MEMORIA AEPD2017

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

prólogo

La Memoria de la Agencia Española de Protección de Datos recoge el funcionamiento y las actividades realizadas por la institución, el análisis de las tendencias legislativas y jurisprudenciales, los retos más importantes a los que se enfrenta la protección de datos y un resumen de las decisiones más relevantes adoptadas por este organismo. El año 2017 ha sido un año trascendente para la protección de datos y, en consecuencia, para la Agencia. Si bien el Reglamento General de Protección de Datos (RGPD) es aplicable el 25 de mayo de 2018, esta Memoria recoge todas las acciones que la Agencia ha puesto en marcha para facilitar y difundir orientaciones que permitan, sobre todo a las pymes, estar en disposición de cumplir con la nueva normativa.

Uno de los objetivos más importantes que nos marcamos en 2017 y que se mantiene en 2018 es buscar fórmulas flexibles para ayudar a empresas y organizaciones a prepararse para la aplicación del RGPD. Como organismo público que tiene como misión garantizar el derecho fundamental de los ciudadanos a la protección de datos, creemos que también es de vital importancia prestar la ayuda y asistencia necesaria a aquellos que están obligados a su cumplimiento.

Estoy convencida de que una protección efectiva de los ciudadanos no puede realizarse sin la implicación de las empresas y organizaciones y, por ello, consideramos que el cumplimiento debe abordarse de una forma global. Fruto de esta filosofía, encontrarán a lo largo de las páginas que siguen el detalle de las casi 80 acciones que la Agencia ha realizado este año tanto para acompañar a los responsables como para concienciar a los ciudadanos. El lanzamiento de la herramienta Facilita_RGPD, la creación del Esquema de certificación junto a ENAC, la puesta en marcha de diversos planes sectoriales de oficio, la formación y difusión realizada en diferentes Comunidades Autónomas con entidades como CEOE y CEPYME para el sector privado, y el INAP para el sector público, además de las acciones llevadas a cabo junto a la FEMP y COSITAL son sólo algunos ejemplos de esa labor de acompañamiento. Por otro lado, la publicación de guías y diversos materiales de ayuda tienen la finalidad exclusiva de fomentar y ayudar en la adaptación al nuevo Reglamento, así como concienciar de los nuevos derechos.

Por otro lado, la Agencia ha recibido durante 2017 más de 10.500 denuncias y reclamaciones de tutela de derechos planteadas por los ciudadanos. En este punto, es importante destacar el descenso considerable de las denuncias y reclamaciones que se encuentran en tramitación, que disminuyen más de un 30% sobre los valores de 2016, y que se corresponde con una mayor eficacia administrativa a la hora de tramitar los procedimientos. El reto para el año 2018 en este sentido será incorporar las novedades legislativas (Reglamento General y nueva LOPD, principalmente) en los procedimientos y conseguir una interlocución fluida con los nuevos actores en el ámbito europeo.

Buena parte de las acciones que se recogen en esta Memoria, y que suponen un impulso indudable para fomentar la faceta preventiva de la Agencia, han podido realizarse en gran medida gracias al compromiso y al esfuerzo de las personas que trabajan en este organismo. La AEPD se enfrenta a retos crecientes de gran envergadura derivados del nuevo escenario que establece el Reglamento. Además, fruto de los avances tecnológicos, este organismo debe impulsar investigaciones punteras, potenciando estudios que permitan adelantarse y mitigar posibles riesgos para los derechos de las personas. Es por ello que, un año más, y pese al aumento en el número de puestos producido en 2017, es necesario solicitar un incremento sustancial en cuanto a los medios humanos de los que dispone la Agencia.

La tecnología avanza rápidamente, pero vamos a disponer de una norma que exige su consonancia con los derechos existentes, permitiendo a las autoridades de control aplicar un nuevo modelo de supervisión con instrumentos preventivos, correctivos y disuasorios ante los incumplimientos. La tecnología es un aliado imprescindible para el progreso, pero no puede desarrollarse de manera ajena a los derechos de las personas. En este sentido, crear productos o servicios respetuosos con la privacidad que impulsen la confianza de los ciudadanos es una condición indispensable para la innovación, el avance de economía digital e, incluso, los propios sistemas democráticos.

MAR ESPAÑA MARTÍ
DIRECTORA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Índice

Memoria 2017

La Agencia en cifras

1. Plan estratégico 2015-2019. Balance de ejecución

En el segundo año de ejecución del Plan Estratégico de la Agencia se había previsto inicialmente la realización de un total de 76 iniciativas, pero tras las actuaciones incorporadas a lo largo del ejercicio, la cifra total de 2017 quedó finalmente en 85 iniciativas, que se reparten en razón a su periodo de ejecución en:

Iniciativas de ejecución continua o plurianual	47
Iniciativas de ejecución no continua o anual	38

Las iniciativas nuevas que han sido incorporadas en 2017 son:

- Guía de tratamiento de datos en el ámbito local
- Plan de Inspección Sectorial de Oficio de Entidades Financieras
- Programa de formación de empleados públicos para fomentar el cumplimiento del RGPD, en colaboración con el INAP
- Herramienta de análisis de riesgos para AAPP
- Guía práctica de Evaluación de Impacto en la Protección de Datos
- Guía práctica de Análisis de Riesgos
- Guía sobre Brechas de Seguridad
- Herramienta de autoevaluación de riesgos para pymes con tratamientos de bajo riesgo FACILITA_RGPD.
- Adaptación de la AEPD al RGPD

En cuanto a su grado de ejecución, las cifras son las siguientes:

- Actuaciones ejecutadas: 78
  - De ejecución continua: 47
  - De ejecución no continua: 31
- Actuaciones aplazadas: 7

1.1. BALANCE FINAL 2017

El desglose de las 85 iniciativas y su correspondiente grado de ejecución aparece recogido en el Informe y cuadro de ejecución del Plan (ejercicio 2017), cuyo contenido se puede consultar de forma completa en esta sección.

Estas modificaciones hacen necesario proceder a una actualización del cronograma general del Plan Estratégico, que inicialmente contemplaba un total de 113 iniciativas, que pasaron a ser 121 tras la revisión que se hizo el pasado año, y que, tras estas nuevas incorporaciones de 2017, más las previstas para 2018, llevan a que el número total de iniciativas contempladas en el Plan, a finales de enero de 2018, sea de 131. La relación completa de las mismas se pueden consultar aquí.

El desglose de las 85 iniciativas y su grado de ejecución aparece recogido en el Informe del Plan Estratégico

1.2. EVOLUCIÓN DE LAS INICIATIVAS DEL PLAN ESTRATÉGICO 2015-2019

Como actuaciones más destacadas del ejercicio 2017 del Plan Estratégico se pueden reseñar las diez siguientes, cuyo alcance se detallará en los apartados correspondientes de esta Memoria.

Estas son:

1 El diseño de la herramienta y materiales para facilitar el cumplimiento del RGPD por parte de las empresas: herramienta FACILITA_RGPD, para pymes que realizan tratamientos de bajo riesgo; la Guía del Reglamento General de Protección de Datos para responsables de tratamiento; las Directrices para la elaboración de contratos entre responsables y encargados de tratamiento, y la Guía para el cumplimiento del deber de informar.

2 El diseño de herramientas y materiales para facilitar la adaptación al RGPD por parte de las Administraciones Públicas: la herramienta de evaluación de riesgos para AAPP (Micropilar); los documentos 'El impacto del RGPD en la actividad de las Administraciones Públicas', 'El Delegado de Protección de Datos en las Administraciones Públicas' y 'El nuevo RGPD y su impacto sobre las actividades de las Administraciones Locales'; vídeos sobre las 'Novedades en materia de Protección de Datos', y 'El RGPD y sus implicaciones para la Administración Local', como resultado de las jornadas de formación celebradas para empleados de la Administración General del Estado y de Diputaciones y Ayuntamientos y realizadas en colaboración con el Instituto Nacional de Administración Pública y la Federación Española de Municipios y Provincias.

3 El diseño de herramientas y materiales para reforzar el ejercicio de los derechos de los ciudadanos: las Guías para Ciudadanos, de Centros Docentes, de Compra Segura en internet, de reclamaciones en materia de telecomunicaciones, publicidad no deseada y de Administradores de Fincas.

4 La aprobación de un Esquema para la certificación de profesionales de la privacidad como Delegados de Protección de Datos (DPD), en colaboración con la Entidad Nacional de Acreditación (ENAC), y con el asesoramiento de un Comité Técnico integrado por 23 miembros, en representación de las Autoridades vasca y catalana de Protección de Datos, asociaciones de profesionales de la privacidad, colegios profesionales y asociaciones empresariales de los sectores más afectados (banca, seguros, salud, etc.), así como las principales asociaciones empresariales sectoriales.

5 El impulso de procedimientos extrajudiciales de resolución de reclamaciones. En particular, el promovido en colaboración con AUTOCONTROL en materia de suplantación de identidad y publicidad no deseada, al que se han adherido Telefónica, Vodafone, Orange y Másmóvil.

6 El impulso de los Planes de inspección sectorial de oficio (P.I.S.O), para reforzar la acción preventiva de la Agencia. En concreto, se han concluido en 2017 los Planes de oficio de Hospitales, de servicios *cloud* en el ámbito educativo y de Sistemas de Información de Visados VIS-II y SIS-II, y se han iniciado los planes sobre contratación a distancia, entidades financieras y supervisión del acervo Schengen.

7 El apoyo y reconocimiento a las buenas prácticas en privacidad en proyectos innovadores y de difusión a través de los Premios AEPD de Comunicación, Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet; iniciativas para adaptarse al Reglamento europeo de Protección de Datos, y de Investigación en Protección de Datos Personales 'Emilio Aced'.

8 La elaboración de nuevos materiales y recursos para fomentar la educación digital de

los menores (Guía de Centros Educativos); la serie de vídeos 'Tú controlas internet'; el Taller para familias 'Los menores y su ciber-mundo', y las Orientaciones sobre uso de plataformas tecnológicas en centros docentes.

9 El refuerzo de la colaboración en materia de consumo, a través del Consejo de Consumidores y Usuarios y la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN).

10 El impulso de medidas de mejora de la gestión interna de la Agencia de carácter organizativo, simplificación administrativa y reducción de plazos mediante la implantación de la productividad por objetivos, el incremento de plantilla, en especial en el ámbito de la Inspección de Datos, para reducir el número de asuntos pendientes, y la reducción progresiva de los plazos de tramitación en todos los procedimientos de la Agencia.

2. Prevención para una protección más eficaz

2.1. PROTECCIÓN A LOS CIUDADANOS

2.1.1. Consultas atendidas por el área de Atención al ciudadano

La AEPD ofrece a los ciudadanos, a través del área de Atención al Ciudadano, varios canales mediante los cuales pueden plantear sus dudas respecto a la normativa de protección de datos: atención telefónica, presencial y por escrito, así como la posibilidad de realizar consultas a través de la Sede Electrónica, y de acceder al catálogo de las consultas más frecuentes (FAQ's) que se encuentran publicadas en la citada Sede.

El número total de consultas planteadas y respondidas por este Área durante el año 2017 ascendió a 255.908, lo que supone un incremento del 8% respecto al año 2016, destacando un incremento significativo en el acceso a las preguntas frecuentes (170.754 en 2017 frente a 147.297 accesos en 2016).

El desglose es el siguiente:

Atención presencial	3.699
Atención telefónica	73.501
Consultas por escrito	516
Consultas por la sede electrónica	7.438
Acceso a las preguntas frecuentes	170.754
Total	**255.908**

Los temas más consultados son los siguientes: inscripción de ficheros (obligación que desaparece con la aplicación del RGPD el 25 de mayo de 2018), el tratamiento de datos personales en los ficheros de solvencia patrimonial, protección de datos en las comunidades de vecinos, videovigilancia y solicitudes de información sobre la forma de interponer denuncias y reclamaciones ante la AEPD.

Respecto a las consultas sobre el ejercicio de derechos por parte de los ciudadanos, destacar que casi el 50% (43,34%) fueron sobre el derecho de cancelación, y un 12,38% sobre el denominado "derecho al olvido", mediante el derecho de oposición y cancelación respecto de los enlaces de servicios de búsqueda en internet. Por lo que respecta al resto de derechos, el 31,36% se plantearon sobre el derecho de acceso, un 8,73% sobre el derecho de oposición, y un 4,16% sobre el derecho de rectificación.

Respecto al catálogo de Preguntas Frecuentes (FAQs) cabe señalar que fueron renovadas a mediados de julio de 2016. Este catálogo permite consultar más de 200 preguntas-respuestas agrupadas por temas y, en muchas ocasiones, la oportuna respuesta se completa con el acceso a materiales publicados por la AEPD.

Esta modificación ha supuesto, como ya se ha referido, que en el año 2017 hayan aumentado las visitas a este catálogo en más de 20.000 visitas respecto al año 2016.

Asimismo, y teniendo en cuenta que el Reglamento General de Protección de Datos (RGPD) será de aplicación el 25 de mayo de 2018, se han publicado nuevas preguntas con sus respuestas agrupadas en dos temáticas nuevas: 'Reglamento General de Protección de Datos' y 'Delegado de Protección de Datos (Certificación)', que son de las más consultadas junto a los apartados de Solvencia Patrimonial ('Ficheros de morosos'), 'Videovigilancia', 'Obligaciones de los responsables de ficheros' y 'Comunidades de propietarios'.

2.1.2. Herramientas más significativas

Guía General sobre derechos de los ciudadanos

El 25 de mayo de 2017, coincidiendo con la celebración de la 9ª Sesión Anual, se publicó esta nueva guía bajo el título 'Protección de datos: Guía para el ciudadano', con la finalidad de que los ciudadanos puedan tener un mayor conocimiento de los derechos que esta normativa les reconoce.

La guía se encuentra dividida en los siguientes apartados: 'Tu derecho a la protección de datos de carácter personal'; 'Obligaciones en el tratamiento de tus datos personales'; 'Cuáles son tus derechos y cómo ejercitarlos'; 'Tratamiento de datos personales en ámbitos específicos'; 'Recursos de la AEPD a disposición del ciudadano'; y 'Términos y definiciones utilizados en esta Guía'.

En relación con este documento cabe destacar los siguientes aspectos:

- Se ha tenido en cuenta la inminente aplicación del RGPD, de forma que contiene un apartado específico explicando los derechos que recoge el citado Reglamento, entre los cuales se encuentran los nuevos derechos a la portabilidad, a la limitación del tratamiento de datos y a no ser objeto de decisiones individuales automatizadas.

- Contiene un apartado específico relativo a las cuestiones que más preocupan a los ciudadanos en relación con el tratamiento de sus datos personales en internet, como son el denominado derecho al olvido así como la eliminación de fotos y vídeos.

- Incluye múltiples enlaces a documentación publicada en la web de la AEPD.

- Para facilitar su comprensión, se ha utilizado un lenguaje sencillo, claro y directo, además de numerosos ejemplos.

- En los ámbitos específicos aparece una descripción breve y sencilla de aquellos temas que más interesan a los ciudadanos: ficheros de solvencia patrimonial, tratamiento de datos en las comunidades de propietarios, videovigilancia, publicidad y telecomunicaciones.

Guía de compra segura en internet

El comercio electrónico facturó en España 24.185 millones de euros en 2016 y aumentó en el segundo semestre de 2017 un 23,4% interanual hasta alcanzar los 7.338,1 millones de euros. No obstante, según datos de INE, la mitad de los usuarios de internet que no han comprado online en el último año alega para ello una preocupación por la privacidad, por las prácticas fraudulentas o engañosas o por la seguridad en el pago.

Con fecha 18 diciembre, se presentó la 'Guía práctica de compra segura en internet'. Esta iniciativa de la AEPD es el resultado del trabajo de la Agencia realizado en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y la Policía Nacional para ofrecer a los ciudadanos en una única publicación los consejos prácticos más relevantes a tener en cuenta antes, durante y después de realizar una compra online. La guía está acompañada de siete fichas que recogen de forma concisa recomendaciones de utilidad.

La guía recoge los derechos que asisten a los usuarios en los procesos de compra o contratación online, ofreciendo recomendaciones desde diversos enfoques: la privacidad, la seguridad, los derechos de los consumidores y la detección de prácticas delictivas o fraudulentas. El objetivo es que resulte de utilidad no sólo a los ciudadanos como consumidores y usuarios de los servicios de comercio electrónico sino también a las empresas que desarrollan su actividad en este ámbito, contribuyendo a fomentar un clima de confianza digital.

La guía agrupa sus contenidos en cuatro bloques: qué aspectos se deben tener en cuenta antes de comprar o contratar un producto o servicio online; recomendaciones en caso de que el ciudadano decida comprar; qué derechos y garantías le asisten después de completar la compra, y cómo reclamar en caso de que sea necesario. Estos apartados se complementan con un decálogo de consejos básicos que recogen algunos de los aspectos más relevantes.

Cómo proteger el dispositivo desde el que se realiza la compra; identificar tiendas de confianza; detectar posibles fraudes; medios de pago recomendados; cómo configurar las cuentas de usuario; qué hacer ante la recepción de un producto defectuoso o qué derechos tiene el ciudadano sobre sus datos personales son algunos de los aspectos tratados tanto en la guía como en las fichas prácticas. Además, los temas planteados se complementan con enlaces a contenidos que amplían la información ofrecida en cada uno de los apartados.

La guía y las fichas pueden consultarse en la web de la AEPD.

Espacio web sobre reclamaciones en materia de telecomunicaciones

La Agencia lanzó en su página web en 2017 un apartado específico con diversa información referida a las reclamaciones en materia de telecomunicaciones, puesto que es una de las cuestiones que más afectan y preocupan a los ciudadanos. En primer lugar, en el apartado 'Qué puedo reclamar' y 'Dónde debo dirigirme', al ser varios los organismos con competencia en este ámbito, se puede consultar un tríptico descriptivo sobre las competencias de la Secretaria de Estado para la Sociedad de la Información y Agenda Digital (SESIAD), los organismos de consumo y la AEPD.

Este apartado se completa con el referente a 'Cómo puedo reclamar', en el que se indica al ciudadano dónde puede dirigirse para interponer la oportuna reclamación, distinguiendo en el caso de la AEPD entre la posibilidad de interponer una denuncia o una reclamación de tutela de derechos, dependiendo del caso concreto.

En segundo lugar, el site contiene un listado de preguntas frecuentes con su oportuna respuesta referente al tratamiento de datos de los ficheros de solvencia de patrimonial, ya que este tipo de ficheros se encuentran directamente relacionados con la contratación irregular o fraudulenta de estos servicios y la inclusión de los afectados en ficheros de esta naturaleza.

Otro de los apartados es el referente a la documentación a presentar ante la AEPD en el caso de que el ciudadano quiera interponer una reclamación, diferenciando entre la que debe ser presentada en función de si la citada reclamación versa sobre 'Contratación irregular o fraudulenta de servicios de telecomunicaciones', 'Deudas derivadas de servicios de telecomunicaciones', o 'Inclusión indebida en guías de abonados'.

Espacio web sobre publicidad no deseada

Junto con las reclamaciones en materia de telecomunicaciones, la recepción de publicidad no deseada es otro de los temas por los que los ciudadanos muestran mayor inquietud, por lo que la AEPD creó otro apartado específico para facilitar la divulgación de información sobre este tema. La finalidad principal de la información es facilitar al ciudadano el conocimiento de una serie de recursos para evitar la recepción de la publicidad cuando no desea recibirla.

Así, se destaca la posibilidad de que los ciudadanos se puedan inscribir en la Lista Robinson, que debe ser consultada por quienes vayan a realizar una campaña de publicidad.

Para los supuestos en que se reciba publicidad por correo electrónico o a través de medios electrónicos equivalentes (como SMS o WhatsApp), se indica que es posible el envío de publicidad por estos medios si existe una relación contractual, siempre que los datos de contacto se hayan obtenido de forma lícita y se trate de productos o servicios similares a los contratados, pero el ciudadano se puede oponer a recibirlos a través de los procedimientos que obligatoriamente deben ofrecer o de un medio sencillo y gratuito como es la citada Lista Robinson.

Por otra parte, en el *site* también se facilitan consejos útiles para evitar la publicidad indeseada, como evitar dar el consentimiento cuando se trate de participación en concursos u ofertas y evitar que los datos de contacto aparezcan en las guías telefónicas. También se indica la posibilidad de revocar el consentimiento previamente prestado ejercitando los derechos de oposición y cancelación, así como la posibilidad de interponer una reclamación ante la AEPD. Por último, y al igual que en el *site* de reclamaciones de telecomunicaciones, se ha incluido un apartado específico dedicado a la mediación.

Sistema de mediación de Autocontrol en materia de telecomunicaciones y publicidad no deseada

El RGPD establece la obligación de que las autoridades de control promuevan la elaboración de códigos de conducta que aseguren la correcta aplicación de la normativa de protección de datos personales. Entre los objetivos de los códigos de conducta se prevé expresamente la posibilidad de articular procedimientos extrajudiciales y otros procesos De resolución de conflictos que permitan resolver las reclamaciones de los ciudadanos.

La experiencia de la AEPD en los últimos años pone de manifiesto que las principales reclamaciones de los ciudadanos son las relacionadas con la suplantación de la identidad en la contratacion de servicios de telecomunicaciones y la publicidad no solicitada. La suplantación produce consecuencias particularmente negativas para los ciudadanos, generando la facturación de servicios que no han contratado, el requerimiento del pago de los mismos y la inclusión en los denominados ficheros de morosidad en el supuesto de impago, entre otras. Por su parte, la recepción de publicidad no solicitada implica una intromisión en los derechos de los ciudadanos, especialmente cuando han manifestado su oposición expresa a no recibirla.

Las principales reclamaciones de los ciudadanos están relacionadas con suplantación de identidad y publicidad no solicitada

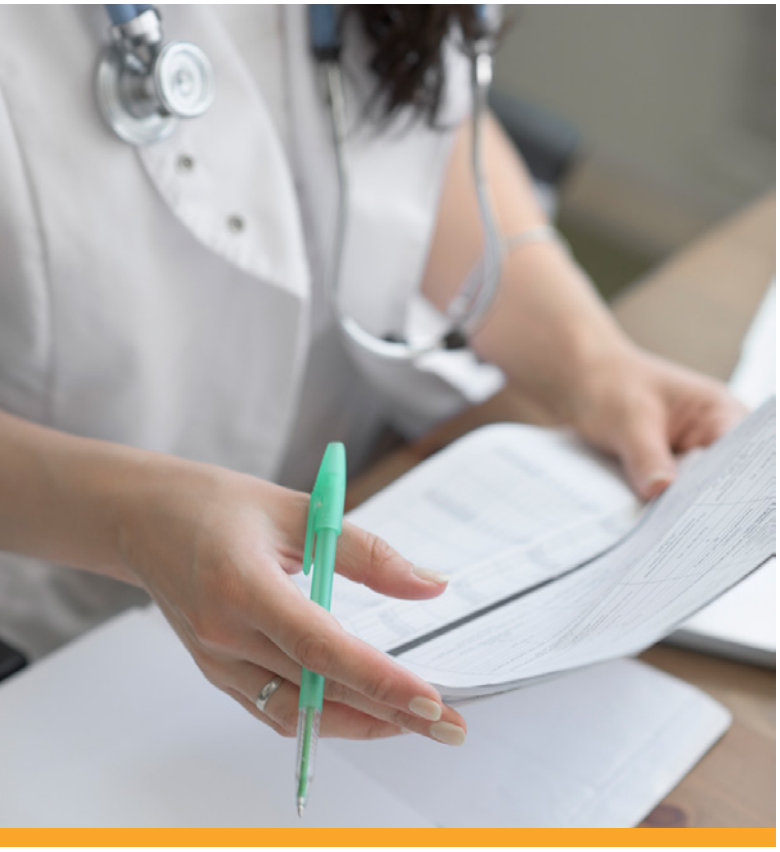
La AEPD suscribió en 2017 con la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL) un Protocolo General de Actuación que respalda la iniciativa para establecer un sistema voluntario de mediación con las operadoras de los grupos Telefónica, Vodafone, Orange y Másmóvil.

El sistema, gestionado por Autocontrol, está dirigido a resolver ágilmente a través de la mediación las principales quejas de los ciudadanos que se han descrito anteriormente. No obstante, este sistema de mediación es independiente de las reclamaciones que los ciudadanos pueden seguir planteando ante la Agencia Española de Protección de Datos. Para solicitar esta mediación voluntaria es necesario rellenar un formulario disponible en la web de Autocontrol.

2.1.2 Inspecciones sectoriales de oficio

Plan de Sanidad

En el año 1995, la Agencia Española de Protección de Datos realizó un Plan Sectorial de Oficio con el objetivo de analizar el nivel de adecuación del sector de la asistencia hospitalaria pública a la normativa de protección de datos vigente en aquel momento.



Durante el año 2010 se realizó un seguimiento mediante un cuestionario remitido a todos los hospitales del Catálogo Nacional, públicos y privados, obteniéndose un informe de situación en el que se reflejaba que, en los centros públicos, las mayores diferencias de cumplimiento se presentaron en las cláusulas informativas de los formularios de recogida de datos y en la realización de la auditoría bienal de seguridad. Otros aspectos con carencias detectados en el sector público fueron los carteles informativos sobre protección datos, las revisiones del documento de seguridad, el registro de los accesos a los datos, la seguridad en el almacenamiento de las historias clínicas en papel para evitar accesos no autorizados, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte.

Con el fin de dar continuidad al seguimiento de las actuaciones realizadas en este sector se contempla dentro del Plan Estratégico 2015-2019 de la Agencia un programa dedicado a la Sanidad, donde se engloba el Plan de Inspección de oficio de Hospitales Públicos.

Este plan se ha centrado en los procedimientos técnicos y políticas de actuación seguidas en los hospitales públicos, con la valoración de su nivel de adecuación a las previsiones de la normativa de protección de datos teniendo como objetivo final elevar el nivel de cumplimiento del sector en esta materia, así como generar confianza en las actuaciones de las instituciones sanitarias tanto en el ámbito asistencial como en el de la investigación.

Durante el año 2016, la Agencia realizó actuaciones de inspección dirigidas a los centros hospitalarios de titularidad pública teniendo en cuenta los gestionados tanto de forma directa como indirecta, centrándose en la auditoría de las medidas de seguridad implementadas, con visitas presenciales a los hospitales que fueron inicialmente auditados y hospitales de nueva creación.

Se auditaron los dos tipos de tratamientos de datos de salud realizados por los hospitales públicos:

- Tratamientos con la finalidad asistencial, encaminada a prestar asistencia sanitaria a los pacientes que acuden a los centros.
- Tratamientos con la finalidad de investigación médica.

El 26 de septiembre de 2017 se hizo público el Informe de la inspección en el que se recogen los resultados y las conclusiones del análisis realizado.

El contenido del informe pone de manifiesto una tendencia en general favorable a la progresiva asunción, no sólo de la normativa, sino de los principios y la "cultura" del tratamiento de los datos en este sector y su debida protección. Hay que indicar que los errores detectados durante la inspección de oficio no constituyen comportamientos generales, sino aspectos puntuales que se pueden y deben mejorar. Entre ellos destacan los siguientes:

- Información ofrecida a los pacientes: se considera conveniente elaborar y situar en lugar visible, al menos en las áreas de admisión y urgencias, carteles informativos sobre la identificación del responsable del fichero, el modo de ejercitar los derechos ARCO y de la dirección o departamento al que deben dirigirse para ello.

Además, en todos los documentos mediante los que se recaben datos de los pacientes se debe de incluir toda la información prevista en el artículo 5 de la LOPD.

- Es necesario recabar el consentimiento del paciente para saber si desea que su presencia y ubicación en el hospital sea comunicada a las personas o familiares que pregunten por ello. Si este no se opone, el hospital puede informar de si se encuentra en urgencias o ingresado y el número de habitación, sin indicar datos de salud o la atención médica prestada.

- Todos los hospitales deberían establecer normas internas que obliguen a la confidencialidad de los datos, tanto al personal del hospital como a todo aquel que pueda tener acceso a los datos de los pacientes como médicos residentes, estudiantes o personal externo. Todo el personal citado, debería suscribir un compromiso de confidencialidad antes de empezar a desempeñar sus funciones, mediante el cual se acepte la norma interna descrita.

En materia de seguridad las deficiencias más importantes están relacionadas con los siguientes aspectos:

Registro de incidencias. La no implantación de un procedimiento de gestión de incidencias como tal, limitándose en la mayoría de los casos a su tramitación por medio de los centros de atención al usuario y, en algunos casos, no se registran ni documentan los procesos de recuperación.

Control de Acceso, Perfiles y Gestión de usuarios. La mayoría de las aplicaciones auditadas permiten que un facultativo acceda sin restricciones a datos de pacientes que no tiene asignados. Se recomienda el establecimiento de alertas de confidencialidad que se muestren al usuario del sistema cuando acceda a los datos de un paciente que no tiene asignado.

En algunas aplicaciones corporativas se ha comprobado que algunos colectivos o perfiles de usuarios tienen acceso a datos que no necesitan para sus funciones, tales como por ejemplo los administrativos que tienen acceso a alertas e informes médicos que no son necesarios para sus funciones.

Autenticación/contraseñas. Todos los tratamientos de datos de salud auditados autentican la identidad del usuario mediante contraseñas, no obstante se han encontrado algunas deficiencias puntuales.

Auditoría de seguridad. Se ha detectado que, en muchos casos, el plazo máximo de dos años para la realización de auditorías de las medidas de seguridad sobre todos los ficheros es superado, realizándose en todo caso auditorías parciales en una selección de ficheros, y en algunas ocasiones no se subsanan las deficiencias encontradas.

Registro de Accesos. No todas las aplicaciones disponen de registro de accesos y las que lo tienen tampoco disponen, en todos los casos, de un periodo definido de conservación, ni conservan las actuaciones concretas que se han realizado sobre un de-

terminado paciente. Habitualmente no se realizan auditorías con la información que consta en los registros de acceso.

Comunicaciones cifradas. Todas las comunicaciones de datos de salud que se realicen a través de redes públicas de telecomunicaciones se deben efectuar utilizando un medio robusto de cifrado o utilizando otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. No está por tanto permitida, por ejemplo, la remisión de datos de salud vía fax sin cifrado.

Aplicaciones de información departamentales. En algunos hospitales se ha detectado un número significativo de aplicaciones instaladas sin conocimiento del responsable de Seguridad del Centro, que no controla las medidas de seguridad implementadas.

Documentos en papel. Deben implantarse medidas para el traslado de documentación médica en papel fuera del hospital que eviten que la historia clínica sea accedida o modificada durante el traslado, tales como sobres cerrados con procedimiento de notificación de recepción por parte de los centros de destino, o bien que fuese trasladada por personal específico que se encargue de su custodia ininterrumpida. Asimismo, se deben establecer mecanismos de comprobación de la integridad de la historia clínica en papel.

Si bien el enfoque de la seguridad de los Sistemas de Información va a sufrir un cambio con la entrada en vigor del nuevo Reglamento Europeo en mayo de 2018, se considera que las medidas de seguridad que se han citado, de obligado cumplimiento en la actualidad, son una buena base para un adecuado cumplimiento de la nueva normativa y, en cualquier caso, orientativas de cara a las resultantes del Análisis de Riesgo y la Evaluación de Impacto que se va a tener que realizar.

La AEPD ha elaborado un decálogo dirigido al personal sanitario y administrativo

Por otra parte, con el fin de profundizar en la cultura y la formación sobre la trascendencia de los tratamientos de los datos personales en este sector la Agencia ha elaborado en 2017 un decálogo dirigido al personal sanitario y administrativo del sector.

Plan de Inspección sectorial de contratación a distancia

El Plan Estratégico 2015-2019 de la Agencia Española de Protección de Datos contempla la actualización del plan sectorial de oficio sobre control de datos en la contratación telefónica y a través de internet. De cara a la consecución de este objetivo, en el año 2017 se ha iniciado un plan sectorial de oficio que, teniendo en cuenta el desarrollo que ha experimentado el comercio electrónico y el cambio legislativo que ha supuesto la entrada en vigor del Reglamento General de Protección de Datos 679/2016, que será aplicable el 25 de mayo de 2018, tiene por objeto la investigación detallada de los procedimientos implementados por las principales entidades que intervienen en el mercado para el tratamiento de la información de carácter personal en las contrataciones de servicios y ventas de productos de forma electrónica y telefónica, y los procesos de adaptación a la nueva realidad legislativa.

Este Plan Sectorial permitirá obtener una visión de los procesos seguidos por las en-

tidades inspeccionadas, tales como los procedimientos de alta de los nuevos clientes, de información, de comunicación de los datos de los clientes a terceros, de contratación con los encargados del tratamiento y de gestión de reclamaciones, con el fin de detectar sus debilidades y proponer los cambios necesarios a través de recomendaciones encaminadas a la mejora de los procedimientos empleados en las técnicas de venta a distancia.

El plan se desarrolla en las siguientes fases consecutivas: 1) venta de productos a través de internet; 2) contratación a distancia, realizada por los operadores de telecomunicaciones; 3) contratación a distancia, realizada por las empresas comercializadoras de energía eléctrica y de gas y 4) entidades prestadoras de servicios electrónicos de confianza.

La primera de ellas se ha iniciado en el año 2017 y se proyecta sobre dos grupos de entidades que contratan con el consumidor a través de internet: los que comercializan sus propios servicios o productos y los que comercializan servicios o productos de terceros.

La primera fase se ha centrado en los procesos de venta a través de internet, debido al incremento significativo que ha experimentado en los últimos años la comercialización de servicios y productos a través de la técnica de venta electrónica. Internet ha cambiado de forma beneficiosa para ambas partes el modo en que los clientes compran y las empresas anuncian y venden sus productos y servicios. Sin embargo, este desarrollo de las técnicas de venta a distancia puede generar riesgos para el derecho fundamental a la protección de datos de los consumidores. Por ello, en esta fase se ha considerado esencial profundizar en los procedimientos implementados a fin de establecer protocolos que minimicen los riesgos de los responsables de los ficheros de efectuar tratamientos de datos no consentidos por los afectados.

A lo largo del año 2018, se desarrollarán las restantes fases del plan, que finalizará con un documento que dará cuenta de los aspectos más relevantes observados en el ámbito de la contratación a distancia y contendrá las recomendaciones precisas en materia de protección de datos para la mejora de los procesos.

Plan de Inspección de oficio de entidades financieras

El Plan Estratégico 2015-2019 de la AEPD contempla la realización de diversos planes de inspección de oficio en aquellos sectores de la sociedad en donde el avance tecnológico y su especial incidencia adquiere mayor relevancia, al afectar de forma significativa al aumento de la capacidad de llevar a cabo tratamientos de datos personales.

Uno de estos sectores es, por su importancia, el de las entidades financieras y establecimientos financieros de crédito y asimiladas. Las facilidades de acceso por los ciudadanos a través de internet a la contratación de los productos ofrecidos por este tipo de entidades permite dinamizar esta actividad productiva en beneficio de todos. Sin embargo, este rápido aumento de actividad puede dar lugar a distorsiones en el sector en materia de protección de datos.

Tal es el caso de la identificación inequívoca a través de herramientas online de los suscriptores de los servicios ofrecidos por el sector ya que, aunque en la actualidad existe tecnología suficiente para llevarla a cabo, su escasa implantación en el sector o los errores de implementación pueden dar lugar a contrataciones fraudulentas indeseadas que originan a su vez múltiples y sucesivos tratamientos de datos ilícitos, como puede ser la inclusión indebida del afectado en ficheros comunes de solvencia, con los perjuicios asociados que ello conlleva.

También se deben mencionar los tratamientos indebidos que, como consecuencia de una mala praxis por parte de ciertas entidades, dan lugar a acciones ilícitas de recobro de deudas.

Por ello, en el año 2017 se puso en marcha un plan de inspección de oficio al sector financiero y asimilado que culminará en 2018.

En el último trimestre de 2017, se ha priorizado en la ejecución del Plan de Oficio el análisis a determinadas entidades financieras y asimiladas, entre las que se encuentran las entidades que ofrecen créditos rápidos de escasa cuantía y con gran impacto en la actualidad.

Sistemas de Información de Visados VIS-II y de Schengen SIS-II

El Sistema de Información de Schengen o SIS, creado en virtud del Convenio de Aplicación del Acuerdo de Schengen, es un sistema de información común que permite a las autoridades competentes de los Estados miembros disponer de información relativa a algunas categorías de personas y objetos y cuyo propósito es el mantenimiento de la seguridad pública, apoyo a la policía, la cooperación judicial y la gestión del control de las fronteras exteriores.

Relacionado con el SIS, la Decisión 2004/512/CE del Consejo, de 8 de junio de 2004, establece el Sistema de Información de Visados (VIS) y el intercambio de datos entre los Estados Miembros y la Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, establece las condiciones para el acceso a consultar el Sistema de Información de Visados por las autoridades designadas de los Estados Miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismos y otros delitos graves.

Ambos sistemas, SIS y VIS, constituyen una de las iniciativas claves de la Unión Europea y se integran dentro del Acervo Schengen.

La AEPD es la autoridad de supervisión encargada de garantizar la correcta aplicación de la legislación de protección de datos en las partes nacionales de ambos sistemas de información, tanto en lo que se refiere a normas generales como en las disposiciones específicas de las citadas regulaciones.

La importancia de estas tareas de supervisión ha hecho que la AEPD haya establecido en su Plan Estratégico una actividad denominada “Supervisión de la AEPD del acervo Schengen” en cuyo marco realiza actuaciones de control periódicas sobre la información que se incluye en la parte nacional del SIS y en la implementación del sistema VIS, tanto en el territorio nacional como en las delegaciones consulares.

Durante 2017 y, con relación a la supervisión al sistema SIS, se han realizado inspecciones presenciales a la Oficina SIRENE, a la Secretaría de Estado de Seguridad del Ministerio del Interior, a la Dirección General de la Guardia Civil y a la Subdirección General de Logística de la Dirección General de la Policía.

Las actividades desarrolladas durante 2017 con relación a la supervisión al sistema VIS, tras las ya ejecutadas en 2016, fueron la inspección al Consulado de España en Moscú y a la empresa subcontratada para la gestión del proceso de recogida de datos.

Ambas actuaciones, sobre el sistema SIS y VIS, dieron lugar a la realización de informes sobre la adecuación de los mismos con las recomendaciones oportunas que fueron cursados por la AEPD a los responsables de los mismos.

Sobre la base de estos informes, y de cara a la organización futura de la actividad de supervisión, se adoptó un Plan de Auditoría continua, que se desarrollará en cuatro años en colaboración estrecha con los responsables de los sistemas y cuyas primeras actuaciones fueron la realización de tres reuniones de seguimiento de la implementación de las recomendaciones de la AEPD con la Oficina SIRENE, la Secretaría de Estado de Seguridad y el Ministerio de Asuntos Exteriores y Cooperación, el establecimiento de un calendario de inspecciones y, en concreto, la preparación de la inspección al consulado español en Shanghai en el primer mes de 2018.

