FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN EN LAS DIPUTACIONES PROVINCIALES

23 de octubre de 2017

© Javier Peña Alonso

El Reglamento prevé que los responsables aplicarán las **medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento**.

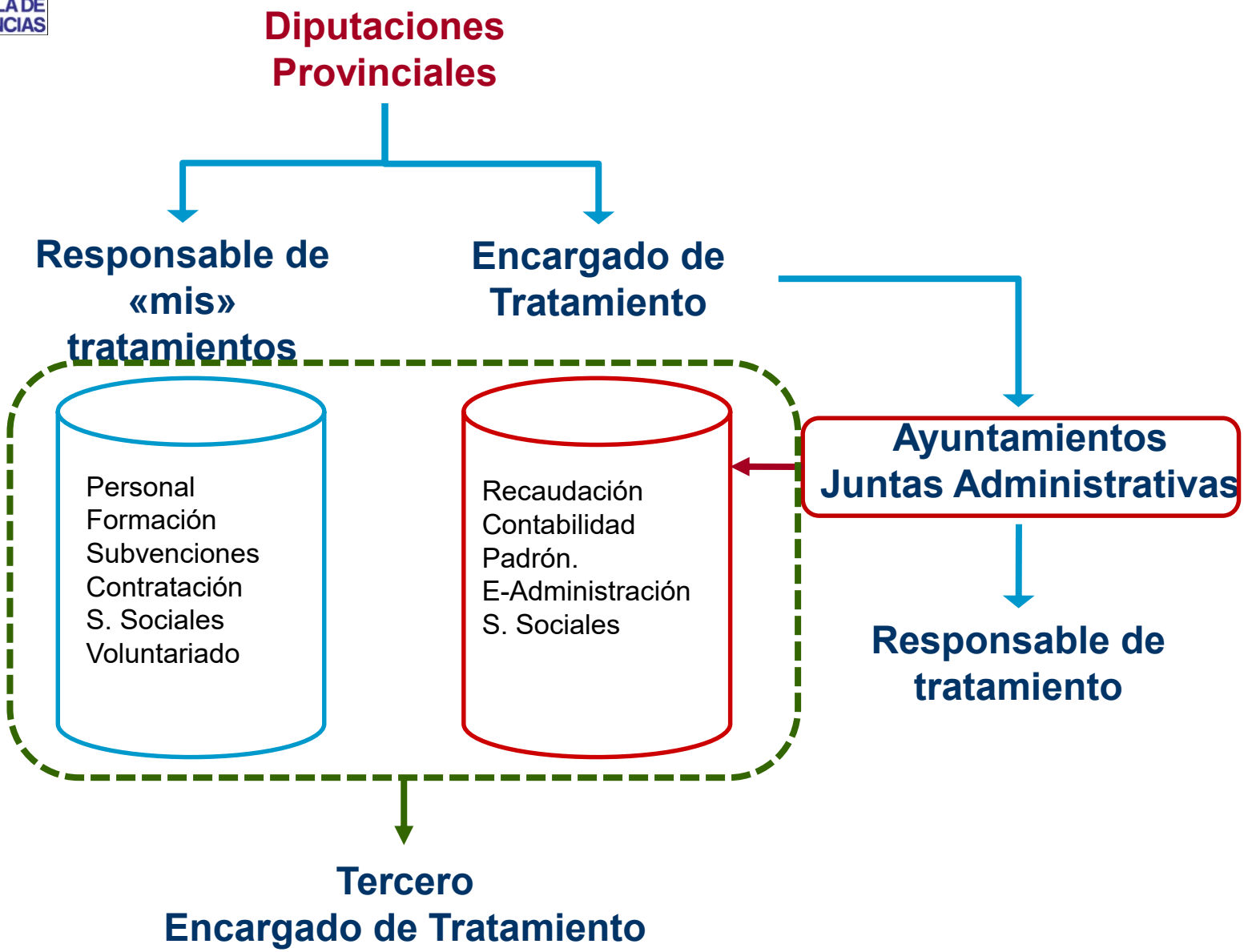
En términos prácticos, este principio requiere que las organizaciones analicen **que datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.**

En síntesis, **este principio exige una actitud consciente, diligente, y proactiva por parte de las organizaciones** frente a todos los tratamientos de datos personales que lleven a cabo.

