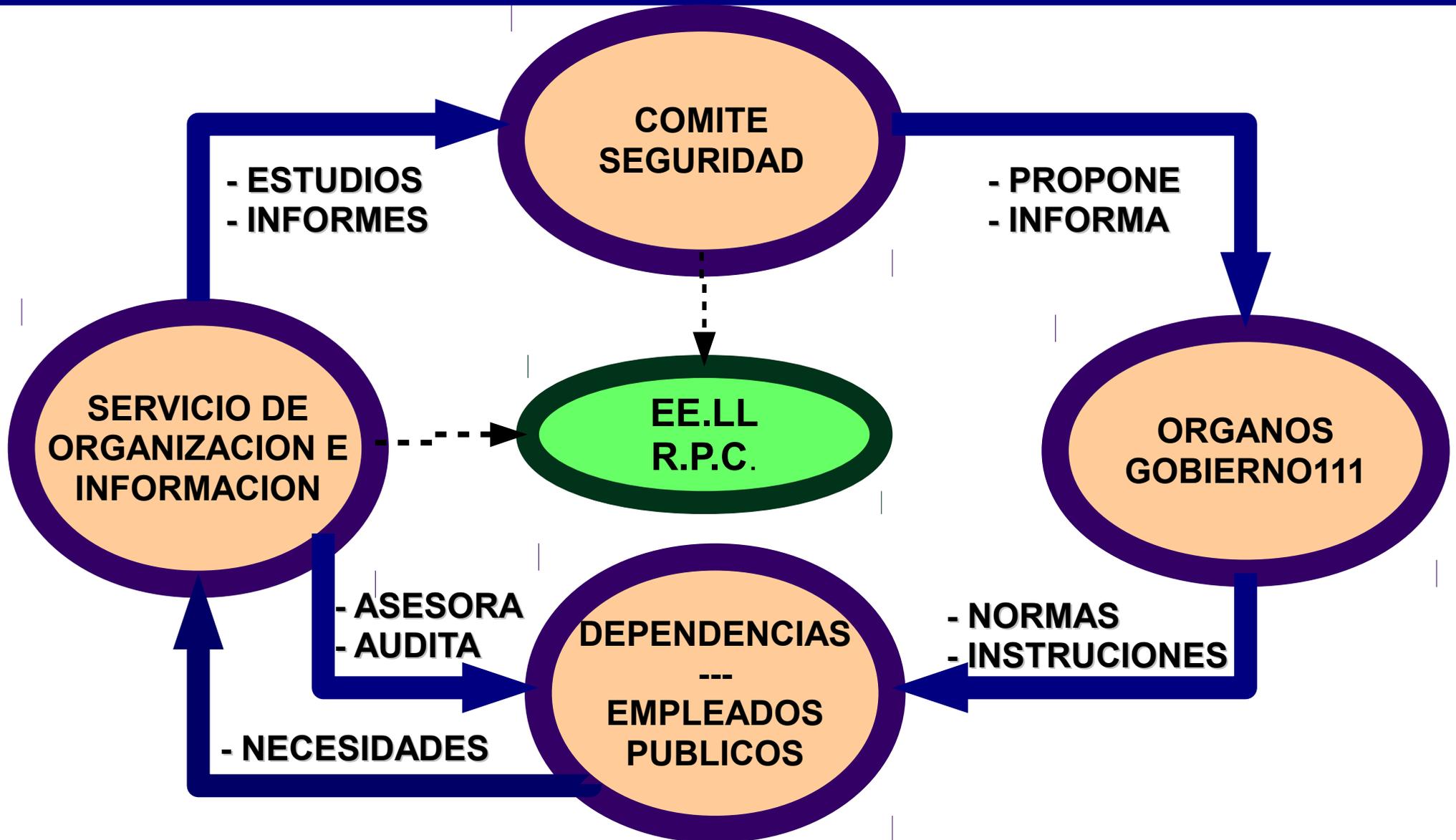
LA GESTION DE LA LOPD SE TIENE QUE IMPLANTAR COMO UN PROCESO CONTINUO:

- Planificar
- Hacer
- Auditar
- Actualizar

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

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

(2.1) ORG.GESTION LOPD EN DIPUTACION



El procedimiento de contestación sobre Derechos ARCO los COORDINA la Sección de Régimen Interior. Y se debe cambiar para que los haga el Servicio Organización e Información

(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 dercho 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 cumplimiento de las normas y directrices e protección 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 gestión de protección de datos según las directrices de la organización.
- Comprobar y hacer cumplir las directrices de seguridad en su dependencia.