Durante 2017 tuvo también lugar la evaluación de la aplicación del Acervo Schengen en España por parte de la Comisión Europea. La evaluación de la aplicación del Acervo Schengen en España se encuentra prevista en el Reglamento (UE) 1053/2013 del Consejo de la Unión Europea, por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del Acervo Schengen respecto del Sistema de Información común entre todos los países miembros. El objetivo de la evaluación es verificar el cumplimiento de la normativa aplicable en los principales ámbitos cubiertos por el Acuerdo Schengen, incluyendo las disposiciones relativas a la protección de datos de carácter personal, además de evaluar el correcto cumplimiento de la labor de supervisión de ambos sistemas por parte, en el caso de España, de la Agencia Española de Protección de Datos.

El Equipo de Evaluación de la Comisión, que incluía a representantes de otras autoridades de protección de datos europeas, examinó las actividades de inspección realizadas por la AEPD así como el funcionamiento del sistema en las unidades de los Ministerios de Interior y Asuntos Exteriores y Cooperación implicadas en su gestión. El equipo recibió también los informes de supervisión de la AEPD.

A finales de 2017 no está aún disponible la versión final del informe del Equipo de Evaluación, pero el primer borrador concluye que España cumple, en general y en particular en su actividad supervisora del Acervo Schengen, con los criterios de calidad establecidos por la Comisión.

Contadores inteligentes

El modelo Smart Grid, también conocido como Red Eléctrica Inteligente, se basa en la gestión de forma eficiente de la energía, producto de la combinación de las mejoras de la ingeniera eléctrica con los avances de las tecnologías de la información y las comunicaciones. Este modelo permite a las empresas de distribución eléctrica tener información de los consumos en tiempo real, pudiendo así realizar estimaciones más precisas de cuánta energía hay que producir, distribuir e incluso diseñar ofertas que se adecuen al perfil de los clientes, dependiendo de sus hábitos de consumo eléctrico.

Los Contadores Inteligentes o Smart-Meters son dispositivos de medición que tienen la capacidad de recopilar los datos del consumo eléctrico de un hogar, almacenarlo y enviar esa información a la compañía eléctrica de forma instantánea, con capacidad para realizar lecturas desde cada 20 segundos hasta cada hora.

Los datos recopilados por los contadores inteligentes son enviados a una plataforma llamada concentrador, donde se recogen las lecturas de varios clientes y posteriormente estos datos son enviados telemáticamente a las compañías eléctricas.

La Unión Europea plantea que para el año 2020 el 80% de los contadores sean inteligentes. En noviembre de 2016, la Comisión Europea publicó una propuesta de directiva de regulación del mercado eléctrico interno en la que incluye el impulso de la instalación de dichos contadores.

El uso de los Smart-meters permite a las compañías eléctricas tener un mayor control de los datos de consumo, una mayor precisión en las lecturas y un control remoto de la conexión. Estas características permiten suspender automáticamente el suministro eléctrico y también volver a conectarlo, mitigar los fraudes hacia las compañías de suministros de servicios de electricidad, diseñar planes a medida para ofrecer a sus clientes, conocer sus hábitos cotidianos de consumo en el hogar y obtener datos de gran valor comercial para terceros.

Por ello, la Comisión Europea publicó la Recomendación de 10 de octubre de 2014 relativa al modelo de evaluación de impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente, donde delega sobre los Estados miembros la responsabilidad de fomentar que los responsables del tratamiento de datos apliquen el modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente y que tengan en cuenta las recomendaciones del Grupo de Trabajo del artículo 29 en lo que respecta al tratamiento de datos personales y, en particular, su dictamen 07/2013.

En dicha Recomendación se previó que los Estados miembros apoyaran la realización de una fase de prueba con despliegues reales de la aplicación del modelo de evaluación de impacto sobre la protección de datos personales para valorar la eficacia de dicho modelo.

A tal efecto, los Estados miembros debían presentar a la Comisión en 2016 un informe de evaluación que recogiera las conclusiones de impacto sobre la fase de prueba.

En noviembre de 2016 el Ministerio de Energía, Turismo y Agenda Digital remitió a esta Agencia un documento de trabajo sobre el cumplimiento de la Recomendación, cuyo contenido se anticipó a la Comisión Europea a la espera de los comentarios que pudiera formular la Agencia Española de Protección de Datos. Tras analizar el documento, se realizó un informe de recomendaciones sobre el resultado de la evaluación de impacto y se propuso un plan de acción para conocer con mayor detalle las actividades de las entidades implicadas y promover acciones correctoras, que se remitió a la Secretaría de Estado de Energía del Ministerio de Turismo, Energía y Agenda Digital, cuyo seguimiento se realizará en 2018.

El plan de acción contemplaba:

- Informar al MINETAD de las carencias detectadas instándole a que realice las siguientes actuaciones:
  - Reclamar a las entidades implicadas en el modelo Smart Grid la documentación acreditativa de la aplicación de las medidas de seguridad desarrolladas en el marco de la Smart Grid Task Force.
  - Reclamar a las mismas entidades la documentación sobre la evaluación de impacto a la privacidad desarrollado a partir de la Recomendación 2014/724/UE siguiendo las recomendaciones y formatos establecidos en el Expert Group 2 de la Smart Grid Task Force.
  - Reclamar el plan de acción para la auditoría y revisión de las medidas, especialmente las medidas correctivas, y conclusiones establecidas en la documentación anteriormente señalada.
- Instar a la realización de la evaluación del grado de cumplimiento, adopción de las medidas oportunas, y traslado de sus conclusiones y de la información recabada a la AEPD.

El seguimiento de estas actuaciones se realizará en 2018.

Ramsonware Petya

La supervisión de la obligatoriedad de gestionar y notificar brechas de seguridad que afecten a datos de carácter personal que establece el nuevo RGPD, que compete a la AEPD, va más allá de mantener un sistema de comunicación de brechas y de seguimiento de las mismas. La AEPD ha de tener una actitud proactiva y estar al tanto de las posibles brechas que afectan a datos personales incluso antes de que se notifiquen o cuando no han sido notificadas. Con este carácter proactivo, ante el ataque masivo mediante *ransomware* Petya, conocido desde el 27 de junio de 2016, la AEPD realizó un seguimiento de oficio de la información publicada por los CERT (Emergency Response Team, Equipo de Respuesta ante Emergencias Informáticas) del Centro Criptológico Nacional (CCN) y del INCIBE, así como de las noticias publicadas por las entidades más relevantes en seguimiento de ataques informáticos en internet, para determinar hasta qué punto puede afectar al tratamiento de datos de carácter personal. Al constatarse que los responsables han adoptado las medidas oportunas respecto de la brecha de seguridad, no se inició procedimiento por infracción de la LOPD.

2.1.3. Garantía de los derechos de los ciudadanos

Denuncias y tutela de derechos

Durante el año 2017 la entrada de denuncias y reclamaciones de tutela de derechos ARCO en la Agencia experimentó un leve ascenso global de un 1,22% sobre el año anterior. Los indicadores de denuncias y reclamaciones resueltas muestran incrementos en ambos procedimientos, creciendo las denuncias resueltas en un 8,39%, y las tutelas resueltas en un 14,29% respeto a 2016.

Como consecuencia del incremento de las denuncias y reclamaciones resueltas, sin variaciones notables en la entrada, se aprecia un descenso muy agudo de las denuncias y reclamaciones que se encuentran en tramitación, que disminuyen un total del 33,37% sobre los valores de 2016. Esta mejora se corresponde con una mayor eficacia administrativa a la hora de tramitar los procedimientos.

Poniendo en relación la cifra de denuncias y reclamaciones resueltas en 2017 respecto a las resueltas en 2015, se observa un descenso (-10,53%) que se debe a los singulares resultados obtenidos en 2015 a raíz del esfuerzo por minimizar el remanente de denuncias, iniciadas en años anteriores, que aún continuaban en tramitación.

Una vez superada esa situación puntual, los datos de 2017 muestran una tónica de estabilidad respecto a los de 2016.

Se aprecia un descenso de las denuncias y reclamaciones que se encuentran en tramitación.

En cuanto a los expedientes iniciados durante el ejercicio 2017, que son los expedientes nuevos que se abren a partir de denuncias (no derivados de otros), se observa un leve descenso de un 5,59% con respecto al año pasado, pero el crecimiento con respecto al 2015 es de un 16,35%. Este comportamiento puede deberse al impulso dinamizador experimentado a finales de 2016, cuando se abrieron numerosos expedientes que se han resuelto a lo largo de 2017.

En cuanto a las resoluciones dictadas, las correspondientes a la potestad sancionadora y de declaración de infracción de las Administraciones Públicas han crecido en un 13,24% y un 22,67% respectivamente, manteniendo el ciclo de crecimiento de años anteriores. Del mismo modo que las reclamaciones de tutelas, cuyas resoluciones de procedimientos también han aumentado un 12,48%.

Atendiendo a la naturaleza de las resoluciones del ejercicio de la potestad sancionadora, un 35% corresponde al archivo de denuncias no subsanadas; un 27% al archivo de las actuaciones de investigación, y los apercibimientos, resoluciones de procedimientos sancionadores y resoluciones de procedimientos de declaración de infracción de las Administraciones Públicas representan un 15%, un 22% y 2% respectivamente. El número de resoluciones mantiene la tendencia al alza en los procedimientos sancionadores (27,57%), y en los procedimientos de declaración de infracción de las Administraciones Públicas (7,14%) con respecto a las equivalentes de 2016, pero no así en los apercibimientos, que permanecen estables con una leve caída del 0,41%. En lo relativo a las resoluciones de tutelas, disminuyen mínimamente las desestimatorias (-7,16%), mientras que las estimatorias y estimatorias formales y parciales experimentan un aumento significativo del 18,06% y 36,30% respectivamente, sobre los valores de 2016.

En lo relativo a tiempos de tramitación desde el registro de denuncias y reclamaciones, los indicadores reflejan descensos significativos en todos los tipos de expedientes. Destacan las reducciones obtenidas en los tiempos de los archivos de denuncia sin actuaciones de investigación y en los archivos por no subsanarse las denuncias. Asimismo, en los expedientes de procedimientos sancionadores, de declaración de infracción de las Administraciones Públicas y de tutela de derechos se han mejorado los tiempos este año. Un elemento dinamizador ha sido la generalización de la notificación electrónica a las personas jurídicas en la segunda mitad del año, que debería seguir mejorando los ratios de eficacia en 2018.

Como conclusiones de las cifras del año 2017, los resultados reflejan una mejora sostenida respecto a los mismos indicadores del 2016 en todas las áreas. Se han consolidado muchas de las reformas emprendidas para mejorar la eficacia, disminuyendo tiempos y reduciendo el volumen de expedientes en tramitación.

El reto para el año 2018 será incorporar las novedades legislativas (Reglamento General y nueva LOPD, principalmente) en los procedimientos y conseguir una interlocución fluida con los nuevos actores en el ámbito europeo. Asimismo, será preciso avanzar con la Administración Electrónica y perfeccionar los métodos de gestión para simplificar los trámites y conseguir una mayor eficacia sin renunciar a la calidad del servicio a los ciudadanos.

Ficheros comunes de solvencia patrimonial

En este sector de actividad destacan dos líneas de actuación de la Agencia. La primera es el control del cumplimiento de los requisitos requeridos para la inclusión de datos de carácter personal en este tipo de ficheros por parte de las entidades acreedoras. La segunda, el control del cumplimiento de las obligaciones exigibles para el mantenimiento de datos de carácter personal en estos ficheros por parte de las entidades responsables de los mismos.

En el primer caso, destacan las denuncias sobre la ausencia total del requerimiento previo de pago o bien el incumplimiento de los requisitos necesarios para su validez. En especial llama la atención el del carácter previo del requerimiento y la acreditación de haberse realizado el envío o la recepción efectiva por el destinatario.

En menor cuantía aparecen las denuncias por otro tipo de deficiencias de tipo formal

que también invalidan el propio requerimiento realizado, como es la falta de información al afectado sobre la posibilidad de incluir sus datos en ficheros de solvencia patrimonial.

Dentro de esta línea es preciso señalar que, aunque la concesión de un determinado plazo para proceder al pago de la deuda no constituye una obligación del acreedor, cuando se otorga al afectado un plazo para el abono de la deuda y éste no se respeta o bien no se otorga dicho plazo pero se procede a realizar la inclusión simultáneamente a la notificación, se declara una infracción.

Los hechos denunciados más frecuentes hacen referencia a la falta de acreditación del envío o recepción de la notificación de inclusión al afectado en ficheros de morosidad.

Aunque en menor medida, también se han tramitado denuncias que concluyen con una declaración de infracción cuando los procedimientos de notificación del requerimiento de pago o de inclusión en el fichero de solvencia patrimonial no se efectúan a través de un medio fiable, auditable e independiente de la entidad notificante.

Asimismo hay que destacar aquellos casos en los que se denuncia que la deuda se encuentra en litigio, tanto en sede judicial como administrativa y, sin embargo, se incluye o mantiene en este tipo de ficheros.

Por último, hay que señalar aquellos casos en los que la deuda informada a este tipo de ficheros ya fue abonada o, como resultado de litigio interpuesto ante órganos competentes para dirimir, resultó no ser cierta.

Contratación irregular

En la contratación irregular destacan por su relevante aumento de denuncias las contrataciones de microcréditos a distancia a través de una web. La falta de protocolos adecuados por parte de este tipo de entidades para proceder a la identificación inequívoca de los solicitantes de crédito da lugar a imputaciones erróneas a terceros ajenos, provocando los consiguientes perjuicios a los afectados.

También deben mencionarse las denuncias respecto de las contrataciones realizadas por entidades de telecomunicaciones, de suministro eléctrico o de gas. La liberalización del sector energético y de telecomunicaciones permite que los ciudadanos puedan cambiar de entidad que les suministra los servicios. Sin embargo, la falta de diligencia por parte de algunas entidades prestadoras de este tipo de servicios, en especial en el debido control de los tratamientos llevados a cabo por las entidades encargadas con las que aquellas contratan, da lugar a tratamientos ilícitos de datos personales de terceros, al tiempo que los protocolos de identificación y para recabar el consentimiento no se cumplen o son defectuosos impidiendo su acreditación.

Entidades financieras

En el sector de la las entidades financieras, las denuncias revelan que con frecuencia se descuidan las garantías en materia de protección de datos de los afectados.

Es el caso de las quitas judiciales, que no se aplican a la cuantía de la deuda, dando lugar no sólo a asientos contables inexactos sino a comunicaciones a terceros de datos inexactos, en especial a los ficheros de solvencia patrimonial antes aludidos o a la Central de Información de Riesgos del Banco de España (CIRBE).

Dentro del sector de entidades financieras, las entidades aseguradoras y las de mediación han generado un incremento de denuncias como consecuencia de las debilidades que se acusan en el tratamiento de los datos de los ciudadanos. Esto sucede especialmente en tratamientos de cambio de tomador del seguro que originan que la prima a abonar se impute contra una cuenta bancaria sin el adecuado soporte físico que permita acreditar el consentimiento para tal tratamiento. En cuanto a los corredores de seguros, la infracción más común se refiere a la gestión de nuevas contrataciones de antiguos clientes sin su consentimiento. Por último, en los agentes de banca-seguros, se aprecia que la infracción principal es la falta de soporte documental que acredite el consentimiento para la contratación.

Entidades de recobro de deudas

Las entidades de recobro de deudas suelen tener la condición de encargadas del tratamiento por cuenta del acreedor para averiguar de los datos identificativos del deudor, al objeto de facilitar el cobro de la deuda reclamada. No obstante, en esta labor de identificación suelen incurrir en tratamientos indebidos cuando la persona supuestamente identificada no se corresponde con la verdadera deudora, dando lugar a enriquecimiento ilícito de datos en el fichero del responsable. Debe señalarse que con respecto a este tipo de entidades que se nutren de información de terceros (como son los detectives privados, entre otros) abundan los tratamientos ilícitos. A veces se debe a la falta de diligencia en la comprobación de la identificación facilitada y, en otras ocasiones, a la ausencia de protocolos adecuados que permitan regularizar diligentemente las identificaciones erróneas y la resolución de las reclamaciones mediante un contacto adecuado con el acreedor al que prestan servicio.

Por último, cabe señalar el aumento de denuncias en relación con deudas no ciertas o ya abonadas al responsable y que, como consecuencia de una falta de diligencia en el seguimiento de la deuda, tanto por el responsable como por la entidad de recobro, continúan reclamándose por la entidad de recobro.

Comunicaciones comerciales

Durante el año 2017, la mayor parte de los procedimientos sancionadores tramitados por el envío de comunicaciones comerciales han tenido como base el hecho de que los responsables de los envíos no pudieran acreditar el origen de los datos utilizados en la campaña publicitaria.

Se han mantenido las investigaciones encaminadas a determinar el grado de participación en las campañas publicitarias de los anunciantes y de otros sujetos que intervienen en la selección del público objetivo de la acción publicitaria, a fin de concretar su responsabilidad en el tratamiento de los datos utilizados en la acción publicitaria, cuando dicho tratamiento no se ha amparado en ninguna de las causas que lo legitiman. Todo ello en aplicación de lo que dispone el Reglamento de desarrollo de la

LOPD, en cuanto a la responsabilidad de las entidades que fijan los parámetros identificativos de los destinatarios de la campaña publicitaria.

Por otro lado, resulta interesante destacar que, respecto del ejercicio anterior, no han experimentado incremento llamativo los expedientes de investigación seguidos como consecuencia de las denuncias presentadas por los destinatarios de llamadas telefónicas, realizadas con fines de venta, que se habían opuesto a recibir este tipo de comunicaciones, bien a través del ejercicio del derecho de oposición o bien con motivo del registro de su línea telefónica en el Servicio Robinson.

También hay que dejar constancia de los procedimientos sancionadores seguidos contra las empresas contratadas por el responsable del tratamiento para el desarrollo y ejecución de campañas publicitarias realizadas telefónicamente que fueron llevadas a cabo contraviniendo las instrucciones dadas por aquél y las cláusulas contractuales pactadas en el contrato de prestación de servicios suscrito por ambas partes.

En materia de publicidad electrónica, una gran parte de los expedientes tramitados se refieren a infracciones producidas por el envío de un número reducido de comunicaciones a un mismo destinatario que no consintió tales envíos o que se opuso a los mismos. Hay que poner de relieve que la mayoría de las denuncias que originan estos procedimientos se producen por la recepción de los primeros envíos comerciales.

Videovigilancia

En materia de videovigilancia, el año 2017 viene a confirmar la tendencia general de los ejercicios anteriores. Por un lado, la apertura de expedientes de apercibimiento directo, incoados tanto a consecuencia de denuncias de Fuerzas y Cuerpos de Seguridad como de particulares, acompañados de prueba indiciaria suficiente.

A este respecto, debe precisarse que la realización de actuaciones previas con anterioridad a la iniciación del procedimiento sancionador, se configura como una potestad atribuida a la Agencia con el objeto de determinar si concurren circunstancias que justifiquen tal iniciación (Sentencia de la Audiencia Nacional de 4 de noviembre de 2014).

En consecuencia, no se trata de un trámite de necesaria concurrencia en el ejercicio de la potestad sancionadora pues tan solo procede la realización de actuaciones previas de investigación cuando se considere por la Agencia que resultan necesarias para determinar los hechos que pudieran justificar la incoación de procedimiento sancionador, el responsable de la comisión de la infracción o cualquier otra circunstancia relevante para la tipificación de los hechos y su imputación al responsable. Por el contrario, si el órgano sancionador cuenta con la información necesaria para delimitar suficientemente la conducta constitutiva de infracción e identificar al responsable, podrá dictar la correspondiente resolución de incoación del procedimiento sancionador o, en su caso, de audiencia de apercibimiento sin necesidad de realizar previamente actuaciones previas de investigación.

En la actividad de videovigilancia las resoluciones recaídas han sido de nuevo mayoritariamente de apercibimiento, debido a la habitual presencia como denunciados de particulares y pymes sobre los que procede aplicar los criterios de disminución de culpabilidad y antijuridicidad exigidos en la LOPD, así como el requisito de no haber sido sancionados o apercibidos previamente.

Asimismo, en materia de videovigilancia, durante 2017 la Agencia ha procedido a interpretar y aplicar en múltiples resoluciones lo dispuesto en el artículo 7.f) de la Directiva 95/46/CE. No obstante, para determinar si procede la aplicación del citado precepto al tratamiento de imágenes de personas físicas identificadas o identificables, realizado a través de cámaras y/o videocámaras, habrá de aplicarse la regla de ponderación prevista en el mismo. Esto es, será necesario valorar si en el supuesto concreto al que se refiera la instalación de un sistema de videovigilancia existe un interés legítimo perseguido por el responsable del tratamiento o, por el tercero o terceros a los que se comuniquen los datos, que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado y que requieran protección conforme a lo dispuesto en el artículo 1 de la LOPD.

Procedimientos de tutela derechos - 'Derecho al olvido'

A lo largo del año 2017 se han efectuado algunas modificaciones en los procesos internos de gestión, tendentes a aumentar la eficacia de los procedimientos.

Destaca la labor que realiza el Área de Admisiones de la Subdirección General de Inspección de Datos, que realiza el examen preliminar de todas las solicitudes de tutelas, de las subsanaciones que se exijan, en su caso, como requisito previo para la admisión a trámite, así como de las resoluciones de inadmisión y de sus correspondientes recursos de reposición.

De este modo, a partir de finales del año 2017,el Área de Procedimientos de Tutela de Derechos se centra específicamente en la tramitación y resolución de los procedimientos de este ámbito y en los recursos de reposición contra la resolución.

En este punto cabría destacar el caso de la solicitud de tutela cuyo reclamante pretendía el bloqueo de enlaces web accesibles en territorio que se encuentra fuera del territorio nacional y fuera del ámbito europeo, motivo por el cual fue desestimada.

Por su plena actualidad merece también destacarse la solicitud de tutela de un interesado, cuya reclamación de cancelación de datos ante Google no había sido atendida. Al efectuar una búsqueda por su nombre, en la lista de resultados aparecía la URL a una página web en la que se describía al reclamante como CEO de una empresa multinacional, indicando que debiera tenerse cautela con él por su praxis poco legal. El reclamante lo consideraba injurioso, sin embargo Google argumentó que la URL en cuestión estaba relacionada con asuntos de interés público en relación con su vida profesional. La información sobre profesiones o negocios en los que había participado recientemente podrían resultar también del interés de sus actuales o potenciales clientes, usuarios o socios. En consecuencia, la URL disputada remitía a informaciones y opiniones que presentaban relevancia e interés público incuestionables, en particular, se trataba de una entrada a una plataforma de denuncia de estafas. En definitiva, la referencia a este documento en los resultados de búsqueda relacionados con su nombre estaba justificada por el interés público en acceder a él. La solicitud de tutela fue desestimada.

A este respecto, es oportuno comentar el criterio novedoso aplicado por la Audiencia Nacional en su sentencia de 11 de mayo de 2017, que da prevalencia al derecho a la libertad de expresión sobre el derecho a la protección de datos respecto a las opiniones y juicios vertidos por el afectado en el ámbito profesional.

Otra solicitud relevante es la de un interesado que pidió la cancelación de unos vídeos, publicados en la plataforma YouTube, en los que aparecía su número de teléfono móvil. Varias personas llamaban a ese número a modo de broma, dado que el número les parecía muy singular, para ver quién contestaba a la llamada. La solicitud se desestimó por considerar que el número de teléfono, por sí solo, no constituye un dato de carácter personal, ya que no permite identificar a su titular sin tener que emplear esfuerzos desproporcionados.

Finalmente, se analizó la solicitud de cancelación efectuada por una persona, ejercida ante Google Inc. y ante la Agencia Estatal del Boletín Oficial del Estado. Se basaba en que, buscando mediante Google, se obtenían unos resultados (URLs del BOE) que hacían mención a una Resolución ministerial relativa a la pérdida de condición de funcionario del reclamante por la comisión de varios delitos. La lista de resultados obtenida en una búsqueda a partir de un nombre, página web o información relativa a una persona facilita la accesibilidad y difusión de la información a cualquier internauta que realice una búsqueda sobre el interesado, constituyendo una injerencia en el derecho fundamental al respeto de la vida privada del interesado. Sin embargo, en este caso, no procedía la desindexación de las URLs reclamadas al tratarse de datos muy recientes -año 2017-, considerando además que no se aportaba prueba documental que acreditase el cumplimiento de sentencia. Por tanto, no tratándose de datos obsoletos, se inadmitió su reclamación de tutela de derechos.

Sanidad, Educación, Administraciones Públicas y otras áreas relevantes

En el sector de sanidad se mantiene estable el número de denuncias recibidas. Las causas de estas denuncias son, principalmente, los accesos injustificados a las historias clínicas de los denunciantes y que, en muchos casos, son profesionales sanitarios que denuncian accesos indebidos de sus compañeros. También se han investigado incumplimientos de medidas de seguridad relacionadas con extravíos de documentos que forman parte de historias clínicas, así como la entrega de documentos integrantes de la historia clínica de una determinada persona a un tercero.

Cabría mencionar el caso de una Mutua que envió datos de salud de una empleada al empleador o el de una clínica denunciada por publicar en su web y en YouTube, con fines publicitarios de su actividad, un vídeo con la imagen de la denunciante mostrando la evolución que había tenido durante el tratamiento. Utilizaron la imagen de la denunciante para la publicación del vídeo sin su consentimiento e incumplieron el deber de secreto por revelar el tratamiento al que se sometió la denunciante.

En el ámbito de las relaciones laborales, se ha sancionado por la vulneración del deber de guardar secreto al haber enviado información de unos trabajadores a otros.

Se siguen recibiendo denuncias sobre abandono de documentación con datos personales en la vía pública

Se siguen recibiendo denuncias que han dado lugar a apercibimientos, procedimientos de declaración de Administraciones Públicas o procedimientos sancionadores, sobre abandono de documentación con datos personales en la vía pública.

En el sector de la enseñanza, algunas denuncias son consecuencia de la publicación de fotos de menores por parte de los centros docentes sin que haya consentimiento de los padres. Estas denuncias frecuentemente provienen de parejas separadas, cuando uno de los progenitores sí había prestado el consentimiento para el tratamiento, cuestión que debe resolverse en la jurisdicción civil.

Por otra parte, se ha sancionado la publicación sin restricciones de listas de admitidos y de clasificaciones de personas que concurren a procesos de concurrencia competitiva.

En este sentido, puede hacerse alusión al caso de una Consejería de Educación que dio a conocer datos de profesores al publicar en la web la concesión de una subvención de 400 euros por tener una titulación de inglés, figurando los dígitos completos de las cuentas bancarias, nombres, apellidos y DNI.

En otra denuncia presentada, el afectado, que había participado en un proceso selectivo de profesores interinos, denunció a la Consejería de Educación porque figuraba como excluido en la página web de la convocatoria, con sus datos. Adicionalmente, constaba como participante por el turno de acceso "discapacidad", así como un extracto del dictamen de su incapacidad absoluta por la Inspección provincial correspondiente. La convocatoria no preveía claves que detallasen genéricamente la causa de exclusión. El denunciante había aportado el documento de la incapacidad para acreditar tal condición y la exclusión de la relación de admitidos se basó en su grado de incapacidad. En estos casos, sería conveniente habilitar para los trámites, medios o sistemas que permitan a los aspirantes acceder los datos que sólo les afectan a ellos, como puede ser a través de clave y contraseña que se puede crear al presentar la solicitud telemáticamente.

En lo concerniente a los procedimientos de declaración de infracción de Administraciones Públicas, cabe mencionar que se mantienen en cuanto a su número. Son motivados por publicaciones de datos personales en páginas web de Administraciones locales, accesos indebidos a datos de terceros por parte de trabajadores públicos, incumplimiento de medidas de seguridad y por prestaciones de servicios que incumplen algunos requerimientos en materia de protección de datos.

En el ámbito de las comunidades de propietarios, se consolida el criterio de tramitación de apercibimiento para los supuestos, muy numerosos, de denuncia por la publicación en los accesos a las viviendas de datos de deudores a los que ya se ha notificado su deuda, publicación en tablones de anuncios cerrados de denuncias entre vecinos y contra la comunidad, así como de sentencias judiciales en las que se encuentran inmersas las partes.

De otra parte, hay que reseñar la remisión que, con fecha 27 de septiembre, realizó la AEPD a la Autoridad Catalana de Protección de Datos (APDCAT) de 20 denuncias recibidas hasta ese momento que hacían referencia a la base de datos de la página en la que se informaba de dónde votar el 1 de octubre. La web, que fue inhabilitada a instancias judiciales, solicitaba datos como el número de DNI y la fecha de nacimiento de los ciudadanos, realizando un contraste con una base de datos que arrojaba como resultado un punto de votación.

La APDCAT es el organismo con competencia para investigar y, en su caso, declarar infracciones respecto de ficheros creados o gestionados por los organismos públicos de Cataluña. La AEPD le trasladó las denuncias recibidas para que pudiese ejercer las funciones previstas en el artículo 5 de la Ley 32/2010, de la APDCAT.

La AEPD había remitido una semana antes a la Autoridad Catalana la primera denuncia recibida, en la que se daba cuenta de hechos que podían implicar la existencia de conductas contrarias a la LOPD. Junto a la denuncia, se remitió un informe analizando la ausencia de base legal para la utilización de determinados datos para crear un censo electoral

por parte de la Generalitat de Cataluña.

En paralelo a la remisión de estas denuncias, que abordan temas competencia de la APDCAT, la AEPD abrió una investigación por posible acceso ilícito a bases de datos estatales para la creación del denominado censo electoral catalán.

Transferencias Internacionales ANC-OMNIUM

En marzo de 2016 se recibieron denuncias de ciudadanos que señalaban que OMNIUM y ANC mantenían ficheros de carácter personal en un servidor de EEUU sin garantías adecuadas, ya que dejaron de estar amparadas por la Decisión 200/520/CE, invalidada por el TJUE en octubre de 2015.

En marzo de 2016 se iniciaron las actuaciones de investigación que evidenciaron que en junio de 2014 OMNIUM y ANC firmaron un contrato con BSD, en calidad de responsables del fichero, cuya ejecución material suponía que un fichero – AHORA ES LA HORA- del que son responsables las citadas entidades, estuviera alojado en los servidores de BSD sitos en EEUU. En el Registro General de Protección de Datos se inscribió el fichero AHORA ES LA HORA sin que conste marcado el campo relativo a transferencias internacionales de datos. En octubre de 2015 se pública en la página web de la Agencia Española de Protección de Datos un comunicado donde se informaba de que, en relación con las transferencias internacionales de datos realizadas al amparo de la Decisión de la Comisión 2000/520/CE, las Autoridades de Protección de datos investigarían aquellos casos de los que tuvieran conocimiento a partir de denuncias para ejercer sus poderes con el fin de proteger a las personas. En la fecha de las actuaciones inspectoras, los ficheros con datos personales seguían en los servidores de EEUU sin que se hubieran tomado las medidas necesarias para corregir la situación.

Por lo tanto, se acordó iniciar un procedimiento sancionador que se resolvió en febrero de 2017 con una sanción de 90.000 euros a cada una de las entidades.

Transferencias Internacionales. Asociación de Técnicos de Informática

Un socio de la Asociación de Técnicos en Informática (ATI) denunció en enero de 2016 que el servicio de correo electrónico de la misma se implementa sobre un producto denominado MailChimp prestado por la sociedad The Rocket Science Group (TRS), con sede en EEUU y que utiliza técnicas de seguimiento de los correos mediante el uso de web beacons que permite a ATI conocer los destinatarios que han abierto los correos y cuándo lo han hecho.

Durante la investigación se obtuvieron evidencias de que ATI realizó transferencias internacionales de datos a la empresa TRS, radicada en los EEUU, desde el 14 de junio de 2014. Estas transferencias dejaron de estar amparadas en el acuerdo de Puerto Seguro desde la invalidación de la Decisión 2000/520/CE adoptada por el TJUE en Sen-

tencia de fecha 6 de octubre de 2015 (Caso C-362/14). La ATI no comunicó en ningún momento la existencia de transferencias internacionales a la AEPD y no tomó las medidas para tener una base legal para la transferencia internacional.

Además, los destinatarios de los correos electrónicos remitidos por ATI a través del servicio MailChimp de TRS no obtenían información clara y completa previa a su instalación sobre el uso y finalidades de los dispositivos de seguimiento que se incluían en dichos envíos por el prestador de dicho servicio de correspondencia electrónica.

Por tanto, se acordó iniciar procedimiento sancionador que se resolvió en marzo de 2017 con sanción de 45.000 euros a ATI por transferencias internacionales de datos y de 5.000 euros por la utilización de dispositivos de almacenamiento y recuperación de datos infringiendo las obligaciones de información y de obtención del consentimiento establecidas en el artículo 22.2 de la LSSI.

Wannacry

En mayo de 2017 se recibió en la AEPD una notificación de la Secretaría General de Telefónica de España SAU y de Telefónica Móviles SAU comunicando una brecha de seguridad que afectaba a los ordenadores personales de la empresa. Posteriormente se constató que había afectado a numerosos sistemas personales de distintas empresas de toda España. El ataque se debía a la propagación de un código dañino denominado Wannacry que explotaba una vulnerabilidad de los sistemas Microsoft Windows. El código es del tipo *ramsonware*, lo que supone que el mismo cifra la información con una clave desconocida para el usuario de los datos, clave que está en poder de un tercero que pide una cantidad económica para desbloquear la información.

Ante la magnitud y la naturaleza novedosa del ataque, la directora de la Agencia Española de Protección de Datos decidió iniciar actuaciones de investigación para determinar si el mismo había afectado a los datos personales. En la misma se constató que no había afectado a datos personales de clientes de Telefónica, no constituía una fuga de información, ni se habían comprometido datos de clientes de Telefónica ni de terceros, por lo que resolvió archivar el expediente.

SIVASA

La Sociedad Integral De Valoraciones Automatizadas, S.A. (SIVASA), sociedad filial del Banco de Santander, notificó a la Agencia Española de Protección de Datos un ataque indebido y deliberado a sus Sistemas Informáticos el 28 de noviembre de 2016.

SIVASA es una sociedad del Grupo Santander dedicada a la realización de validaciones de tasaciones inmobiliarias. Se detectó una primera alerta de ataque el 7 de noviembre de 2016. El atacante utilizó direcciones IP pertenecientes a un *hosting* de Holanda y usando una red TOR (red a nivel mundial diseñada para habilitar el anonimato en línea y la evasión de censura).

Por otra parte, con la información descargada no se puede acceder a los sistemas del Banco de Santander para la realización de transacciones. La entidad comunicó a los clientes la incidencia, que también ha sido publicada en medios de comunicación, y se publicó un aviso en la web del Banco de Santander. La empresa ha implementado acciones correctoras y no hay constancia de utilización de los datos obtenidos por el ataque, por lo que se acordó el archivo de las actuaciones de investigación en octubre de 2017.

Lexnet

Ante la notificación de una violación de seguridad en el sistema LexNET, realizada por la Subdirección General de Nuevas Tecnologías de la Justicia, la Agencia Española de Protección de Datos decidió iniciar actuaciones de investigación, con el objeto de determinar el origen y alcance de la violación y realizar el seguimiento de las acciones tomadas por los responsables del sistema en el marco de la gestión del incidente. La vulnerabilidad detectada afectaba al buzón de correo y consistía en que mediante la modificación deliberada de la dirección URL del navegador, cambiando la identificación del usuario, se puede acceder a los buzones de otros usuarios.

Las investigaciones, que incluyeron la inspección presencial en los locales de la Subdirección General de Nuevas Tecnologías de la Justicia en colaboración con los servicios de inspección del Consejo General de Poder Judicial, concluyeron que, por un lado, y según resolución del CGPJ, que el sistema LexNET no constituye un fichero jurisdiccional y que la plena competencia corresponde a la AEPD y, por otro, que terceras personas, usuarias del sistema LexNET, habían accedido sin autorización a información bajo la responsabilidad de otros usuarios del mismo sistema debido al fallo de los sistemas de control de acceso. Por lo tanto, se acordó iniciar un procedimiento de infracción a las Administraciones Públicas, ya que los hechos podrían suponer la comisión por el Ministerio de Justicia de una infracción del artículo 9 de la LOPD, relativo a medidas de seguridad.

Agencia Española de Administración Tributaria

En mayo de 2017 se resolvió el procedimiento de infracción a la Administración Tributaria declarando una infracción por medidas de seguridad, artículo 9 de la LOPD, en relación a una quiebra de seguridad en la campaña del IRPF notificada por la propia AEAT en abril de 2016.

La violación consistió en mostrar el borrador de la declaración de renta de 2.793 declarantes a terceros. A raíz de dicha notificación, la AEPD realizó una inspección en la AEAT constatando que la gestión de la incidencia fue diligente en cuanto al bloqueo de los sistemas y la corrección de los errores. Las actuaciones de inspección evidenciaron que los hechos se produjeron por un error de programación que no fue detectado en las fases de pruebas y en la puesta en producción.

Por lo tanto, en mayo de 2017 se resolvió el procedimiento de infracción a las Administraciones Públicas declarando que se había producido una infracción de las medidas de seguridad establecidas en el artículo 9 de la LOPD por parte de la AEAT aunque, durante el trascurso de dicho procedimiento, se entendía que la entidad ya había adoptado las medidas necesarias para impedir que en el futuro pueda producirse de nuevo un hecho similar al examinado en el mismo expediente.

Cámara de Comercio de Madrid

La Cámara de Comercio de Madrid notificó a la Agencia Española de Protección de Datos un ataque deliberado a sus sistemas informáticos en diciembre de 2016 que se repitió en días sucesivos, a pesar de encontrarse deshabilitada la web. Los atacantes utilizaron direcciones IP de Suecia usando también una red TOR. En otro ataque utilizaron servidores OVH (proveedor de alojamiento web francés). Las técnicas utilizadas evidenciaron la debilidad de los sistemas de la entidad, por lo que se acordó iniciar un procedimiento sancionador por medidas de seguridad con multa de 6.000 euros, que se resolvió por el reconocimiento de la infracción y el pronto pago por la entidad sancionada.

Posible brecha de seguridad en los certificados del DNI

En relación a un posible fallo de seguridad conocido como ROCA 'Regreso del Ataque Coppersmith' que, según la página oficial del DNI del Ministerio del Interior afectaría a la confidencialidad de las claves generadas en los DNI electrónicos expedidos en España a partir de abril de 2015, la AEPD inició actuaciones de investigación de oficio que se encuentran en curso.

Vodafone

Los representantes de Vodafone notificaron en febrero de 2017 una quiebra de seguridad ocurrida en la denominada base de datos Cellebrite, que emplea la empresa y sus distribuidores para el diagnóstico de terminales averiados y que ha dado lugar a que terceros hayan tenido acceso a datos de correo electrónico y número de teléfono de 543 clientes. La Agencia inició actuaciones de investigación de oficio que están en curso.

2.1.4. Sentencias sobre resoluciones de la Agencia

Por otra parte, el análisis del grado de seguridad jurídica en la aplicación de la LOPD obliga a contemplar en qué medida las Resoluciones de la AEPD son ratificadas o revocadas por los Tribunales.