El RGPD, señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta **la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas**

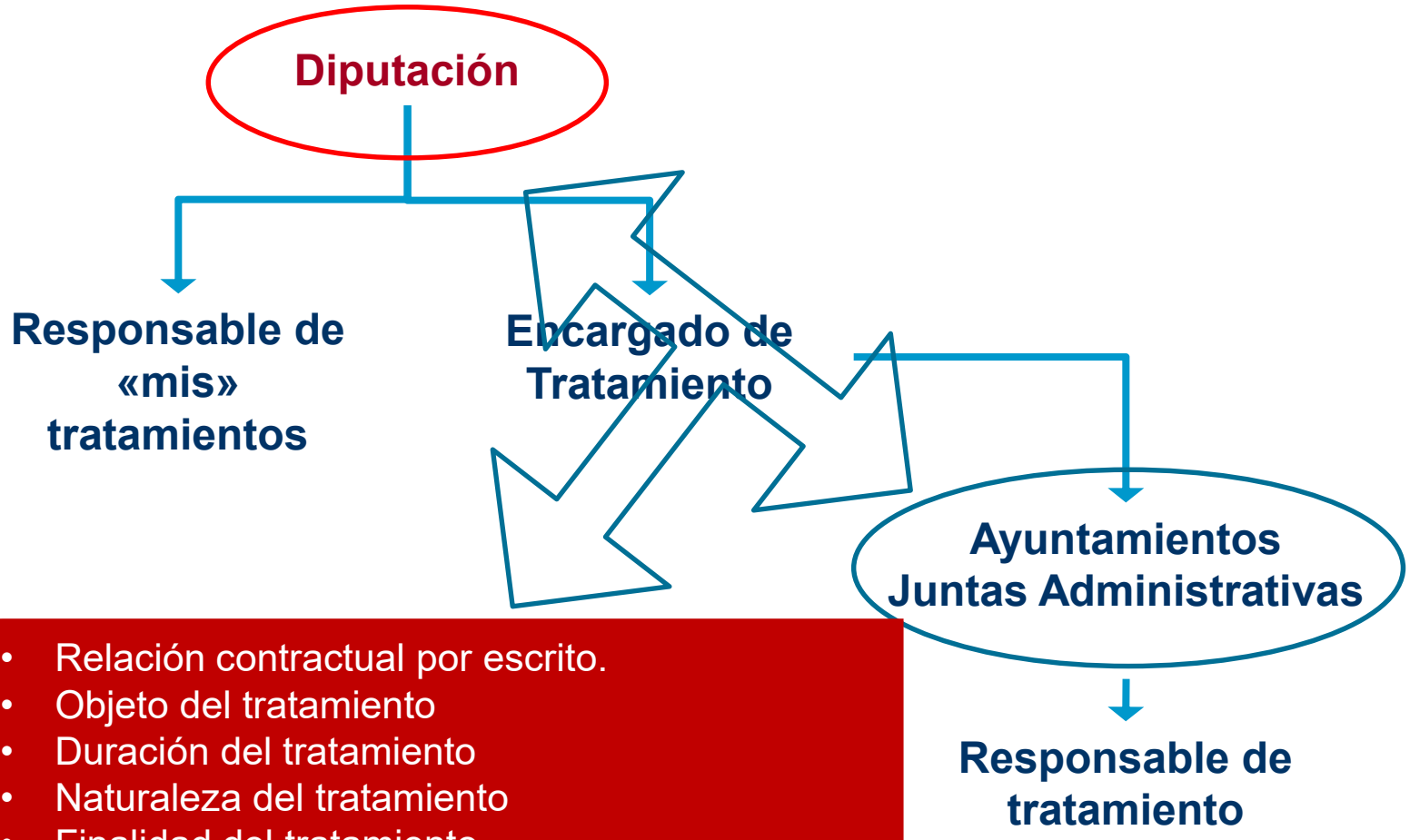
Privacy by design

Doble posición de las Diputaciones



Doble posición de las Diputaciones

¿Cuál es mi figura?



