Verificación, inspección y sanción, experiencias comparadas. Vulneraciones de Seguridad.

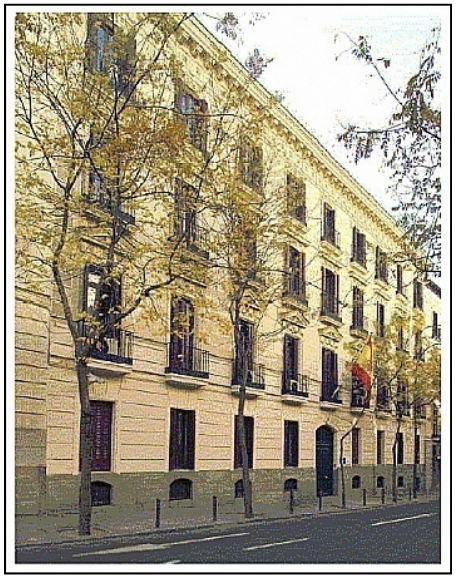
Julián Prieto Hergueta
Subdirector General del Registro General
de Protección de Datos
Agencia Española de Protección de Datos
México, 1 de diciembre de 2016

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

- **QUÉ ES**

- La Agencia es la autoridad de control independiente que vela por el cumplimiento sobre la normativa de protección de datos, garantizando y tutelando el derecho fundamental a la protección de datos de carácter personal



- **CÓMO ACTÚA**

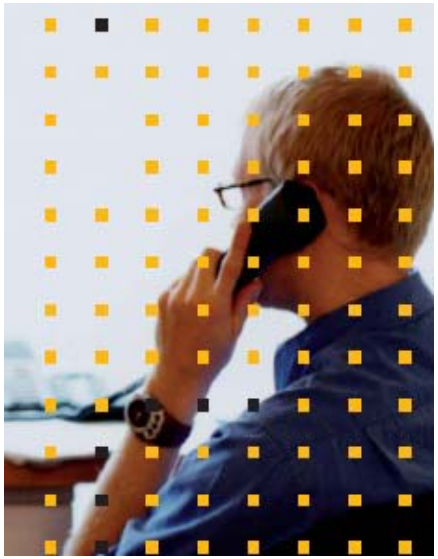
- Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones
- Presupuesto diferenciado

PROTECCIÓN DE DATOS EN ESPAÑA

- **LOS CUATRO PILARES DE LA ACTIVIDAD DE LA AEPD**

1. CAPACIDAD DE APLICACIÓN DE LA LEY

- **Auditoría e inspección**
- **Protección y tutela de derechos**
- **Registro**



2. ASESORÍA

- **Servicio Legal**
- **Servicio de atención al ciudadano**

3. COMUNICACIÓN

4. COOPERACIÓN INTERNACIONAL

NORMATIVA APLICABLE

REGIMEN SANCIONADOR - COMPETENCIA

- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**

Ley General de Telecomunicaciones:
- **Guía de telecomunicaciones**
- **Publicidad telefónica**
- **Quiebras de seguridad**