Durante el año 2017 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 166 sentencias, de las cuales:

- 121 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (73%).
- 17 estimaron parcialmente los recursos (10%).
- 20 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (12%).
- 8 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (5%).

A la vista de las cifras generales que se han mencionado, cabe concluir que la confirmación de los criterios de la Agencia en cuanto al fondo del asunto ha sido de un 78%, lo que supone una cifra idéntica a la del año 2016. Dentro de esta cifra, se mantienen los porcentajes de sentencias desestimatorias del recurso y de inadmisión del mismo. Se confirma así la relevancia del porcentaje de supuestos en que las sentencias confirman las resoluciones de la Agencia previa valoración jurídica de los criterios de fondo que la fundan. En todo caso el porcentaje de sentencias que confirma las resoluciones de la Agencia es, junto con el de 2016, el más elevado desde el año 2005.

El porcentaje de sentencias que confirma las resoluciones de la Agencia es el más elevado desde el año 2005

Por otra parte, se observa un repunte de la litigiosidad referida a la actuación de la Agencia, por cuanto el número total de sentencias se incrementa en un 124%, pese a lo cual el descenso acumulado de la litigiosidad en el período entre 2013-2017 de más de un 39%.

En relación con los sectores de actividad a los que afectan las sentencias dictadas, se ha producido, en consonancia con lo anteriormente señalado, un incremento en la práctica totalidad de los sectores. No obstante, sigue resultando relevante el peso adquirido respecto del total por los sectores de las telecomunicaciones, banca y seguros y agua y energía, que representan en conjunto un 55% del total.

De ellos, como en años anteriores, el sector que presenta una mayor litigiosidad sigue siendo el de las telecomunicaciones, con un 27% del total, aumentando en términos absolutos en un 96%. Asimismo, las sentencias relacionadas con el sector de banca y seguros se incrementan en un 167%, representando casi un 20% del total.

Es igualmente significativo el incremento de las sentencias referidas a recursos formulados por particulares, que aumentan en un 192%, pasando de representar un 18% en 2016 a suponer un 23% en 2017.

Asimismo, las sentencias referidas con prestadores de servicio de la sociedad de la información pasan de 1 en 2016 a 12 en 2017. Finalmente, las sentencias referidas al sector de la solvencia patrimonial, respecto del que no existía litigiosidad en 2016 pasa a representar en 2017 un 4% del total.

El único descenso significativo se produce en el sector de la publicidad y prospección, que se reduce en un 67%, existiendo una única sentencia referida al sector dictada en 2017.

Es preciso indicar que, en un buen número de sentencias estimatorias, la decisión final del recurso se ha fundado en la ampliación, mediante la prueba practicada en el ámbito del recurso, de la llevada a cabo por la Agencia. En este sentido, conviene precisar que la mayor parte de los criterios estimatorios de la Audiencia Nacional se han fundado en una distinta interpretación de la prueba obrante en autos y no en discrepancias con las resoluciones recurridas en lo que a la aplicación de las normas sustantivas de protección de datos se refiere.

Por su parte, en el año 2017 únicamente se han dictado por el Tribunal Supremo dos providencias de inadmisión de recursos de casación planteados contra sentencias de la Audiencia Nacional que habían confirmado a su vez sendas resoluciones de la Agencia, por lo que no procede hacer referencia a ninguna resolución judicial del Tribunal Supremo que siente doctrina en materia de protección de datos.

De las materias analizadas por la Audiencia Nacional destacan las siguientes cuestiones:

- En relación con el ámbito de aplicación de las normas de protección de datos, la SAN de 3 de febrero de 2017 considera que no se encuentra sujeto a la LOPD el envío de un correo electrónico con información supuestamente vejatoria del denunciante, sin perjuicio de la aplicabilidad al caso de la legislación de protección del derecho al honor. A su vez, la SAN del 15 de diciembre de 2017 considera que no puede determinarse la existencia de un fichero por la mera aportación de una carta en que se incorporan los datos de la denunciante. Tampoco es de aplicación, conforme al artículo 2.2 del RLOPD, la publicación de unas actas de la inspección de trabajo en que aparecen los datos de representantes de la empresa en su condición de tales (SAN de 14 de febrero de 2017).

- Por lo que respecta al ámbito de aplicación territorial de la LOPD, la SAN de 25 de octubre de 2017 considera que el mero hecho de que una empresa sea titular de una cuenta corriente y un apartado de correos en España no son indicios suficientes de la existencia de establecimiento a los efectos de la aplicación de la LOPD.

- Respecto del deber de información, la SAN de 27 de noviembre de 2017 lo considera infringido cuando en el formulario de alta de clientes se prevé la comunicación de los datos a “empresas del grupo empre-

sarial", sin especificar las finalidades de la cesión ni ofrecer un mecanismo para que el interesado pueda oponerse. Igualmente, la SAN de 22 de diciembre de 2017 afirma infringido el deber al indicarse en formulario web que se cederán datos a las empresas del grupo, sin especificar las finalidades ni existir un enlace a un sitio en que se incluya una relación de dichas empresas.

En relación con la legitimación para el tratamiento, la SAN de 16 de junio de 2017 se refiere a la prevalencia del interés legítimo en un supuesto de aportación a juicio de datos de un tercero que no tiene relación con la parte defendida, al prevalecer el derecho a la defensa.

En este ámbito, la Audiencia Nacional ha considerado que no existe legitimación en supuestos tales como la publicación en abierto de un documento relativo a la posible comisión de una infracción deontológica por un colegiado como anexo a la convocatoria de la asamblea general de un Colegio Profesional (SAN de 11 de julio de 2017), la transmisión por una entidad financiera a un tercero de un crédito que ya había sido liquidado y no se incorporó al sistema por un error (SAN de 7 de julio de 2017), la transmisión de datos de un crédito satisfecho a una empresa de recobros, que los utilizó para efectuar llamadas amenazantes al supuesto deudor (SAN de 10 de octubre de 2017) o la publicación en abierto por un instituto autonómico de vivienda de datos de arrendatarios junto con el pliego de condiciones para concurrir a licitación para enajenación de bienes litigiosos por instituto de vivienda autonómico, al considerar la Sala que dichos datos deberían haberse incluido en una zona de acceso no público limitada a los licitadores (SAN de 1 de diciembre de 2017).

Como en ejercicios anteriores, existen numerosas sentencias relacionadas con el tratamiento ilícito de datos en supuestos de contratación irregular, habiendo declarado la Sala que existe ilicitud en casos de emisión de facturas aun cuando existe sentencia de un órgano jurisdiccional civil en que se declara resuelto el contrato (SAN 14 de diciembre de 2017), cambio de titularidad eléctrica sin que conste documento alguno firmado ni grabación acreditativa de la solicitud (SAN 13 de octubre de 2017), inexistencia de verificación posterior (SSAN de 10 de febrero y 7 de abril de 2017), pagos del servicio únicamente efectuados en metálico (SAN de 7 de abril de 2017), celebración de contrato a nombre de quien había manifestado expresamente su voluntad de no celebrarlo (SAN 27 de enero de 2017) o de aceptación de cambio de suministro eléctrico solicitada por la hija del abonado, presumiendo la existencia de una representación (SAN 11 de julio de 2017). Asimismo, se afirma que el responsable no puede ampararse en estos casos en la confianza de que el encargado disponga de una grabación de verificación, dada su potestad de control sobre aquél (SAN de 7 de febrero de 2017).

En cuanto al encargado del tratamiento, la SAN de 31 de diciembre de 2017 recuerda que responsable y encargado responden como consecuencia de los incumplimientos de la Ley producidos por el segundo de ellos, siendo imputable al responsable, según la SAN de 12 de abril, el hecho de que el encargado no ha consultado las listas Robinson antes de llevar a cabo llamadas publicitarias. Sin embargo, la SAN de 21 de noviembre de 2011 imputa únicamente al encargado la infracción derivada del envío por error de información con cambios de destinatarios que afectó a 91 afectados.

Entrando ya en la doctrina relacionada con el ejercicio de los derechos, las SSAN de 5 de mayo y 14 de julio de 2017 aplican lo previsto en el art. 25.8 RLOPD, considerando improcedente la aplicación del procedimiento de ejercicio de los derechos previstos en la LOPD para solicitar la rectificación o cancelación del saldo de puntos del permiso de circulación o del grupo de cotización del afectado en la Seguridad Social.

Respecto de las historias clínicas, la SAN de 17 de mayo de 2017 considera que el derecho de acceso no incluye el derecho a obtener fotocopias compulsadas o cotejadas de la misma, considerando la SAN de 21 de noviembre de 2017 que no procede el acceso a los datos de las personas que han accedido a la historia, al no tratarse de un derecho de acceso. Por su parte la Audiencia Nacional considera improcedente la rectificación y cancelación en la historia sobre la base de entender infundado un informe médico (SAN de 26 de septiembre de 2017) o alegar que se ha cumplido el plazo de conservación de cinco años, aun cuando se considera por el centro que la información es necesaria para la adecuada asistencia sanitaria (SAN de 7 de abril de 2017).

En relación con el ejercicio de derechos respecto de datos de personas fallecidas, la SAN de 3 de mayo de 2017 indica que, en caso de no atenderse una solicitud de cancelación por los familiares del fallecido, no es posible la apertura de un procedimiento sancionador, pero sí la atención de la tutela del derecho respecto de dicha cancelación.

Son varias las sentencias relacionadas con el derecho de los afectados a la supresión de enlaces en motores de búsqueda a partir de las llevadas a cabo por su nombre. La Audiencia Nacional ha considerado que procede acceder a lo solicitado en el caso de una publicación en prensa de los supuestos hechos de una sentencia que no se corresponden con los que aparecen recogidos en la misma (SAN de 18 de julio de 2017), la publicación referida a una sentencia penal relacionada con una actuación médica y que tenía una antigüedad superior a 20 años (SAN de 13 de julio de 2017), la mención del afectado en relación con una sentencia de más de diez años en cuyos hechos sólo aparece de forma “tangencial” (SAN de 31 de octubre de 2017), la publicación de una información en la que se cita al afectado, persona carente de toda relevancia pública, como interviniente en una manifestación, siendo lo relevante el propio hecho y no la participación del afectado (SAN de 25 de julio de 2017) o la publicación en un blog de comentarios vejatorios y basados, como se reconoce, en opiniones subjetivas, llevados a cabo por un competidor, incorporando además la foto de la afectada (SAN 16 de noviembre de 2017).

Por el contrario, no procede atender el derecho en el caso de un solicitante que ni es ciudadano de la UE ni acredita vinculación clara con ningún estado miembro de la UE, encontrándose las webs indexadas en URLs fuera de la UE (SAN de 31 de octubre de 2017). Tampoco procede respecto de datos referidos a la trayectoria profesional reciente del afectado, que es figura vinculada con el periodismo digital, aun cuando contienen comentarios peyorativos, tales como denominarle “mentiroso” (SAN de 6 de junio de 2017) ,ni en relación con comentarios sobre la pericia profesional de un médico de cierto renombre efectuados por un paciente (SAN de 11 de mayo de 2017), ni respecto de la publicación en un medio de comunicación de los datos del interesado como candidato en unas elecciones munici-

pales (SAN de 19 de junio de 2017) ni respecto de la publicación de una sentencia por robo y asesinato cometidos por un guardia civil cuando incluso sigue cumpliendo la condena (SAN de 4 de diciembre de 2017). Finalmente, no se considera obsoleta una información publicada en multitud de medios de comunicación entre dos y tres años antes de la fecha de la reclamación (SAN de 21 de noviembre de 2017), aunque sí se considera como tal una información de más de veinte años (SAN de 8 de noviembre de 2017).

En materia de seguridad, se considera que el responsable no es imputable en los supuestos en los que se produce un ataque informático que exige el quebrantamiento de las barreras de seguridad establecidas por el responsable, no tratándose de una vulneración del deber de seguridad, dada la existencia de estas medidas (SAN de 10 de noviembre de 2017).

En el ámbito de los ficheros de solvencia, se ha considerado que no cumple los requisitos necesarios la inclusión por todo su importe de deudas parcialmente reducidas por laudo arbitral (SAN de 27 de junio de 2017) o anuladas por sentencia civil (SAN 14 de diciembre de 2017), la inclusión por confusión del DNI del denunciante con el de su hijo (SAN de 10 de mayo de 2017), el mantenimiento en el fichero de una deuda contraída con tarjeta de crédito por un pago que luego fue objeto de retrocesión (SAN de 21 de julio de 2017), la inclusión de deuda con anterioridad al vencimiento del plazo fijado para el pago en el requerimiento (SAN de 18 de julio de 2017).

Son, como en años anteriores, reiteradas las sentencias relacionadas con el incumplimiento del requisito de requerimiento de pago, reproduciendo la doctrina contenida en anteriores memorias. No obstante resulta relevante indicar que la SAN de 19 de diciembre de 2017 que el cómputo del plazo de prescripción de esta infracción se inicia cuando el interesado tiene conocimiento de la inclusión de los datos en el fichero. Por otra parte, la SAN de 28 de marzo de 2017 considera que la exigibilidad de este requisito es conforme a derecho, según los artículos 1100 del CC y 63 del CCOM, dado que para constituirse en mora es preciso interpelar al deudor para el pago y, en tanto no se haga el requerimiento, la mora no existe técnicamente. Por su parte, la SAN de 28 de diciembre de 2017 considera que no puede imputarse la falta de requerimiento a quien adquirió una deuda que ya estaba incluida en el fichero de solvencia, habiéndose producido el requerimiento por la cedente y notificado la inclusión. Finalmente, la SAN de 28 de marzo de 2017 indica que es insuficiente el requerimiento efectuado por SMS o a través del correo electrónico.

Son reiteradas las sentencias relacionadas con el incumplimiento del requisito de requerimiento de pago

En el ámbito de la videovigilancia, la SAN de 13 de octubre de 2017 confirma la infracción cometida en el caso en que la captación de las imágenes abarca toda la acera de la entidad responsable y la calzada adyacente.

En el ámbito del marketing, la Audiencia Nacional ha considerado vulnerada la LOPD en caso de realización de llamadas a clientes de una compañía ofreciendo productos de terceros cuando la cláusula contractual únicamente se refería a la oferta de los propios (SAN de 9 de marzo de 2017), así como la realización de llamadas telefónicas a quien figuraba en una Lista Robinson que no comenzó a consultarse hasta una fecha posterior (SAN de 28 de marzo de 2017) o a quienes habían manifestado expresamente su oposición a seguir recibiendo llamadas (SSAN de 12 de abril y 16 de mayo de 2017).

En relación con la infracción del artículo 21 de la LSSI, la SAN de 28 de febrero de 2017 recuerda que debe tenerse en cuenta la oposición del interesado aun cuando no haga uso de los medios puestos a su disposición en la comunicación que se le remite, recordando la SAN de 9 de febrero de 2017 que en caso de oposición ésta también afecta al envío de comunicaciones sobre productos o servicios similares a los adquiridos. Por otra parte, la SAN de 13 de junio de 2017 considera que no es suficiente para acreditar el consentimiento la existencia de un acuerdo entre quien envía la comunicación y una asociación a la que pertenecen los destinatarios, al tener que constar su consentimiento expreso. Finalmente, la SAN de 14 de diciembre de 2017 señala que no existe vulneración de la LSSI cuando la comunicación se dirige a una cuenta asociada a varias personas y sólo una de ellas se ha negado a recibir publicidad (SAN 14/12/17).

En lo que afecta a la aplicación de las causas de atenuación previstas en el artículo 45.5 de la LOPD, se ha apreciado por la SAN de 14 de junio de 2017 la atenuación por regularización de la conducta tan pronto se tuvo conocimiento de la existencia de una reclamación ante la SETSI. Asimismo, la SAN de 28 de marzo de 2017 considera que un 3% de cuota de mercado de una entidad bancaria no puede considerarse relevante a efectos de agravación. Por otra parte, la Sala ha considerado que no cabe alegar falta de beneficios cuando se han girado facturas al afectado ni cabe alegar falta de perjuicios cuando se han tenido que presentar reclamaciones a la SETSI y la AEPD y una demanda civil (SAN de 31 de marzo de 2017). Tampoco cabe alegar regularización cuando habiéndose producido el pago de una deuda se vuelve a incluir en un fichero de solvencia (SAN de 27 de marzo de 2017), o cuando la regularización se produce ocho meses después de la reclamación (SAN de 7 de febrero de 2017) ni cabe atenuar la responsabilidad por el hecho de que el denunciante plantee una suerte de "acuerdo amistoso" para evitar la denuncia (SAN de 9 de febrero de 2017). Finalmente, la SAN de 26 de mayo de 2017 indica que en los supuestos de contratación de servicios no solicitados no puede apreciarse ausencia de beneficios ni falta de daños al denunciante, dado que se celebra un contrato, se factura y se obliga al denunciante a acudir a la AEPD (SAN 26/5/17 Telefónica de España).

2.1.5. Sentencias TJUE

En relación con la jurisprudencia del TJUE recaída en materia de protección de datos durante el año 2017, resulta relevante reseñar cuatro sentencias.

La primera de ellas es de 15 de marzo de 2017, asunto C536/15, Tele2 (Netherlands) BV. En esta sentencia el Tribunal se plantea si una empresa de telecomunicaciones está obligada a poner los datos relativos a sus abonados a disposición de un proveedor de servicios de información sobre números de abonados y el suministro de guías establecido en otro Estado miembro. El Tribunal de Justicia declara que si un abonado fue informado por la empresa que le ha asignado un número de teléfono de la posibilidad de que se transmitan sus datos de carácter personal a otra empresa, para publicarlos en una guía pública, y consintió dicha publicación, no debe ser objeto de un nuevo consentimiento, porque ello no atenta a la esencia del derecho a la protección de datos de carácter personal. Igualmente, tampoco sería preciso que en su caso se formule dicha solicitud de consentimiento de manera diferenciada en función del Estado miembro al que dichos datos pueden ser transmitidos.

También citamos, por su interés para la materia, la sentencia de 4 de mayo de 2017, asunto C-13/16, "Rīgas satiksme". El Tribunal aborda la cuestión de si la existencia de un interés legítimo en un tercero, como base jurídica del tratamiento de datos personales previsto en la Directiva

95/46, obligaría a comunicar datos personales a dicho tercero. El Tribunal considera que dicha base jurídica no establece una obligación de comunicar los datos a dicho tercero, sino que confiere la facultad de llevar a cabo ese tratamiento, de acuerdo con lo que estableciese la legislación nacional, pero en cualquier caso no se opondría a dicha comunicación en el supuesto de que el Derecho nacional lo permitiese.

Tiene una gran importancia, por lo relevante de la opinión del Tribunal, el Dictamen 1/15, de 26 de julio de 2017, sobre el Acuerdo sobre la transferencia de datos del registro de nombres de los pasajeros, previsto entre la Unión Europea y Canadá (Acuerdo sobre el PNR). El TJUE estudia, a petición del Parlamento europeo, la compatibilidad del Acuerdo sobre el PNR (proyecto de Acuerdo internacional en virtud del cual se permite la transferencia sistemática y continuada a Canadá de los datos de la totalidad de los pasajeros aéreos) con la Carta de Derechos Fundamentales de la Unión Europea, y concluye que el Acuerdo sobre el PNR no puede celebrarse en su forma actual por incompatibilidad de varias de sus disposiciones con los derechos fundamentales reconocidos por la Unión.

El Tribunal reconoce que el contenido del Acuerdo implica una injerencia en el derecho fundamental al respeto de la vida privada y a la protección de los datos de carácter personal; no obstante considera que determinadas injerencias están justificadas en aras de un objetivo de interés general (garantizar la seguridad pública en el marco de la lucha contra los delitos de terrorismo y otros delitos graves de carácter transnacional), pero que en otros casos no se da dicha justificación, como por ejemplo en el supuesto de transferencia de datos sensibles, que exigirían una justificación concreta basada en motivos distintos de la protección de la seguridad pública contra el terrorismo. Además, durante la estancia de los pasajeros aéreos en Canadá, la utilización de los datos del PNR conservados debe estar supeditada al control previo de un órgano judicial o de una entidad administrativa independiente. Igualmente no se justifica la conservación, tras la partida de los pasajeros aéreos de Canadá, de los datos de aquellos respecto de los cuales no se haya identificado ningún riesgo en materia de terrorismo o de delincuencia grave de carácter transnacional.

En definitiva, en su Dictamen, el Tribunal de Justicia considera que el Acuerdo debería:

- Determinar con mayor claridad y precisión algunos de los datos del PNR que han de transferirse;
- Disponer que los modelos y criterios utilizados en el marco del tratamiento automatizado de los datos del PNR sean específicos y fiables y no discriminatorios;
- Disponer que las bases de datos utilizadas se limiten a las empleadas por Canadá en relación con la lucha contra el terrorismo y con los delitos graves de carácter transnacional;
- Disponer que los datos del PNR únicamente puedan ser comunicados por las autoridades canadienses a las autoridades públicas de un país no miembro de la UE si existe un acuerdo entre la Unión y dicho país equivalente al Acuerdo previsto o bien una decisión de la Comisión Europea en ese ámbito;
- Establecer un derecho a la información individual de los pasajeros aéreos en caso de que se utilicen datos del PNR referentes a ellos durante su estancia en Canadá y tras su salida de dicho país, así como en caso de divulgación de esos datos por la autoridad canadiense competente a otras autoridades o a particulares, y
- Garantizar que una autoridad de control independiente se encargue de la supervisión de las normas sobre protección de los pasajeros aéreos frente al tratamiento de sus datos del PNR.

Por último, mencionar la sentencia de 20 de diciembre de 2017, asunto C 434/16, Nowak, en la cual se plantea ante el Tribunal una solicitud de derecho de acceso en materia de datos personales a las respuestas escritas proporcionadas durante un examen profesional y a las posibles anotaciones del examinador. El Tribunal considera que ambos conceptos constituyen datos de carácter personal del aspirante, respecto a los cuales puede ejercitar, en principio, un derecho de acceso, ya que el contenido de esas respuestas refleja el nivel de conocimientos y competencia del aspirante en un área determinada y, en ocasiones, sus procesos de reflexión, su discernimiento y su capacidad de análisis, y las anotaciones del examinador sobre las respuestas del aspirante son igualmente datos que afectan a aquel, pues el contenido de esas anotaciones expresa la opinión o valoración del examinador acerca del rendimiento individual del aspirante en el examen.

El Tribunal de Justicia pone de relieve, no obstante que dicha conceptuación como datos de carácter personal no permite alterar las respuestas o las observaciones por el hecho de ejercitar los derechos de acceso y rectificación, ya que este derecho no puede servir para permitir a un candidato "rectificar" posteriormente las respuestas "incorrectas". Ahora bien, aclara el Tribunal, el derecho de acceso y rectificación no incluye las preguntas del examen, las cuales no serían datos personales.

2.2. PROTECCIÓN A LOS MENORES

2.2.1. Atención al Canal Joven. Canal de consultas

Como se viene señalando en anteriores memorias, la Agencia Española de Protección de Datos considera la prevención en la utilización que puedan hacer los menores de sus datos personales en internet y en general en las redes sociales, así como la concienciación tanto de las familias como de los profesores y de los propios menores, una de sus máximas prioridades a la hora de proteger a un colectivo especialmente vulnerable que puede verse involucrado en situaciones de alto riesgo en internet y que, tanto la protección de los derechos de las personas en internet como la de los propios menores, se recogen como actuaciones prioritarias en el Plan Estratégico de la Agencia.

La encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares, realizada por el Instituto Nacional de Estadística y publicada el 5 de octubre de 2017, indica un uso de internet prácticamente universal a la edad de 15 años, llegando al 99,2%. No cabe duda que internet abre un gran abanico de posibilidades para crecer y formarse en un mundo totalmente globalizado, pero desafortunadamente, no

está exento de riesgos que, en el caso de los menores, pueden tener graves consecuencias para su desarrollo, muchas veces por desconocimiento de los datos de carácter personal que se facilitan al utilizar la mayoría de los servicios que ofrece: redes sociales, servicios de almacenamiento, mensajería instantánea, correo electrónico, etc.

Fruto del interés por proporcionar la máxima información posible a todos los actores participantes en el derecho a la protección de los datos personales de los menores, la Agencia creó el Canal Joven con varias vías de comunicación específicas dirigidas a resolver las cuestiones o dudas que, en su ámbito de actuación, se puedan plantear referentes a este colectivo.

El Canal Joven integra, además de la dirección de correo electrónico canaljoven@agpd.es, un teléfono específico para consultas sobre temas de menores (901 233 144) y un servicio de información de WhatsApp (616 172 204). A las consultas que llegan por estos medios, se añaden las recibidas a través de la Sede Electrónica de la Agencia y que son atendidas por el mismo equipo.

A través de estas vías, el Canal Joven ha dado respuesta, durante 2017, a 895 consultas realizadas tanto por menores como por instituciones educativas, empresas privadas relacionadas con el ocio infantil, entidades locales, profesores y familias, facilitando información en relación con la privacidad y el tratamiento de datos personales de y por menores de edad. El número de consultas supone un incremento de más de un 32% frente a las contestadas durante 2016.

2.2.2. Acciones de difusión, concienciación y fomento del derecho a la protección de datos

Siguiendo con el objetivo de fomentar la información y promover la concienciación de los menores de edad sobre el buen uso de los datos personales en internet, el 19 de octubre de 2017 tuvo lugar la presentación de nuevos recursos y materiales de la Agencia para formar, concienciar y fomentar la privacidad y el derecho a la protección de datos de los menores, que tienen en los centros docentes, el profesorado y las familias el vehículo más adecuado para conseguirlo, pues el objetivo de la Agencia es que estos materiales se conozcan y puedan llegar al entorno más cercano a los más de 8 millones de alumnos escolarizados en España en enseñanzas de régimen general no universitarias, de forma que sirvan de herramientas para fomentar y reforzar la privacidad y la protección de los datos personales de los menores.

Estas acciones se han llevado a cabo en el marco del convenio de colaboración suscrito por ambas entidades para impulsar, entre otros aspectos, la sensibilización y la formación de los menores en materia de privacidad y protección de datos, en especial en internet. La difusión se realizó de forma masiva a los agentes de la comunidad educativa, involucrados en velar por los derechos de los menores, en concreto a las Administraciones educativas, estatal y autonómicas, a cerca de 8.000 centros educativos de todo el territorio nacional, inspectores de educación, a las confederaciones de asociaciones de madres y padres de alumnos (CEAPA, CONCAPA), asociaciones y sindicatos más representativos de profesores y de inspectores de educación, además de otras instituciones y organismos que también velan por el superior interés del menor.

Los nuevos materiales presentados consisten en:

- La Guía sobre protección de datos dirigida a los centros educativos, que surge de la necesidad de dar respuesta a las cuestiones planteadas por los integrantes de la comunidad educativa, tanto centros docentes como profesores y AMPAs, así como a las dudas más habituales que se habían for-

mulado en el Canal Joven de la Agencia. El resultado presentado es una guía práctica que, además de los conceptos y principios básicos sobre protección de datos, incluye la respuesta directa a más de 80 preguntas, muchas de ellas relacionadas con la expansión de las nuevas tecnologías en el entorno escolar al que va dirigida.

La Guía incluye además un Decálogo simplificado con los aspectos más relevantes para realizar un uso adecuado de los datos personales en los centros educativos, así como una sección específica sobre los cambios que producirá la aplicación del nuevo Reglamento General de Protección de Datos el 25 de mayo de 2018 y a los que el sector educativo habrá de prestar atención.

La serie de vídeos Tú controlas en internet, compuesta por cuatro vídeos, todos ellos dirigidos a los menores que pueden ser visionados tanto en el aula como en familia y en los que se abordan situaciones como el ciberacoso (En este partido nos la jugamos), el grooming (Planazo de fin de semana), el sexting (Un vídeo muy especial) o la dependencia tecnológica y la huella digital (Un crack del BMX). La finalidad de estos vídeos es que sean utilizados como herramienta para fomentar la educación digital de los menores, contribuyendo a evitar que puedan verse involucrados en situaciones de riesgo que, en ocasiones, producen un daño difícil de reparar debido al efecto multiplicador de internet, como redes sociales o servicios mensajería instantánea. La Agencia se ha decantado por utilizar el dibujo como un medio útil para captar la atención y facilitar la comprensión de estos conceptos en grupos de diferentes edades.

El taller para familias Los menores y su cibermundo, conducido por el experto Ángel-Pablo Avilés, autor de El blog de Angelucho. Este taller incluye orientaciones y pautas dirigidas a los padres para que puedan acompañar a sus hijos en su relación con las nuevas tecnologías. Está compuesto por nueve vídeos de corta duración, de entre dos y diez minutos, en los que se abordan temas como el funcionamiento de las aplicaciones más utilizadas por los jóvenes y los riesgos más comunes asociados a las mismas.

Estos recursos se han incorporado a la web de la Agencia Tú decides en internet que se configura como un proyecto global con varias líneas de actuación sobre protección de datos de menores, y que apuesta por la prevención y la concienciación como herramientas imprescindibles para el reforzar las garantías del derecho a la protección de datos, mediante su formación, facilitando consejos, materiales y recursos con las claves necesarias para el uso seguro y responsable de los datos personales en la Red.

Así mismo, la Agencia viene impulsando la inclusión de la privacidad y el derecho a la protección de datos en el mundo online entre los contenidos del desarrollo curricular

de las materias o asignaturas relacionadas con las TIC, ya se trabajen de manera transversal o constituyan la materia de asignaturas concretas (troncales, específicas o de configuración autonómica) de la enseñanza no universitaria.

La incorporación de los menores al mundo digital, cada vez a edades más tempranas, y la intensidad de su actividad en distintos servicios y aplicaciones de internet requieren que se les forme en un uso razonable y responsable, entre otros aspectos en lo que respecta a la utilización que hacen de la información personal tanto propia como de terceros. Se hace necesario y urgente el desarrollo de estas materias en el currículum escolar de manera que se proporcione a los menores, en el ámbito de la escuela y desde un primer momento, formación y recursos para que puedan obtener el mayor provecho de las posibilidades que internet ofrece, disminuyendo a su vez la exposición a los riesgos que puede comportar un uso inadecuado o irresponsable de la información personal a través de Internet.

Con este objetivo, se ha continuado con la distribución entre las autoridades educativas de un Marco de competencias digitales como orientación para el desarrollo curricular de esta materia, que resulta también de utilidad para la adquisición de competencias por el profesorado.

Otra de las actuaciones abordadas durante 2017 ha sido la actualización de la web para dotarla de nuevos contenidos y hacerla más accesible a familias, profesores y alumnos. Entre los nuevos contenidos, aparte de los materiales a los que se han hecho referencia, cabe destacar la inclusión de las FAQs para facilitar, de manera ágil y rápida, a las familias y centros educativos las respuestas sobre las cuestiones más comunes que se presentan en relación con el tratamiento de datos de menores. Se ha actualizado la sección de "Informes jurídicos de referencia" para dar a conocer los criterios que sobre diferentes aspectos del tratamiento de datos de menores se han venido adoptando por la Agencia a través de su Gabinete Jurídico. También se han seleccionado e incorporado aquellas resoluciones de la Agencia, tanto de expedientes sancionadores como de procedimientos de tutela de derechos más destacadas en este ámbito, a fin de que los interesados conozcan los criterios de la Agencia en la tramitación y resolución de las denuncias y tutelas que se le han formulado y les puedan servir de orientación ante supuestos de vulneración de los derechos de los menores.

Se hace necesario incluir el uso responsable de internet en el currículum escolar

Igualmente, se ha llevado a cabo una actualización de todos los enlaces con las instituciones que trabajan con el colectivo de menores y que tienen una estrecha relación de colaboración con la Agencia. Asimismo, en el apartado destinado a proporcionar referencias para ayuda ante situaciones de riesgo, "Si tienes problemas", además de la información sobre cómo contactar con la Agencia para temas relacionados con la protección de datos de menores, se incluyen una serie de teléfonos y enlaces de instituciones y organismos públicos que pueden prestar ayuda en caso de acoso a los menores o sus familias.

En el año 2017 se han registrado 101.500 visitas a los distintos contenidos de la página web Tú decides en internet, realizadas por 66.810 visitantes distintos. Cabe destacar el incremento de visitas recibidas que se produjo en el mes posterior a la presentación de los nuevos materiales a los que se ha hecho referencia.

2.2.3. Participación en eventos y acciones de difusión

Difusión en la comunidad educativa

La comunidad educativa, entendida en sentido amplio que incluye a todos los actores implicados en la educación de los menores, constituye uno de los objetivos de la Agencia Española de Protección de Datos dentro del enfoque de prevención, mediante distintas iniciativas destinadas al impulso de la formación y concienciación del derecho a la protección de datos de los menores y a la difusión de materiales y recursos para su sensibilización.

En este entorno, la Agencia ha desplegado una serie de actuaciones dirigidas a los distintos actores de la comunidad educativa, como los equipos directivos de los centros educativos, los docentes o los inspectores de educación, que tienen en sus manos el desarrollo de la función educativa, así como la tarea de organizar diariamente la gestión de las aulas, entendiendo éstas como un lugar de encuentro en el que, cada vez más, se utilizan nuevas tecnologías con el consiguiente uso de datos personales de los alumnos. También se han mantenido reuniones con representantes del otro gran colectivo implicado en la tarea de conocer y velar por la educación y el desarrollo de los menores, y por tanto de su privacidad, que es el de las familias, a través de las Asociaciones de Madres y Padres de Alumnos (AMPA).

Estas iniciativas tienen como objetivo fundamental difundir de manera clara y sensibilizar sobre la aplicación de la normativa de protección de datos en el sector educativo, impulsar el conocimiento de los derechos que establece, en particular en los menores, y aclarar las dudas que en la vida diaria de las aulas se pueden llegar a plantear.

Además, la Agencia ha desplegado una serie de actuaciones con distintas administraciones (autonómicas y locales) e instituciones (INCIBE), que tienen como fundamento o parte de su actividad la relación con menores, lo que implica el tratamiento de sus datos, así como la defensa y protección de sus derechos.

La Agencia ha tenido una participación activa en jornadas organizadas por distintos agentes de la comunidad educativa:

- El 24 de enero en la Jornada sobre Inspección Educativa, organizada por la Unión de Cooperativas de Enseñanza de Trabajo Asociado de Madrid (UCETAM).
- El 8 de marzo en la Pasantía del Ministerio de Educación de Panamá por parte del Ministerio de Educación, Cultura y Deporte español para conocer temas de acoso y convivencia escolar.
- El 21 de marzo en la Jornada de formación de los coordinadores informáticos de los centros educativos de Teruel.
- El 30 de marzo en la Jornada de Formación del Servicio Inspección de Huesca (Servicio Provincial de Educación).
- El 26 de abril en el Taller sobre protección de datos en centros escolares organizado por el Colegio de Enseñanza Infantil y Primaria (CEIP) Esperanza, de Madrid.
- El 26 de mayo, en el I Congreso Estatal de Convivencia Escolar organizado por el Ministerio de Educación, Cultura y Deporte (Sigüenza).
- El 13 de junio en el proyecto 'Compartiendo Experiencias' de la Dirección del Área Territorial de Educación Madrid Sur, de la Comunidad de Madrid.

También en el ámbito autonómico y de la Administración Local:

- El 31 de marzo en la Jornada 'Sistema de Protección a la Infancia y la Adolescencia: Novedades Jurídicas', organizada por el Ayuntamiento de San Sebastián de los Reyes.
- El 12 de junio en la Jornada Protección a la Infancia de la Comunidad de Madrid.

- El 17 de noviembre en la Jornada técnica de presentación del protocolo de detección y notificación de situaciones de maltrato y/o desprotección infantil, organizada por el Ayuntamiento de Alcobendas.

Con otros actores:

- El 7 de febrero, en el Día de Internet Segura.
- El 3 de diciembre, participación en el Cybercamp organizado por Instituto de Ciberseguridad de España (INCIBE).

Se han mantenido reuniones con representantes de la Confederación de Asociaciones de Padres y Madres de Alumnos (CEAPA).

Entre las actividades desarrolladas en este ámbito, también hay que mencionar la participación en los trabajos del Grupo de Trabajo sobre Educación Digital, creado en el seno de la Conferencia Internacional de Autoridades de Protección de Datos, y que durante 2017 enfocó su actuación en la ejecución de la 'Resolución de Marrakech para la adopción de un marco internacional de competencias sobre la educación en privacidad', adoptada en octubre de 2016, en la que se aprobó un marco de competencias en protección de datos y privacidad para escolares y se acordó su promoción y seguimiento.

2.2.4. Premios

Entrega de Premios a las buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet

Coincidiendo con la presentación de los nuevos materiales destinados a los menores y al sector educativo, en la sede del Ministerio de Educación, Cultura y Deporte, la Agencia hizo entrega de los premios de la primera edición del concurso de 'Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet'.

En la modalidad de buenas prácticas en centros escolares que favorezcan que los alumnos de educación primaria, secundaria, bachillerato y formación profesional posean un mayor conocimiento acerca del derecho a la protección de datos, se premió al Colegio Sagrado Corazón Hijas de Jesús de Salamanca por su "labor continuada de concienciación sobre los riesgos asociados a internet y el uso de las nuevas tecnologías", reconociendo especialmente su 'Plan de Ciberseguridad en el Centro Escolar'.

La Agencia reconoció este proyecto que desde 2014 viene concienciando a alumnos, padres y profesores sobre las implicaciones de las nuevas tecnologías, fomentando el uso adecuado y alertando de las situaciones de riesgo que pueden producirse.

Por otra parte, en la modalidad que premia el compromiso de personas, instituciones, organizaciones y asociaciones, se reconoció la trayectoria de Emilio Aced Félez, que fue responsable de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia, por su compromiso con la difusión de la protección de datos en el ámbito de los menores.

Estos premios, creados con la finalidad de incentivar la cultura de un buen uso de las aplicaciones y servicios que ofrece internet relacionado con la información personal que a través de la Red se utiliza y difunde, tanto propia como de terceros, se convocaron el 26 de julio de 2017 en su segunda edición.

Premio Ellos te enseñan

La Agencia Española de Protección de Datos colaboró, junto con la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN), el Instituto Nacional de Ciberseguridad (INCIBE) y la Confederación Española de Asociaciones de Padres y Madres de Alumnos (CEAPA) en el concurso organizado por la Organización de Consumidores y Usuarios (OCU) y Google 'Ellos te enseñan'. Iniciativa enmarcada dentro de la campaña 'Vive un Internet seguro', creada con el objetivo de que alumnos y padres aprendan a navegar seguros en internet. Para facilitar la participación en el concurso, la Agencia facilitó diferente material disponible en la web 'Tú decides en internet', como las guías 'No te enredes en internet' y 'Sé legal en internet', o las fichas didácticas.

Los premios recayeron, el primero, en el trabajo realizado por Alberto Segurado Díaz y Sergio Valverde, del IES Martínez Uribarri, de Salamanca. El segundo premio se concedió a Nerea Tristán, del Colegio Castilla de Torrejón de la Calzada, Madrid, mientras que el tercer premio se otorgó al equipo formado por Pablo Álvarez y Jorge Cordón del IES Martínez Uribarri.