- Los responsables máximos de las Dependencias serán 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 protección de datos personales.
- El Presidente de la Diputación es el Responsable máximo de la Gestión de la Protección de Datos Personales.

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

**3- ASPECTOS
IMPORTANTES
CUMPLIMIENTO DE LA
LOPD**

(3.1) QUE SUPONE LA GESTION DE LA LOPD

La LOPD le obliga a realizar y actualizar las siguientes acciones:

- 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 información), 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) Difusión y Formación al Personal**
- L) Se hace necesario el Apoyo a la EELL de la provincia.**

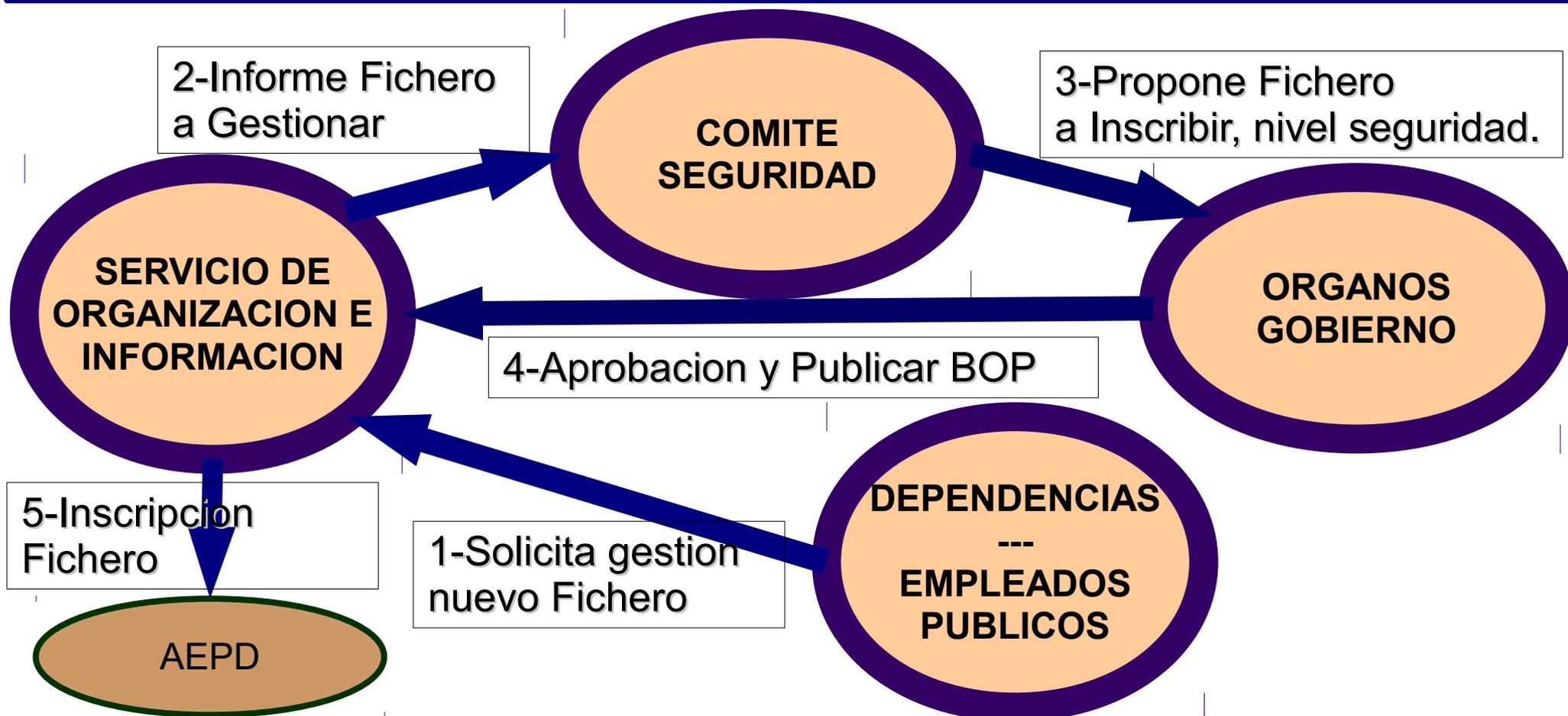
**GESTION DE LA PROTECCION DE DATOS
PERSONALES EN LA
DIPUTACION DE ALMERIA**

**3.A- INSCRIPCION DE
FICHEROS EN LA AEPD**

(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.