Ley de Servicios de la Sociedad de la Información:
- **SPAM**
- **COOKIES**

Artículo 40. Potestad de inspección

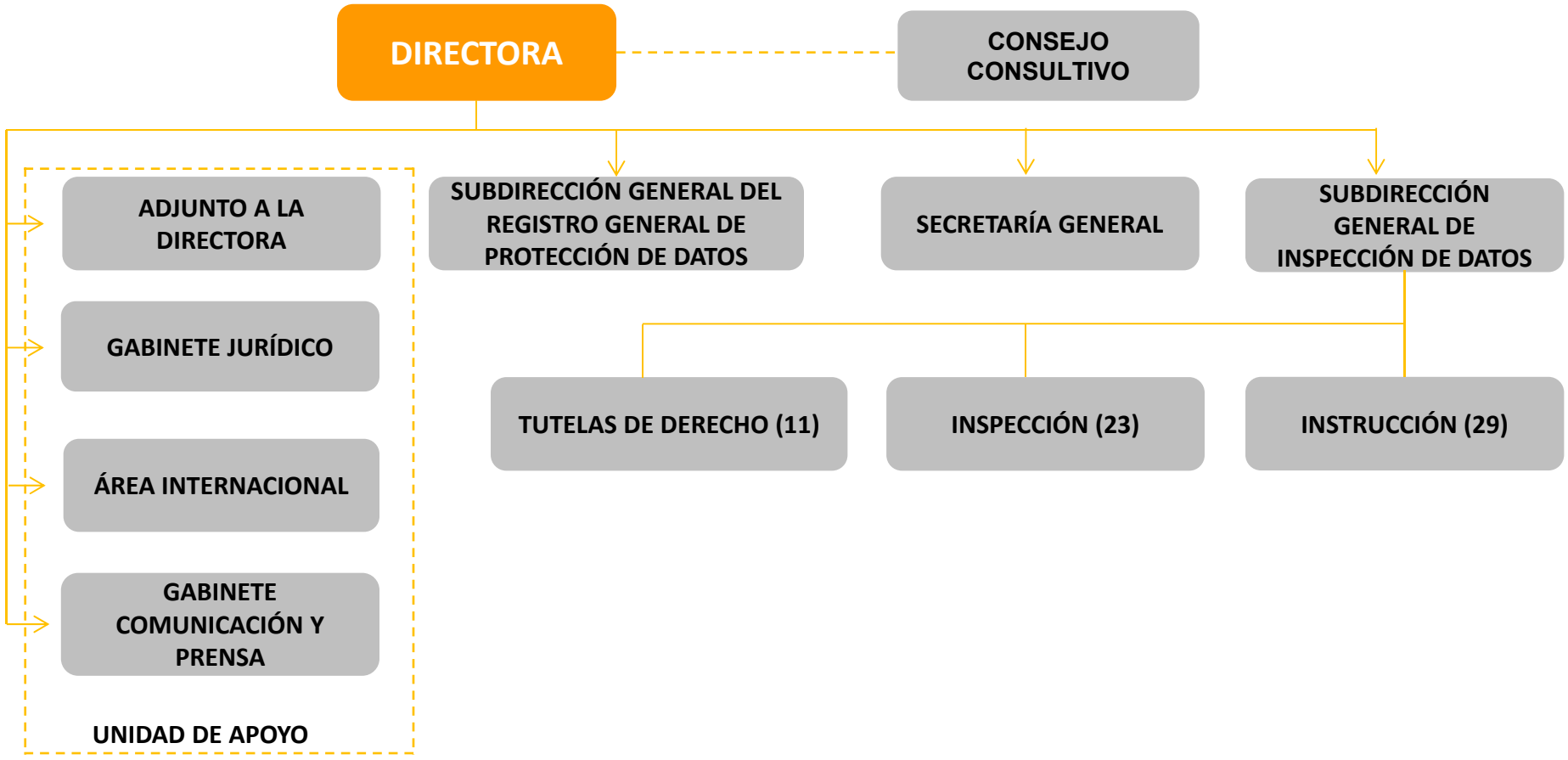
1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

ORGANIGRAMA



UNIDAD DE INSPECCIÓN

- **SUBDIRECCIÓN GENERAL DE INSPECCIÓN**

Engloba tanto las labores de inspección como las de instrucción:

UNIDAD DE INSPECCIÓN (FUNCIONES)

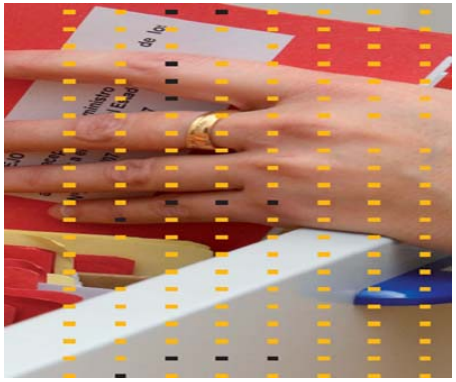
1. Estudia y analiza las reclamaciones formuladas por los ciudadanos
2. Colabora en el desarrollo de planes de oficio sectoriales