2.3. ACCIONES EN RELACIÓN CON LAS INSTITUCIONES PÚBLICAS

2.3.1. Colaboración con la Administración General del Estado (AGE)

La colaboración con la Administración General del Estado ha estado orientada durante este ejercicio, y lo va a seguir estando durante el próximo año, a facilitar la implantación del Reglamento General de Protección de Datos en los diversos ámbitos de la actividad administrativa que van a resultar afectados por su aplicación efectiva el 25 de mayo de 2018. La actividad desplegada por la Agencia en este ámbito se ha centrado especialmente en posibilitar que la AGE esté en las mejores condiciones de poder cumplir a tiempo con las exigencias que establece el RGPD para las Administraciones Públicas, y de modo especial en la obligación de designar un Delegado de Protección de Datos.

Al respecto, la AEPD ha llevado a cabo un gran número de reuniones de trabajo y actividades con diversos organismos de la Administración General del Estado. En particular, con la Secretaría de Estado para la Sociedad de la Información, y la Agenda Digital (SESIAD), para abordar aspectos tanto de la próxima aplicación del RGPD, como para estudiar los aspectos que afectan a la protección de datos en el contexto de la trasposición de la Directiva NIS, en especial lo relativo a la notificación de brechas de seguridad; la Secretaría de Estado de Función Pública; la Secretaría de Estado de Presupuestos y Gastos; la Secretaria General de Administración Digital del Ministerio de Hacienda y Función Pública, la Agencia Estatal de Administración Tributaria, la Gerencia de Informática de la Seguridad Social y el Centro Criptológico Nacional, para constituir un Grupo de Trabajo de Análisis de Riesgos del nuevo Reglamento Europeo en las Administraciones Públicas; el Comité Sectorial de la Administración Electrónica para abordar, entre otros aspectos, la incidencia del RGPD en la administración electrónica, y el Comité de Dirección de las Tecnologías de Información y Comunicaciones del Ministerio de Hacienda y Función Pública con el objeto de facilitar la adecuación al RGPD de las Administraciones Públicas.

Con esta misma finalidad, el Centro Criptológico Nacional (CCN-CERT) y la AEPD han establecido un instrumento de colaboración con el objetivo de ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad. El Esquema Nacional de Seguridad (ENS) y el RGPD establecen la obligación de que las Administraciones Públicas realicen

análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables. Fruto de esta colaboración, ha sido la puesta a disposición de las Administraciones Públicas de una herramienta que les permita evaluar de manera sistemática y objetiva los posibles riesgos en materia de protección de datos y de seguridad de la información. Así, la herramienta PILAR incluye un módulo de cumplimiento que permite a las Administraciones Públicas verificar los requisitos establecidos en el RGPD, facilitando la gestión normativa tanto del RGPD como del ENS. La obligatoriedad de contar con un registro de actividades de tratamiento, designar un DPD o notificar las quiebras de seguridad en caso de producirse son algunos de los aspectos recogidos en este nuevo módulo.

Además de la referida herramienta, la AEPD ha impulsado la publicación de documentos específicos sobre el impacto de la aplicación del RGPD en las Administraciones Públicas, y en concreto 'El impacto del RGPD sobre la actividad de las Administraciones Públicas', y 'El Delegado de Protección de Datos en las Administraciones Públicas'. Dichos materiales están disponibles en la sección creada específicamente en la web de la AEPD sobre el RGPD.

2.3.2. Colaboración con las Comunidades Autónomas y las Entidades Locales

Comunidades Autónomas

La colaboración de la AEPD con las Comunidades Autónomas se ha producido en distintas actuaciones a lo largo del ejercicio 2017. Así, en relación con los menores y la Educación, mediante la remisión a las Consejerías de Educación, por diversos conductos (carta de la directora de la AEPD a los consejeros, email desde el Canal Joven a los directores generales, etc.) de todos los materiales y recursos producidos por la AEPD en este ámbito. Está pendiente su presentación en la Comisión General de Educación, ya fuera del ámbito temporal de esta Memoria.

En el ámbito de la Sanidad, la principal actuación ha sido la presentación del Plan de Inspección Sectorial de Oficio de Hospitales Públicos que hizo la AEPD a las Comunidades Autónomas con fecha 4 de julio en el marco de la Subcomisión de Sistemas de Información del Sistema Nacional de Salud.

La colaboración con CCAA se ha centrado en el asesoramiento e impulso para el cumplimiento del RGPD

Junto con las actividades que se han comentado anteriormente, la información sobre la colaboración con las Comunidades Autónomas y las Entidades locales se ha centrado principalmente en el asesoramiento e impulso para el cumplimiento del RGPD, por lo que se detalla en otro apartado de esta Memoria.

2.3.3. Colaboración con las Universidades

La colaboración de la Agencia con el ámbito universitario se ha concretado en un amplio número de actividades y de eventos, a través fundamentalmente de la Conferencia de Rectores de las Universidades Españolas (CRUE):

- 'VI Jornadas de Observatorios de Empleo Universitario', organizadas por la Universidad de Jaén y la CRUE.

- 'Jornadas de la sectorial CRUE-TIC sobre Seguridad de la Información en las Universidades Españolas'. La AEPD intervino en la mesa redonda sobre cambios en el marco normativo derivados de la aprobación del RGPD.

- Jornadas de Secretarías Generales, organizadas por la CRUE.

- V Conferencia Internacional de la Cátedra Google sobre Privacidad, Sociedad e Innovación, organizada por la Universidad San Pablo CEU, y centrada en esta edición en el 'Derecho e innovación tecnológica ante el nuevo marco europeo de privacidad'.

Encuentro 'Una Justicia de futuro: III Edición', organizado por la Universidad Internacional Menéndez Pelayo de Santander.

- '31 Encuentro de la economía digital y las telecomunicaciones', organizado por la UIMP. En dicho Encuentro, que lleva como lema La realidad digital de España, se analizan aspectos como el panorama tecnológico a corto, medio y largo plazo, la satisfacción de los consumidores, clientes y ciudadanos, y sus demandas presentes y futuras.

- Jornadas de la Sectorial de Tecnologías de la Información y las Comunicaciones (TIC) de la CRUE: 'Estrategias TIC para la Universidad del Futuro', organizadas por la Facultad de Informática de la Universidad Complutense de Madrid.

- Finalmente, hay que mencionar la participación de la CRUE como miembro del Comité Técnico encargado de asesorar en la elaboración y seguimiento del Esquema para la certificación de personas como delegados de Protección de Datos que se presentó el 13 de julio de 2017 en colaboración con la Entidad Nacional de Acreditación (ENAC).

De otra parte, cada vez es más importante la apertura de canales estables de relación con aquellos ámbitos universitarios cuya actividad está orientada específicamente al campo de la investigación e innovación tecnológica, a fin de que la AEPD pueda servirles de ayuda y asesoramiento para que los parámetros de privacidad puedan ser tenidos en cuenta desde el propio diseño del proyecto y en su desarrollo posterior.

En 2017 la AEPD ha participado, en distinto grado, en diversas iniciativas y proyectos promovidos por grupos universitarios de investigación e innovación tecnológica en el contexto del Horizonte 2020, y en particular:

- Colaboración con la UNED para la elaboración del curso de experto en protección de datos.

- Participación con la Universidad Carlos III en el proyecto OLIN, para la calificación de sitios web por el usuario.

Participación en el Proyecto europeo 'SMOOTH', en colaboración con la Universidad Carlos III. El objetivo es crear herramientas que permitan a micro empresas (menos de 10 empleados) auto-chequear si sus procesos de tratamiento de datos se alinean con el RGPD, facilitando recomendaciones y guías prácticas online. La propuesta ha sido aprobada por la Comisión y dotada presupuestariamente.

Apoyo a propuestas de investigación y proyectos europeos en calidad de miembros del Comité Asesor de los mismos:

- Proyecto para la certificación y de productos y servicios en aspectos relacionados con los derechos humanos (TRUESSEC). Es resultado de la colaboración con la Universidad Politécnica de Madrid.
- Proyecto TYPES para la transparencia en los procesos de seguimiento de usuarios en internet con fines de publicidad en colaboración con la Universidad Carlos III.

2.3.4. Colaboración con el Consejo de Transparencia y Buen Gobierno

Como es sabido, El artículo 36.1 f) de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno (LTAIBG), establece que integrará en la Comisión de Transparencia y Buen Gobierno un representante de la Agencia Española de Protección de Datos, habiendo sido designado en representación de la Agencia el abogado del Estado-jefe del Gabinete Jurídico.

La función de la Agencia en esta materia no se limita a la participación del miembro de la Comisión designado por aquélla en los trabajos de la misma, sino que además, de conformidad con lo establecido en la disposición adicional quinta, corresponderá de forma conjunta a la Agencia y al Consejo de Transparencia y Buen Gobierno la adopción conjunta de los criterios de aplicación de las reglas contenidas en el artículo 15 de la propia Ley, "en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma".

A lo largo de 2017 se han celebrado cuatro reuniones de la Comisión.

2.3.5. Colaboración con el Consejo General del Poder Judicial

En este apartado hay que mencionar la firma, en julio de 2017, por el presidente del Tribunal Supremo y del Consejo General del Poder Judicial y la directora de la AEPD de un convenio de colaboración en relación con las diversas tareas que, como autoridades de control, deben llevar a cabo y, en especial, sobre la inspección de órganos judiciales en materia de protección de datos.

El convenio establece mecanismos de cooperación para el desarrollo de investigaciones por posible infracción de la normativa de protección de datos. El CGPJ es la institución competente en relación con los tratamientos de datos efectuados con fines jurisdiccionales en ficheros de esta naturaleza; mientras que los tratamientos de datos no jurisdiccionales y sus correspondientes ficheros son competencia de la AEPD.

En el caso de ficheros jurisdiccionales, el CGPJ notificará a la AEPD su intención de iniciar una inspección a un determinado órgano judicial para investigar si existe una posible infracción del derecho a la protección de datos. Los inspectores del CGPJ realizarán la visita acompañados de inspectores de la AEPD, que prestarán la asistencia técnica requerida, sin que ello suponga asunción de ninguna competencia en la materia.

De igual manera, cuando se trate de ficheros no jurisdiccionales, la AEPD comunicará al CGPJ su intención de inspeccionar un determinado órgano judicial ante una posible infracción de la normativa de protección de datos. Los inspectores de la AEPD llevarán a cabo la inspección acompañados de inspectores del CGPJ.

En caso de que existieran indicios suficientes que determinaran la apertura de un expediente por la posible participación de un miembro de la Carrera Judicial en la infracción de la normativa de protección de datos, la incoación y tramitación del mismo corresponderá en exclusiva al CGPJ.

El Convenio suscrito recoge igualmente la colaboración entre ambas instituciones en la elaboración de códigos de buenas prácticas para usuarios de los sistemas de información de la administración de justicia, que ayuden a cumplir con las obligaciones de responsabilidad activa que introduce el RGPD.

Finalmente, el texto recoge el desarrollo de actuaciones conjuntas en materia de formación sobre normativa española y comunitaria de protección de datos, en especial el RGPD y la Directiva de la Unión Europea 2016/680 relativa a la protección de datos de personas físicas en los ámbitos policial y judicial penal.

2.3.6. Colaboración con el Defensor del Pueblo

Se consolida durante este período la tendencia descendente marcada en el ejercicio anterior. En concreto, se han remitido a la Agencia desde la Oficina del Defensor del Pueblo un total de 21 asuntos, uno menos que en 2016, año en el que ya se había producido una caída del 40% con respecto a 2015.

En cuanto a los principales asuntos o temas objeto de la atención del Defensor del Pueblo, estos hacen referencia a cuestiones muy variadas, como las relativas a la morosidad, y a la inclusión indebida en ficheros de solvencia (5); la videovigilancia (2); el tratamiento de los datos por las entidades financieras (2) o por las operadoras de telecomunicaciones (2); las llamadas publicitarias no deseadas (1), o la historia clínica (1).

Sobre los principales motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, más de la mitad de las quejas (12) se interesan por el estado de tramitación de un determinado procedimiento, solicitando una respuesta de la Agencia. Otros motivos de queja han sido para solicitar que se abra un expediente sancionador (2), mostrar su disconformidad con el criterio seguido por la Agencia en alguna de sus resoluciones (1), o que se posibilite el acceso a los registros de llamadas de una persona fallecida (1).

Hay que destacar especialmente este año los casos en los que el Defensor del Pueblo ha requerido la información de esta Agencia para poder llevar a cabo un estudio más profundo sobre los temas planteados. Así ha ocurrido con la nueva política de privacidad de Whatsapp y Facebook, la problemática derivada de la suplantación de identidad en la contratación telefónica, o el control del buzoneo en viviendas.

Se consolida la tendencia descendente de asuntos remitidos por el Defensor del Pueblo

2.3.7. Colaboración con las Autoridades autonómicas de protección de datos

La colaboración con las Agencia vasca y la Autoridad catalana de protección de datos se ha concretado en 2017 en los siguientes términos:

- Participación en la elaboración de nuevos materiales y recursos de la AEPD para facilitar a las pequeñas y medianas empresas su adaptación al RGPD: 'Guía del Reglamento para responsables de tratamiento', 'Directrices para elaborar contratos entre responsables y encargados' y 'Guía para el cumplimiento del deber de informar'. Estos materiales fueron presentados con ocasión de la Jornada conmemorativa del Día Europeo de la Protección de Datos.

- Creación de un Grupo de Trabajo conjunto para abordar aspectos relacionados con la aplicación práctica del Reglamente General de Protección de Datos.

- Participación de ambas autoridades como miembros del Comité Técnico de Seguimiento creado para la elaboración y posterior desarrollo del Esquema de la AEPD de Certificación de Delegados de Protección de Datos, al que se aludirá con mayor detalle en el apartado correspondiente de esta Memoria.

- Participación de la AEPD en eventos y actividades organizadas por las autoridades autonómicas:

  - Ciclo de conferencias sobre el nuevo Reglamento General de Protección de Datos organizado por la APDCAT y el Ilustre Colegio de la Abogacía de Barcelona.

  - Jornada 'Privacidad: una cuestión de democracia', organizada por la APDCAT.

- Encuentros institucionales de la directora de la Agencia con el director del Consejo de Transparencia y Protección de Datos de Andalucía.

2.3.8. Fomento de la seguridad jurídica mediante la emisión de informes preceptivos de proyectos normativos

La AEPD ha continuado trabajando en el objetivo de lograr mayor seguridad jurídica a través de los informes preceptivos sobre disposiciones de carácter general, dirigidos a mejorar la sistemática del ordenamiento jurídico integrando una norma de carácter transversal con las regulaciones sectoriales.

De este modo en 2016 fueron informadas 98 disposiciones de carácter general, lo que supone un incremento del 34% respecto las que fueron informadas en el ejercicio anterior, si bien una gran parte de las mismas eran órdenes de creación de ficheros de distintos departamentos ministeriales y organismos vinculados o dependientes de los mismos. No obstante, cabe mencionar algunas disposiciones:

- Anteproyecto de Ley Orgánica de Protección de datos de Carácter Personal.

- Anteproyecto de Ley sobre determinados aspectos de los servicios electrónicos de confianza.

- Anteproyecto de Ley por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual, aprobado por RDL 1/1996 y por la que se incorpora al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, relativa a la gestión colectiva de los derechos de autor y derechos afines a la concesión de licencias multiterritoriales de derechos sobre obras musicales para su utilización en línea en el mercado interior.

- Anteproyecto de Ley de modificación parcial de la Ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Anteproyecto de Ley del Mercado de Valores y de los Instrumentos Financieros.

- Anteproyecto de Ley por la que se modifica el texto refundido de la Ley General para la Defensa de los consumidores y usuarios y otras leyes complementarias aprobado por RDL 1/2007 de 16 de noviembre.

- Anteproyecto de Ley de distribución de seguros y reaseguros privados.

- Anteproyecto de Ley de Archivos y Documentos de la Comunidad de Madrid.

- Anteproyecto de Ley Reguladora de la Inspección General de Servicios y del Sistema de Alertas para la Prevención de las malas prácticas en la Administración de la Generalitat Valenciana y su sector público institucional.

- Proyecto de Real Decreto por el que se aprueba el Reglamento de Adopción Internacional.

- Proyecto de Real Decreto por el que se regula la figura del consumidor vulnerable, el bono social y otras medidas de protección para los consumidores domésticos de energía eléctrica.

- Proyecto de Real Decreto por el que se modifica el Reglamento de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, aprobado por RD 887/2006 de 21 de julio en materia de Base de Datos Nacional de Subvenciones.

- Proyecto de Real Decreto de modificación parcial de R.D. 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010.

- Proyecto de Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley 49/1999, de 20 de diciembre, sobre medida de control de sustancias químicas susceptibles de desvío para la fabricación de armas químicas.

- Proyecto de Real Decreto de Comunicaciones Comerciales de las Actividades de Juego y de Juego Responsable.

- Decreto por el que se aprueba la política de seguridad del información del Servicio de Salud de las Islas Baleares.

- Proyecto de Orden por la que se aprueba la política de seguridad de información en el ámbito de la administración electrónica del Ministerio de Justicia.

3. Innovación y protección de datos: factor de confianza y garantía de calidad

3.1. ACTUACIONES DESARROLLADAS POR LA UEET

Guía de Buenas Prácticas en Big Data

La AEPD elaboró en colaboración con ISMS Forum Spain un código de buenas prácticas en protección de datos para proyectos en los que se emplee tecnología Big Data. En la elaboración de esta guía ha participado un grupo independiente de expertos en tratamientos masivos de datos que han aportado sus conocimientos y experiencia en este campo con el objetivo de asesorar a aquellas entidades que desarrollen o puedan desarrollar proyectos de big data.

Esta guía se ha desarrollado teniendo en cuenta el RGPD y constituye un marco de referencia práctica para las empresas que utilicen grandes volúmenes de datos con el fin de establecer correlaciones o elaborar perfiles de personas que pueden generar riesgos para los derechos y libertades de los interesados. La guía tiene en cuenta estos riesgos en relación a la responsabilidad que pueda suponer para aquellas entidades que llevan a cabo estos tratamientos y que en todo momento deben preservar la privacidad de las personas cuyos datos están siendo tratados mediante soluciones técnicas, organizativas o garantías jurídicas.

El documento detalla la necesidad de llevar a cabo acciones encaminadas a garantizar los principios del RGPD como la privacidad desde el diseño, el principio de responsabilidad activa (*accountability*) y la necesidad de llevar a cabo evaluaciones de impacto con el objeto de minimizar riesgos para los derechos y libertades de las personas.

Puesta en marcha del esquema de certificación de DPO

La figura del Delegado de Protección de Datos es una novedad para los responsables y encargados de tratamientos de nuestro país. La AEPD, consciente de la necesidad de disponer de un marco de referencia en este nuevo sector, ha trabajado en colaboración con ENAC y un Comité de Expertos con el objeto de definir este marco de referencia en el contexto de la norma ISO/IEC 17024:2012 para la certificación de personas.

La elección de esta norma, la participación de ENAC y los Acuerdos Multilaterales de Reconocimiento (MLA) que ENAC suscribe en colaboración con la organización europea de acreditadores (*European Accreditation*), hacen que este esquema de certificación de delegados de protección de datos tenga una proyección global y pueda servir como referencia dentro y fuera de España.

En el esquema de certificación de delegados de protección de datos intervienen tres partes: la AEPD, como propietaria y responsable del esquema, es la responsable del desarrollo y revisión del mismo; ENAC es la entidad de encargada de verificar y validar (acreditar) los requisitos que deben de cumplir las entidades de certificación; y las propias entidades de certificación, que son las encargadas de llevar a cabo los procesos para certificar a las personas dentro de este esquema. La supervisión de estos procesos se lleva a cabo por ENAC y la AEPD en el marco de sus respectivas funciones.

Para la elaboración de este esquema la AEPD ha suscrito un convenio de colaboración con ENAC con el objeto de coordinar las actividades necesarias en el ámbito de las competencias que corresponden a ambas entidades.

La certificaciones de los delegados de protección de datos no son, en ningún caso, un requisito obligatorio para el ejercicio de esta actividad profesional, si bien pueden ser tenidas en cuenta por el responsable y encargado del tratamiento como una ayuda a la hora de evaluar los conocimientos, capacidades y competencias de los candidatos a ser designados como Delegado de Protección de Datos.

Herramienta FACILITA_RGPD

Teniendo en cuenta la información contenida en el Registro General de Ficheros y el hecho de que más del 95% de las empresas españolas cuentan con menos de diez trabajadores, ha sido prioritario dotar a los responsables y encargados de tratamientos de datos personales de una herramienta sencilla que ayude a su adaptación al RGPD, proporcionando una hoja de ruta con la que iniciar esta adecuación.

Esta iniciativa se suma a otras que han sido llevadas a cabo durante el pasado año con el fin de permitir a los responsables de pymes su adecuación al nuevo modelo de cumplimiento del RGPD.

La herramienta FACILITA_RGPD es una solución para más del 72% de los tratamientos habituales de escaso riesgo que se llevan a cabo en pequeñas empresas y, más concretamente, los tratamientos de datos de clientes, proveedores, nóminas, recursos humanos, personal y videovigilancia, información que ha sido obtenida de las estadísticas de inscripción de ficheros obtenidas del Registro General de Ficheros de la AEPD. La información más detallada sobre esta herramienta se describe en un apartado posterior de esta Memoria.

FACILITA_RGPD es una herramienta para más del 72% de los tratamientos habituales de escaso riesgo que se llevan a cabo en pequeñas empresas

3.2. OTRAS ACTUACIONES

3.2.1. Guía práctica para administradores de fincas

En 2017 la AEPD publicó su guía 'Protección de datos y administración de fincas' para facilitar a este sector el cumplimiento de la normativa de protección de datos.

El tratamiento de datos personales en el ámbito de las comunidades de propietarios viene dando lugar a múltiples consultas realizadas tanto por profesionales como por ciudadanos.

Para dar respuesta a las mismas, la Agencia Española de Protección de Datos ha publicado la guía '‹Protección de datos y administración de fincas', un documento que forma parte del conjunto de iniciativas adoptadas por la Agencia para facilitar y fomentar el cumplimiento de la normativa de protección de datos.

El documento recoge la aplicación práctica de la normativa de protección de datos vigente, incorporando referencias al Reglamento General de Protección de Datos, que será aplicable a partir del 25 de mayo de 2018, y que supone una gestión distinta de la que se realiza en la actualidad en el seno de las comunidades de propietarios.

La AEPD considera que publicar una guía orientada a abordar la protección de datos en las comunidades de vecinos a través de los administradores de fincas contribuye tanto a facilitar el trabajo de estos, ofreciéndoles una información ajustada a sus necesidades, como a mejorar el nivel global de protección de los ciudadanos. Según datos del Consejo General de Colegios de Administradores de Fincas, estos gestionan el 80% del parque total de viviendas en España.

'Protección de datos y administración de fincas' aborda en primer lugar cuestiones generales de la normativa de protección de datos que se aplican a los administradores de fincas que actúan por cuenta de las comunidades de propietarios. Incluye secciones dedicadas a las definiciones de conceptos básicos, a la inscripción de ficheros y el futuro registro de actividades, a la forma de organizar las relaciones entre la comunidad de propietarios y el administrador, así como a las principales obligaciones de las partes.

Por otro lado, la guía analiza con detalle algunos supuestos específicos que se plantean con frecuencia ante la Agencia, tanto en forma de consulta como de denuncia: información sobre propietarios con pagos pendientes (publicación en el tablón de avisos de la finca de la identidad de los propietarios deudores y/o de las cuotas vencidas e impagadas), acceso y obtención de copias de la documentación de la comunidad, requisitos para la instalación de cámaras de videovigilancia o tratamiento de datos de empleados.

4. Una agencia colaboradora, transparente, más ágil y eficiente

4.1. HERRAMIENTAS DE COMUNICACIÓN

Durante 2017, la Agencia Española de Protección de Datos ha desarrollado numerosas acciones para dar a conocer sus iniciativas. En este apartado se muestran aquellas que tienen que ver con el departamento de prensa y comunicación, y también se incluyen tanto las acciones de divulgación realizadas a través de página web de la AEPD como un resumen de la agenda institucional desplegada durante el año.

4.1.1. Blog

El blog de la Agencia inició su andadura en diciembre de 2016, acumulando cerca de 4.500 accesos en sus tres primeros meses. La cifra de accesos ha crecido en 2017 hasta rebasar ampliamente los 88.000. Este recurso, que nació con el objetivo de favorecer la difusión del derecho fundamental a la protección de datos, está contemplado en el eje 'Una Agencia colaboradora, transparente y participativa' del Plan Estratégico de la AEPD.

Los contenidos publicados en 2017 en el blog han girado en torno a dos grandes objetivos: de una parte, que los ciudadanos conozcan el contenido de sus derechos y cómo ejercerlos y, de otra, facilitar a los responsables el cumplimiento de sus obligaciones.

En este contexto, el blog de la Agencia ha abordado, entre otros, asuntos como los derechos de los ciudadanos recogidos en el Reglamento General de Protección de Datos; la videovigilancia en entornos particulares; las cámaras on-board; consejos para evitar la publicidad no deseada; así como la Guía de Seguridad y Privacidad en internet y la Guía para centros educativos elaboradas por la Agencia. Por otra parte, se han publicado varias entradas relacionadas con distintas vertientes del RGPD, como las transferencias internacionales, el registro de actividades, las brechas de seguridad, los Delegados de Protección de Datos o el enfoque de riesgos.

4.1.2. Relaciones con los medios

Los medios de comunicación cumplen una función fundamental no sólo para fomentar la sensibilización de los ciudadanos acerca del derecho a la protección de sus datos personales sino también para que los responsables sepan cuáles son sus obligaciones. La labor informativa que desarrollan constituye un factor esencial para potenciar y fortalecer el conocimiento de la protección de datos. Durante 2017, la Agencia atendió cerca de 500 consultas de medios de comunicación relacionadas con este derecho fundamental. Entre los temas consultados con mayor frecuencia se encuentran los siguientes:

- **Reglamento General de Protección de Datos.** Publicación de las directrices de las Autoridades Europeas de Protección de Datos (GT29) sobre la aplicación del Reglamento; avance de los trabajos para la publicación del Esquema de certificación de Delegados de Protección de Datos de la AEPD; trabajos realizados para adaptar la normativa española al RGPD; nuevos derechos e implicaciones del Reglamento en la actividad de las pymes.

- **'Derecho al olvido'.** Ámbito de aplicación y cifras de reclamaciones recibidas; cambios

que introduce el Reglamento General en relación con este derecho; seguimiento de solicitudes de tutela de derechos recibidas desde la sentencia del Tribunal de Justicia de la Unión Europea sobre el denominado derecho al olvido; tratamiento de datos de personas fallecidas y ejercicio del derecho en casos de personajes de relevancia pública.

Videovigilancia. Instalación de cámaras en el interior de aulas de institutos; cuestiones vinculadas a la legalidad de las cámaras on-board; utilización de cámaras de videovigilancia en el ámbito privado dirigidas a la vía pública; solicitud de datos sobre la inscripción de ficheros con la finalidad de videovigilancia.

Menores: marco legal y consejos en relación con el *sharenting* o publicación de fotos de menores en redes sociales por parte de sus padres; difusión de diferentes iniciativas impulsadas por la Agencia; implicaciones en la privacidad de los menores derivadas de los juguetes conectados y recomendaciones por parte de la Agencia.

Resoluciones de la AEPD. Destacan aquellas relacionadas con, entre otros aspectos, la reclamación de un ciudadano vinculada a la publicación de su número de teléfono en internet y la recepción de varias llamadas diarias a consecuencia de ello; la sanción impuesta por la AEPD a Facebook por tratar datos, incluso especialmente protegidos, con fines de publicidad sin recabar el consentimiento y no cancelar totalmente la información de los usuarios cuando ya no es útil para el fin para el que se recogió ni cuando estos lo solicitan; la inclusión de contactos de ciudadanos en grupos de WhatsApp creados por empresas y administraciones públicas sin su consentimiento, y la sanción impuesta a Google por la captación de datos de redes WiFi a través de los coches de su servicio *Street View*.

Cifras y tendencias recogidas en la memoria 2016 de la AEPD. Análisis cualitativo en contratación irregular e inserción indebida en ficheros de morosidad, así como análisis cuantitativo de sectores con mayor volumen de sanciones.

Otros temas de actualidad. Datos sobre reclamaciones relacionadas con ficheros de solvencia en el ámbito de las telecomunicaciones o publicación de imágenes en redes sociales sin consentimiento.

A esta labor de atención personalizada a las consultas planteadas por los medios hay que sumar la comunicación proactiva realizada por la Agencia, con cerca de 250 notas de prensa, convocatorias y notas de agenda informativa publicadas en la web. En este sentido, en cumplimiento del compromiso adquirido en el Plan Estratégico 2015-2019 de fomentar y ampliar la publicación de su agenda institucional para que ciudadanos y responsables puedan conocer las actividades que organiza o en las que participa la Agencia, en 2017 se ha continuado con la publicación de actos en los que participa el equipo directivo de la Agencia, con más de 175 notas de reuniones o actos públicos en los que han participado diferentes miembros de esta institución, disponibles todas ellas de manera sistemática para su consulta en este enlace.

4.1.3. Agenda institucional

La Agencia concede una gran importancia a los encuentros con organizaciones públicas y privadas y asociaciones profesionales y empresariales para potenciar el diálogo y trabajar para fomentar de forma efectiva el derecho a la protección de datos. Así, este organismo ha mantenido reuniones con diferentes entidades para difundir y promover este derecho fundamental desde diferentes ámbitos, así como impulsar la colaboración y el cumplimiento de la legislación.

A continuación se recogen algunas de las reuniones institucionales y de trabajo celebradas durante 2017, así como la asistencia a actos y jornadas. En cualquier caso, todas ellas pueden consultarse cronológicamente en la sección 'Notas de Agenda' de la página web de la AEPD.

El Consejo Consultivo de la Agencia de Protección de Datos, establecido por el artículo 37 de la Ley Orgánica 5/1992, de 29 de octubre, es un órgano colegiado de asesoramiento a la dirección de la Agencia. Este se reúne cuando lo convoca la dirección de la AEPD y, en todo caso, una vez cada seis meses. Las reuniones del Consejo Consultivo para exponer y analizar la actividad de la institución tuvieron lugar el 16 de enero y el 20 de julio de 2017. En la primera de ellas se abordaron las principales actividades de la institución realizadas durante 2016, fallándose también la vigésima edición de los Premios Protección de Datos, y en la segunda se expusieron las acciones realizadas en el primer semestre de 2017.

En el ámbito de las reuniones institucionales, la Agencia ha celebrado encuentros con organismos públicos y asociaciones profesionales. Así, la AEPD ha mantenido reuniones institucionales con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, así como con representantes de, entre otros, la Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC); el Consejo de Consumidores y Usuarios y la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN); la Cámara Baja del Parlamento alemán (*Bundestag*); el Consejo de Transparencia y Protección de Datos de Andalucía; la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital; el Consejo para la Transparencia de Chile; la Autoridad japonesa de protección de datos; o el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), de México.

Este año se ha celebrado la 20 edición de los 'Premios Protección de datos'

Asimismo, la Agencia ha mantenido decenas de encuentros informativos dirigidos a los responsables para facilitar la adaptación en relación con los nuevos requerimientos que establece el Reglamento General de Protección de Datos. En este sentido, la Agencia ha continuado con la celebración de reuniones de trabajo periódicas con representantes de la Agencia Vasca y la Autoridad Catalana de Protección de Datos en el marco del Grupo de Trabajo establecido *ad hoc* para abordar esta materia. Igualmente, ha llevado a cabo reuniones para abordar este tema con, entre otros, representantes del Consejo General de Colegios de Gestores Administrativos de España; el Consejo General de Secretarios, Interventores y Tesoreros de Administración Local (COSITAL); la Federación Espa-

ñola de Municipios y Provincias (FEMP); la Asociación Española de la Economía Digital (Adigital); el Comité Sectorial de la Administración Electrónica; la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, Servicios Sociales e Igualdad; así como con compañías que, por su actividad, tratan un gran volumen de datos personales. A estas reuniones hay que añadir las jornadas formativas sobre las novedades del RGPD celebradas en coordinación con los centros o institutos de formación autonómicos de diez comunidades autónomas, así como con organizaciones empresariales para fomentar la adaptación de las pymes al RGPD.

En el capítulo dedicado a fomentar la concienciación y promover la cooperación específica en proyectos realizados en colaboración con diferentes entidades, la Agencia también ha mantenido reuniones de trabajo con representantes de la Confederación Española de la Pequeña y Mediana Empresa (CEPYME); el Departamento de Seguridad Nacional; Unión Profesional; el Instituto Nacional de Ciberseguridad (INCIBE) y la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España, entre otros.

Por otra parte, la Agencia Española de Protección de Datos ha participado en multitud de jornadas y conferencias para difundir diferentes aspectos del derecho fundamental a la protección de datos. Entre sus intervenciones, cabe citar las V Jornadas sobre Inspección Educativa, organizadas por la Unión de Cooperativas de Enseñanza de Trabajo Asociado de Madrid (UCETAM); el III Congreso Internacional ENATIC, organizado por la Asociación de Expertos Nacionales de la Abogacía Tecnológica; las VI Jornadas de Observatorios de Empleo Universitario, organizadas por la Universidad de Jaén y la Conferencia de Rectores de las Universidades Españolas (CRUE); el Foro 'Retos ante la nueva legislación de protección de datos', organizado por la Asociación Española de Gerencia de Riesgos y Seguros; la Jornada 'La investigación y la protección de la salud en la era del Big data: ¿Oportunidad o mito?', organizada por el Ministerio de Sanidad, Servicios Sociales e Igualdad, la UNESCO y la Universidad Pontificia Comillas ICAI-ICADE; el XX Congreso Nacional de la Sociedad Española de Informática y Salud (SEIS); I Congreso Estatal de Convivencia Escolar, organizado por los ministerios de Educación, Cultura y Deporte y de Empleo y Seguridad Social; AsticNet, evento organizado por la Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC); la Jornada sobre protección de datos e información al consumidor, en colaboración con el Consejo de Consumidores y Usuarios (CCU) y la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN); y el 8º Foro sobre el Sistema de Información del Sistema Nacional de Salud, organizado por el Ministerio de Sanidad, Servicios Sociales e Igualdad, entre otros.

4.1.4. Página web

La página web de la Agencia ha registrado en 2017 más de 6,7 millones de accesos (6.724.113). Ante la cercanía del 25 de mayo de 2018, fecha de aplicación del RGPD, la Agencia ha seguido trabajando para ofrecer nuevos materiales orientados a ciudadanos y responsables del tratamiento de datos. En este sentido, ha publicado en su página las informaciones, guías, documentos de interés o secciones elaboradas para facilitar la consulta y el rápido acceso a los nuevos contenidos de ayuda.

Con respecto a las acciones online específicas, la Agencia Española de Protección de Datos conmemoró el Día mundial de los derechos de los consumidores de Internet, que tiene lugar el 15 de marzo, con la publicación de un espacio web para ayudar a los ciudadanos a reclamar sus derechos en materia de telecomunicaciones. La elección de este tema responde a un doble motivo: de una parte, debido a que gran parte de las denuncias que recibe la Agencia en asuntos como la inserción indebida en

'ficheros de morosidad' o la contratación irregular tiene relación con el sector de las telecomunicaciones; de otra, porque al haber varios organismos públicos con competencias en esta materia, resulta fundamental que el ciudadano conozca ante qué organismo debe presentar su reclamación en función de las causas que la motivan. A 31 de diciembre de 2017, este *microsite* había recibido 23.000 visitas.

Con esta sección web, elaborada en colaboración con la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN), se incorpora un nuevo recurso al conjunto de iniciativas adoptadas por la Agencia para fomentar la concienciación de los ciudadanos sobre las garantías y los derechos que les asisten y cómo ejercerlos.

Por otra parte, al margen de las informaciones publicadas en la web, desde la entrada en vigor del Reglamento General de Protección de Datos el 25 de mayo de 2016, la AEPD ha publicado contenidos específicos para facilitar la comprensión del nuevo contexto normativo y la adaptación de los responsables a los cambios y cumplir así con sus obligaciones. En esta línea, se ha ampliado la sección que comprende la legislación, las guías sobre el Reglamento, así como las orientaciones de la AEPD para facilitar la labor de adaptación, las directrices de las Autoridades europeas de Protección de Datos sobre la aplicación del RGPD, los enlaces a las sesiones anuales abiertas de la Agencia que han tratado sobre aspectos vinculados al nuevo marco europeo y otros recursos útiles tanto para los ciudadanos como para los sujetos obligados. Al cierre del ejercicio 2017, esta sección había sido consultada más de 112.000 ocasiones.

En mayo de 2017, la Agencia publicó dos documentos que incluyen un conjunto de medidas de necesaria implantación el 25 de mayo de 2018 por parte de las Administraciones Públicas, con el objetivo de fomentar que estas conozcan las implicaciones prácticas de la nueva normativa y poder adoptar las medidas necesarias para cumplir con las previsiones establecidas en la misma.

El primero de los documentos, 'El impacto del RGPD sobre la actividad de las AAPP', condensa en 15 puntos los aspectos más relevantes que deben estar establecidos cuando el Reglamento sea de aplicación, mientras que el segundo está centrado en 'El Delegado de Protección de Datos en las Administraciones Públicas', ya que el Reglamento establece como obligatoria la designación de esta figura en el caso de autoridades u organismos públicos.

Estos documentos se complementan con la publicación en la página web de la AEPD de los vídeos de la jornada realizada junto con el Instituto Nacional de Administración Pública (INAP), donde se abordaron las novedades del Reglamento para las AAPP, así como los vídeos de la jornada de formación celebrada conjuntamente con la Federación Española de Municipios y Provincias (FEMP) en diciembre de 2017 con el objetivo de facilitar la adaptación de las entidades locales al RGPD.

Por otra parte, la Agencia presentó el 28 de julio de 2017 un espacio web con consejos prácticos para ayudar a los ciudadanos a evitar la recepción de publicidad no deseada, incluyendo tanto llamadas telefónicas como correos electrónicos. Con la creación de este espacio, estructurado en ocho secciones, la Agencia pretende ofrecer al ciudadano una información clara y completa para conocer los derechos que le asisten y qué pasos puede seguir para impedir la recepción de publicidad que, en el caso de las llamadas telefónicas, son calificadas habitualmente por los ciudadanos como las más molestas. Desde su publicación hasta finales de 2017, esta sección web ha recibido más de 14.250 accesos.

La entrada en vigor, el 25 de mayo de 2018, del nuevo Reglamento General de Protección de Datos (RGPD) conlleva una necesaria actualización de los materiales informativos para el ciudadano, ofreciendo una magnífica ocasión para acometer un cambio de fondo en el diseño, la estructura y la forma en que se almacenan y acceden a los contenidos del portal.