- Relación contractual por escrito.
- Objeto del tratamiento
- Duración del tratamiento
- Naturaleza del tratamiento
- Finalidad del tratamiento
- Tipo de datos personales
- Categorías de interesados
- Obligaciones y derechos del responsable

Las relaciones entre el responsable y el encargado deben formalizarse en un **contrato o en un acto jurídico** que vincule al encargado respecto al responsable.

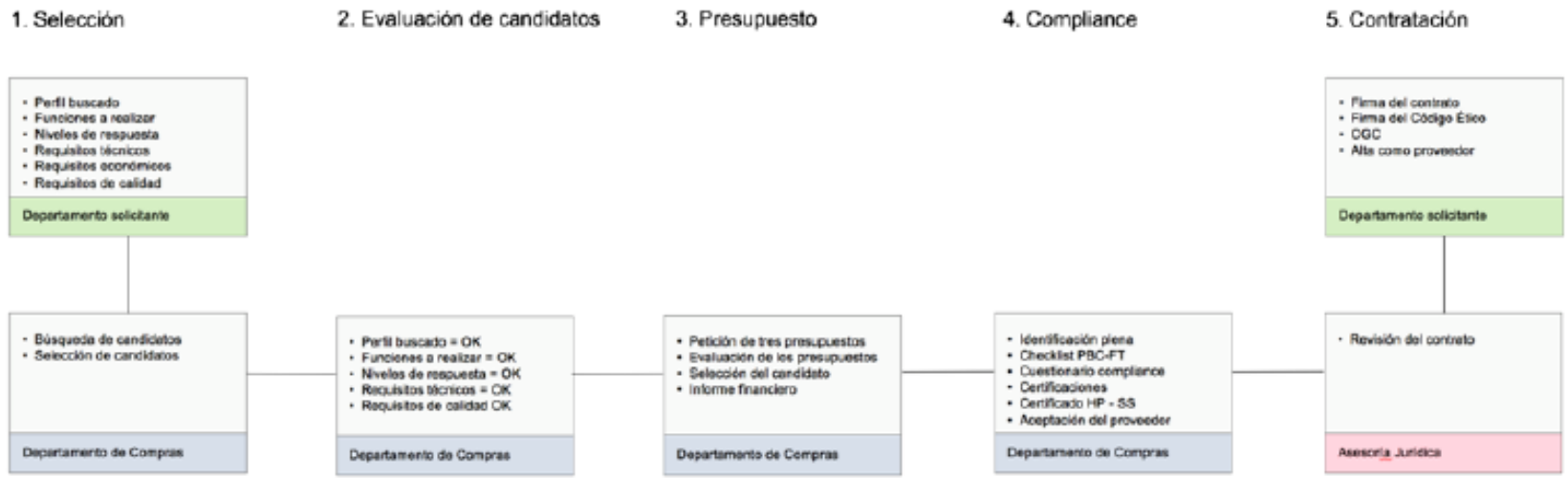
Se regula de forma minuciosa el **contenido mínimo de los contratos de encargo**, debiendo preverse aspectos como:

- Objeto del tratamiento.
- Duración del tratamiento.
- Naturaleza del tratamiento.
- Finalidad del tratamiento.
- Tipo de datos personales.
- Categoría de interesados.
- Obligaciones y derechos del responsable.

Los **contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido**, sin que sean válidas las remisiones genéricas al artículo del RGPD que los regula.

- **Los encargados tienen obligaciones propias** que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo:
  - Deben mantener un registro de actividades de tratamiento.
  - Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.
  - Deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

Relaciones Responsable - Encargado.



Inventario de los tratamientos de datos de carácter personal.

Esta tarea tendrá como resultado principal la obtención de la información necesaria para la creación de un inventario lo más detallado posible de los procesos, sistemas e instancias de datos personales que van a constituir el alcance de la organización.

Establecer la sensibilidad de la información.