UNIDAD DE INSTRUCCIÓN (FUNCIONES)

Incoa tres clases de procedimientos:

1. Procedimiento sancionador contra responsables de fichero de titularidad privada por infracción de la LOPD
2. Procedimiento por infracciones de las Administraciones Públicas
3. Procedimiento de tutela de derechos

SECTORES:
Comunicaciones electrónicas comerciales – spam.
Asociaciones, clubes, colegios profesionales, partidos políticos y ONGs.
Comercio, transporte, y hostelería
Recursos humanos y asuntos laborales
Servicios de Internet
Sanidad
Suministro de gas, electricidad o agua
Seguros
Medios de comunicación
Publicidad y prospección comercial
Ficheros de solvencia patrimonial y crediticia



ACTUACIONES PREVENTIVAS

- **INSPECCIONES SECTORIALES: PLANES Y RECOMENDACIONES DE OFICIO**
  - **Criterios**
    - **Tratamientos masivos**
    - **Sensibilidad de la información**
    - **Desarrollos tecnológicos**
    - **Complejidad de los tratamientos**
    - **Coordinación con otras APD**
    - **Acumulación de denuncias (suplantación en la contratación, encargado del tratamiento: Recobro)**
  - **Resultados**
    - **Descripción de las actuaciones**
    - **No identificación**
    - **Conclusiones**
    - **Recomendaciones (sector, terceros interesados)**

ACTUACIONES PREVENTIVAS

- **Relación de inspecciones sectoriales**
  - **Transferencias internacionales y Telemarketing en compañías de telecomunicaciones**
  - **Llamadas telefónicas no solicitadas con fines de venta directa**
  - **Mensajes electrónicos comerciales no solicitados y servicios *premium* en telefonía móvil**
  - **Sistemas de geolocalización**
  - **Difusión en Internet de imágenes captadas con videocámaras en lugares públicos**
  - **Identificación de menores en servicios de Internet**
  - **Videocámaras en Internet**
  - **Hospitales**
  - **Servicios cloud computing por el sector educativo**

POTESTAD SANCIONADORA

- **ACTUACIONES PREVIAS: Denuncias, iniciativa de la Directora, petición razonada**
  - **determinación de hechos, presuntos responsables, sin análisis jurídico**
  - **Personal competente y especializado:**
    - **SDG Inspección habilitados**
    - **Actúa como autoridad pública**
    - **Obligación de imparcialidad**
    - **Deber de secreto**
    - **La obstrucción a su labor constituye una infracción grave**
  - **Plazo: 12 meses máximo**

POTESTAD SANCIONADORA

❑ OBTENCIÓN DE INFORMACIÓN

- Requerimientos de información: envío documentos y datos

❑ ACTUACIONES PRESENCIALES

- Sede del social del inspeccionado y otros locales donde se encuentren los ficheros
- Examen de documentación
- Inspección de equipos físicos y lógicos
- Requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte de ficheros

POTESTAD SANCIONADORA

- **RESULTADOS ACTUACIONES PREVIAS**
  - **Presunción de certeza (iuris tantum)**
  - **Determinación hechos sin calificación jurídica**
  - **Archivo o**
  - **INICIO PROCEDIMIENTO SANCIONADOR**

POTESTAD SANCIONADORA

PROCEDIMIENTO SANCIONADOR

- Inicio:
  - Posibilidad de reconocer la responsabilidad (-20%)
  - Posibilidad pago inmediato (-20%)
- Medidas provisionales
- Alegaciones y pruebas (posibilidad de inadmisión)
- Resolución: 6 meses
- Apercibimiento