Es posible que existen ficheros sin inscribir o anular. Hay que hacer una revision de cara al nuevo RGPD (UE)

(3.A.2) RGPD(UE)– REGISTRO TRATAMIENTO

Según lo previsto en el artículo 30 del RGPD, las organizaciones que habitualmente realicen tratamiento de datos de riesgo para la privacidad de los interesados, o traten datos sensibles, deberán contar con un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

1-Evaluacion Impacto

Se establece la obligación de realizar una evaluación de impacto para las organizaciones que realicen tratamientos de datos que puedan implicar un alto riesgo para los derechos y libertades de las personas físicas, en la que se evalúe el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo.

Contratar consultoria EIPD

2-Registro Tratamiento de datos

Según lo previsto en el artículo 30 del RGPD, las organizaciones que habitualmente realicen tratamiento de datos de riesgo para la privacidad de los interesados, o traten datos sensibles, deberán contar con un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

Definir procedimiento y Fichero

**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 ficheros a la responsabilidad activa, que implica entre otras las siguientes medidas:

- Protección de datos desde el diseño
- Protección de datos por defecto
- Evaluación de impacto.

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

**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

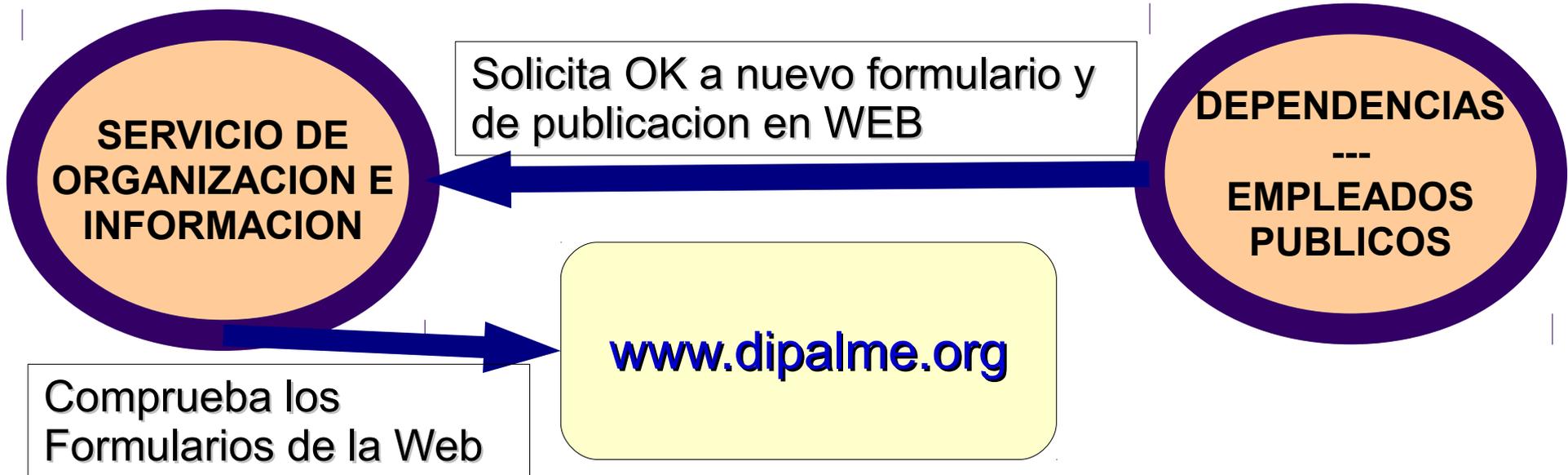
Para poder recoger datos personales, se tiene que informar de para qué se quieren esos datos, cómo se van a utilizar, si se van a comunicar a terceros y hay que habilitar un medio para que los interesados se pongan en contacto para que pueden ejercitar sus derecho ARCO.

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 comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento

Se incluye en los formularios de recogida de información

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

Revisión de formularios de recogida de información



(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 Administración, 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 información y Carteles de Información

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.

Revisión de formularios de recogida de información 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.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 Diputación tiene que revisar los distintos sistemas de recogida de datos de los que dispone, para informar adecuadamente. (Ejemplo. Sistemas GPS en vehículos)



(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 Básica
- 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/

(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.