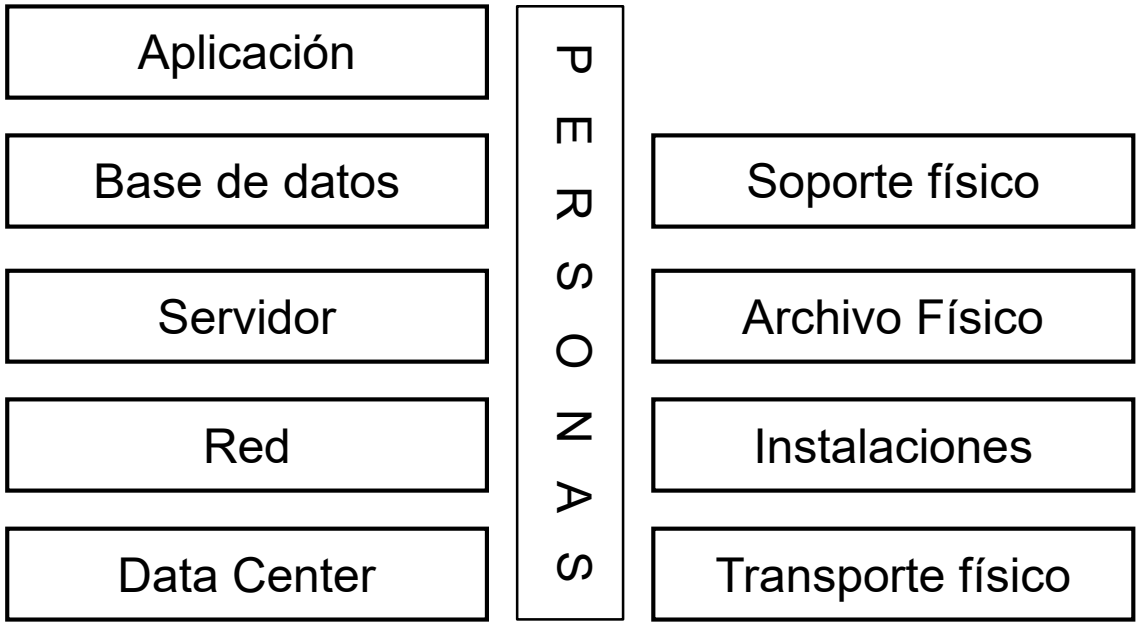
Evaluar el grado en que la información permite la identificación de un individuo concreto.

1. Casi imposible
2. Bajo
3. Significativo.
4. Alto

Este inventario será el eje a partir del cual se organizarán el resto de procesos, análisis de riesgos, definiciones de controles….

Inventario de los tratamientos de datos de carácter personal.

Identificar los activos de Información secundarios, es decir donde viven los activos de información.



Registro de actividades de tratamiento.

- Partir de los ficheros actualmente inscritos
- Desgajar las operaciones de tratamiento concretas vinculándose a una finalidad.

Registro de ficheros. → Registro actividades de tratamiento.

Finalidades
Operaciones de tratamiento

Archivos
Base de datos
Archivos físicos

Fichero de Personal →

- Tratamiento Recursos Humanos.
- Tratamiento Gestión Nóminas.
- Tratamiento Prevención Riesgos Laborales.

#ANLOPD

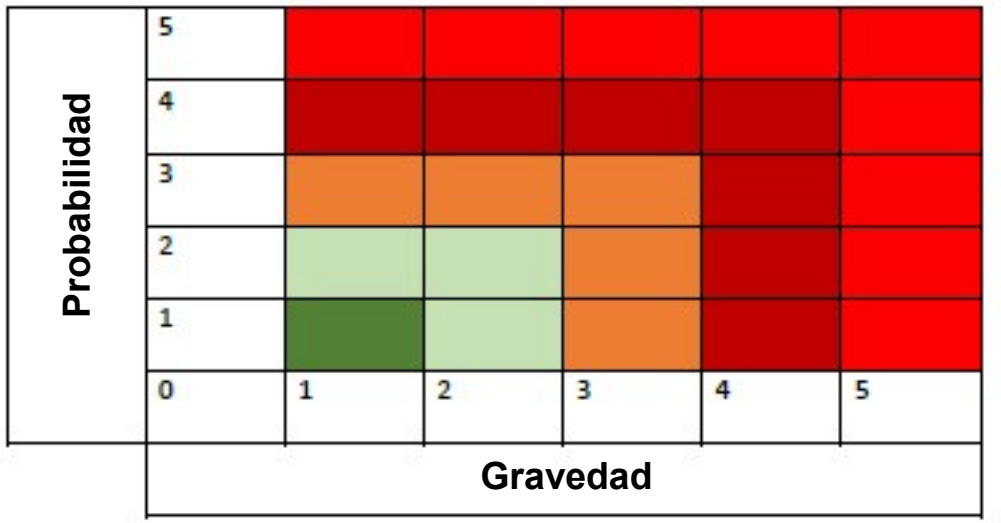
Artículo 33. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