INFRACCIÓN DE ADMINISTRACIONES PÚBLICAS

- Medidas correctoras
- Archivo de actuaciones si se adoptan las medidas
- Comunicación al Defensor del Pueblo

POTESTAD SANCIONADORA

PROCEDIMIENTO DE TUTELA DE DERECHOS

- Denuncia la infracción vs. reclamación de la tutela de derechos
- Actuaciones: audiencia responsable del fichero, afectado, informes, pruebas,..
- Plazo: 6 meses
- No declaración de infracción. Estimación o desestimación
- En caso de estimación cumplimiento en 10 días
- Infracción en caso de incumplimiento

QUIEBRAS DE SEGURIDAD

- **EN LA LEGISLACIÓN DE TELECOMUNICACIONES. EN EL RGPD desde 25/05/2018 -art.33-)**
- **Operadores que exploten redes públicas o presten servicios de comunicaciones electrónicas disponibles al público.**
- **Deben adoptar las medidas adecuadas con el fin de garantizar la protección de los datos personales. La AEPD puede examinar las medidas y proponer mejores prácticas**
- **En caso de violación de datos personales: *«la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público”***

QUIEBRAS DE SEGURIDAD

- Notificación a AEPD
- Notificación a abonados o particulares (si puede afectar a su intimidad o a los datos personales). Medidas a adoptar
- Sin dilaciones indebidas
- Posibles excepciones (prueba de que el proveedor ha aplicado medidas tecnológicas suficientes se han aplicado a los datos afectados, como datos incomprensibles para terceros no autorizados)
- Posibilidad de exigir la notificación por AEPD
- Inventario de violaciones de datos personales
- Incompetencia para sancionar la omisión de notificación
- AEPD: Directrices e instrucciones sobre las circunstancias para la notificación
- Sin perjuicio LOPD

INFRACCIONES Y SANCIONES LOPD

Nivel de la infracción	Descripción de la infracción	Sanción prevista
LEVE PRESCRIPCIÓN 1 AÑO	a) No remitir a la AEPD las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo. b) No solicitar la inscripción del fichero. c) El incumplimiento del deber de información cuando los datos sean recabados del propio interesado. d) La transmisión de los datos a un encargado sin cumplir formalmente las garantías que la Ley exige (contrato).	900 € 40.000 €

INFRACCIONES Y SANCIONES LOPD

Nivel de la infracción	Descripción de la infracción	Sanción prevista
GRAVE PRESCRIPCIÓN 2 AÑOS	a) Crear ficheros público o recogida sin publicar en Boletín b) No recabar el consentimiento de las personas afectadas, cuando sea necesario c) Conculcación del principio de calidad de datos y de las garantías establecidas, salvo que fuese muy grave d) La vulneración del deber de guardar secreto e) Impedir los derechos ARCO. f) El incumplimiento del deber de información cuando los datos no proceden del propio interesado g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado. h) Falta de medidas de seguridad. i) No atender los requerimientos de la AEPD. j) La obstrucción al ejercicio de la función inspectora. k) La comunicación o cesión de los datos salvo muy grave.	40.001 € 300.000 €

INFRACCIONES Y SANCIONES LOPD

Nivel de la infracción	Descripción de la infracción	Sanción prevista
MUY GRAVE PRESCRIPCIÓN 3 AÑOS	a) La recogida de datos en forma engañosa o fraudulenta. b) Cesión de datos especialmente protegidos c) No cesar en el tratamiento ilícito tras requerimiento. d) La transferencia internacional sin garantías.	300.001 € 600.000 €

GRADUACIÓN DE LA SANCIÓN

La cuantía de las sanciones se graduará según:

- Carácter continuado de la infracción
- Volumen de tratamientos efectuados
- Vinculación de la actividad del infractor con la realización de tratamientos
- Volumen de negocio o actividad del infractor
- Beneficios obtenidos como consecuencia de cometer la infracción
- Grado de intencionalidad
- Reincidencia en la comisión de infracciones de igual naturaleza
- Naturaleza de los perjuicios causados a las personas interesadas o terceros
- Acreditación de implantación de procedimientos, consecuencia de anomalía
- Cualquier otra circunstancia relevante para delimitar grado culpabilidad

GRADUACIÓN DE LA SANCIÓN

El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

Cuando

- se aprecie una cualificada disminución de la culpabilidad del imputado o concurran varias circunstancias de las incluidas en la ficha anterior
- la entidad haya regularizado la situación irregular de forma diligente
- el infractor reconozca espontáneamente la culpabilidad
- se haya producido un proceso de fusión por absorción y la infracción fuese anterior a ese proceso, no siendo imputable a la entidad absorbente

APERCIBIMIENTO

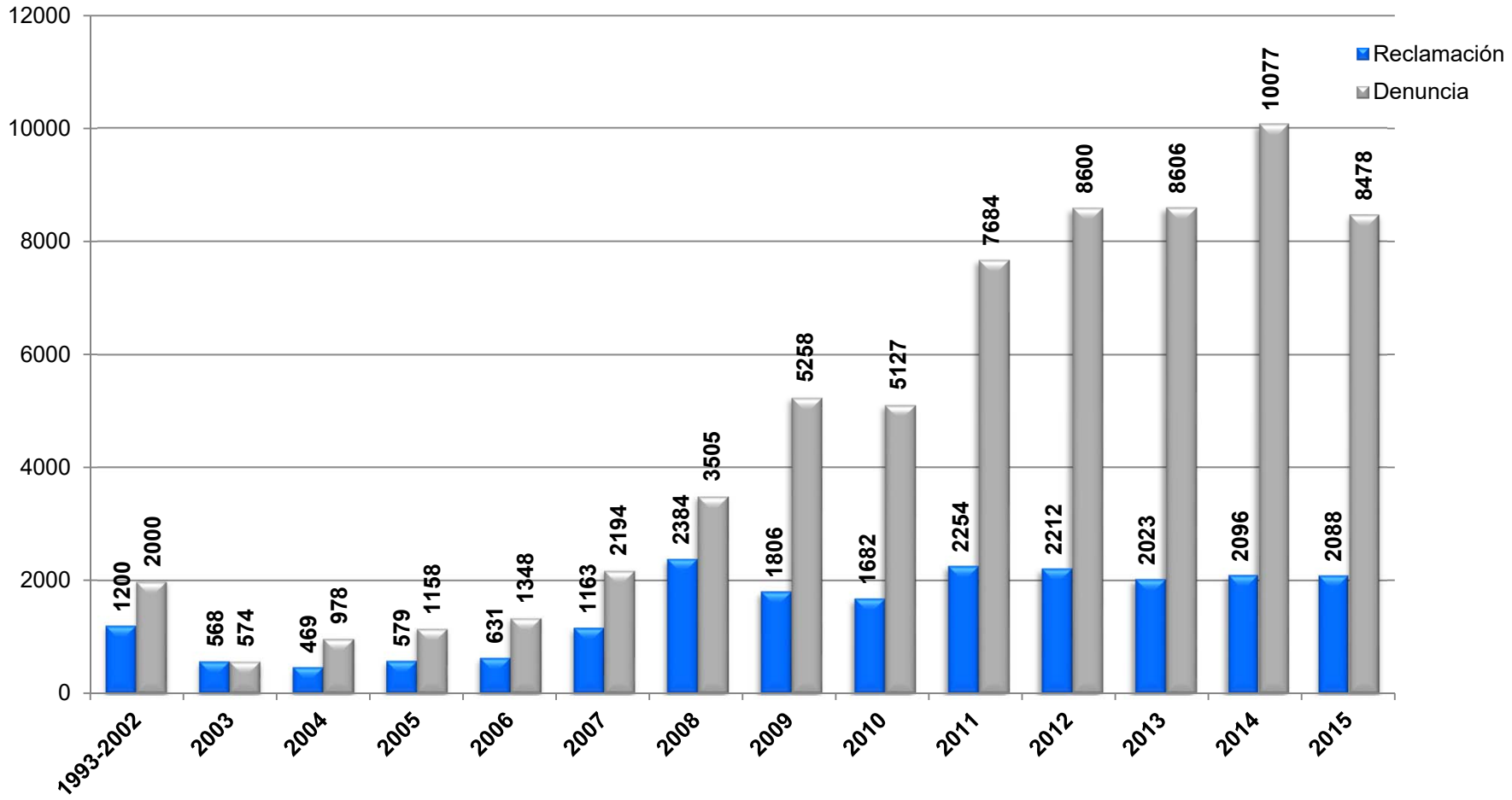
- **EXCEPCIONAL**
- **ATENDIDA LA NATURALEZA DE LOS HECHOS**
- **CONCURRENCIA SIGNIFICATIVA DE CIRCUSNTANCIAS**
  - -una cualificada disminución de la culpabilidad del imputado o concurran varias circunstancias atenuantes
  - - La entidad haya regularizado la situación irregular de forma diligente
  - - El infractor reconozca espontáneamente la culpabilidad
  - - Se haya producido un proceso de fusión por absorción y la infracción fuese anterior a ese proceso, no siendo imputable a la entidad absorbente
- **INFRACCIÓN LEVE O GRAVE**
- **NO HABER SIDO SANCIONADO CON ANTERIORIDAD**
  - -