La visión de una Agencia colaboradora, transparente y participativa, tercer eje del Plan Estratégico 2015-2019, establece el marco de trabajo para el proyecto de actualización del portal corporativo de la Agencia.

Este proyecto comienza ya en 2017, con la realización del nuevo diseño del portal, tanto de su estética como de la estructura de la información, organizando los contenidos para facilitar una navegación que, centrada en el usuario, le permita alcanzar los contenidos que busca de manera intuitiva; respetando los estándares de accesibilidad, interoperabilidad y neutralidad tecnológica.

Con la nueva web, se llevará a cabo una profunda actualización tecnológica de la plataforma, destacando la figura de un nuevo buscador facetado que reducirá el tiempo de acceso a los contenidos que ofrece el portal, las resoluciones de la Agencia y otra documentación que solicita el usuario.

El principal propósito del nuevo portal es el acercamiento a los ciudadanos, facilitando el acceso a la información sobre privacidad y protección de datos a través de una navegación intuitiva y una óptima experiencia de usuario, teniendo en cuenta el previsible incremento en el número de visitas y consultas que despertará el cambio normativo.

4.1.5. Canal de transparencia

Durante el año 2017, se ha actualizado la información que se publica en este canal web de la AEPD, denominado 'Transparencia: la Agencia', que fue creado en cumplimiento de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, y cuya finalidad es facilitar a los ciudadanos de una forma clara y ordenada todos los contenidos de publicidad activa que regula la citada Ley.

El canal de transparencia se muestra dividido en cinco grandes apartados, mostrando en cada uno de ellos, respectivamente, datos de Información institucional y organizativa; gestión económica financiera; recursos humanos; enlaces de interés (Portal de la transparencia del Gobierno de España); datos anuales estadísticos de interés referidos a denuncias y reclamaciones registradas y resueltas, ficheros inscritos o autorizaciones de transferencias internacionales, entre otros. A estas secciones se suman los apartados relativos a los Premios que concede la AEPD, un enlace para solicitar información, la actividad de agenda institucional o información referente a becas. Este canal recibió un total de 856.245 visitas en el año 2017.

Respecto a las peticiones de acceso a la información pública, se recibieron 59 solicitudes (una menos que en el año 2016), de las cuales se atendieron 33, se inadmitieron 13, en 1 supuesto desistió el solicitante, y 6 fueron denegadas.

Sobre las inadmisiones cabe señalar que se motivaron en la aplicación del artículo 18 de la Ley 19/2013 (abuso de derecho, solicitudes repetidas y elaboración de la información), así como en la Disposición Adicional 1ª de la citada Ley (aplicación de otra normativa específica que regula el derecho de acceso).

Por último, señalar que de esas 59 solicitudes, es conveniente indicar que 6 de ellas fueron resueltas como consultas y no como solicitudes de acceso a la información, aunque se recibieran a través del Portal de Transparencia del Gobierno de España.

4.1.6. Actividades de divulgación

En el plano de los foros y eventos organizados por terceros, la AEPD participó en 2017 en jornadas, seminarios, mesas redondas, cursos y charlas informativas para difundir una cultura de protección de datos entre los ciudadanos, empresas y administraciones públicas, como puede comprobarse en la sección 'Agenda' de la página web. Esta presencia fue particularmente significativa en relación con las charlas informativas sobre las implicaciones del Reglamento General de Protección de datos en la actividad de pymes y administraciones públicas. Consciente de la necesidad de estar presente en el mayor número posible de foros, la Agencia diseñó un calendario de jornadas de formación sobre las novedades del RGPD en centros o institutos de formación autonómicos de las comunidades autónomas, así como en organizaciones de empresarios a escala autonómica. La AEPD prosigue con estos actos en los primeros meses de 2018, ya fuera del ámbito temporal de esta Memoria.

La AEPD participó en 2017 en jornadas, seminarios, y charlas informativas para difundir una cultura de protección de datos

Jornada sobre la 'Incidencia del nuevo Reglamento de protección de datos sobre las pymes'

El día 26 de enero la AEPD celebró, en conmemoración del Día Europeo de la Protección de Datos, la jornada sobre la 'Incidencia del nuevo Reglamento de protección de datos sobre las pymes'. El evento incluyó la presentación de nuevos materiales y recursos encaminados a facilitar a las pequeñas y medianas empresas su adaptación al RGPD: la 'Guía del Reglamento para responsables de tratamiento', las 'Directrices para elaborar contratos entre responsables y encargados' y una 'Guía para el cumplimiento del deber de informar', elaborados junto a la Autoridad Catalana y la Agencia Vasca de Protección de Datos.

Tras el acto de inauguración, por el ministro de Justicia, Rafael Catalá, y la presentación de la jornada por parte de la directora de la AEPD, se desarrolló una mesa redonda sobre los retos que plantea la nueva normativa en la que participaron representantes de la Cámara de Comercio de España, CEPYME y Unión Profesional.

9ª Sesión Anual Abierta de la AEPD

El 25 de mayo de 2017 se celebró la 9 ª Sesión Anual Abierta de la AEPD en el Centro de Conferencias Fundación Pablo VI de Madrid, que en esta ocasión se centró en las novedades del RGPD y, especialmente, en su implementación práctica en las organizaciones, así como en las actividades realizadas por la Agencia, las novedades legislativas y jurisprudenciales acaecidas en el último año, y los principales retos que afronta este derecho fundamental.

La Sesión Anual, evento abierto, gratuito y de carácter esencialmente práctico dirigido a representantes de instituciones, empresarios, profesionales de la protección de datos y ciudadanos interesados en la materia, fue retransmitida en *streaming* como ya se hiciera en la edición de 2016. A las más de 600 personas que asistieron de manera presencial, se sumaron más de 1.000 que siguieron el evento online.

Durante la Sesión Anual se presentó 'Protección de Datos: Guía para el Ciudadano', se expusieron las principales herramientas de ayuda al cumplimiento del Reglamento General –entre las que se encuentra una orientada a empresas y profesionales que realicen tratamientos de datos personales de escaso riesgo- y se entregaron los 'Premios Protección de Datos 2016'. Asimismo, se analizaron, entre otros aspectos, los nuevos materiales de ayuda a las pymes para el cumplimiento del RGPD; las nuevas funciones de las autoridades de control; las evaluaciones de impacto; los informes y sentencias relevantes y la actualización de criterios de la Agencia.

Un año más, la AEPD publicó con posterioridad a la celebración de la sesión un espacio web específico desde el que se pueden visualizar todos los vídeos de la jornada, así como acceder a cada una de las presentaciones realizadas durante la misma.

Entrega de los 'Premios Protección de Datos 2016' (XX edición)

Estos galardones, que se entregan cada año en el marco de la Sesión Anual Abierta, reconocen los trabajos de Comunicación e Investigación que promueven en mayor medida la difusión y la investigación del derecho fundamental a la protección de datos. Así, la AEPD premió en este contexto la labor realizada por los medios de comunicación en la difusión de este derecho fundamental y el trabajo de los investigadores, que con sus análisis sobre la legislación y la evolución de las sociedades contribuyen a la reflexión sobre esta materia.

El jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio principal de comunicación *ex aequo* al periodista Carlos Enrique Carrasco del programa Repor de RTVE, por el reportaje 'Las redes las carga el diablo', en el que se analizan cuestiones como el ciberacoso, la suplantación de identidad o la falsa sensación de anonimato e impunidad que se vive en internet, y a la Corporación RTVE, por su campaña de educación digital emitida en Clan TV y protagonizada por los personajes de '*Big Band* Clan' para difundir un uso responsable de internet y las redes sociales entre los más jóvenes.

Asimismo, el accésit recayó, por un lado, en Azucena Hernández, directora editorial de la revista *One Magazine*, por los reportajes sobre privacidad online englobados bajo el título 'Se venden tus secretos', donde se abordan aspectos como los datos que las grandes compañías de internet podrían tener sobre los ciudadanos o el precio que se paga a cambio de obtener determinados servicios de manera gratuita. Por su parte, José Manuel Sánchez, periodista de ABC y abc.es, recibió el accésit por los reportajes dedicados, entre otros temas, a la nueva normativa europea de protección de datos, el internet de las cosas o el cambio en los términos de uso de WhatsApp.

En la categoría de Investigación, se otorgó un accésit a Laura Davara por su trabajo 'Menores en internet y redes sociales. Derecho aplicable y deberes de los padres y centros educativos – Breve referencia al fenómeno Pokémon Go', en el que profundiza en el estudio de las implicaciones que Internet y las redes sociales generan en la privacidad de las personas más jóvenes desde una perspectiva tanto jurídica como preventiva, abordando el papel que desempeñan los centros educativos y los padres por su responsabilidad en la educación de los menores.

En la modalidad de Investigación sobre trabajos originales e inéditos que tratan acerca del derecho a la protección de datos en países iberoamericanos, se concedió el premio a Karina Ingrid Medinaceli por 'El tratamiento de los datos sanitarios en la historia clínica electrónica: caso boliviano', en el que describe, entre otros aspectos, la organización del sistema sanitario, políticas y estrategias de salud de Bolivia y analiza el estado de la e-salud en Europa y el nivel de implantación de la historia clínica electrónica en distintos países del mundo.

La Agencia Española de Protección de Datos editó los trabajos galardonados en la categoría de Investigación, que pueden descargarse en la sección 'Publicaciones' de página web de la AEPD.

Esquema de certificación de Delegados de Protección de Datos

El 13 de julio de 2017 la AEPD, en colaboración con la Entidad Nacional de Acreditación (ENAC), presentó su Esquema de certificación de Delegados de Protección de Datos, cuya elaboración contó con la participación de un Comité Técnico de Expertos formado por 23 miembros, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas. Con esta iniciativa, la Agencia se convertía así en la primera autoridad europea en realizar un Esquema de certificación de Delegados de Protección de Datos (DPD).

La creación de este esquema supuso un punto de partida en un proceso de revisión constante que requiere ser alimentado con la experiencia práctica del acreditador y certificador. La AEPD y ENAC suscribieron un convenio de colaboración para coordinar sus actuaciones en el marco de sus respectivas actividades y competencias.

Presentación de la herramienta FACILITA_RGPD

La Agencia Española de Protección de Datos (AEPD) presentó el 6 de septiembre de 2017, con la colaboración de CEOE y CEPYME, FACILITA_RGPD, una herramienta para ayudar a las empresas y profesionales que traten datos personales de escaso riesgo a cumplir con el nuevo Reglamento General de Protección de Datos (RGPD). En el acto de presentación participó el presidente de CEOE, Juan Rosell; el presidente de CEPYME, Antonio Garamendi; y la directora de la AEPD, Mar España. Estas entidades suscribieron un Protocolo General de Actuación para fomentar la difusión del RGPD y de aquellas herramientas, guías y publicaciones realizadas por la Agencia que pudieran servir de ayuda a las empresas en el cumplimiento de sus obligaciones.

Presentación de nuevos materiales para menores, familias y centros docentes

El 19 de octubre la Agencia presentó, junto con el Ministerio de Educación, Cultura y Deporte, nuevos recursos y materiales de ayuda para fomentar la privacidad y la protección de datos de los menores. Este objetivo quedó plasmado en tres proyectos orientados tanto a los centros docentes y el profesorado como al entorno familiar.

La presentación contó con la participación del secretario de Estado de Educación, Formación Profesional y Universidades, Marcial Marín, tras la cual tuvo lugar la entrega de premios de la primera edición del concurso de 'Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet'.

Así, la Agencia presentó la guía 'Protección de datos en centros educativos', un recurso con el que dar respuesta a las dudas más habituales que plantean ante el Canal Joven de la Agencia tanto centros docentes como profesores, AMPAs o las propias familias, sumando además las aportaciones de la comunidad educativa.

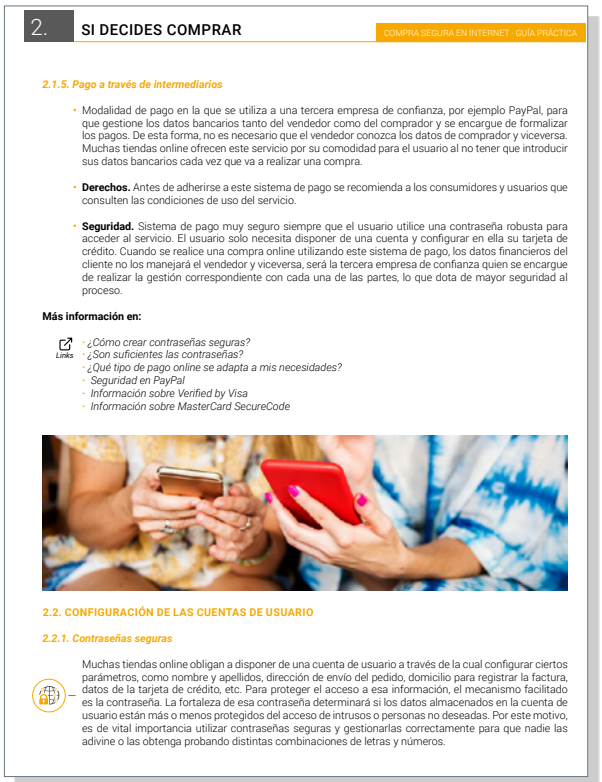
La Agencia también presentó la serie 'Tú controlas en internet', cuatro vídeos que pueden ser visionados tanto en el aula como en familia y que abordan situaciones como el ciberacoso 'En este partido nos la jugamos', el *grooming* 'Planazo de fin de semana', el *sexting* 'Un vídeo muy especial' o la dependencia tecnológica 'Un crack del BMX'.

El tercer proyecto presentado por la Agencia y que se describe en el apartado 2.2.2 de esta Memoria es el taller para familias 'Los menores y su cibermundo', conducido por el experto Ángel-Pablo Avilés, autor de El blog de Angelucho. El taller, que incluye orientaciones y pautas, está compuesto por nueve vídeos de entre dos y diez minutos de duración en los que se abordan temas de interés para los padres a la hora acompañar a sus hijos en su relación con las nuevas tecnologías.

Entrega de los Premios de 'Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet'

La Agencia Española de Protección de Datos entregó el 19 de octubre de 2017 los premios de la primera edición del concurso de 'Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet', tanto en su modalidad de centros educativos, como en aquella que reconoce el compromiso de personas, instituciones, organizaciones y asociaciones. La información relacionada con este premio puede consultarse con más detalle en otro apartado de esta Memoria.

Presentación de la Guía de Compra Segura en internet


2. SI DECIDES COMPRAR

COMPRA SEGURA EN INTERNET. GUÍA PRÁCTICA

2.1.5. Pago a través de intermediarios

- Modalidad de pago en la que se utiliza a una tercera empresa de confianza, por ejemplo PayPal, para que gestione los datos bancarios tanto del vendedor como del comprador y se encargue de formalizar los pagos. De esta forma, no es necesario que el vendedor conozca los datos de comprador y viceversa. Muchas tiendas online ofrecen este servicio por su comodidad para el usuario al no tener que introducir sus datos bancarios cada vez que va a realizar una compra.
- **Derechos.** Antes de adherirse a este sistema de pago se recomienda a los consumidores y usuarios que consulten las condiciones de uso del servicio.
- **Seguridad.** Sistema de pago muy seguro siempre que el usuario utilice una contraseña robusta para acceder al servicio. El usuario solo necesita disponer de una cuenta y configurar en ella su tarjeta de crédito. Cuando se realice una compra online utilizando este sistema de pago, los datos financieros del cliente no los manejará el vendedor y viceversa, será la tercera empresa de confianza quien se encargue de realizar la gestión correspondiente con cada una de las partes, lo que dota de mayor seguridad al proceso.

Más información en:

Links
- *¿Cómo crear contraseñas seguras?*
- *¿Son suficientes las contraseñas?*
- *¿Qué tipo de pago online se adapta a mis necesidades?*
- *Seguridad en PayPal*
- *Información sobre Verified by Visa*
- *Información sobre MasterCard SecureCode*

2.2. CONFIGURACIÓN DE LAS CUENTAS DE USUARIO

2.2.1. Contraseñas seguras

Muchas tiendas online obligan a disponer de una cuenta de usuario a través de la cual configurar ciertos parámetros, como nombre y apellidos, dirección de envío del pedido, domicilio para registrar la factura, datos de la tarjeta de crédito, etc. Para proteger el acceso a esa información, el mecanismo facilitado es la contraseña. La fortaleza de esa contraseña determinará si los datos almacenados en la cuenta de usuario están más o menos protegidos del acceso de intrusos o personas no deseadas. Por este motivo, es de vital importancia utilizar contraseñas seguras y gestionarlas correctamente para que nadie las adivine o las obtenga probando distintas combinaciones de letras y números.

El 18 de diciembre de 2017 la AEPD, el Instituto Nacional de Ciberseguridad (INCIBE), la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y la Policía Nacional presentaron la 'Guía práctica de Compra Segura en internet. Esta iniciativa fue el resultado de un trabajo conjunto para ofrecer a los ciudadanos en una única publicación los consejos prácticos más relevantes a tener en cuenta antes, durante y después de realizar una compra online. La guía, disponible en las respectivas webs de estos organismos, se acompañó de siete fichas que recogen de forma concisa recomendaciones de utilidad.

La presentación corrió a cargo de la directora de la AEPD, la directora ejecutiva de AECOSAN, Teresa Robledo, y el jefe central de Seguridad Ciudadana y Coordinación de la Policía Nacional, José Antonio de la Rosa.

4.1.7. Premios recibidos por la AEPD

Por otra parte, la Agencia Española fue objeto de varios galardones y menciones en 2017 por parte de diferentes instituciones y entidades en reconocimiento a su labor de divulgación y concienciación en los diferentes ámbitos donde despliega su actividad, y en particular:

III Premios ENATIC. La Asociación Nacional de Expertos de la Abogacía Tecnológica hizo entrega a la AEPD del galardón a la 'Mejor institución en derecho digital 2016' en reconocimiento a "su ambicioso Plan Estratégico 2015-2019, que ha supuesto la creación de la Unidad de Estudios Tecnológicos, y por su diálogo y colaboración con las asociaciones profesionales del sector". Estos premios tienen por objeto reconocer y estimular la excelencia profesional, el trabajo y la dedicación, así como la aportación en el ámbito del derecho digital.

XXII Premios Zapping. La Asociación de Consumidores de Medios Audiovisuales de Cataluña (TAC) concedió a la AEPD el premio 'Mejor iniciativa en internet' por su web www.tudecideseninternet.es, orientada a jóvenes, padres y profesores. La TAC es una organización sin ánimo de lucro integrada por más de 17.000 personas, cuyo objetivo, abierto a todos los ciudadanos, es colaborar en la mejora del ocio audiovisual.

Distinción de Colegiada de Honor del CPEIG. El Colegio Profesional de Ingeniería Informática de Galicia (CPEIG) otorgó la distinción de Colegiada de Honor a la Directora de la AEPD "por su apoyo continuo a la difusión de la protección de datos de carácter personal y al uso de las tecnologías de la información como herramienta de progreso, invitando a su vez a la reflexión sobre los peligros de un uso no adecuado", según la candidatura aprobada por la Junta de Gobierno.

Premio a la institución pública de ASCOM. La Asociación Española de *Compliance* (ASCOM) concedió a la AEPD el 'Premio a la institución pública' en la primera edición de unos galardones creados para contribuir al fomento de las buenas prácticas en empresas y organizaciones y de la prevención de la corrupción, así como para destacar la figura del *'compliance officer'*. Con este premio, ASCOM reconocía la labor de la AEPD en relación con la elaboración del esquema de certificación de delegados de protección de datos (DPD), "con el que se ha conseguido ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD", según ASCOM.

4.2. MÁS Y MEJORES SERVICIOS

4.2.1 Sede Electrónica (uso del registro electrónico)

Actualmente, más del 95% de las comunicaciones con la Agencia se realizan en formato electrónico, siendo la sede electrónica el canal prioritario con el 66% de las transacciones.

Todos los nuevos trámites que se generan en el marco del RGPD, se desarrollan en formato electrónico, estando disponibles desde el principio en la sede de la Agencia y siendo esta vía de comunicación obligatoria para las personas jurídicas. Este es el caso de los nuevos servicios de descarga de ficheros inscritos y de registro de delegados de protección de datos.

4.2.2 Digitalización. AEPD Digital

Los sistemas de información de la AEPD han sido dotados de las capacidades determinantes (sistema gestor de expedientes, Sede/Registro Electrónico, Firma Electrónica reconocida y Notificaciones Electrónicas) que permiten convertir los procedimientos tradicionales en procedimientos electrónicos.

En 2017 se han llevado a cabo importantes avances que nos acercan a los objetivos de digitalización marcados en el plan estratégico de la AEPD:

Se ha extendido el uso de la firma electrónica en la práctica totalidad de los trámites de la Agencia, incluyendo el procedimiento de denuncias y tutelas, así como al servicio de consultas al Gabinete Jurídico de la AEPD.

Los sistemas de información de la Agencia ya cuentan con la capacidad de notificación electrónica, incluyendo los servicios electrónicos de la AGE (NOTIFIC@, Carpeta Ciudadana y Dirección Electrónica Habilitada) y el acceso telemático al expediente por parte de los interesados.

Al finalizar el año 2017, este modo de notificación ya está implantado para las personas jurídicas en los procedimientos que representan el principal volumen de tramitación de la Agencia:

- Inscripción, modificación, supresión o cancelación de ficheros
- Denuncias en materia de protección de datos
- Registro de Delegados de Protección de datos
- Recaudación de sanciones
- Consultas generales

Ya es posible acceder a la información de los servicios intermediados de consulta y verificación de identidad, siendo utilizados actualmente en el procedimiento de denuncias y tutelas de derechos.

Finalmente, es importante indicar que la 'plataforma de servicios electrónicos' de la AEPD (pieza tecnológica estructural que da acceso a todos los servicios electrónicos horizontales de las Administraciones Públicas), desarrollada durante el año 2017, ofrece importantes sinergias para los nuevos servicios, siendo previsible un crecimiento en el ritmo de implantación de servicios electrónicos en un futuro.

4.3. SIMPLIFICACIÓN Y MEJORA DE LA GESTIÓN INTERNA DE LA INSPECCIÓN

Las líneas de mejora emprendidas en 2017 están orientadas a los siguientes objetivos:

- Implantación de la Administración Digital. Partiendo de la premisa de que debemos dirigirnos a un modelo de gestión documental enteramente Electrónica, progresivamente se irán modificando los métodos de trabajo. De este modo, podremos generar expedientes electrónicos, desde su nacimiento hasta su archivo. Puesto que la política de gestión documental es transversal y afecta a todas las unidades del organismo, la realización de los cambios en los sistemas de trabajo habrá de llevarse a cabo necesariamente coordinando todas las unidades de la Agencia.

- En relación directa con el punto precedente, cabe subrayar el continuo proceso de estudio y mejora al que se encuentra sometido el sistema SIGRID de la Subdirección General de Inspección de Datos. Con carácter habitual se van introduciendo modificaciones, a la vista de las necesidades manifestadas por los usuarios. No obstante, desde una perspectiva a medio y largo plazo, se está analizando la forma de materializar en SIGRID los grandes cambios en el régimen de procedimiento administrativo asociados al RGPD.

- Simplificación administrativa. Se aprovechará la oportunidad que supone el cambio de normativa (RGPD) para modificar los procedimientos y revisar los documentos, tanto los que se emiten como los que se requieren a los ciudadanos. Todo ello al objeto de reducir, en la medida de lo posible, la carga administrativa.

- A su vez, el cambio importante en las normas y en los procedimientos lleva implícito la conveniencia de adecuar la estructura funcional y organizativa de la Subdirección de Inspección de Datos. La finalidad perseguida es, en primer término, lograr que los procedimientos discurran con fluidez de unas unidades a otras. En segundo lugar, se pretende avanzar hacia una relación más ágil entre las distintas unidades. Todo ello redundará, en conjunto, en un trabajo más eficiente. Por último, los ajustes en el esquema organizativo de la Subdirección también responden a la necesidad de mantener, con carácter permanente, intensas relaciones de colaboración con las autoridades de protección de datos del ámbito europeo y nacional.

- Perfeccionamiento de la capacitación de los empleados públicos. La aplicación del RGPD, con las novedades que introduce, aconseja que la Agencia promueva un refuerzo específico en los programas de formación del personal de las Administraciones Públicas, siendo de capital importancia la consolidación de la formación del personal de la Agencia.

4.4. PROGRAMA PILOTO DE TELETRABAJO

Con el objeto de mejorar la calidad de la prestación de los Servicios Públicos, durante el año 2017 se implantó mediante Resolución de la Directora de 24 de noviembre de 2016 un Programa Piloto de Teletrabajo con el objeto de adquirir la experiencia necesaria para considerar en el futuro su extensión. Tras finalizar el 'Programa Piloto' de Teletrabajo en el que han participado 17 funcionarios de las distintas áreas de la AEPD durante 6 meses, se ha realizado un estudio pormenorizado de la adaptación de los trabajadores de la Agencia Española de Protección de Datos a esta modalidad de trabajo, así como los efectos del mismo en el funcionamiento de toda la organización, valorándose muy positivamente la experiencia en su conjunto.

En virtud de lo dispuesto anteriormente se aprobó el 'Programa de Teletrabajo' de la 'Agencia Española de Protección de Datos', publicitando la convocatoria para el año 2018. Mediante Resolución de 14 de diciembre de 2017 se han nombrado los 47 empleados públicos que participarán en el programa de teletrabajo correspondiente al año 2018, lo que supone un 27% de la plantilla de funcionarios. Esta organización del trabajo sitúa a la AEPD dentro de los organismos punteros en lo referente a conciliación de la vida familiar y laboral, mejorando así el atractivo que supone su Relación de Puestos de Trabajo para profesionales de la Función Pública.

4.5. NECESIDADES DE RECURSOS HUMANOS Y MATERIALES

La Agencia Española de Protección de Datos se enfrenta desde hace tiempo a dificultades para hacer frente a la creciente carga de trabajo, derivadas de dos circunstancias: por una parte la Relación de Puestos de Trabajo no se había modificado desde 2008 para adaptarse a la evolución que ha experimentado el uso de las nuevas tecnologías, y por otra parte no disponía de un crédito de incentivos al rendimiento suficiente para ofertar productividad a los puestos que la precisan.

A partir de mayo de 2018 con la entrada en vigor del Reglamento General de Protección de Datos se plantea un nuevo escenario con importantes variaciones en la carga de trabajo que la AEPD debe asumir, por lo que durante este ejercicio se han intensificado esfuerzos para lograr la adecuación de sus medios materiales y de sus Recursos Humanos.

Los incrementos obtenidos tras las negociaciones llevadas a cabo con el Ministerio de Hacienda y Función Pública (MINHFP) han sido los siguientes:

- Un incremento de 11 puestos de trabajo de niveles 26 y 28 que se han distribuido entre las distintas unidades de la AEPD en función de sus necesidades con importantes refuerzos de la Subdirección General de la Inspección de Datos y de la Unidad de Evaluación y Estudios Tecnológicos.

- Se han asignado por el MINHFP 8 puestos de la Oferta Empleo Público cubiertos por funcionarios de nuevo ingreso de los Cuerpos Superior de Administradores Civiles del Estado, Superior de Técnicos de Sistemas y Tecnologías de la Información, del Cuerpo de Gestión que se incorporarán próximamente y tres auxiliares administrativos.

- Un incremento de 120.000 € en el crédito de productividad ordinaria que se ha dedicado a dar de alta en este complemento a aquellos puestos en los que, aun siendo necesaria una dedicación horaria especial, no pudieron ser dotados antes por no disponer de crédito suficiente.

- La aprobación de un programa de productividad adicional por consecución de objetivos diseñado en base a los siguientes indicadores: Avance de ejecución del Plan Estratégico 2015-2019, Volumen de denuncias y reclamaciones de la Subdirección General de Inspección de Datos, Reducción de los tiempos medios de actuación de la SGID, Reducción del tiempo medio de respuesta a consultas ciudadanas y, por último, incremento de comunicaciones telemáticas.

- También se han dedicado importantes esfuerzos a la mejora de la formación interna de los funcionarios de la AEPD.

5. Una agencia cercana a los responsables y profesionales de la privacidad

Procesos de selección de funcionarios de la AGE

Dentro de la estrategia de difusión de conocimientos sobre protección de datos en el sector público, desde la AEPD se ha impulsado la introducción de un tema sobre protección de datos en los programas de todos los procesos selectivos gestionados por la Secretaría de Estado de Función Pública, con diferente grado de dificultad en función del grupo de titulación al que pertenezcan los diferentes Cuerpos y Escalas.

En línea con lo anterior, y con el fin de que esta materia se incorpore de una manera transversal y similar en los procesos selectivos para el ingreso en los Cuerpos y Escalas de funcionarios adscritos a los Departamentos ministeriales, se ha solicitado la inclusión de un tema sobre protección de datos en los procesos selectivos que gestionen los diferentes ministerios.

5.1. RECURSOS PARA FACILITAR EL CUMPLIMIENTO DEL RGPD POR LOS RESPONSABLES

5.1.1 Para las pymes

Convenio CEOE y CEPYME

Desde la adopción del Reglamento General de Protección de Datos (RGPD) la Agencia ha venido desarrollando una serie de recursos destinado a facilitar el conocimiento y la comprensión, así como la adaptación de los responsables y encargados del tratamiento al nuevo marco normativo.

En la labor de impulso y promoción de estos recursos y materiales entre las empresas, la Agencia suscribió un Protocolo General de Actuación con CEOE y CEPYME con la finalidad de facilitar, en el marco de sus respectivas actividades y competencias, la más amplia difusión de los principios del RGPD y de las herramientas, guías y publicaciones, en particular la herramienta FACILITA_RGPD, que puedan ayudar a las empresas en el cumplimiento de las obligaciones que establece el RGPD, sobre todo a las pequeñas empresas que, debido a la especial importancia que desempeñan en la economía española, constituyen uno de los objetivos prioritarios para la Agencia como lo recoge en su Plan Estratégico .

En el acto de la firma del Protocolo, el 6 de octubre, se presentó públicamente la herramienta FACILITA_RGPD.

La ejecución del Protocolo ha dado lugar a la organización y celebración de jornadas informativas sobre el impacto del RGPD en las empresas, que incluyen la presentación de los recursos puestos a su disposición para su cumplimiento, en especial de la herramienta FACILITA_RGPD, con las Federaciones de Empresarios de Valladolid, de Toledo, de Cantabria y la Confederación de Empresarios de Andalucía.

Colaboración con la Unión Profesional. Jornadas sectoriales

Otro de los colectivos a los que la Agencia presta una especial atención es el de las profesiones cuyo ejercicio está sujeto a colegiación en la correspondiente corporación, y que también tratan datos de carácter personal en el ejercicio de su actividad.

La Agencia, en cumplimiento de la obligación de promover la sensibilización entre los responsables del tratamiento del cumplimiento del RGPD, mantiene contactos periódicos con la Unión Profesional, que agrupa a 33 Consejos y Colegios Generales que comprenden cerca de 1.000 colegios profesionales y millón y medio de profesionales liberales, que dieron lugar a la celebración de una sesión sobre 'Protección de datos en las corporaciones colegiales' celebrada el 11 de octubre, durante la que se realizó una presentación práctica de la herramienta FACILITA_RGPD para aquellos profesionales que por las características de su actividad les pueda ser de utilidad para la aplicación del RGPD, además del resto de recursos disponibles.

Herramienta FACILITA_RGPD

La herramienta FACILITA_RGPD es un recurso de ayuda disponible a través de la web de la AEPD y su uso es gratuito. La información que las empresas aportan no es conservada ni monitorizada por la Agencia de forma alguna.

La herramienta FACILITA_RGPD se estructura en cuatro fases, la primera de ellas tiene por objeto excluir aquellos tratamientos de datos personales que, por el sector de actividad de una organización, la propia tipología del tratamiento o los datos involucrados, requiera un análisis de riesgo; dicho de otra forma la herramienta en esta fase excluye los tratamientos que no impliquen un escaso riesgo para los derechos y libertades de las personas. En una segunda fase, la herramienta solicita información acerca del responsable del tratamiento para pasar a una tercera fase en la que solicita información relativa a cada uno de los tratamientos de datos personales que lleva a cabo, así como sobre los encargados del tratamiento para cada caso. Finalmente, la herramienta proporciona a los responsables o encargados del tratamiento que utilicen esta herramienta, un documento en el que se facilita la información necesaria para su adecuación al RGPD.

En concreto, los responsables y encargados del tratamiento, con esta herramienta obtienen un borrador para crear su registro de actividades de tratamiento, cláusulas informativas para cumplir con el deber de información en la recogida de datos personales, cláusulas contractuales a incluir en los contratos de encargado del tratamiento y un anexo con medidas de seguridad mínimas que deben ser tenidas en cuenta sin perjuicio de otras que, por la especificidad de cada tratamiento, pudieran ser necesarias.

Tras la puesta en marcha de esta herramienta el 6 de septiembre y hasta finales de 2017, se han registrado más de 29.000 accesos a la misma, de los cuales más de 9.000 han sido descartados en la primera fase de esta herramienta y un total de 6.177 finalizaron y obtuvieron el documento o la hoja de ruta para la adecuación al RGPD.

Desde su puesta en marcha, esta herramienta ha ido recogiendo las sugerencias de mejora propuestas por asociaciones de profesionales y por profesionales de la protección de datos.

Otras actuaciones de sensibilización

Igualmente con la finalidad de informar, sensibilizar y facilitar el proceso de adaptación al RGPD, se han mantenido reuniones con la Cámara de España y la Asociación de Trabajadores Autónomos (ATA), así como con la Asociación Española de Profesionales de la Privacidad (APEP) e ISMS Fórum.

Plan de difusión del RGPD en las CCAA (sesiones dirigidas al sector público y al sector privado)

El nuevo marco normativo establecido por el RGPD tiene un fuerte impacto sobre los ciudadanos, las empresas y las Administraciones Públicas, y requiere un importante esfuerzo para adaptarse a sus previsiones.

La AEPD desplegó en los últimos meses de 2017 una intensa labor de concienciación, información y formación organizando diversos tipos de actividades dirigidas a los sectores afectados, con el objetivo de que estén preparados en el momento que el RGPD sea aplicable a partir del 25 de mayo de 2018.

Destaca en este contexto la programación de jornadas informativas en las comunidades autónomas sobre las novedades en materia de protección de datos establecidas por el RGPD, en las que se ha querido llegar tanto al sector público como al sector empresarial.

El objetivo es celebrar en cada comunidad autónoma dos sesiones: una dirigida al sector público coorganizada con el correspondiente centro o instituto de formación autonómico y otra dirigida al sector empresarial coorganizada con organizaciones y asociaciones de empresarios de ámbito autonómico. Las jornadas han sido impartidas por personal especializado de la AEPD y se dirigen a personas que desarrollan funciones y tienen responsabilidades en el ámbito de la protección de datos en las respectivas organizaciones.

La sesión dirigida al sector público de las CCAA es similar a la que se organizó el 14 de septiembre de 2017 en la sede del Instituto Nacional de Administración Pública (INAP), en la que la AEPD trasladó información sobre el impacto del nuevo marco normativo en las Administraciones Públicas y la nueva figura del Delegado de Protección de Datos a un auditorio de alrededor de 100 empleados públicos de la AGE y de las CCAA.

La sesión dirigida al sector empresarial pretende igualmente difundir y sensibilizar a empresas y profesionales sobre el nuevo marco normativo y ha venido acompañada de la difusión de FACILITA_RGPD, la herramienta desarrollada y puesta a disposición por la AEPD para ayudar a las empresas y profesionales a conocer, de la manera más sencilla posible, las implicaciones y los cambios que supone la nueva normativa, de forma que puedan tomar las medidas necesarias.

Al finalizar 2017 la AEPD había celebrado encuentros en once CCAA, teniendo previsto proseguir con estas jornadas en los primeros meses de 2018, con el fin de llegar de manera muy directa a estos sectores en todo el territorio español.

Su detalle es el siguiente:

CCAA	FECHA JORNADA
Galicia	29 de septiembre 2017
Castilla-La Mancha	15 noviembre 2017
Canarias	21 y 22 noviembre 2017
Cantabria	22 noviembre 2017
Aragón	22 de noviembre 2017
Navarra	24 noviembre 2017
Murcia	28 noviembre 2017
Madrid	30 noviembre 2017

CCAA	FECHA JORNADA
Castilla y León	1 diciembre 2017
Andalucía	12 diciembre 2017
Baleares	12 diciembre 2017
Valencia	25 enero 2018
Asturias	14 de febrero 2018
La Rioja	21 febrero 2018
Extremadura	12 abril 2018

5.1.2 Administraciones Públicas

Formación para empleados de las Administraciones Públicas

Junto a esta labor de difusión e información, la AEPD está desarrollando una labor formativa dirigida a las distintas Administraciones Públicas articulada principalmente a través de la línea de colaboración establecida con el INAP.

En este sentido, la Agencia, continuando una dilatada trayectoria en la realización de programas de formación para empleados públicos en el conocimiento y la aplicación práctica de la materia de protección de datos en la actividad pública, puso en marcha durante 2017 un curso específico de formación online para funcionarios sobre las principales novedades del Reglamento, del que se desarrollaron tres ediciones en las que participaron 120 empleados públicos de la AGE, CCAA y Entidades Locales.

En 2018 la cooperación entre la AEPD y el INAP para ofrecer formación sobre el Reglamento también contempla, además de diversas ediciones del curso online mencionado, la celebración en 2018 de una sesión sobre los pasos a seguir para adaptar las organizaciones públicas al RGPD y de un curso de formación especializada dirigida específicamente a los Delegados de Protección de Datos designados.

Estas dos últimas acciones formativas tendrán una versión dirigida específicamente a funcionarios de Entidades Locales, ya que en la planificación de estas se ha tenido siempre muy presente la necesidad de atender las especialidades de los entes que componen la Administración Local en relación con los tratamientos de datos de carácter personal que realizan. Por ello, se vienen organizando acciones dirigidas específicamente a esta Administración, colaborando con entidades como la Federación Española de Municipios y Provincias (FEMP), con quien se ha firmado un Protocolo General de Actuación, o el Consejo General de Colegios de Secretarios, Interventores y Tesoreros de Administración Local (COSITAL), por el gran colectivo que agrupa y su capacidad de difusión a toda su red de asociados.

Entre estas acciones destacan las jornadas informativas para Ayuntamientos y Diputaciones Provinciales celebradas en colaboración con la FEMP en octubre y diciembre de 2017, para analizar las implicaciones del RGPD en el ámbito de la Administración local, y en especial la relativa a la implantación de la figura del Delegado de Protección de Datos, sobre todo en las entidades locales de menor tamaño.