Medidas de seguridad, riesgos, evaluación de impacto.

probabilidad	
Descripción	nivel
inminente	5
muy probable	4
probable	3
poco probable	2
improbable	1

gravedad	
Descripción	nivel
extremadamente grave	5
significativamente grave	4
grave	3
leve	2
irrelevante	1



Artículo 37 (RGPD) establece como supuesto obligatorio de designación de un DPO

"Cuando el tratamiento lo lleve a cabo una autoridad u organismo público"

- Nombramiento basado en:
  - **Cualidades profesionales**
  - **Conocimientos especializados** del Derecho
  - **Práctica en materia de protección de datos.**
  - **Capacidad para desempeñar las tareas** que tiene designadas en el Reglamento.

- Relación **laboral** o mediante **contrato de servicios**
- Podrá desempeñar **otras funciones**, si no hay conflicto de intereses
- No podrá recibir **ninguna instrucción** en lo que respecta al desempeño de dichas funciones
- No podrá ser destituido ni sancionado por desempeñar sus funciones
- **Rendirá cuentas** directamente al **más alto nivel jerárquico**
- Podrá ser **contactado por interesados y APD**

Delegado de Protección de Datos (DPO)

- Nombramiento basado en:

  - **Cualidades profesionales**
  - **Conocimientos especializados** del Derecho
  - **Práctica en materia de protección de datos.**
  - **Capacidad para desempeñar las tareas** que tiene designadas en el Reglamento.

- Relación **laboral** o mediante **contrato de servicios**
- Podrá desempeñar **otras funciones**, si no hay conflicto de intereses
- No podrá recibir **ninguna instrucción** en lo que respecta al desempeño de dichas funciones
- No podrá ser destituido ni sancionado por desempeñar sus funciones
- **Rendirá cuentas** directamente al **más alto nivel jerárquico**
- Podrá ser **contactado por interesados y APD**

El delegado de protección de datos tendrá entre otras las siguientes funciones:

- **Informar y asesorar al responsable o al encargado** y a los trabajadores sobre las **obligaciones** que impone la normativa de protección de datos.
- **Supervisar el cumplimiento de la normativa.**
- **Asesorar** respecto de la **evaluación de impacto** relativa a la protección de datos.
- **Cooperar con la autoridad de control.**
- Prestar la debida **atención a los riesgos asociados a las operaciones de tratamiento**, teniendo en cuanta la naturaleza, el alcance, el contexto y fines del tratamiento.
- **Atender a los interesados.**
- **Mantener el secreto o la confidencialidad** en lo que respecta al desempeño de sus funciones.

FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Delegado de Protección de Datos (DPO)

1. Cumplimiento de principios relativos al tratamiento: limitación de finalidad, minimización o exactitud de los datos
2. Identificación de las bases jurídicas de los tratamientos
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
4. Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas
5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos requeridos
9. Identificación de los instrumentos de TID adecuados a las necesidades y características de la organización y de las razones que la
10. Diseño e implantación de políticas de protección de datos
11. Auditoría de protección de datos
12. Establecimiento y gestión de los registros de actividades de tratamiento
13. Análisis de riesgo de los tratamientos realizados
14. Implantación de las medidas de protección de datos desde el diseño y por defecto adecuadas a los riesgos y naturaleza de los tratamientos
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos y de notificación a las autoridades y a los afectados
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
18. Realización de evaluaciones de impacto sobre la protección de datos
19. Relaciones con las autoridades de supervisión
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos

AEPD, “el RGPD ofrece la posibilidad de que se contraten externamente las funciones de DPD.