INMOVILIZACIÓN FICHEROS

Potestad de inmovilización de ficheros

- Supuesto de infracción muy grave
- En que la persistencia en el tratamiento de datos o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados
- Además de ejercer la potestad sancionadora,
- Requerir a los responsables de los ficheros de (públicos o privados) la cesación en la utilización o cesión ilícita de los datos, en cualquier momento del procedimiento sancionador.
- Si el requerimiento no se atiende, mediante resolución motivada, la AEPD podrá inmovilizar tales ficheros para restaurar los derechos de las personas afectadas.

DENUNCIAS Y RECLAMACIONES REGISTRADAS



ÁREAS CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2012	2013	2014	2015	% RELATIVO DEL TOTAL 2015	Δ% 2014/2015
Telecomunicaciones	15.368.938	15.035.008	10.750.502	**7.090.004**	51,70	–34,05
Entidades financieras	2.853.004	1.811.501	2.018.501	**2.395.902**	17,47	18,70
Suministro y comercialización de energía/agua	1.270.001	2.084.901	1.862.900	**1.205.002**	8,79	–35,32
Comunicaciones electrónicas comerciales – *spam* (LSSI)	541.507	526.010	645.506	**897.403**	6,54	39,02
Organizaciones asociativas incluyendo partidos políticos y sindicatos	147.202	40.400	19.800	**525.500**	3,83	2.554,04*
Publicidad (excepto *spam*)	137.000	481.004	751.411	**502.108**	3,66	–33,18
TOTAL DE LAS 6 PRIMERAS ACTIVIDADES	20.317.652	19.978.824	16.048.620	**12.615.919**	92	–21,39

* El incremento obedece a la tramitación de un procedimiento sancionador en el que se impusieron sanciones con un importe total de 440.000 euros.

COOPERACIÓN INTERNACIONAL

- WORKING PARTY 29
- Consejo de Europa (T-PD, CAHDATA)
- Grupos de cooperación entre autoridades y con los sectores implicados (Conferencia internacional, GPEN…)
- Red Iberoamericana de Protección de Datos (RIPD)
- RGPD: La Comisión Europea y las DPA tomarán medidas para:
  - Crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación
  - Prestarse asistencia en la aplicación de la Ley, en especial: Notificación, remisión reclamaciones, asistencia en las investigaciones, intercambio de información (…)


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS


PLVS
VLTRA