Herramienta de análisis de riesgo microPILAR

El Esquema Nacional de Seguridad establece la necesidad de utilizar una metodología de análisis de riesgos para que las Administraciones Públicas puedan determinar las medidas de seguridad necesarias para proteger su información. Esta exigencia se prevé en el artículo 32 del RGPD sobre la seguridad de los datos personales para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

El CCN pone a disposición de las Administraciones Públicas la herramienta de análisis de riesgos PILAR basada en la metodología de análisis de riesgos MAGERIT para los sistemas de la información, a la que es necesario incorporar los mecanismos pertinentes para facilitar la adecuación de las administraciones públicas al enfoque de riesgos del RGPD. Esta línea de colaboración supone hacer uso de los conocimientos y recursos de análisis y gestión de riesgos que ya están implantados en las Administraciones Públicas para la adecuación de las Administraciones al RGPD.

Con este objetivo, CCN-CERT y la AEPD han establecido un mecanismo de colaboración para ofrecer a las administraciones públicas una herramienta de análisis de riesgos que constituya una metodología única que permita abordar tanto los riesgos para los sistemas de información como los riesgos para los derechos y libertades de los ciudadanos.

Como resultado de esta colaboración, la herramienta PILAR ha sido dotada de un módulo de cumplimiento normativo que permite a las Administraciones Públicas verificar los requisitos establecidos en el RGPD. La línea de colaboración para adecuar la herramienta PILAR seguirá evolucionando y dará lugar a nuevas versiones de la herramienta. Complementariamente, se está trabajando para facilitar la tarea de efectuar las notificaciones de brechas de seguridad de las Administraciones Públicas.

5.1.3. Funcionalidad para obtener de forma automatizada y editable copias de la inscripción de ficheros

Ante la supresión de la obligación de notificar los ficheros a la autoridad de control a partir del 25 de mayo de 2018 y la obligatoriedad de que aquellos que traten datos elaboren un Registro de Actividades de Tratamiento, la Agencia, en el mes de noviembre, lanzó una nueva funcionalidad del servicio de solicitud de copia del contenido para las inscripciones de los ficheros en su Sede Electrónica. Esta funcionalidad permite obtener en un fichero editable (Excel o XML) una copia del contenido completo de la inscripción de ficheros por su responsable, de manera que este pueda servir como orientación para la elaboración del Registro de Actividades del Tratamiento que los responsables deben llevar.

5.1.4 Códigos Tipo

El Reglamento General de Protección de Datos, en su considerando 98 y en su artículo 40, insta a las autoridades de protección de datos, entre otras, a impulsar entre las asociaciones u otros organismos que representen a categorías de responsables o encargados la elaboración de códigos de conducta que, respetando los límites del Reglamento, faciliten su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y, en particular, de las pymes.

A su vez, el proyecto de LOPD, en tramitación parlamentaria en el momento en el que se cierra el texto de esta Memoria, prevé que también se puedan promover por empresas o grupos de empresas, así como por las Administraciones Públicas y las entidades pertenecientes al sector público, además de por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el RGPD.

Los códigos de conducta se constituyen como instrumentos de autorregulación que deben facilitar el cumplimiento del RGPD, teniendo en cuenta las características específicas del tratamiento llevado a cabo por determinados sectores y las necesidades específicas de los tratamientos de datos efectuados por quienes se adhieren a los mismos, aportando valores añadidos de garantía, calidad y confianza en materia de protección de datos.

La Agencia cuenta con experiencia en este ámbito, pues ya se recogían los códigos de conducta en la Directiva 95/46 y cuya regulación fue desarrollada por la LOPD y su Reglamento, habiéndose acordado la inscripción en el Registro General de Protección de Datos de 16 códigos tipo, y encontrándose en proceso de revisión otros nuevos proyectos.

La adopción de un código tipo o de conducta por un sector de actividad aporta garantías adicionales a la voluntad y el compromiso de la entidad que se adhiere a dicho código, además de transparencia en el tratamiento de los datos.

Además de asesorar a los promotores de los códigos tipo inscritos para que adapten su contenido para una correcta aplicación del RGPD, la Agencia viene manteniendo reuniones y contactos con representantes de diversos sectores de actividad al objeto de promover la elaboración de códigos de conducta, que habrán de tener en consideración las necesidades específicas de los responsables y encargados de los tratamientos.

Los códigos de conducta se constituyen como instrumentos de autorregulación que deben facilitar el cumplimiento del RGPD

Durante el año 2017 se ha constatado un mayor interés por la figura de los códigos tipo o códigos de conducta, que probablemente hay que atribuir a la cercanía de la aplicación del RGPD para estar en disposición, lo antes posible, de adaptar los tratamientos que regulan a la nueva normativa y beneficiarse de los incentivos que se establecen para estos instrumentos, como servir a los responsables del tratamiento para poder demostrar el cumplimiento de las obligaciones que el RGPD estipula.

En 2017 se han presentado formalmente cinco solicitudes de inscripción de códigos tipo, en algunos casos incorporando adaptaciones al RGPD, cuya evolución ha sido la siguiente:

La Universidad Nacional de Educación a Distancia presentó una primera solicitud de inscripción de código tipo de la que desistió para posteriormente reiterarla, estando pendiente de resolución a la finalización de 2017.

La Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) solicitó la inscripción del 'CÓDIGO TIPO DEL FICHERO DE PREVENCIÓN DEL FRAUDE EN SEGUROS DE RAMOS DIVERSOS CÓDIGO TIPO DEL FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL', que fue objeto de inscripción en el Registro General de Protección de Datos por resolución de 11 de diciembre, y del 'CÓDIGO TIPO DEL FICHERO DE INDEMNIZACIONES A PERJUDICADOS EN ACCIDENTES DE TRÁFICO' que, tras desistimiento del promotor, fue archivada por resolución de igual fecha.

La Asociación Nacional de Empresas de Investigación de Mercados y Opinión Pública (ANEIMO) y la Asociación Española de Estudios de Mercado, Marketing y Opinión (AEDEMO) han solicitado la inscripción del 'CÓDIGO DE CONDUCTA PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR ORGANIZACIONES DE INVESTIGACIÓN DE MERCADOS, SOCIAL Y DE LA OPINIÓN Y DEL ANÁLISIS DE DATOS', cuya resolución se encontraba pendiente al finalizar 2017.

Asimismo, durante el año 2017, se han mantenido reuniones y conversaciones para su asesoramiento con los promotores de los proyectos de códigos tipo que se citan a continuación, de los que de algunos de ellos se han recibido borradores que se han analizado al objeto de revisar su contenido:

Con la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) sobre la modificación del 'CÓDIGO TIPO DEL FICHERO DE AUTOMÓVILES PERDIDA TOTAL, ROBO E INCENDIOS'.

Con la Unión Catalana de Hospitales (UCH) para la modificación de su código tipo 'CÓDIGO TIPO DE LA UNIÓN CATALANA DE HOSPITALES'.

Con la asociación Española de Microprés-tamos (AEMIP) sobre el proyecto de código tipo 'CÓDIGO TIPO DE LA ASOCIACIÓN ESPAÑOLA DE MICROPRÉSTAMOS'. AEMIP.

Con la Asociación Multisectorial de la Información (ASEDIE), sobre el proyecto de 'CÓDIGO DE CONDUCTA DEL SECTOR INFOMEDIARIO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL'.

Con Kumon sobre el proyecto de 'CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES KUMON'.

Con la Unión de Federaciones Deportivas Madrileñas (UFEDEMA) sobre el proyecto de 'CÓDIGO DE CONDUCTA PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIÓN DE FEDERACIONES DEPORTIVAS MADRILEÑAS'.

5.1.5. Consultas al Gabinete Jurídico

En cuanto a las consultas de mayor complejidad dirigidas a facilitar la aplicación de la LOPD a los responsables de tratamientos públicos y privados, se atendieron un total de 334, de las cuales 206 (62%) fueron planteadas por las Administraciones Públicas y 128 (38%) por el sector privado.

Se produce así una disminución de un 13.5% en el volumen de consultas planteadas respecto a las formuladas el año anterior, produciéndose una disminución significativa en las consultas formuladas por el sector público, que disminuyen desde un 45.5% a un 38% del total, al tiempo que se mantiene prácticamente inalterado el número de consultas procedentes del sector público (211 en 2016 y 206 en 2017). Ello se debe a que parte de las consultas que plantean una problemática más sencilla han sido atendidas por otras unidades de la Agencia, reservándose el informe del Gabinete Jurídico a las que revisten mayor complejidad.

En cuanto a las materias objeto de consulta destacan las siguientes conclusiones:

- El mantenimiento de un número relativamente significativo de consultas relacionadas con las cesiones de datos de carácter personal, que sigue siendo la cuestión objeto de un mayor número de las mismas, pese a que en 2017 se produce una disminución de su número de en torno al 5%.

- La importante disminución de las cuestiones relacionadas con el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (un 67%), así como de las relacionadas con la videovigilancia (un 70%).

- El incremento de la importancia relativa de las cuestiones relacionadas con los requisitos del consentimiento, que en los últimos dos años han aumentado desde el 16% en 2015 hasta el 31% en 2017, incrementándose además en términos absolutos un 20% respecto de las planteadas en el ejercicio anterior. Ello se debe probablemente a las modificaciones que sobre esta materia se derivan de la entrada en vigor del Reglamento General de Protección de Datos.

- El lógico crecimiento de las cuestiones concretas relacionadas con el Reglamento General de Protección de Datos, que representan más del 17% del total y que han ido incrementándose de forma paulatina a lo largo del ejercicio.

- El repunte en un 50% de las cuestiones relacionadas con la implantación de medidas técnicas y organizativas encaminadas a garantizar la seguridad de los datos, teniendo en cuenta el nuevo régimen de responsabilidad activa establecido en el Reglamento general de Protección de Datos.

- El significativo incremento, de un 43%, de las cuestiones relacionadas con el tratamiento de datos que tienen que ver con la salud.

- El mantenimiento en términos prácticamente idénticos al ejercicio anterior de las cuestiones relacionadas con la conciliación de las normas de protección de datos con el principio de transparencia y el acceso a la información pública, la aplicación de la regla de legitimación basada en la prevalencia del interés legítimo y el régimen del encargado del tratamiento.

- El incremento significativo de las consultas relacionadas con el tratamiento de datos en el ámbito de las comunicaciones electrónicas (un 87%), los ficheros de titularidad pública (un 13%) y el ámbito de aplicación de las normas de protección de datos (un 11%).

- La importante disminución de las consultas relacionadas con el deber de informar (un 54%), los principios de calidad de datos (un 27%) o las transferencias internacionales de datos (un 23%).

Dentro del sector público el peso de las consultas formuladas por las distintas Administraciones Territoriales y la Administración Corporativa y los Órganos Constitucionales se mantiene en términos parcialmente similares a los del año 2016, si bien se produce un descenso de más del 2.5% del peso de las consultas formuladas por la Administración General del Estado y sus Organismos vinculados o dependientes, que en términos absolutos supone una disminución de en torno al 8%. Por el contrario, las consultas planteadas por las Entidades Locales incrementan su peso en prácticamente un 5%. En cuanto al sector privado, atendiendo a la distribución sectorial de las consultas, las principales conclusiones son:

- El muy notable incremento de casi un 35% de las consultas planteadas por operadores de telecomunicaciones y prestadores de servicios de la sociedad de la información, representando casi una cuarta parte del total, con lo que se convierte en el sector con mayor número de consultas.

- El mantenimiento de un buen número de cuestiones planteadas por particulares, si bien reduciendo su número en un 40%.

- En este mismo sentido se duplican las consultas planteadas por sindicatos y partidos políticos, lo que devuelve las cifras a valores similares a los del año 2014.

- El significativo incremento de las cuestiones planteadas por centros docentes (que pasan de una sola en 2016 a cinco en 2017), así como las procedentes de los sectores de la publicidad y banca y seguros, que se multiplican por dos en este ejercicio.

- La disminución muy sustancial de las consultas formuladas por los sindicatos (un 67%) y las empresas energéticas (un 80%).

- La inexistencia de informes procedentes de las empresas de distribución, solvencia patrimonial, seguridad u hostelería, que en 2016 representaban entre todas sin embargo casi un 10% del total.

Los informes no preceptivos relacionados con consultas externas que pueden revestir una mayor trascendencia, versan, entre otras, sobre las siguientes materias:

- La consideración de que las direcciones IP ya sean estáticas o dinámicas, constituyen datos personales, no siendo posible considerar que por el mero hecho de que los interesados hayan participado en campañas de marketing ello signifique que dichos interesados acepten de forma inequívoca el uso y tratamiento de sus datos personales por terceros para una finalidad distinta.

- El carácter de dato personal de la matrícula de un vehículo que contrata un parking “por tiempo” de acuerdo con la ley 40/2002, de 14 de noviembre, reguladora del contrato de aparcamiento de vehículos, porque el dato de la matrícula puede identificar no sólo al dueño sino también al conductor del vehículo.

Las Entidades Locales acudieron al Gabinete Jurídico de la AEPD un 5% más que en años anteriores

- La necesidad de que se determine individualizadamente si resulta preciso recabar el certificado negativo del Registro Central de delincuentes sexuales de los trabajadores de un parque temático, a fin de establecer qué perfiles profesionales implican un contacto directo y regular con los menores, no siendo preciso obtenerlo de todo el personal, sino de quienes, por ejemplo, desarrollen tareas de monitor en talleres para niños, celebraciones de cumpleaños y comuniones o quienes realicen habitualmente labores de guía o acompañante para los niños.

La delimitación de los diversos supuestos en que los tratamientos de datos llevados a cabo por las entidades financieras de crédito para fines distintos del mantenimiento de la relación contractual con sus clientes podrían considerarse amparado en la existencia de un interés legítimo prevalente de dichas entidades.

La licitud de la realización de determinados tratamientos a partir de datos accesibles en redes sociales al tratarse de proyectos de investigación aprobados en el Programa 'Horizonte 2020' de la Unión Europea, siempre que se limiten al tratamiento para fines de investigación y se implanten las necesarias garantías de cumplimiento de los principios previstos en la normativa de protección de datos.

Por el contrario, se considera contraria a los principios de calidad de datos la recopilación a través de un software específico de toda la información accesible de un usuario en todas las redes sociales, no siendo suficiente ampararla en el artículo 7 f) de la Directiva 95/46/CE.

La licitud de la captación de imágenes por cámaras de videovigilancia en un establecimiento abierto al público (Spa en un hotel) al amparo de la existencia de un interés legítimo de su titular (en este caso por razones de seguridad), siempre y cuando se diferencie entre zonas comunes de uso público (vasos de las piscinas, pasillos, etc.) en los cuales los usuarios de las piscinas conocen que son o pueden ser observados por otros usuarios y en los cuales su derecho a la intimidad ha de convivir con dichos terceros, de otras zonas que, aun siendo también de uso público, las personas pueden legítimamente pretender excluir a cualquier otro en aras de una protección de su derecho a la intimidad (aseos, vestuarios, etc.).

La conformidad a derecho de que un padre que está abonando una pensión por alimentos a un hijo, mayor de edad, pueda conocer las calificaciones académicas de dicho hijo, aunque no satisfaga directamente cantidad alguna por los estudios del hijo, sobre la base de la existencia de un interés legítimo consistente en la posibilidad de solicitar la exoneración de la obligación de alimentos como consecuencia del retraso de su hijo en los estudios.

La licitud del acceso por una empresa a los datos relativos a la existencia de una situación de discapacidad o de mejora de esta en el trabajador, a través de la liquidación de la TGSS, en la medida que la misma puede dar lugar a la aplicación de un tipo de cotización diferente en la contingencia de desempleo en los contratos de duración determinada. El acceso no se extiende, sin embargo a la causa de dicha discapacidad.

La conformidad con la normativa de protección de datos de que una entidad bancaria entregue al titular de una cuenta corriente los datos personales mínimos necesarios para identificar a quien ha cobrado indebidamente un cheque que ha sido cargado en la cuenta corriente bancaria de dicho titular.

La licitud del tratamiento de los datos necesario para el cumplimiento por un sujeto obligado de las medidas de diligencia debida establecidas en la legislación de prevención del blanqueo de capitales y la financiación del terrorismo, sin que sea exigible a la vista de la normativa vigente recabar el consentimiento de los interesados, dado que se trata de un tratamiento necesario para el cumplimiento de obligaciones legales.

La conformidad con la normativa de protección de datos de la entrega sin consentimiento de los contribuyentes por la concesionaria cuyo contrato se ha extinguido de los datos personales necesarios para la prestación del servicio (en este caso de suministro de aguas) a la Administración a la cual revierte el servicio.

La licitud de la solicitud por un Ayuntamiento a un centro de mayores de los datos de los residentes a fin de incorporarlos al Padrón Municipal de Habitantes, al estar obligada la corporación al mantenimiento actualizado del Padrón.

La licitud de la cesión por la Administración Tributaria a la Inspección de Trabajo, sin mediar requerimiento de colaboración previo, de datos relevantes para el desempeño de las competencias de ésta última, al existir habilitación legal expresa en la Ley general Tributaria y en la Ley 23/2015.

La licitud de la cesión de determinados datos personales (número de afiliación, DNI, nombre y apellidos, domicilio y entidad de adscripción) de los beneficiarios de la asistencia sanitaria prestada por entidades privadas concertadas con MUFACE residentes en municipios en que no exista un "convenio rural", a fin de que los servicios públicos de salud puedan conocer el colectivo a quienes pueden tener que prestar el servicio sanitario, por ser necesario para la prestación de la asistencia sanitaria.

La posibilidad de grabación de las sesiones del consejo escolar siempre que se encuentre prevista en su Reglamento de funcionamiento sin perjuicio del derecho de oposición que pueda ser ejercido por los interesados.

La licitud de la cesión a un Consulado de datos de prestaciones sociales concedidas a un menor extranjero, legitimada en el Convenio de Viena de 1963 sobre Relaciones Consulares, por constituir una de las funciones consulares velar por los intereses de los menores dentro de los límites que impongan las leyes y reglamentos del Estado receptor.

La disconformidad con la legislación de protección de datos de la grabación a través de dispositivos particulares de los miembros de las Fuerzas y Cuerpos de Seguridad y el envío telemático de fotografías de las personas a quienes se intenta identificar en la vía pública en virtud de la Ley de protección de la seguridad ciudadana.

La inexistencia de legitimación para la publicación de los datos referidos a las personas a las que se refieren determinadas muestras incautadas en una operación de lucha contra el dopaje, teniendo en cuenta que no se llegó a abrir respecto de las mismas procedimiento sancionador alguno.

La inexistencia de amparo que legitime la cesión de datos de evaluación del desempeño de los trabajadores de una empresa para su posterior publicación en este mismo ámbito.

La necesidad de que se establezcan garantías adicionales de los derechos de los afectados para que pueda ampararse en el interés legítimo el establecimiento de un sistema de identificación en un comercio

para lograr la identificación de quienes cometen pequeños hurtos, guardando una plantilla que permite al sistema de videovigilancia la detección de dicha persona cuando entra de nuevo en el centro comercial.

- La posible vulneración del principio de proporcionalidad en la videovigilancia y captación de la imagen y voz de empleados y personas que acceden a los edificios municipales, en la medida que el sistema va a permitir captar comentarios privados.

- La posible vulneración del principio de proporcionalidad en la instalación de cámaras para grabar exámenes con el fin de disuadir a los estudiantes de determinadas actuaciones fraudulentas durante los mismos, teniendo en cuenta que el Dictamen 4/2004 del grupo de Trabajo del artículo 29 considera que la utilización de estos sistemas sólo debe tener lugar con carácter subsidiario.

- La falta de legitimación suficiente para replicar y hacer pública una base de datos privada con los datos personales de funcionarios objeto de publicación en boletines oficiales, dado que no puede considerarse amparada, a diferencia de la publicación oficial, en el principio de transparencia, sino que supone una publicidad añadida, no prevista en la ley y una restricción aún mayor del derecho a la protección de datos.

- La falta de base legítima suficiente para la realización de una tratamiento que mide la popularidad del afectado a partir de los datos disponibles de fuentes accesibles al público como boletines oficiales o medios de comunicación, sin que sea posible acudir en este caso al artículo 7 f) de la Directiva 95/46/CE.

- La procedencia de llevar a cabo una interpretación estricta de la normativa estadística en lo que afecta al acceso de datos especialmente sensibles de fuentes distintas del interesado, teniendo en cuenta que se establece el principio de aportación estrictamente voluntaria de los interesados, de modo que el acceso sólo tenga lugar cuando la norma interna o de la Unión Europea exija tratar estos datos.

- El deber de conservación de las historias clínicas durante el plazo establecido en la ley, aun cuando la entidad clínica responsable del fichero se encuentre en situación concursal.

- La necesidad de que la Administración Tributaria proceda a disociar, mediante su difuminado, los datos referidos a las imágenes de las personas que puedan encontrarse en mesas o veladores situadas en la vía pública, captadas en el ejercicio de funciones inspectoras para la verificación de los elementos del tributo antes de incorporar la imagen al expediente administrativo.

- El alcance del derecho a la portabilidad de los datos, teniendo en cuenta las directrices adoptadas por el Grupo de Trabajo del artículo 29, indicando que no puede establecerse de forma genérica un límite temporal en cuanto a los datos que podrán ser objeto de este derecho, debiendo tenerse en cuenta las condiciones en que se lleva a cabo el tratamiento por parte del responsable.

- La necesidad de adopción de medidas de seguridad adicionales para el tratamiento de datos en dispositivos propios del interesado, tomando en consideración las recomendaciones del *International Working Group on Data Protection in Telecommunications*, en su documento de trabajo sobre privacidad y los riesgos de seguridad con el uso de “dispositivos propios” en redes corporativas, adoptado en Berlín en 2014.

5.2. COLABORACIÓN CON LOS PROFESIONALES DE LA PRIVACIDAD

5.2.1. Colaboración con Asociaciones de profesionales

Esta colaboración se ha traducido principalmente este año en la participación de las asociaciones de profesionales de la privacidad y colegios profesionales como miembros del Comité Técnico constituido para asesorar en la elaboración del Esquema que ha promovido la AEPD para la certificación de los Delegados de Protección de Datos, cuyo alcance se detallará en el apartado de esta Memoria relativo al mismo.

De otra parte, la Agencia ha participado activamente en diversos eventos y actividades organizadas por las asociaciones de profesionales, especialmente aquellas orientadas a la formación y divulgación del nuevo marco europeo, entre las que pueden señalarse las siguientes:

- II Encuentro anual de la Asociación de Profesiones de Cumplimiento Normativo (CUMPLEN). La AEPD intervino en la mesa redonda que trató sobre el RGPD.

- Jornada sobre el Delegado de Protección de Datos, organizada por la Asociación Profesional Española de Privacidad (APEP).

- V Congreso Nacional de la Asociación Profesional Española de Privacidad (APEP). La AEPD impartió la ponencia inaugural de la segunda jornada.

- IV Jornada Habeas Data y Delitos Informáticos, organizada por la Asociación Profesional Española de Privacidad (APEP). La AEPD intervino en la mesa redonda dedicada al RGPD.

- Foro Asesores Wolters Kluwer, organizado por el Grupo Wolters Kluwer. La AEPD participó dentro de las 'Sesiones Técnicas para el profesional del Despacho', girando su intervención sobre las claves del RGPD.

- Reunión de trabajo con representantes de la Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC).

- Participación de la Directora en el III Congreso Internacional organizado por la Asociación de Expertos Nacionales de la Abogacía Tecnológica (ENATIC).

- IX Foro de la Privacidad del *Data Privacy Institute*, organizado por la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain). La ponencia inaugural corrió a cargo de la AEPD con el título de 'Retos para la implementación del RGPD'.

- XIX Jornada Internacional de Seguridad de la Información, organizada por el ISMS Forum Spain. La AEPD participó en la ponencia 'Data Breach Notification y su impacto en el negocio'. Asimismo, en el marco de dicho evento, la directora presentó el 'Código de buenas prácticas en protección de datos para proyectos de Big Data', editado conjuntamente por ambas instituciones, cuyo contenido se analizará con detalle en el apartado de este Informe correspondiente a la iniciativa 63 del Plan Estratégico.

- La AEPD participa en la *High Level Conference on Assurance* 2017, organizado por ISACA.

- AsticNet, organizado por ASTIC. La AEPD intervino con una ponencia sobre las implicaciones del nuevo RGPD para las Administraciones Públicas y las iniciativas que en este ámbito está desarrollando la Agencia.

- Jornada sobre la adaptación de la normativa española al nuevo marco europeo de protección de datos, organizada por el Colegio de Ingeniería Informática de Galicia. La directora de la AEPD participó con la ponencia 'La nueva Ley de Protección de Datos'.

Una mención específica merece la intensa colaboración producida entre la AEPD y los

Colegios Profesionales para facilitar la implantación del RGDP entre los colegiados y, entre otras cuestiones, favorecer la posibilidad de que los profesionales colegiados puedan beneficiarse de los servicios de un Delegado de Protección de Datos contratado a través del correspondiente Colegio. Esta colaboración se ha concretado en las siguientes actuaciones de la Agencia:

- Jornada sobre el Reglamento Europeo de Protección de Datos, organizado por el Ilustre Colegio de Abogados del Señorío de Vizcaya (ICASV).

- X Jornada de formación para miembros de Juntas de Gobierno de los Colegios de Administradores de Fincas, organizada por su Consejo General.

- Reunión de trabajo con representantes de Unión Profesional para analizar posibles vías de colaboración que faciliten el cumplimiento y la divulgación de las obligaciones que dimanan del RGPD entre las profesiones colegiadas.

- Seminario 'Actualidad del Reglamento europeo de protección de datos a menos de un año de su aplicación', organizado por la Sección de Derecho de las Tecnologías de la Información y la Comunicación del Ilustre Colegio de Abogados de Barcelona (ICAB).

- Primera Jornada anual del Consejo General de la Abogacía Española sobre Protección de Datos y Abogacía.

- Jornada 'Protección de Datos en las Corporaciones Colegiales', organizada por la AEPD en colaboración con la Unión Profesional y la Unión Interprofesional de la Comunidad de Madrid.

- La Directora participó en el desayuno-ponencia 'Nuevo marco de Protección de Datos', organizado por el Consejo General de Graduados Sociales de España. Su intervención gira en torno al impacto del RGPD en este colectivo.

- Encuentro organizado por el Consejo General de Colegios de Gestores Administrativos de España, analizando el impacto del RGPD en la actividad de este colectivo.

5.2.2 El denominado 'Coste 0'

El denominado 'Coste 0' consiste en ofrecer cursos sobre protección de datos a empresas mediante ayudas para la formación a sus trabajadores que se financian, mediante bonificaciones con cargo a las cuotas del sistema de Seguridad Social, a través de la Fundación Estatal para la Formación en el Empleo (FUNDAE), y ofrecer gratuitamente la 'implantación' de la LOPD. En ocasiones, ofrecen igualmente de manera gratuita sus servicios de asesoría en protección de datos tras una supuesta formación con cargo a la formación subvencionada. En estos casos, la formación de los empleados, que sería el objetivo de estos fondos, no se lleva a cabo y, a cambio, la empresa de formación afirma realizar una labor de 'implantación' de la LOPD.

Los efectos de estas prácticas, por lo que se refiere al ámbito del derecho fundamental a la protección de datos de carácter personal y a la aplicación de su normativa, son los propios de un asesoramiento básico que no suele reunir los mínimos requisitos para que las empresas cumplan con la normativa de protección de datos. Ello conlleva una disminución de las garantías ofrecidas a las personas que confían en que sus datos van a ser tratados por las empresas con arreglo a la Ley y, además, unas prácticas que en estos momentos resultan más preocupantes si se tiene en cuenta que el 25 de mayo de 2018 será de aplicación efectiva el Reglamento General de Protección de Datos que, con el objetivo de reforzar el control de los datos por sus titulares, introduce cambios significativos en el modelo de cumplimiento, estableciendo la responsabilidad proactiva de la empresas. Ello exige un asesoramiento con la suficiente calidad y solidez para que

las empresas puedan adaptarse a la nueva regulación, traten los datos de manera que no se vulnere el derecho de sus titulares y las empresas afectadas puedan acreditar un adecuado cumplimiento de la normativa. Objetivo que no puede cumplirse con un asesoramiento meramente formal que no garantice la implantación de las medidas exigidas por el Reglamento.

Con el objetivo de proteger el derecho a la protección de datos de las personas, la Agencia Española de Protección de Datos está trabajando con el Servicio Estatal de Empleo Público (SEPE) de cara a la adopción de medidas que pongan fin a estas prácticas.

6. La protección de datos en Europa

A lo largo del año 2017 el Grupo de Autoridades europeas de Protección de Datos, conocido como Grupo del Artículo 29 (GT29) ha concentrado la práctica totalidad de su actividad en los trabajos preparatorios para la aplicación del Reglamento General de Protección de Datos (RGPD) y de la Directiva de Protección de Datos en los ámbitos policial y judicial penal (Directiva de Policía), aunque con especial énfasis en el RGPD.

Para el GT29 esta tarea de preparación sigue dos líneas paralelas, ya que al análisis y desarrollo de los contenidos materiales de ambas normas se une la necesidad de adelantarse a su sustitución por el futuro Comité Europeo de Protección de Datos (CEPD).

En desarrollo de la primera de estas líneas de actuación, el Grupo ha adoptado una extensa lista de documentos destinados a guiar a las Autoridades de Protección de Datos y a los responsables en la aplicación del RGPD.

Entre los destinados principalmente a las Autoridades destacan las Directrices sobre la identificación de la autoridad principal, las Directrices sobre aplicación y determinación de multas administrativas y el formulario común para la notificación de quiebras de seguridad.

Las Directrices sobre identificación de la autoridad principal ofrecen criterios para aplicar las previsiones del RGPD en los procedimientos basados en el mecanismo de cooperación, conocido comúnmente como “de ventanilla única”. El RGPD contiene una definición de establecimiento principal de responsables y encargados, de la que derivaría la elección de la correspondiente autoridad de control, que no da respuesta directamente a la diversidad de situaciones en que pueden encontrarse las empresas

con varios establecimientos en la Unión Europea. El documento del GT29 aborda esta variedad de casos y proporciona a las autoridades pautas para determinar qué autoridad es la competente para liderar el procedimiento en cada caso.

Entre las conclusiones más destacadas de las Directrices se encuentra la de que el Grupo considera que pueden existir varios establecimientos principales de una misma organización, dependiendo de dónde se adoptan las decisiones sobre fines y medios para cada tratamiento, así como que corresponde en primera instancia a los propios responsables y encargados identificar su o sus establecimientos principales, sin perjuicio de que esta valoración esté sujeta a la verificación de las autoridades, cuya apreciación prevalecerá, en caso de discrepancia, sobre la de responsables y encargados.

Una de las principales novedades del RGPD es que atribuye a todas las Autoridades una potestad sancionadora idéntica incluyendo un catálogo de infracciones y sanciones, así como criterios para determinar qué tipo de medida correctiva aplicar en respuesta a una infracción y qué cuantía puede alcanzar una posible sanción económica.

La aplicación coherente y uniforme de este régimen sancionador es clave en el funcionamiento del sistema de protección diseñado por el RGPD. De hecho, el Reglamento atribuye al Comité Europeo de Protección de Datos (CEPD) la función de aprobar directrices para la determinación consistente de las multas administrativas.

Las Directrices sobre aplicación y determinación de multas administrativas adoptadas por el GT29 no son, obviamente, las mencionadas en el RGPD, dado que el CEPD no ha sido aún establecido. Estas directrices ilustran, solamente, el entendimiento común que las Autoridades han alcanzado sobre el modo de aplicar uno de los elementos del régimen sancionador: los criterios contenidos en el art. 83.2 del Reglamento para decidir si, ante una infracción, la respuesta adecuada es una multa, alguna otra de las medidas correctivas también previstas por el Reglamento, o ambas.

Un elemento importante del documento es que aclara que las multas administrativas no han de considerarse ni como un último recurso para sanciones especialmente graves o con importantes circunstancias agravantes, ni tampoco, en sentido contrario, como la respuesta que, como regla general, ha de darse ante cualquier infracción, salvo excepciones. El documento señala que las multas son un instrumento más para lograr el cumplimiento del RGPD, al que el propio Reglamento presta una atención especial, y que por ello deben usarse habitualmente junto con las demás medidas correctivas, y siempre atendiendo a las circunstancias de cada caso.

El GT29 ha concentrado sus trabajos en el nuevo RGPD y la Directiva de protección de datos (judicial, penal y policial)

Los trabajos del Grupo en este ámbito continuaron a través de una "*task force*" establecida en el segundo semestre del año cuya actividad se centró en desarrollar criterios uniformes sobre la fijación de la cuantía de las multas en el marco del RGPD.

La creación de este grupo responde al hecho de que el Reglamento plantea un régimen sancionador muy abierto, no sólo, como se ha señalado, en cuanto a la posibilidad de imponer multas u otro tipo de medidas, sino

también en la cuantía de las sanciones. El Reglamento prevé multas que van desde los cero euros hasta los 10 millones o el 2% de la facturación anual y global de la entidad o de hasta 20 millones o del 4% de la facturación, todo ello dependiendo del artículo infringido.

Por ello, al igual que se han publicado interpretaciones comunes sobre la aplicación de los criterios para decidir entre los distintos tipos de sanciones que permite el RGPD, se ha considerado necesario buscar esas interpretaciones compartidas en lo relativo a la cuantía que puede corresponder a diferentes infracciones o tipos de infracciones.

El grupo de trabajo se reune con una periodicidad bimensual y está previsto que en los primeros meses de su actividad se centre en recopilar información y experiencias sobre la aplicación de los sistemas sancionadores en los Estados Miembros.

El formulario común para notificación de quiebras de seguridad se utilizará para que los responsables notifiquen la información asociada a una quiebra de seguridad. El uso de este formulario será voluntario para las Autoridades, pero el Grupo espera que, en la medida en que pueden existir quiebras de seguridad de carácter transfronterizo, las autoridades tiendan a usarlo mayoritariamente a fin de conseguir que la información proporcionada por los responsables sea homogénea y pueda ser fácilmente compartida entre las autoridades afectadas.

El GT29 ha adoptado en 2017 una lista relativamente extensa de documentos cuyo principal objetivo es transmitir a responsables, encargados y ciudadanos cuál es la interpretación que las autoridades de supervisión hacen de algunas de las disposiciones del RGPD que contienen elementos innovadores. Entre ellas se encuentran:

- Directrices sobre Delegados de Protección de Datos
- Directrices sobre Portabilidad
- Directrices sobre Decisiones individuales automatizadas y Perfilado
- Directrices sobre Consentimiento
- Directrices sobre Transparencia según el Reglamento
- Directrices sobre Notificación de Violaciones de Seguridad según el RGPD
- Marco de Adecuación
- Elementos y Principios que han de encontrarse en las BCR
- Elementos y Principios que han de encontrarse en las BCR de Encargado

Algunas de estas Directrices, como sucede con la relativa al consentimiento o los tres documentos que tratan aspectos del régimen de transferencias internacionales, son actualizaciones o complementos de Dictámenes o Documentos de Trabajo aprobados por el GT29 en el pasado. En otros casos, los documentos no tienen precedente inmediato en la actividad del Grupo, fundamentalmente porque la cuestión a la que se refieren no estaba regulada en el todavía vigente marco de protección de datos europeo.

Todas ellas fueron sometidas a un proceso de consulta pública tras su aprobación preliminar por el Grupo. Las versiones definitivas incorporan las aportaciones recibidas en ese periodo de consulta. De hecho, en el momento de redactar esta Memoria, todavía no ha sido aprobada la versión definitiva de algunas de ellas, como sucede con las relativas a transferencias internacionales, a la espera de incorporar las aportaciones recibidas en los correspondientes periodos de consulta pública.

En relación con la preparación para el tránsito desde su actual configuración al futuro CEPD, el Grupo ha trabajado principalmente en asegurar que el Comité pueda comenzar materialmente a funcionar el día de su constitución, el 25 de mayo de 2018.

En ese sentido, el GT29 aprobó en su último plenario del año un Memorando de Entendimiento con el Supervisor Europeo de Protección de Datos, que como se ha indicado desempeñará la Secretaría del CEPD, en el que se establece el modo en que se prestará ese servicio de secretaría.

Paralelamente, un grupo de redacción, en el que participa la AEPD, está redactando las Reglas de Procedimiento del CEPD. Éstas son especialmente relevantes en el marco del RGPD, ya que, a diferencia de lo que sucede con las que hoy día se aplican al GT29, incluyen procedimientos concretos para la adopción de los dictámenes y decisiones vinculantes del CEPD.

Conviene señalar en este punto que tanto las Reglas de Procedimiento, una vez que sean finalizadas y adoptadas por el GT29, como todos los demás documentos aprobados y que, de una forma u otra, están adelantando la actividad del CEPD, deberán ser ratificados por éste tan pronto como se constituya, a fin de que puedan surtir los efectos que en cada caso les asigna el RGPD.

Una tercera área de actuación en esta preparación, realmente crítica, es la que se refiere al desarrollo del sistema de información del CEPD.

El RGPD determina unos mecanismos de supervisión basados en el intercambio de información y la cooperación entre las autoridades de supervisión. Para que esos mecanismos funcionen es fundamental que las autoridades y el Comité dispongan de un sistema de información y comunicación que no solo permita una difusión rápida de la información, sino que se configure como una auténtica herramienta de gestión para los procesos de toma de decisión en los procedimientos de 'ventanilla única' y relacionados con el 'mecanismo de coherencia'.

Desde 2016 venía desarrollando sus trabajos un grupo de trabajo especial dedicado al diseño y desarrollo de este sistema. Este grupo dedicó parte del año 2017 a identificar con precisión las necesidades de las autoridades y del comité y a traducirlas en procesos que debieran formar parte del sistema.

La variedad y complejidad de requerimientos hicieron evidente que no sería posible dentro del plazo hasta mayo de 2018 desarrollar un sistema de información *ex novo* específicamente adaptado a las necesidades del Comité y de sus miembros.

Por ello, se exploró la posibilidad de utilizar un sistema ya existente en la Unión Europea, previa su adaptación al entorno definido por el RGPD. Este sistema es el IMI, Sistema de Información del Mercado Interior, que se usa en la actualidad para una gran variedad de procedimientos de intercambio de información entre autoridades de los Estados Miembro en materias relacionadas con el funcionamiento del Mercado Unico.

La decisión de aprovechar los recursos que ofrece el IMI para poder tener a punto el sistema de información del CEPD en mayo de 2018, fue adoptada por el GT29 en su reunión plenaria del mes de octubre.

No obstante, hay que indicar que esta decisión fue tomada con cierta cautela por parte de los miembros del Grupo. Todos ellos eran conscientes de la imposibilidad material de desarrollar e implantar un sistema propio an-

tes de la fecha de constitución del CEPD. Sin embargo, el IMI plantea algunos problemas para su adaptación al marco del RGPD.

En primer lugar, el IMI es un sistema propiedad de los Estados Miembros y la Comisión, que se rige por normas estrictas. Por ello, ha sido preciso que la decisión del GT29 fuera aceptada y corroborada formalmente por el comité que gestiona el IMI. Ello supone que no ha sido posible desarrollar una versión de prueba que permitiera a los miembros del GT29 conocer con detalle cómo funcionará el sistema una vez adaptado al CEPD. Su decisión se ha basado solo en previsiones de cómo podría operar. De hecho, la decisión del GT29 era el requisito indispensable para que se pudieran iniciar los trabajos de adaptación.