Esta opción puede ser utilizada en determinados casos, como podría ser el de pequeños municipios que se beneficien de un servicio que ofrezca una diputación provincial o una comunidad autónoma o, incluso, que donde ese servicio no exista puedan optar por los servicios de entidades privadas especializadas”.

#ANLOPD Dice que puede ser una persona física o jurídica

A. **Órgano unipersonal.**
B. **Órgano colectivo.** Especialistas de distintas áreas de La gestión (jurídica, auditoría, financiera, recursos humanos)

En los supuestos de que se trate de un órgano colectivo ha dicho el WP29DPN que en “aras a la claridad jurídica y la buena organización es aconsejable tener una asignación clara de tareas dentro del equipo del DPO y asignar a una sola persona como una persona `cargo` y principal contacto para cada cliente. Generalmente también sería útil especificar estos puntos en el contrato de servicio”

Notificación de “violaciones de seguridad de los datos”.

- **Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.**
- La **notificación de la quiebra** a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
- La notificación ha de incluir un contenido mínimo:
  - la naturaleza de la violación.
  - categorías de datos y de interesados afectados.
  - medidas adoptadas por el responsable para solventar la quiebra.
  - si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados
- **Los responsables deben documentar todas las violaciones de seguridad.**
- En los casos en que sea probable que la **violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados**, la notificación a la autoridad de supervisión deberá complementarse con una **notificación dirigida a estos últimos**.
- El **objetivo de la notificación a los afectados** es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.
- El RGPD añade a los contenidos de la notificación **las recomendaciones sobre las medidas que pueden tomar los interesados** para hacer frente a las consecuencias de la quiebra.

Notificación de “violaciones de seguridad de los datos”.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

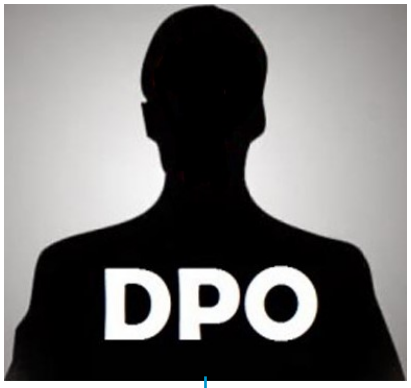
CCN-CERT centro criptológico nacional

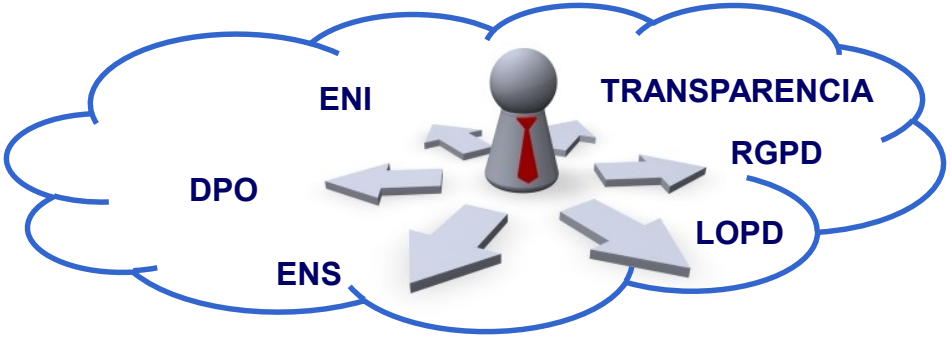
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

¿Y las Diputaciones?