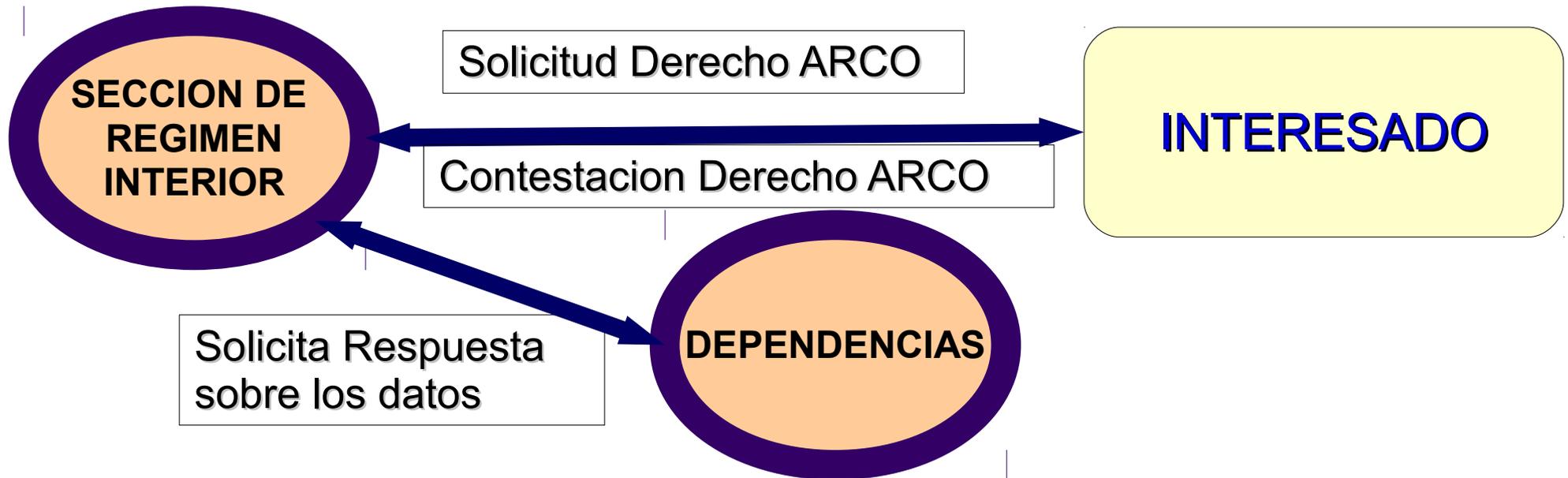
En la Diputacion la mayoría de ocasiones la cesion de datos personales viene regulado por las leyes, por lo que no se tiene que pedir consentimiento, pero si hay que informar.

En el Servicio Admon Tributaria a veces se tienen que comunicar datos de Tributos a Interesados no Titulares, y se comunican si 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 resolucioin de las Solicitudes del Derecho ARCO, según el actual procedimiento 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 (UE9)

LOPD

- Derecho de acceso
- Derecho de rectificación
- Derecho de oposición
- Derecho de cancelación.

RGPD (UE)

- 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.



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

**3.D- DEBER DE SECRETO.
CONFIDENCIALIDAD.**

(3.D.1) DEBER DE SECRETO

Artículo 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 desecreto (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 Almería, dispone de un Documento de seguridad, tal y como exige la LOPD. Pero:

- La mayoría del Personal lo desconoce.**
- No está actualizado, ni es mantenido correctamente.**
- Gran parte de los procedimientos y protocolos se están 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.

**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) ¿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)
- 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.2) ¿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)**
- Trituración 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, cesión de información a terceros **NO**
- Procedimiento envíos telemáticos **NO. (Editran, DipalBox)**
- Procedimiento uso de Email. **NO**
- Protocolo traslado documentos papel. **NO**
- Las auditorías obligatorias cada dos años. **SI (última 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.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, Tuiteer, FaceBook, etc... (se deben prohibir para datos personales).
Es necesario Informar al Personal sobre no utilizar estas herramientas.



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

**3.H- CONTRATO 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 Almería, en los pliegos de las Licitaciones, pone las cláusulas 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 Protección de Datos de la Diputación, y que han firmado el deber de secreto.

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

**3.1- 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

(3.1.2) 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 PUBLICAD TIENE QUE NOMBRAR U DELEGADO DE PROTECCION DE DATOS. DEBE TENER FORMACION JURIDICA EN PROTECCION 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 Protección de Datos Personales este el personal de Diputación, mas se depende de auditorias externas. Ultima 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 Jorandas y cursos de Proteccion 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 colaboración de la Diputación a las EE.LL. de la Provincia de Almería para implantación y mantenimiento de nuevas tecnologías se regula por el Convenio Marco de Gestión de la RPC. Siendo en particular para la Gestión en LOPD en:

- Colaboración y subvención en las Auditorías de LOPD
- Asesoramiento en la Gestión de la LOPD
- Resolución de todo tipo de dudas y consulta.
- Atención telefónica y en línea.
- Plazas para formación dentro de Plan Agrupado.

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

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

GRACIAS POR SU ATENCION

**Servicio de Organizacion y Seguridad
Manuel Soler Hernandez
msolerhe@dipalme.org
6 de Octubre de 2017**