Por otro lado, el IMI es un sistema ya consolidado, con una estructura y formas de funcionamiento propias y pensadas para el tipo de tareas para las que originariamente fue diseñado. Eso supone que sería posible que algunas de las necesidades expresadas por las autoridades de supervisión respecto al futuro sistema del CEPD no puedan ser satisfechas o, al menos, no puedan serlo en una primera etapa.

Esto sucede, por ejemplo, con dos aspectos en los que la AEPD ha insistido durante todo el proceso. Uno de ellos es el relativo a la necesidad de incorporar al sistema una utilidad de traducción automática que garantice un nivel razonable de calidad de las traducciones.

Este mecanismo de traducción ha sido considerado siempre como pieza clave para el funcionamiento del sistema por parte de la AEPD. Los procedimientos de 'ventanilla única' se basan en que una autoridad principal coordina a las demás autoridades afectadas, intercambia información con ellas, prepara una propuesta de decisión y estudia y, en su caso, acepta las objeciones que las autoridades afectadas puedan plantear sobre esa propuesta.

Todos estos procesos requieren de una lengua de trabajo común, que el GT29 ha acordado que sea el inglés. Es posible que algunos documentos puedan redactarse directamente en ese idioma por la autoridad que los presente. Pero hay otros, empezando por las propias reclamaciones que originen los procedimientos, las aportaciones de las partes o determinados elementos de prueba que solo estarán disponibles en un idioma y que deberán necesariamente ser traducidos para poder ser compartidos con las demás autoridades que participan en el procedimiento.

En principio, hay también acuerdo en el GT29 en que estos documentos deberán ser traducidos al inglés por la autoridad que los incorpora. Sin embargo, el problema puede derivar del volumen de casos que puedan ser tramitados en el sistema de 'ventanilla única' y el correspondiente volumen de documentos que habrán de ser traducidos.

Una estimación realizada por uno de los Subgrupos del GT29, a instancias y bajo la coordinación de la AEPD, situaba esa cifra en torno a los 15.000 casos por año.

Aunque esta cifra resulte finalmente inexacta, es indicativa de que los casos que deberán canalizarse por el mecanismo de cooperación o ventanilla única excederán con mucho de las decenas o centenares y de que, paralelamente, la cantidad de documentos que podría ser preciso traducir puede estar lejos de las posibilidades de la mayoría de las autoridades de supervisión.

De ahí la importancia de que el sistema de información cuente con herramientas que permitan una primera traducción de los textos, que sea suficiente para que las autoridades implicadas puedan trabajar con ellos y que, al mismo tiempo, sirva de base para las traducciones más completas y precisas que pudieran ser necesarias dependiendo de los requisitos que en materia de idioma de los procedimientos establezcan las legislaciones nacionales.

La información proporcionada sobre el IMI indica que los formularios o formatos de pantalla que emplea y sus contenidos estarán disponibles en todos los idiomas oficiales de la Unión. Asimismo, el sistema permite la traducción de textos libres incorporados a esos formularios hasta un determinado volumen de caracteres. Finalmente, el sistema podrá acceder a un sistema de traducción automática desarrollado y empleado por la Comisión que debería permitir la traducción de otros documentos con una calidad aceptable para los fines que se persiguen.

Un segundo punto que resulta también de gran trascendencia a la vista del número de casos a tramitar en el procedimiento de 'ventanilla única' es el de la comunicación entre el sistema de información del CEPD y los sistemas de información nacionales.

Si no existe un modo de que las informaciones que se introduzcan en uno de ellos sean automáticamente replicadas en los lugares correspondientes de los otros, será preciso duplicar el trabajo e introducir toda la información dos veces, una en el sistema nacional y otra en el sistema europeo.

Las informaciones sobre el IMI indican que la posibilidad de desarrollar una interfaz que permita el tránsito de información entre un sistema nacional y el sistema del CEPD existe, pero que no estaría disponible en las primeras fases de implantación del sistema del CEPD.

Una vez que se ha tomado la decisión de utilizar el IMI como base para el sistema de información del Comité, se ha establecido un grupo de trabajo de "futuros usuarios", en el que participa la AEPD y que está dirigido por los técnicos de la Comisión responsables del IMI para definir las especificaciones funcionales sobre la base de lo ya identificado por el GT29 y contribuir a la puesta en marcha del sistema antes de mayo de 2018.

Como complemento a todos estos trabajos sobre el RGPD, el GT29 ha aprobado también un Dictamen sobre aspectos claves de la Directiva de Policía 2016/680. El objetivo de este dictamen es ofrecer a los Estados Miembros criterios de transposición comunes en algunos puntos concretos, dado que la Directiva como tal solo se aplica a través de las normas nacionales de trasposición.

Estos puntos son, fundamentalmente, los que tienen que ver con la actividad de las APD en el contexto de la Directiva, otros en los que el Grupo considera que es necesario proporcionar guía o aclaraciones sobre el contenido de la Directiva o aquellos en los que se ha detectado que los trabajos de transposición en curso en algunos Estados Miembros están siguiendo líneas inconsistentes entre sí.

En concreto, el Dictamen aborda los seis temas siguientes:

- Límites temporales para almacenamiento de los datos y revisión de esos límites
- Tratamiento de categorías especiales de datos
- Decisiones individuales automatizadas y perfilado
- Derechos de los interesados
- Registros de actividad (logs)
- Potestades de las Autoridades de Protección de Datos

El Grupo señala que este dictamen no excluye nuevos documentos futuros y, de hecho, para 2018 está previsto que publique posiciones sobre cuestiones tales como la determinación de las autoridades designadas con competencias en materia de cumplimiento de la Ley en el marco de la Directiva de Policía o la determinación de los actos que siendo contrarios a derecho resultan controvertidos a la hora de definir una frontera entre ilícitos administrativos y penales.

7. Desafíos globales para la privacidad

7.1. Política de privacidad de Facebook

En septiembre de 2017 se resolvió el procedimiento sancionador iniciado a la empresa Facebook para analizar si los tratamientos de datos que realiza la red social se adecúan a la normativa de protección de datos.

En el marco de la investigación realizada, la AEPD constató que Facebook recababa datos sobre ideología, sexo, creencias religiosas, gustos personales o navegación sin informar de forma clara acerca del uso y finalidad que le iba a dar a los mismos. En concreto, se verificó que la red social trataba datos especialmente protegidos con fines de publicidad, entre otros, sin obtener el consentimiento expreso de los usuarios como exige la normativa de protección de datos. La investigación también permitió comprobar que Facebook no informaba a los usuarios de forma exhaustiva y clara sobre los datos que iba a recoger y los tratamientos que pretendía realizar con ellos, sino que se limitaba a dar algunos ejemplos. En particular, la red social recogía otros datos derivados de la interacción que llevan a cabo los usuarios en la plataforma y en sitios de terceros sin que estos puedan percibir claramente la información que Facebook recoge sobre ellos ni con qué finalidad la va a utilizar.

La AEPD también confirmó que los usuarios no eran informados de que se iba a tratar su información mediante el uso de cookies –algunas de uso específicamente publicitario y alguna de uso declarado secreto por la compañía– cuando navegan por páginas que no son de Facebook y que contienen el botón 'Me gusta'. Esta situación también se producía cuando los usuarios no son miembros de la red social pero han visitado alguna vez una de sus páginas, así como cuando usuarios que sí están registrados en Facebook navegan por páginas de terceros, incluso sin iniciar sesión en Facebook. En estos casos, la plataforma añade la información recogida en dichas páginas a la que figura asociada a su cuenta en la red social. Por ello, la AEPD consideró que la información facilitada por Facebook a los usuarios no se ajusta a la normativa de protección de datos.

En septiembre de 2017 se resolvió el procedimiento sancionador iniciado a la empresa Facebook

Igualmente se constató que la política de privacidad de Facebook contenía expresiones genéricas y poco claras, y obligaba a acceder a multitud de enlaces distintos para conocerla. La red social hacía referencia de forma imprecisa al uso que va a hacer de los datos que recoge, de forma que un usuario de Facebook con un conocimiento medio de las nuevas tecnologías no llega a ser consciente de la recogida de datos, ni de su almacenamiento y posterior tratamiento, ni de para qué van a ser utilizados. Por su parte, los internautas no registrados desconocen que la red social recoge sus datos de navegación.

También se pudo constatar que Facebook no eliminaba la información que recoge a partir de los hábitos de navegación de los usuarios, sino que la retiene y reutiliza posteriormente asociada al mismo usuario.

En relación con la conservación de datos, cuando un usuario de la red social ha eliminado su cuenta y solicita el borrado de la información, Facebook capta y trata información durante más de 17 meses a través de una cookie de la cuenta eliminada. Por ello, la AEPD consideró que los datos personales de los usuarios no son cancelados en su totalidad ni cuando han dejado de ser útiles para el propósito para el que se recogieron ni cuando el usuario solicita explícitamente su eliminación, conforme a las exigencias de la LOPD.

Teniendo en cuenta todo ello, la Agencia declaró la existencia de dos infracciones graves, por falta de consentimiento y por retención excesiva de información, y una muy grave por tratamiento de datos especialmente protegidos sin el consentimiento explícito de los usuarios, e impuso a Facebook una sanción de 1.200.000 euros.

7.2 Facebook Messenger

En mayo de 2016 una usuaria de Facebook denuncia que las cuentas de la red social disponen de un servicio de mensajería integrado denominado Chat que permite conocer a un usuario de Facebook cuándo otros usuarios de Facebook están activos y cuándo ha sido su última conexión, sin existir una opción para impedir que un usuario pueda monitorizar la actividad de otros usuarios.

Se iniciaron actuaciones de inspección en las que se constató que, ligado a este servicio de chat, aparece un listado de los 'amigos' del usuario y si un 'amigo' del usuario tiene una sesión iniciada en Facebook y el servicio de Chat activado, en la cuenta del usuario y asociado al nombre del 'amigo' aparece una señal, un indicador verde, que revela que el 'amigo' tiene sesión abierta en ese momento. Si no aparece un indicador verde, aparecerá un valor numérico, cuando el servicio de chat se ha desactivado, que revela en minutos cuánto tiempo hace que tuvo sesión abierta en por última vez. A su vez, se ha constatado que en la página principal de la política de privacidad de Facebook no se encuentra una información explícita y completa sobre la revelación de la información de conexión como podría ser la recopilación de información en el Chat/Messenger y su posterior utilización o revelación a terceros o una referencia a cómo administrar el registro de tiempos de conexión, entre otras.

Se decidió abrir acuerdo de inicio a la empresa Facebook por vulneración del deber de secreto. El procedimiento está en curso.

7.3. WhatsApp - Facebook

Ante los cambios producidos en la política de privacidad y los términos de servicio de Whatsapp que se produjeron el 25 de agosto de 2016, la Agencia Española de Protección de Datos emitió una nota en la que anunciaba el análisis de dichos cambios en las condiciones, así como dando indicaciones a los usuarios sobre los elementos más determinantes de los mismos.

La AEPD decidió abrir actuaciones de oficio en octubre de 2016 para determinar el modelo general de tratamiento, la extensión de los datos transferidos, el ámbito de procesamiento y la base jurídica de la comunicación de datos en los que están implicadas tanto la empresa Whatsapp como Facebook.

Durante las actuaciones ambas entidades admitieron que comparten información de los usuarios de la aplicación Whatsapp. En concreto, Whatsapp confirmó que "actualmente" comparte con Facebook información de todos los usuarios de la aplicación

Whatsapp, sean o no usuarios de Facebook, advirtiendo al respecto que esa información se transmite con periodicidad tanto diaria como en tiempo real. En concreto, ambas entidades detallaron que comparten el identificador de la cuenta de usuario de WhatsApp, información sobre el dispositivo (incluyendo un identificador común incluido en las aplicaciones de Facebook y WhatsApp, el prefijo y código de la red móvil del país, información de la plataforma, versión de la aplicación e identificadores que permiten un seguimiento de la aceptación de la Actualización y las opciones de control); el "estado de última conexión" del usuario (esto es, información sobre la última vez en que el usuario utilizó el servicio); y la fecha en que el usuario se dio de alta en su cuenta de WhatsApp.

Por otro lado, se constató que las cesiones o comunicaciones de datos personales entre Whatsapp y Facebook que no guardan relación con las finalidades que determinaron la recogida de datos personales, se realizan sin ofrecer a los usuarios opción alguna para mostrar su negativa a las mismas, por cuanto Whatsapp únicamente habilitó mecanismos para aceptar la cesión de información con la finalidad de "mejorar mi experiencia con los productos y publicidad en Facebook" y únicamente en el caso de usuarios existentes. Por tanto el consentimiento que se presta con la aceptación de la Política de Privacidad y Términos de Servicio no puede considerarse libre, y ello impide que el consentimiento prestado pueda considerarse válido.

Cabe añadir que la información sobre los posibles destinatarios de los datos, sobre las finalidades para las que se le ceden o la utilización que harán de los mismos los cesionarios se ofrece de forma poco clara, con expresiones imprecisas e inconcretas que no permiten deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos los datos.

Por lo tanto, en septiembre de 2017 se acordó iniciar un procedimiento sancionador a Whatsapp por la presunta infracción del artículo 11 de la LOPD, y a la entidad Facebook por la presunta infracción del artículo 6 de la LOPD. Al término de 2017 el procedimiento seguía su curso.

7.4. Google – 'Derecho al olvido'

El 28 de noviembre de 2014 la AEPD emitió un comunicado acerca del documento aprobado por el Grupo de Autoridades europeas de protección de datos sobre 'derecho al olvido', en el que se analizaban los pronunciamientos del TJUE y se dictaban los criterios interpretativos comunes para su aplicación.

En marzo de 2015 se recibió denuncia de un ciudadano en relación a Google, por un posible incumplimiento legal en relación con dos cuestiones abordadas en el comunicado de la AEPD: por un lado, la política de avisos a los usuarios sobre resultados incompletos y, por otro, la comunicación a terceros de los resultados que han sido desindexados por el buscador.

En mayo de 2015 se iniciaron actuaciones de inspección que determinaron que a través del servicio *Webmaster Tools*, Google comunicaba con carácter general a los *webmasters* (en un panel del servicio o mediante correo electrónico) información con respecto a aquellas URLs de sus respectivos sitios web que eran eliminadas de los resultados de búsqueda.

Por lo tanto, se acordó iniciar procedimiento sancionador que resolvió en noviembre de 2016 multando a Google con 150.000 euros por infracción del deber de secreto y, a su vez, iniciaba actuaciones de inspección para determinar además que se corregía la conducta infractora.

Estas actuaciones se centraban en verificar la existencia de comunicaciones con información no anonimizada efectuadas por Google a la organización Lumen y en determinar las posibles responsabilidades que pudieran derivarse de la práctica de Google de informar a los usuarios, en las páginas de resultados de búsquedas por nombre, que la lista de resultados pudiera no estar completa.

De las mismas se evidenció que el aviso incluido por la compañía se muestra siempre que el sistema identifica nombres de personas en los criterios de búsqueda pero, en ocasiones, dicho sistema no es capaz de identificar un nombre de persona como tal y por tanto no muestra el aviso. Por lo tanto, se entiende que la información contenida en el aviso insertado en la página de resultados no permite deducir que una persona concreta haya solicitado la retirada del buscador de ciertos resultados asociados a su nombre. Además, el enlace a LumenDatabase.org ha sido suprimido y ya no se tiene constancia de comunicaciones a dicha página por parte de Google con relación al ejercicio del derecho al olvido. Por ello, se resolvió archivar la investigación en agosto de 2017.

7.5. Google Street View

La AEPD inició de oficio en el año 2010 la investigación a la empresa Google en relación a la recogida y tratamiento de datos personales de redes WiFi llevada a cabo por los vehículos empleados en el proyecto *Street View*. A pesar de las numerosas actuaciones de investigación realizadas dicho año sobre los vehículos de Google y las bases de datos de dicha empresa, la existencia de un procedimiento judicial penal abierto obligó a la AEPD a suspender la tramitación de su procedimiento sancionador.

En 2017, una vez se tuvo conocimiento de la firmeza del auto por el que se acuerda el sobreseimiento provisional y archivo de las diligencias previas, la Agencia reanudó el procedimiento administrativo.

En el marco de la investigación realizada, se había comprobado que Google recogió información de las WiFi abiertas de los usuarios, sin que los afectados tuviesen conocimiento de que dicha recogida de datos se estaba llevando a cabo y sin su consentimiento. La compañía recabó, entre otra, información relativa a direcciones de correo electrónico de personas físicas, códigos de usuario y contraseña que permiten el acceso a cuentas de correo electrónico, direcciones IP, direcciones MAC de los routers y de los dispositivos conectados a los mismos o nombres de redes inalámbricas (SSID) configurados con el nombre y apellidos de su responsable. No se constató que Google tratase datos especialmente protegidos a través de estos sistemas.

En octubre de 2017 se dictó resolución declarando la existencia de una infracción grave e imponiendo a Google una sanción de 300.000 euros. En cuanto a que los datos se recogiesen de redes WiFi abiertas, la resolución especifica que “el hecho de que los titulares de redes WiFi no aseguren el cifrado de estas redes, en perjuicio de la seguridad de sus datos, no autoriza en modo alguno la recogida de la información llevada a cabo ni ningún uso posterior de la misma”.

7.6. Google y recogida de datos de geolocalización

En varios medios de comunicación se hizo pública una práctica que Google vendría realizando desde principios de año, consistente en recopilar la información relativa a la ubicación de los terminales móviles que utilizan sistema operativo Android, independientemente de que el usuario lo hubiera autorizado en los ajustes del sistema, e incluso aunque se encontrase desactivado el GPS del terminal. Por ello la Directora de la AEPD instó a que realizasen las Actuaciones Previas de Investigación precisas en orden a determinar un posible incumplimiento de la normativa en el ámbito competencial de la Agencia Española de Protección de Datos.

La investigación, iniciada en noviembre de 2017, se encuentra en curso a finales de ese mismo año.

7.7. Privacy Shield

En la Memoria de 2017 se recogía cómo el 12 de julio de 2016 la Comisión Europea aprobó mediante una Decisión de Ejecución la adecuación de la protección conferida por el 'Escudo de Privacidad UE-EE.UU.' (*Privacy Shield*, en su denominación en inglés), que sustituía a la Decisión 2000/520/CE, conocida como Decisión de 'Puerto Seguro', declarada inválida por sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015 (Sentencia *Schrems*).

Se señalaba también que durante la fase de preparación de la decisión, la propuesta presentada por la Comisión había sido objeto de un dictamen del Grupo de Trabajo del Artículo 29 (Dictamen 1/2016 – WP238), en que el Grupo había expresado una favorable acogida general a la iniciativa pero identificaba una serie de materias en las que entendía que el Escudo de Privacidad no reflejaba de forma adecuada algunos de los principios centrales del sistema europeo de protección de datos.

Este dictamen fue en parte la causa de que la propuesta se modificara tras una nueva ronda de negociación entre los EEUU y la Comisión Europea, adoptándose finalmente la Decisión de julio de 2016.

El Grupo del Artículo 29 manifestó, en una Declaración hecha pública el 26 de julio de 2016, que a pesar de que la versión definitiva de la Decisión acogía algunas de las observaciones planteadas en su Dictamen, subsistían algunos motivos de preocupación.

En este punto, es preciso recordar que en la Decisión pueden distinguirse dos tipos de contenidos. Uno correspondería, en líneas generales, a los principios del *Privacy Shield*, respecto a los cuales se autocertifican las compañías estadounidenses que deseen obtener las ventajas que el esquema ofrece. El otro se refiere a las garantías que las autoridades norteamericanas ofrecen para la aplicación de las excepciones a la aplicación de los principios del Escudo por motivos de seguridad nacional, interés público o seguridad pública.

En su declaración, y en relación con la parte correspondiente a los principios del esquema, el Grupo lamentaba que la Decisión no contuviera reglas específicas sobre decisiones automatizadas, así como que no existiera un derecho de oposición formulado de manera general.

En el terreno del acceso por parte de las autoridades por motivos de seguridad nacional, el Grupo señalaba que habría sido deseable que se ofrecieran garantías más estrictas sobre la independencia y poderes del *"Ombudsperson"* y lamentaba la falta de garantías concretas que permitieran asegurar que se cumplieran en todos los casos los

compromisos de las autoridades norteamericanas de no llevar a cabo una recogida masiva e indiscriminada de datos personales.

En la declaración se recogía también la opinión del GT29 de que la primera revisión anual conjunta del sistema debería ser la ocasión para valorar su robustez y eficacia, y señalaba algunos de los requisitos que consideraba necesarios para el desarrollo de la revisión, en especial en lo relativo al papel y facultades de las autoridades de protección de datos europeas que participen en ella.

Esta primera revisión conjunta tuvo lugar en el mes de septiembre de 2017. En ella participaron, junto con la Comisión Europea, ocho representantes de autoridades de protección de datos.

El último plenario del GT29, celebrado en noviembre, adoptó formalmente su informe de la evaluación (paralelo al que, por su parte, publicó la Comisión) describiendo los resultados de la revisión y la valoración que de ellos hace el Grupo.

En el informe se señala que, en la parte comercial, es decir, en la relativa a la aplicación en condiciones normales del Escudo, las autoridades americanas han puesto en marcha un amplio marco procedimental para apoyar el funcionamiento del Escudo.

No obstante, hay un número de cuestiones no resueltas que siguen causando preocupación a las autoridades. Entre ellas, pueden citarse la falta de directrices e información clara sobre los principios del Escudo, las transferencias ulteriores o los derechos de los interesados. Asimismo, de la revisión se desprende la necesidad de una mayor supervisión del cumplimiento por parte de las empresas autocertificadas, por ejemplo mediante inspecciones realizadas de oficio por las autoridades estadounidenses encargadas de la monitorización del esquema. También se solicita de las autoridades norteamericanas una mejor definición de la posición de los encargados de tratamiento, distinguiéndolos de los responsables en la aplicación del Escudo.

El informe se refiere también a la necesidad de mejorar la interpretación tanto de las normas sobre perfilado y decisiones automatizadas como del concepto de datos de recursos humanos y su tratamiento, dado que estos datos se benefician de un régimen especial en el marco del *Privacy Shield*. En la misma línea, se considera que las autoridades estadounidenses deben hacer una mejor definición de la posición de los encargados de tratamiento, distinguiéndoles de los responsables en la aplicación del Escudo.

Todos estos temas se sumarían a algunos de los identificados en el Dictamen de 2016 que no han sido todavía adecuadamente atendidos, como por ejemplo las carencias en definiciones clave y en relación con derechos de los interesados, especialmente el de oposición, o la exageradamente abierta excepción aplicable a la información disponible públicamente.

El informe recoge igualmente los aspectos en que considera que sigue habiendo dificultades en el terreno de las excepciones a la aplicación de los principios del Escudo y, en concreto, al acceso por parte de las autoridades de seguridad e inteligencia a la información transferida. Algunas de estas cuestiones se refieren a la falta de evidencias o compromisos legalmente vinculantes que respalden las afirmaciones de las autoridades estadounidenses de que la recogida de datos, en virtud de la Sección 702 de la *Foreign Information Security Act* (FISA), no es indiscriminado y que no se produce un acceso generalizado en el marco de alguno de los programas de uso de la información existentes.

Asimismo, se apunta la necesidad de una mayor transparencia en la aplicación de algunas de las bases legales que permiten el acceso a la información por motivos de seguridad nacional, como la mencionada Sección 702, la Orden Ejecutiva 12333 o la Directriz de Política Presidencial 28. En relación con los dos primeros textos mencionados esa mayor transparencia debería obtenerse mediante la publicación o actualización de informes del *Privacy and Civil Liberties Oversight Board* (PCLAOB), mientras que respecto al último el obstáculo es que el informe correspondiente está todavía sometido a privilegio presidencial y no es por tanto de acceso público.

Otras cuestiones que también generan dudas tienen que ver con los poderes del "*Ombudsperson*" previsto en el Escudo o con el nombramiento de los miembros que han cesado en el PCLOB, organismos que tienen un papel central en la supervisión externa de la aplicación de las bases legales que permiten el acceso de los servicios de inteligencia a información transmitida en el marco del Escudo.

Se ha publicado una nota en relación con el informe del Equipo de evaluación con los pasos a seguir a partir de las conclusiones de esta primera revisión conjunta. En ella se resumen las deficiencias que el GT29 considera que deben ser resueltas por parte de la Comisión Europea y los EEUU y se apunta que las soluciones debieran producirse antes de mayo de 2018, fecha en que se aplica el nuevo RGPD y comienza a funcionar el CEPD.

7.8. Pokemon

En julio de 2016, se iniciaron actuaciones de oficio sobre el producto 'Pokemon Go' y servicios o sistemas relacionados con él, para determinar si su política de privacidad cumple con lo establecido en la normativa española.

'Pokemon Go' ha sido desarrollado por *Niantic INC* con sede en EEUU, y las actuaciones de investigación se han centrado en el análisis del producto, la información proporcionada a los usuarios, los términos de sus políticas y las manifestaciones realizadas por la empresa ante los requerimientos de la Agencia. De estas actuaciones se deduce que, incluso tras borrado de la cuenta de un usuario o solicitud de cancelación de los datos, estos pueden almacenarse de forma indefinida en los sistemas de *backup* de la empresa *Niantic*.

A partir de las evidencias obtenidas se acordó iniciar procedimiento sancionador por infracción de los principios de conservación de datos, (Art. 4.5 en relación art. 16 LOPD).

7.9. Microsoft

La Agencia Española de Protección de Datos ha desarrollado un plan de oficio para determinar si la instalación y operación del sistema operativo Windows 10 de Microsoft cumple con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Windows 10 es un sistema operativo diseñado y desarrollado por *Microsoft Corporation*. Como tal sistema operativo, Windows 10 se instala sobre un equipo terminal (ordenador, teléfono móvil, tableta electrónica, etc.) y permite la comunicación entre el usuario y los programas que tiene instalados y los componentes electrónicos que tiene conectados el equipo terminal.

Los sistemas operativos en general, y Windows 10 en particular, vienen acompañados de una serie de herramientas y servicios que extienden su funcionalidad. Entre las herramientas incluidas con Windows 10 se encuentran el navegador *Microsoft Edge*, el sistema de comunicaciones *Skype*, el asistente personal Cortana, el correo electrónico Outlook, el servicio de almacenamiento en la nube *OneDrive* o el buscador *Bing*. Dispone, además, de una plataforma de distribución digital de software denominada *Windows Store*.

Windows 10 presenta como novedad, frente a versiones anteriores del mismo sistema operativo, la posibilidad de una monitorización exhaustiva de las actividades del usuario a través de internet. Por su privilegiada posición de intermediario entre el usuario y el resto de programas y componentes, el sistema operativo trata una ingente cantidad de datos y, a través de los componentes que gestiona, permite conectarse remotamente a otros equipos, ya sea en una red local o en internet. El análisis del sistema operativo desde el punto de vista de la protección de datos de carácter personal requiere tener en cuenta, especialmente, la información que Microsoft facilita a los usuarios y los mecanismos habilitados para que los afectados presten su consentimiento para la recogida y tratamiento de sus datos personales.

El plan se encuentra, al finalizar el año 2017, en fase de análisis de los resultados obtenidos.

7.10. Nuevos productos: juguetes conectados a internet

Ante la alarma creada por la aparición en el mercado de juguetes infantiles conectados a internet, que capturaban voz y vídeo de los menores, se decidió iniciar investigaciones de oficio en particular sobre dos de los productos que se comercializaban en el mercado español: la muñeca *Cayla* y el robot *I-Que.*

Actualmente las actuaciones están en curso, centrándose fundamentalmente en las entidades *Genesis/Toyquest*, ambas con sede en Hong-Kong, que comercializan los juguetes y las apps, y que utilizan medios ubicados en España; y la empresa *Nuance*, como encargado de tratamiento para el tratamiento de voz. A cierre del texto relativo a esta Memoria, la investigación continúa abierta.

8. Respuesta a los retos internacionales

8.1. COOPERACIÓN CON IBEROAMÉRICA. LA RIPD

Las actividades y eventos en los que ha participado la AEPD, en su condición de Secretaría Permanente de la Red Iberoamericana de Protección de Datos (RIPD), han sido los siguientes:

- Programa de capacitación de cinco empleados del Consejo para la Transparencia de Chile, en la sede de la AEPD. Esta actividad es consecuencia de la convocatoria realizada por la Agencia para formación y capacitación de empleados y directivos de las entidades de la RIPD.

- Taller sobre 'Un nuevo marco normativo para la protección de los datos personales: los estándares iberoamericanos'. Centro de la Cooperación Española en Cartagena de Indias. 9, 10 y 11 de mayo. Asistieron representantes de las Autoridades Iberoamericanas de Protección de Datos, de la Unidad de Flujos Internacionales de la Comisión Europea (virtual), del Supervisor Europeo de Protección de Datos y de la OEA. Se elaboró el proyecto de 'Estándares de Protección de Datos Personales para los Estados Iberoamericanos'.

- XV Encuentro Iberoamericano de Protección de Datos. Santiago de Chile. 20, 21 y 22 de junio. Organizador: Consejo para la Transparencia de Chile. Sesión Cerrada (día 20): se aprobó el plan de trabajo 2018; se informó sobre distintas iniciativas normativas nacionales en la materia y se examinó el I Informe de la Red sobre la situación de la protección de datos en la Región. Se admitieron como nuevos Miembros de la RIPD a los Institutos locales de la Ciudad de México (INFODF) y del Estado de México (INFOEM). Como acuerdo más destacado, se aprobaron los Estándares Iberoamericanos de Protección de Datos. Sesión Abierta (días 21 y 22): se abrió con una Charla Magistral sobre el estado de la protección de datos en el contexto internacional, y seis paneles, que abordaron cuestiones como el *big data*, el Internet de la cosas o la videovigilancia, así como el estado actual de la tramitación del proyecto de ley chileno de protección de datos. Asimismo, tuvo lugar la presentación pública de los Estándares Iberoamericanos de Protección de Datos. Dicha sesión contó con una amplia asistencia de más de 300 participantes del ámbito profesional, académico y del sector público.

- Visita a la AEPD de una Delegación del Instituto de Acceso a la Información Pública y Ministerio de Salud de El Salvador, acompañados por representantes del Ministerio de Sanidad y de la FIIAPP, en el marco del Programa europeo EUROsociAL+. La reunión tuvo por objeto la presentación de un proyecto piloto de implantación de la historia clínica en hospitales de El Salvador.

- Curso General de Protección de Datos Personales. Impartido por personal de la AEPD, en colaboración con la Fundación CEDDET, y financiado por el Programa Intercoonecta de la AECID, preferentemente para empleados y directivos de las entidades integrantes de la RIPD. Se han organizado en esta edición dos grupos de 40 alumnos cada uno.

- Reunión con la Secretaría General Iberoamericana (SEGIB) para la presentación de los Estándares Iberoamericanos de Protección de Datos. Se evaluó la posibilidad de que se pudiese promover una iniciativa regional de cooperación en materia de protección de datos personales con vistas a la próxima Cumbre Iberoamericana en noviembre de 2018, en Guatemala.

- Seminario 'Privacidad y Comunicaciones electrónicas'. Lugar: Centro de la Cooperación Española en Montevideo. 22 y 23 de noviembre. Asistieron cuarenta representantes de autoridades de protección de datos y demás entidades integrantes de la RIPD de Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador,

España, México, Perú, República Dominicana y Uruguay. En dicho evento se debatió sobre cuestiones relativas a las comunicaciones electrónicas que suscitan una mayor inquietud desde la perspectiva de la normativa de protección de datos, a la luz del nuevo RGPD y del proyecto de Reglamento europeo sobre Privacidad y Comunicaciones Electrónicas (conocido como *E-Privacy*).

- Visitas institucionales a la AEPD del Presidente del Consejo para la Transparencia de Chile, y del Comisionado Presidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

8.2. CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Entre los días 25 y 29 de septiembre de 2017 tuvo lugar en Hong Kong la 39ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, bajo el lema 'Conectando Oeste y Este en la Protección y el Respeto a la Privacidad de los Datos'.

La AEPD participó en la Conferencia a través del Área Internacional.

Según el actual formato de la Conferencia, las sesiones fueron de dos tipos: cerradas, reservadas para autoridades de protección de datos y privacidad, que se celebraron los días 25 y 26; y abiertas, con participación de representantes de empresas, administraciones, mundo académico, etc.

El primer día de la sesión cerrada estuvo dedicado a debatir en torno a cómo proteger datos sensibles, impedir la discriminación y gestionar el riesgo cuando autoridades públicas comparten información.

La segunda jornada estuvo dedicada tanto a la discusión y aprobación de varias resoluciones como a conocer los informes de actividad de los grupos que funcionan en el ámbito de la Conferencia, como el grupo de educación digital o el grupo de cooperación en materia de "*enforcement*".

Las resoluciones aprobadas se referían a 'Protección de Datos en vehículos automáticos conectados', 'Colaboración entre las autoridades de protección de datos y de consumo para una mejor protección de los ciudadanos y consumidores en la economía digital' y 'Explorando nuevas opciones para la cooperación internacional en materia de enforcement'.

Por otro lado, la Conferencia presentó dos novedades este año.

Por una parte, se entregaron los primeros premios de Protección de Datos y Privacidad, que fueron convocados en la anterior conferencia de Marrakech.

Por otra, una parte sustancial de las discusiones durante la sesión cerrada se centró en cuestiones relativas al futuro de la conferencia.

La Conferencia ha crecido en tamaño y variedad de sus miembros. También ha ampliado su extensión en el tiempo, pasando a convertirse en un evento que, incluyendo las sesiones cerradas y abiertas y los eventos organizados en paralelo por numerosas entidades y organizaciones, dura una semana. Al mismo tiempo, las cuestiones relacionadas con la protección de datos y la privacidad han cobrado mayor importancia y relieve en todo el mundo, tanto en regiones con una tradición legislativa y de aplicación práctica en este terreno como en países que han adoptado recientemente normas de protección de datos o se plantean hacerlo en un futuro próximo.

Todo ello ha llevado a los miembros de la Conferencia a plantearse cómo avanzar en el desarrollo de la Conferencia de cara al futuro. Cuestiones como el número de miembros, relacionada con los requisitos que deberían cumplir las autoridades de protección de datos o privacidad para incorporarse a la Conferencia, la organización de los trabajos, el tipo de actuaciones que se deberían potenciar o, en su caso, abandonar, o la continuidad de la actividad de la conferencia entre las ediciones anuales son algunos de los temas que se han planteado.

Este debate se inició ya en la Conferencia de Marrakech, de 2016, donde se constituyó un grupo de trabajo que circuló varios cuestionarios entre los miembros y preparó, sobre la base de las respuestas recibidas, una serie de documentos de trabajo que sirvieron de base para las discusiones de esta edición.

La Conferencia acordó continuar estas discusiones, pero partiendo de un enfoque descentralizado, en el que los temas deberán debatirse primeramente en los diferentes foros regionales de protección de datos (entre ellos, la RIPD), para posteriormente mantener una discusión más estructurada en la próxima conferencia, que tendrá lugar en Bruselas.

Esta Conferencia suponía el tercer y último año de la presidencia del Comisionado de Nueva Zelanda. La Conferencia eligió para reemplazarlo a la Comisión Nacional de Libertades e Informática, CNIL, de Francia.

ANEXO.

LA AGENCIA EN CIFRAS

1. Actividad global

Resumen de actividad global

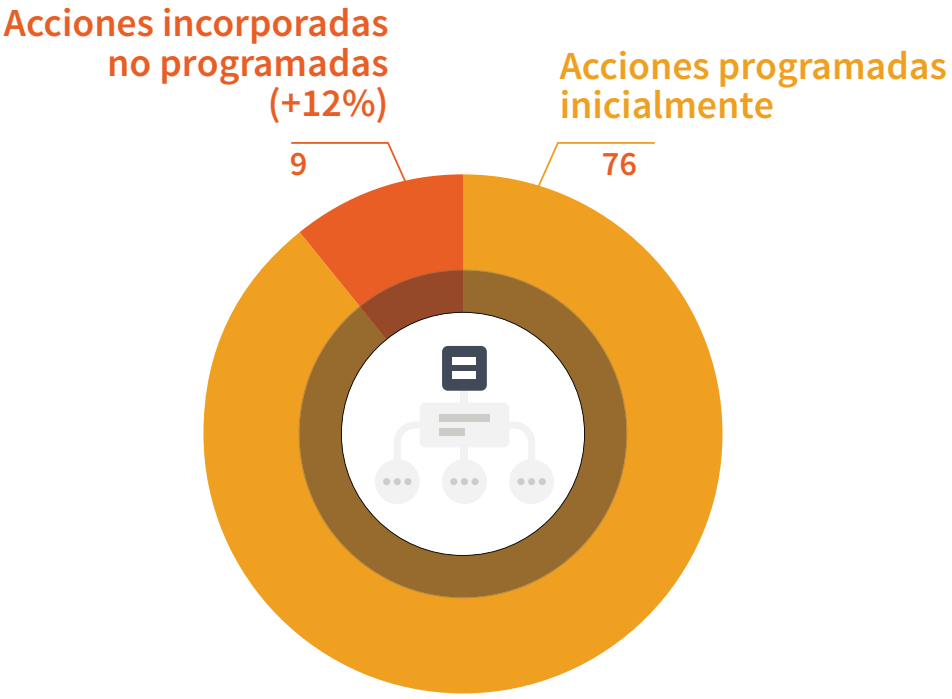
El desglose de estas y otras actividades se detalla en páginas posteriores de esta sección.

Resumen de actividad global			
	2016	2017	Δ% 2016-2017
Denuncias y reclamaciones en tramitación al acabar el ejercicio	3.039	2.025	-33,37%
Denuncias y reclamaciones que han tenido entrada durante el ejercicio	10.523	10.651	1,22%
Denuncias y reclamaciones resueltas	10.583	11.617	9,77%
Actuaciones del Plan Estratégico ejecutadas o puestas en marcha	74	78	5,41%
Consultas atendidas Atención al ciudadano	236.955	255.908	8%
Visitas recibidas en la web	5.534.282	6.724.113	21,5%
Consultas especializadas sobre tratamiento de datos de menores	696	895	28,59%
Accesos a la página de transparencia	305.538	856.245	180,24%
Accesos a la herramienta Facilita_RGPD*	-	29.009	-
Ficheros inscritos	4.510.346	4.914.934	9%

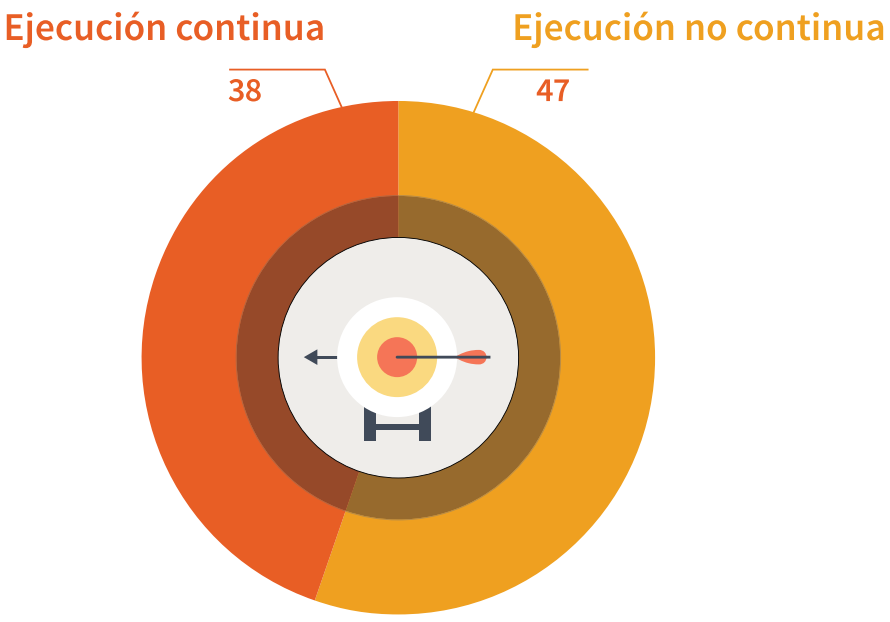
*Aplicación presentada en septiembre de 2017.