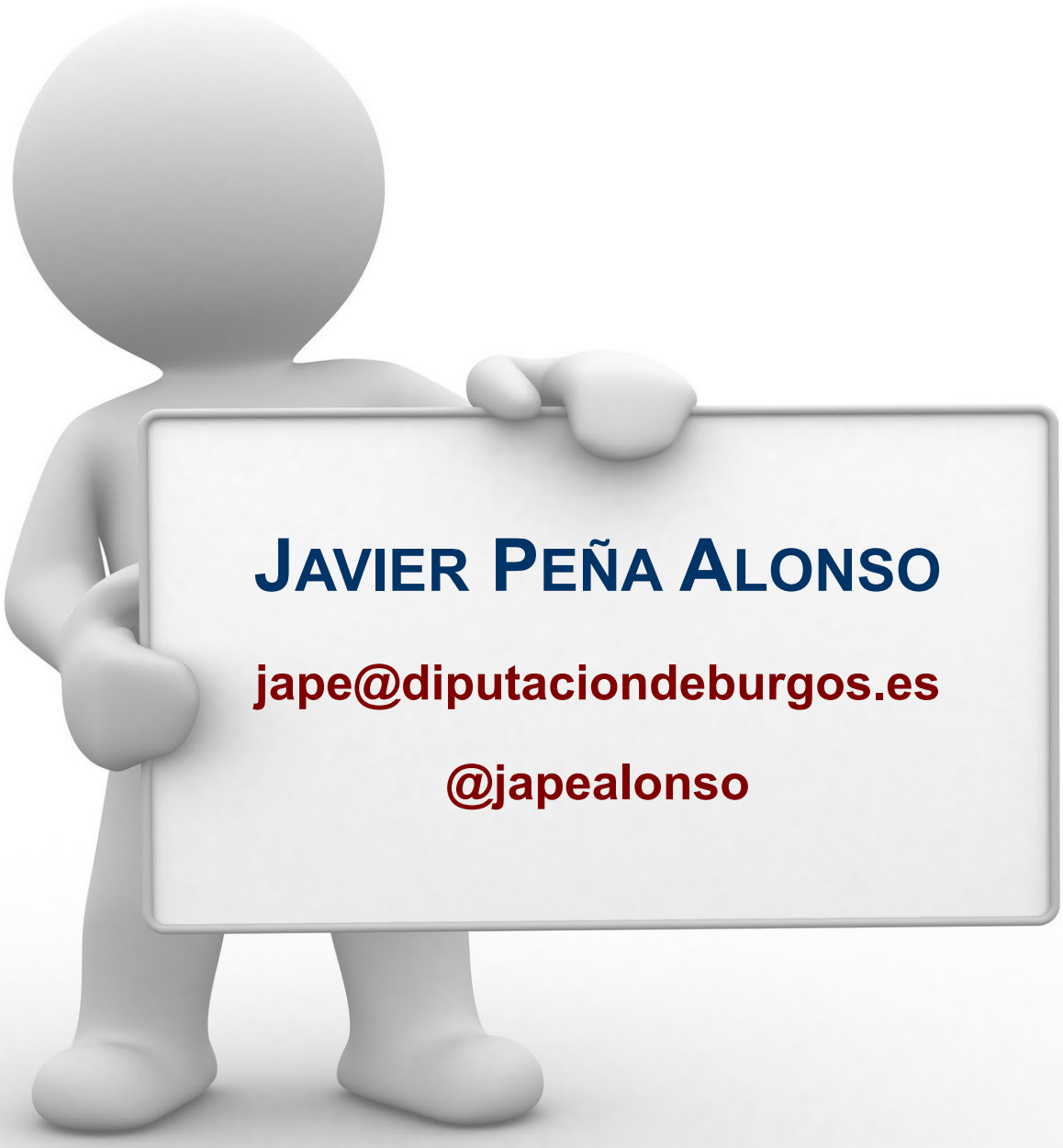
Tiene que **haber personal interno especializado** que gestione de forma eficiente la PRIVACIDAD.

Delegado de Protección de Datos (DPO)





Identificar e Inventariar datos y proceso	Evaluar situación de cumplimiento actual	Planificar y corregir deficiencias de control	Mantener y evolucionar el marco de control
¿Qué tipo de datos personales se procesan y donde se procesan? ¿Quiénes son los usuarios y cómo se procesan los datos? ¿Qué destino tienen los datos?	¿Cuáles son los riesgos de cada tratamiento de datos? Definir requisitos de control. Evaluar controles y aplicados. Identificar deficiencias	Comunicación acciones. Definir y aprobar plan. Implantación de medidas. Evaluación post-implementación.	Establecer procedimiento nuevos procedimientos y cambios en los existentes. Establecer programa periódico de revisión del cumplimiento. Monitorización. Formación.
Apoyo y dotación de recursos			


JAVIER PEÑA ALONSO
jape@diputaciondeburgos.es
@japealonso