2. Plan estratégico

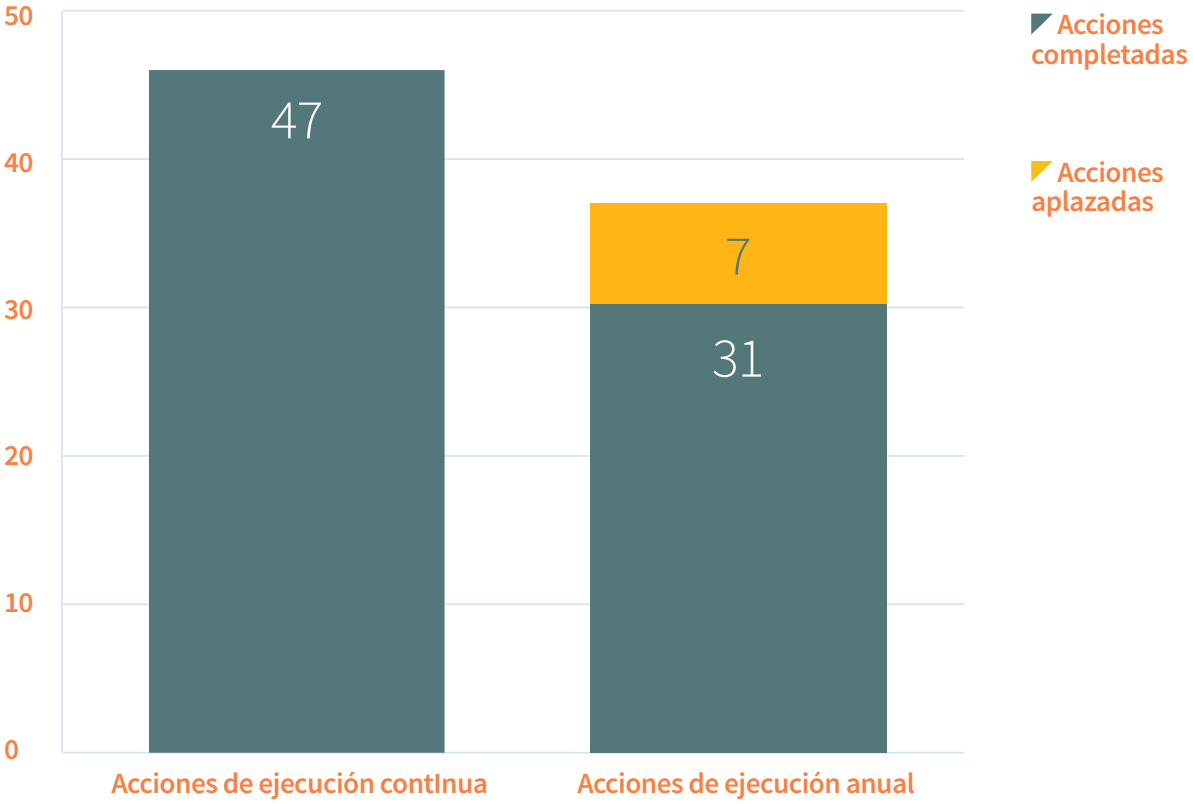
Acciones programadas en 2017



Tipo de ejecución

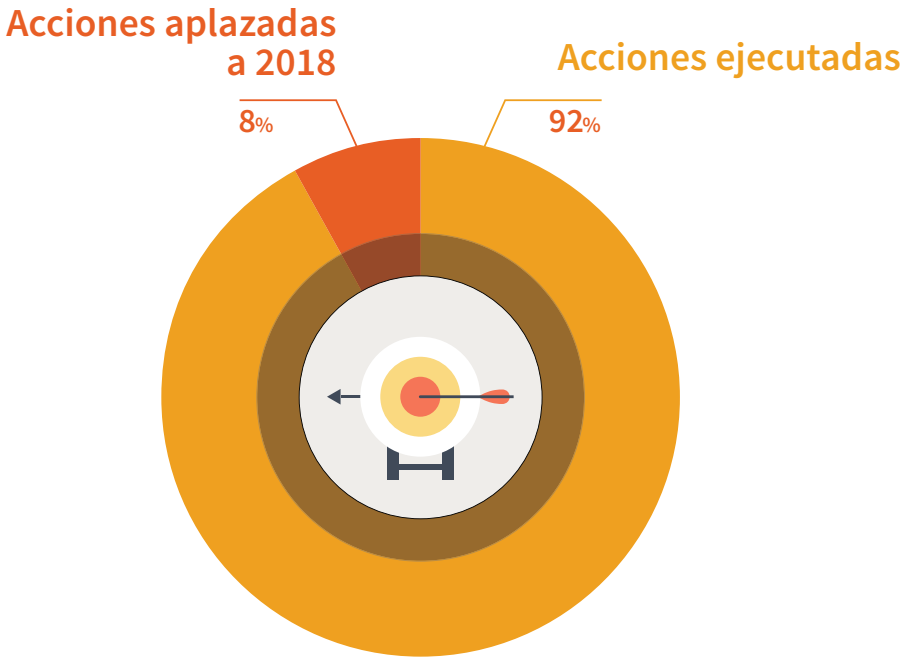


Grado de ejecución

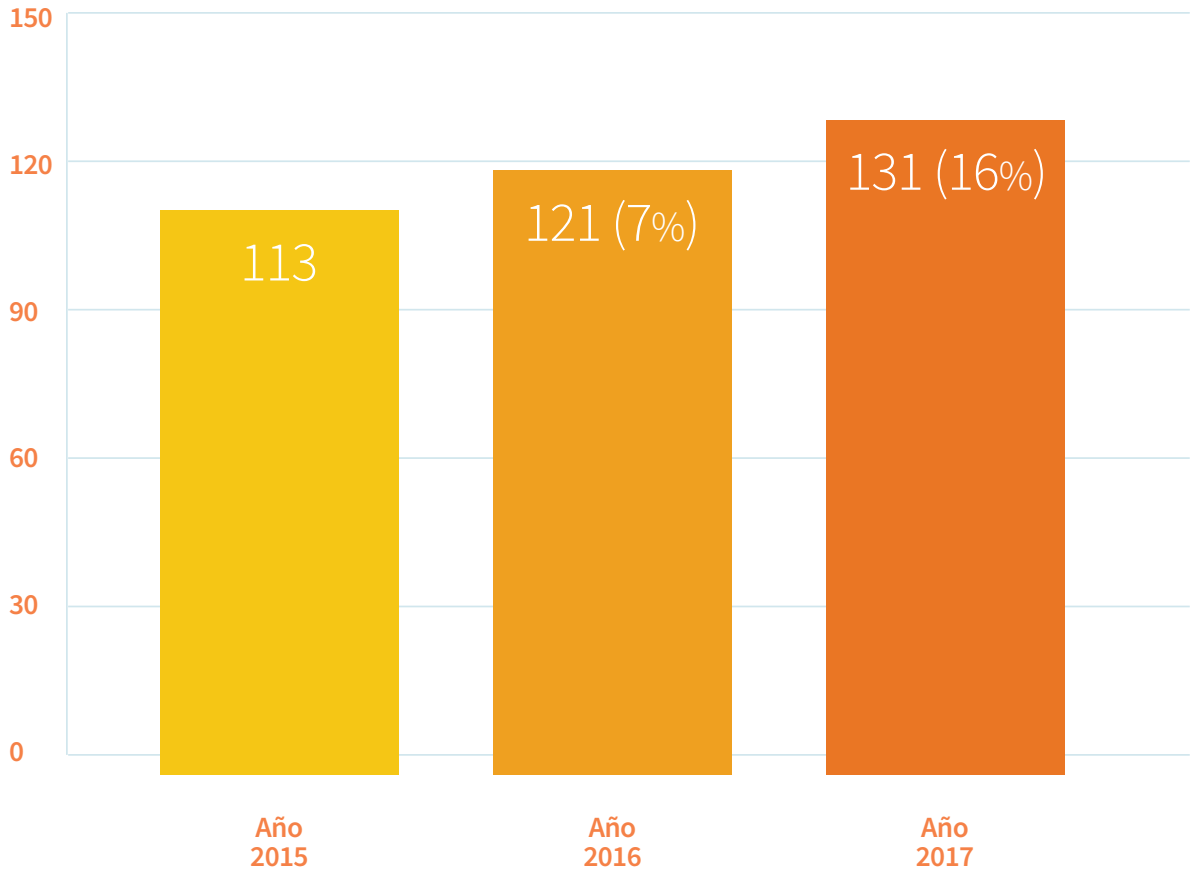


La Agencia ha incorporado al Plan 9 actuaciones nuevas en 2017.

En porcentaje



Evolución iniciativas del Plan – Periodo 2015-2017



3. Inspección de datos

Datos globales

Denuncias y reclamaciones en tramitación al acabar el ejercicio						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Reclamaciones de tutela	439	476	552	27,00%	15,97%	25,74%
Denuncias	2.634	2.563	1.473	73,00%	-42,53%	-44,08%
TOTAL	**3.073**	**3.039**	**2.025**	**100,00%**	**-33,37%**	**-34,10%**

Denuncias y reclamaciones que han tenido entrada durante el ejercicio						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Reclamaciones de tutela	2.082	2.588	2.654	25,00%	2,55%	27,47%
Denuncias	8.489	7.935	7.997	75,00%	0,78%	-5,80%
TOTAL	**10.571**	**10.523**	**10.651**	**100,00%**	**1,22%**	**0,76%**

Denuncias y reclamaciones resueltas						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Reclamaciones de tutela	2.113	2.471	2.824	24,00%	14,29%	33,65%
Denuncias	10.871	8.112	8.793	76,00%	8,39%	-19,12%
TOTAL	**12.984**	**10.583**	**11.617**	**100,00%**	**9,77%**	**-10,53%**

Resoluciones – Ejercicio de la potestad sancionadora

El número de denuncias tramitadas no tiene que coincidir necesariamente con las resoluciones firmadas: varias denuncias referidas a un mismo denunciado pueden agruparse, y paralelamente en una denuncia pueden aparecer múltiples denunciados dando origen a múltiples procedimientos sancionadores.

	Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
TIPO DE PROCEDIMIENTO	Archivo de actuaciones tras no subsanarse denuncia	691	949	1.159	35,00	22,13%	67,73%
	Archivo de actuaciones de investigación	1.040	883	907	27,00	2,72%	-12,79%
	Resolución de procedimientos de apercibimiento	397	492	490	15,00	-0,41%	23,43%
	Resolución de procedimientos sancionadores	693	573	731	22,00	27,57%	5,48%
	Resolución de procedimientos de infracción de las AAPP	65	56	60	2,00	7,14%	-7,69%
	TOTAL	**2.886**	**2.953**	**3.347**	**100,00%**	**13,34%**	**15,97%**

	Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
SEGÚN SENTIDO DE LA RESOLUCIÓN	Archivo actuaciones previas iniciadas	1.731	1.832	2.066	83,00	12,77%	19,35%
	Archivo de procedimiento de apercibimiento	216	311	289	12,00	-7,07%	33,80%
	Archivo de procedimiento sancionador	99	100	119	5,00	19,00%	20,20%
	Archivo de procedimiento de infracción de las AAPP	13	13	15	1,00	15,38%	15,38%
	TOTAL RESOLUCIONES DE ARCHIVO	**2.059**	**2.256**	**2.489**	**74,00**	**10,33%**	**20,88%**
	Declarativa de infracción con apercibimiento	181	181	200	23,00	10,50%	10,50%
	Declarativa de infracción con sanción económica	594	473	610	71,00	28,96%	2,69%
	Declarativa de infracción de las AAPP	52	43	45	5,00	4,65%	-13,46%
	TOTAL RESOLUCIONES DECLARATIVAS DE INFRACCIÓN	**827**	**697**	**855**	**26,00**	**22,67%**	**3,39%**
TOTAL RESOLUCIONES POTESTAD SANCIONADORA		**2.886**	**2.953**	**3.344**	**100**	**13,24%**	**15,87%**

Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
Inadmisión a trámite de denuncias sin actuaciones de investigación	6.049	4.681	4.752	1,52%	-21,44%

Resoluciones – Tutela de Derechos

Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Estimatoria	468	371	438	36,00%	18,06%	-6,41%
Estimatoria formal o parcial	252	270	368	30,00%	36,30%	46,03%
Desestimatoria	347	433	402	33,00%	-7,16%	15,85%
TOTAL	**1.067**	**1.074**	**1.208**	**100,00%**	**12,48%**	**13,21%**

Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
Inadmisión o desestimiento de reclamaciones de tutela	1.097	1.538	1.616	5,07%	47,31%

Eficacia administrativa

Se reflejan tiempos medios de tramitación (en días) desde que se registra la denuncia o se abren actuaciones de oficio hasta que se dicta resolución.

	Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
TIPO DE PROCEDIMIENTO	Archivo de denuncia sin actuaciones de investigación	106	64	**23,7**	-62,97%	-77,64%
	Archivo de actuaciones tras no subsanarse denuncia	179	83	**70,99**	-14,47%	-60,34%
	Archivo de actuaciones de investigación	372	323	**268,88**	-16,76%	-27,72%
	Resolución de procedimientos de apercibimiento	386	267	**239,05**	-10,47%	-38,07%
	Resolución de procedimientos sancionadores	507	507	**399,68**	-21,17%	-21,17%
	Resolución de procedimientos de infracción de las AAPP	522	477	**410,87**	-13,86%	-21,29%
	Resolución de procedimientos de tutela de derechos	136	120	**98,57**	-17,86%	-27,52%

Expedientes iniciados durante el ejercicio					
Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
Expedientes iniciados	2.293	2.826	2.668	-5,59%	16,35%

Sector privado

En este apartado se detallan cifras sobre infracciones declaradas en resoluciones de procedimientos sancionadores y de apercibimiento, pudiendo haberse declarado más de una infracción en cada uno de ellos.

Número de infracciones según Ley infringida						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
LOPD	782	1.174	1.256	90,95%	6,98%	60,61%
LSSI	100	117	110	7,97%	-5,98%	10,00%
LGT	13	11	15	1,09%	36,36%	15,38%
TOTAL	**895**	**1.302**	**1.381**	**100,00%**	**6,07%**	**54,30%**

Número de infracciones según gravedad						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Muy grave	3	2	7	0,51%	250,00%	133,33%
Grave	759	1.095	1.177	85,23%	7,49%	55,07%
Leve	133	205	197	14,27%	-3,90%	48,12%
TOTAL	**895**	**1.302**	**1.381**	**100,00%**	**6,07%**	**54,30%**

Aplicación de criterios de graduación en la declaración de infracciones y reducción de sanciones												
Año	2015	2016				2017				% relativo	Δ% 2016/ 2017	Δ% 2015/ 2017
	TOTAL	LOPD	LSSI	LGT	TOTAL	LOPD	LSSI	LGT	TOTAL			
Apercibimiento	187	461	29	0	490	483	46	0	529	38,31%	7,96%	182,89%
Sanción sin atenuación	231	465	81	11	557	772	59	15	846	61,26%	51,89%	266,23%
Sanciones reducidas por art. 85 de la Ley 39/2015	0				100				422	30,56%	322,00%	
TOTAL	**895**	**1.174**	**117**	**11**	**1.302**	**1.256**	**110**	**15**	**1.381**	**100%**	**6,07%**	**54,30%**

Evolución de las infracciones con sanción económica					
Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
Total sanciones	708	560	694	23,93%	-1,98%

Sector público

Procedimientos de infracción resueltos						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Local	38	23	30	43%	30,43%	-21,05%
Autonómica	25	20	20	29%	0,00%	-20,00%
General del Estado	12	10	17	25%	70,00%	41,67%
Otras Entidades de Derecho Público	3	3	2	3%	-33,33%	-33,33%
TOTAL	**78**	**56**	**69**	**100%**	**23,21%**	**-11,54%**

En un mismo procedimiento de infracción pueden figurar investigados de distintas administraciones territoriales, computándose tales procedimientos en una sola de las administraciones afectadas.

Áreas de actividad

Distribución de las actuaciones previas iniciadas*						
Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Ficheros de Morosidad	-	1.313	1.408	19,71%	7,24%	-
Reclamación de deudas	6.081	2.219	1.332	18,64%	-39,97%	-78,10%
Videovigilancia	1.157	1.036	975	13,65%	-5,89%	-15,73%
Administración pública	292	344	398	5,57%	15,70%	36,30%
Servicios de Internet (excepto spam)	427	435	395	5,53%	-9,20%	-7,49%
Publicidad y prospección comercial (excepto spam)	398	414	375	5,25%	-9,42%	-5,78%
Comunidades propietarios, admón. fincas, otros profesionales	260	107	327	4,58%	205,61%	25,77%
Comunicaciones electrónicas comerciales - spam (LSSI)	321	282	292	4,09%	3,55%	-9,03%
Contratación fraudulenta	-	356	291	4,07%	-18,26%	-
Recursos humanos, asuntos laborales	177	219	217	3,04%	-0,91%	22,60%
Comercio, transporte, hostelería	189	169	208	2,91%	23,08%	10,05%
Sanidad	206	225	207	2,90%	-8,00%	0,49%
Inscripción de ficheros / Información artículo 5	74	123	118	1,65%	-4,07%	59,46%
Organizaciones asociativas (excepto partidos políticos y sindicatos)	103	86	79	1,11%	-8,14%	-23,30%
Medios de comunicación	76	72	78	1,09%	8,33%	2,63%
Seguros	114	58	78	1,09%	34,48%	-31,58%
Enseñanza	47	49	72	1,01%	46,94%	53,19%
Otros	133	93	72	1,01%	-22,58%	-45,86%
Fuerzas y cuerpos de seguridad	52	38	60	0,84%	57,89%	15,38%
Asuntos relacionados con procedimientos judiciales	40	42	49	0,69%	16,67%	22,50%
Partidos políticos	88	50	42	0,59%	-16,00%	-52,27%
Sindicatos	53	40	39	0,55%	-2,50%	-26,42%
Documentación desechada sin destruir o borrar	20	25	33	0,46%	32,00%	65,00%
TOTAL	**8.132**	**7.039**	**7.145**	**100,00%**	**1,51%**	**-12,14%**

*Las actuaciones previas incluyen: las actuaciones de investigación incoadas por denuncia o de oficio (EI), las solicitudes de documentación adicional que no son subsanadas por el denunciante (AT) y el análisis de denuncias que finalmente no se admiten a trámite (IT).

Resoluciones sancionadoras del sector privado

Año	2015	2016	2017	% relativo	Δ% 2016/2017	Δ% 2015/2017
Ficheros de Morosidad		141	254	29,81%	80,14%	
Contratación fraudulenta		74	131	15,38%	77,03%	
Publicidad y prospección comercial (excepto spam)	22	54	124	14,55%	129,63%	463,64%
Reclamación de deudas	325	41	80	9,39%	95,12%	-75,38%
Videovigilancia	158	170	71	8,33%	-58,24%	-55,06%
Servicios de Internet (excepto spam)	51	43	55	6,46%	27,91%	7,84%
Comunicaciones electrónicas comerciales - spam (LSSI)	88	77	53	6,22%	-31,17%	-39,77%
Sanidad	12	5	16	1,88%	220,00%	33,33%
Inscripción de ficheros / Información artículo 5	5	1	14	1,64%	1300,00%	180,00%
Otros	18	13	13	1,53%	0,00%	-27,78%
Seguros	13	10	9	1,06%	-10,00%	-30,77%
Recursos humanos, asuntos laborales	3	1	9	1,06%	800,00%	200,00%
Documentación desechada sin destruir o borrar	6	2	6	0,70%	200,00%	0,00%
Sindicatos	2	1	5	0,59%	400,00%	150,00%
Partidos políticos		4	4	0,47%	0,00%	
Comunidades propietarios, admón. fincas, otros profesionales	10	6	3	0,35%	-50,00%	-70,00%
Organizaciones asociativas, excepto partidos políticos y sindicatos	10	4	3	0,35%	-25,00%	-70,00%
Comercio, transporte, hostelería	39	5	2	0,23%	-60,00%	-94,87%
Seguridad privada	11	0	0	0,00%		-100,00%
Enseñanza	2	2	0	0,00%	-100,00%	-100,00%
TOTAL	**775**	**654**	**852**	**100,00%**	**30,28%**	**9,94%**

Áreas con mayor importe global de sanciones						
ACTIVIDAD	2015 (€)	2016 (€)	2017 (€)	% relativo	Δ% 2016/2017	Δ% 2015/2017
Ficheros de Morosidad		5.835.007	6.318.008	39,64%	8,28%	
Contratación fraudulenta		3.420.003	3.328.401	20,88%	-2,68%	
Publicidad (excepto spam)	502.108	1.964.305	2.695.382	16,91%	37,22%	436,81%
Servicios de internet			2.146.440	13,47%		
Reclamación de deudas	9.485.906	1.065.801	1.152.104	7,23%	8,10%	-87,85%
Comunicaciones electrónicas comerciales - spam (LSSI)	897.403	439.851	297.322	1,87%	-32%	-66,87%
TOTAL (6 PRIMERAS)	**10.885.417**	**12.724.967**	**15.937.657**	**100,00%**	**25,25%**	**46,41%**
% relativo al total del año	**79,38%**	**89,67%**	**93,64%**	**-**	**4,43%**	**17,97%**

Año	2015	2016	2017	Δ% 2016/2017	Δ% 2015/2017
Importe total sanciones	13.712.621	14.190.173	17.319.962	22,06%	26,31%

El importe total se refiere a la cuantía de las sanciones impuestas en el ejercicio (incluyendo las posibles modificaciones en la cuantía como consecuencia de los correspondientes recursos de reposición).

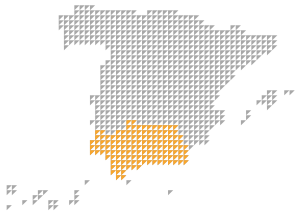
Procedimientos de tutela de derechos

Distribución de Derechos tutelados según resultado de la resolución				
	Estimatoria	Estimatoria formal o parcial	Desestimatoria	TOTAL
Cancelación	247	215	282	744
Acceso	160	121	95	376
Rectificación	9	15	13	37
Oposición/exclusión	22	17	12	51
TOTAL	**438**	**368**	**402**	**1.208**

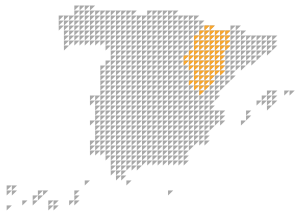
En cada procedimiento resuelto puede haberse tutelado más de un derecho ARCO.

Distribución geográfica

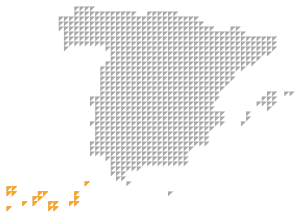
Distribución geográfica de las actuaciones previas iniciadas en 2017 (provincia del denunciante)



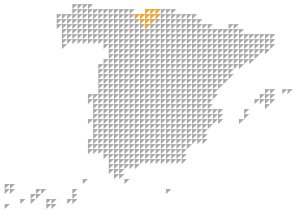
Comunidad Autónoma de Andalucía	Provincia	Nº	% relativo
	Almería	78	1,12%
	Cádiz	154	2,21%
	Córdoba	96	1,38%
	Granada	141	2,03%
	Huelva	64	0,92%
	Jaén	65	0,93%
	Málaga	236	3,39%
	Sevilla	291	4,18%
	TOTAL COMUNIDAD	**1.125**	**16,18%**

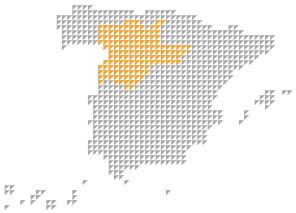


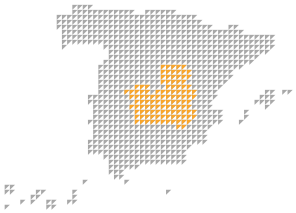
Comunidad Autónoma de Aragón	Provincia	Nº	% relativo
	Huesca	18	0,26%
	Teruel	14	0,20%
	Zaragoza	143	2,06%
	TOTAL COMUNIDAD	**175**	**2,52%**

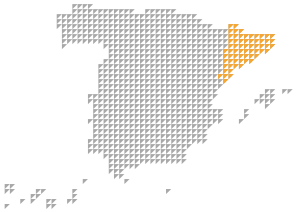


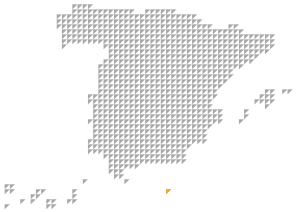
Comunidad Autónoma de Canarias	Provincia	Nº	% relativo
	Las Palmas	226	3,25%
	Santa Cruz De Tenerife	145	2,09%
	TOTAL COMUNIDAD	**371**	**5,34%**

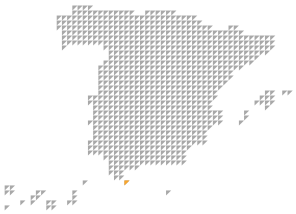
Comunidad Autónoma de Cantabria	Provincia	Nº	% relativo
	Cantabria	85	1,22%
	TOTAL COMUNIDAD	**85**	**1,22%**

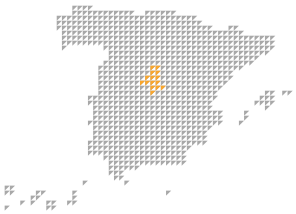
Comunidad Autónoma de Castilla y León	Provincia	Nº	% relativo
	Ávila	12	0,17%
	Burgos	55	0,79%
	León	66	0,95%
	Palencia	24	0,35%
	Salamanca	52	0,75%
	Segovia	29	0,42%
	Soria	1	0,01%
	Valladolid	91	1,31%
	Zamora	25	0,36%
	TOTAL COMUNIDAD	**355**	**5,10%**

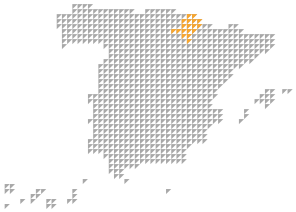
Comunidad Autónoma de Castilla-La Mancha	Provincia	Nº	% relativo
	Albacete	42	0,60%
	Ciudad Real	60	0,86%
	Cuenca	17	0,24%
	Guadalajara	46	0,66%
	Toledo	99	1,42%
	TOTAL COMUNIDAD	**264**	**3,80%**

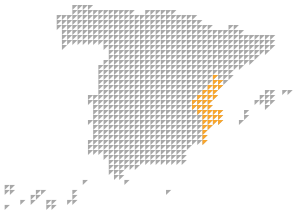
Comunidad Autónoma de Cataluña	Provincia	Nº	% relativo
	Barcelona	619	8,90%
	Girona	60	0,86%
	Lleida	27	0,39%
	Tarragona	89	1,28%
	TOTAL COMUNIDAD	**795**	**11,43%**

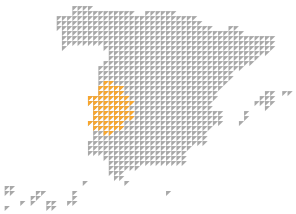
Ciudad Autónoma de Ceuta	Región	Nº	% relativo
	Ceuta	5	0,07%
	TOTAL COMUNIDAD	**5**	**0,07%**

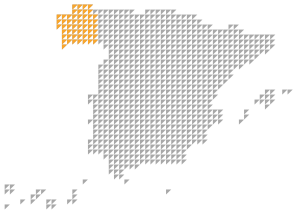
Ciudad Autónoma de Melilla	Región	Nº	% relativo
	Melilla	8	0,12%
	TOTAL COMUNIDAD	**8**	**0,12%**

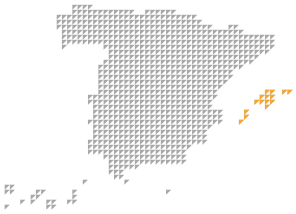
Comunidad de Madrid	Provincia	Nº	% relativo
	Madrid	1.645	23,66%
	TOTAL COMUNIDAD	**1.645**	**23,66%**

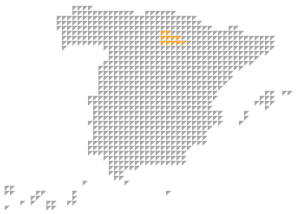
Comunidad Foral de Navarra	Provincia	Nº	% relativo
	Navarra	52	0,75%
	TOTAL COMUNIDAD	**52**	**0,75%**

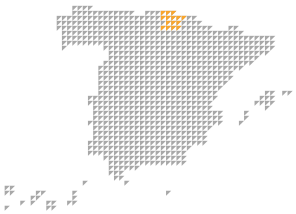
Comunitat Valenciana	Provincia	Nº	% relativo
	Alicante / Alacant	227	3,26%
	Castellón / Castelló	74	1,06%
	Valencia / València	342	4,92%
	TOTAL COMUNIDAD	**643**	**9,25%**

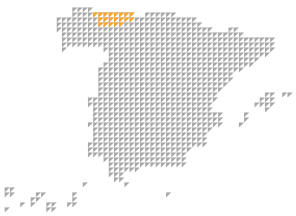
Comunidad Autónoma de Extremadura	Provincia	Nº	% relativo
	Badajoz	113	1,62%
	Cáceres	53	0,76%
	TOTAL COMUNIDAD	**166**	**2,39%**

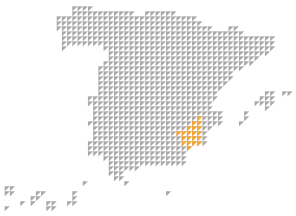
Comunidad Autónoma de Galicia	Provincia	Nº	% relativo
	A Coruña	224	3,22%
	Lugo	48	0,69%
	Ourense	40	0,58%
	Pontevedra	175	2,52%
	TOTAL COMUNIDAD	**487**	**7,00%**

Comunidad Autónoma de Illes Balears	Provincia	Nº	% relativo
	Illes Balears	142	2,04%
	TOTAL COMUNIDAD	**142**	**2,04%**

Comunidad Autónoma de La Rioja	Provincia	Nº	% relativo
	La Rioja	42	0,60%
	TOTAL COMUNIDAD	42	0,60%

Comunidad Autónoma del País Vasco	Provincia	Nº	% relativo
	Araba / Álava	32	0,46%
	Bizkaia	93	1,34%
	Gipuzkoa	39	0,56%
	TOTAL COMUNIDAD	**164**	**2,36%**

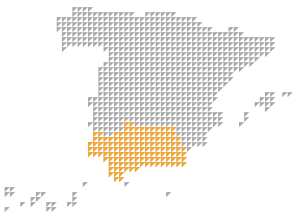
Comunidad Autónoma del Principado de Asturias	Provincia	Nº	% relativo
	Asturias	216	3,11%
	TOTAL COMUNIDAD	**216**	**3,11%**

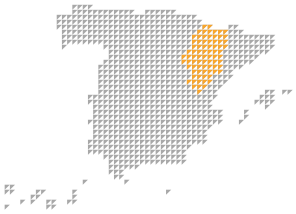
Comunidad Autónoma de la Región de Murcia	Provincia	Nº	% relativo
	Murcia	214	3,08%
	TOTAL COMUNIDAD	**214**	**3,08%**
	**TOTAL**	**6.954**	**100,00%**

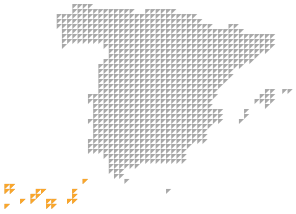
Se incluyen denuncias archivadas sin actuaciones (expedientes IT), denuncias no subsanadas (AT) y expedientes de investigación previa (EI).

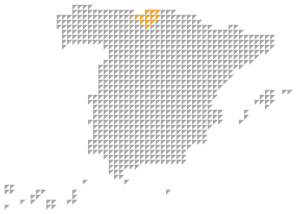
No se consideran las actuaciones previas iniciadas de oficio a iniciativa de la Directora o las iniciadas por solicitud de colaboración de otras autoridades extranjeras de protección de datos.

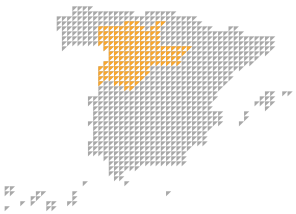
Establecimiento de investigados en procedimientos sancionadores y de apercibimiento resueltos en 2017

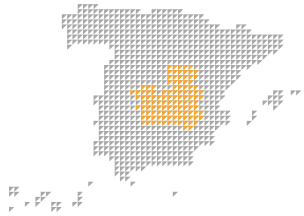
Comunidad Autónoma de Andalucía	Provincia	Nº	% relativo
	Almería	10	0,82%
	Cádiz	12	0,99%
	Córdoba	0	0,00%
	Granada	12	0,99%
	Huelva	3	0,25%
	Jaén	9	0,74%
	Málaga	29	2,38%
	Sevilla	30	2,47%
	TOTAL COMUNIDAD	**105**	**8,63%**

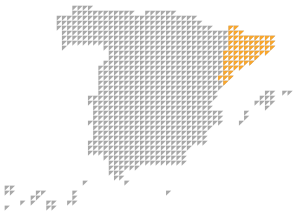
Comunidad Autónoma de Aragón	Provincia	Nº	% relativo
	Huesca	1	0,08%
	Teruel	1	0,08%
	Zaragoza	15	1,23%
	TOTAL COMUNIDAD	**17**	**1,40%**

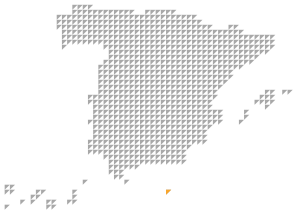
Comunidad Autónoma de Canarias	Provincia	Nº	% relativo
	Las Palmas	37	3,04%
	Santa Cruz De Tenerife	19	1,56%
	TOTAL COMUNIDAD	**56**	**4,61%**

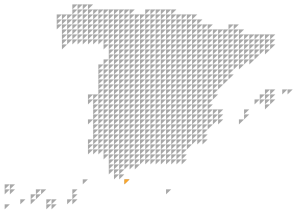
Comunidad Autónoma de Cantabria	Provincia	Nº	% relativo
	Cantabria	13	1,07%
	TOTAL COMUNIDAD	**13**	**1,07%**

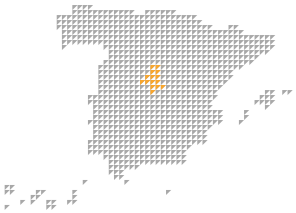
Comunidad Autónoma de Castilla y León	Provincia	Nº	% relativo
	Ávila	1	0,08%
	Burgos	5	0,41%
	León	7	0,58%
	Palencia	1	0,08%
	Salamanca	2	0,16%
	Segovia	1	0,08%
	Soria	0	0,00%
	Valladolid	22	1,81%
	Zamora	4	0,33%
	TOTAL COMUNIDAD	**43**	**3,54%**

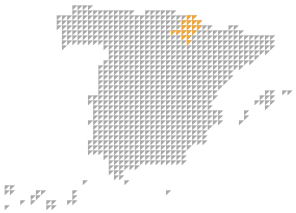
Comunidad Autónoma de Castilla-La Mancha	Provincia	Nº	% relativo
	Albacete	4	0,33%
	Ciudad Real	2	0,16%
	Cuenca	0	0,00%
	Guadalajara	4	0,33%
	Toledo	7	0,58%
	TOTAL COMUNIDAD	**17**	**1,4%**

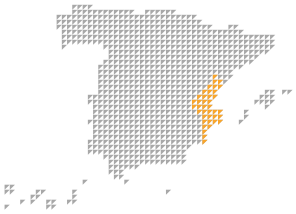
Comunidad Autónoma de Cataluña	Provincia	Nº	% relativo
	Barcelona	148	12,17%
	Girona	9	0,74%
	Lleida	4	0,33%
	Tarragona	3	0,25%
	TOTAL COMUNIDAD	**164**	**13,49%**

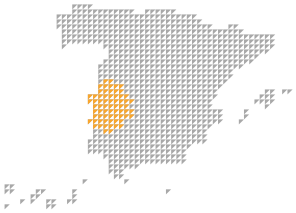
Ciudad Autónoma de Ceuta	Región	Nº	% relativo
	Ceuta	1	0,08%
	TOTAL COMUNIDAD	**1**	**0,08%**

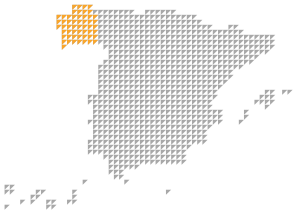
Ciudad Autónoma de Melilla	Región	Nº	% relativo
	Melilla	0	0,00%
	TOTAL COMUNIDAD	**0**	**0,00%**

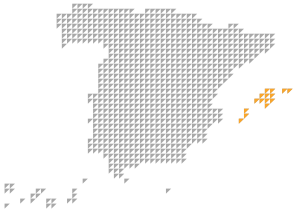
Comunidad de Madrid	Provincia	Nº	% relativo
	Madrid	570	46,88%
	TOTAL COMUNIDAD	**570**	**46,88%**

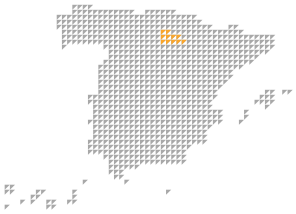
Comunidad Foral de Navarra	Provincia	Nº	% relativo
	Navarra	8	0,66%
	TOTAL COMUNIDAD	**8**	**0,66%**

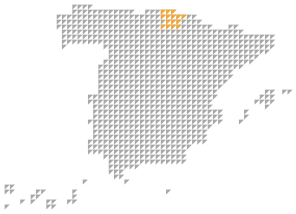
Comunitat Valenciana	Provincia	Nº	% relativo
	Alicante / Alacant	17	1,40%
	Castellón / Castelló	10	0,82%
	Valencia / València	31	2,55%
	TOTAL COMUNIDAD	**58**	**4,77%**

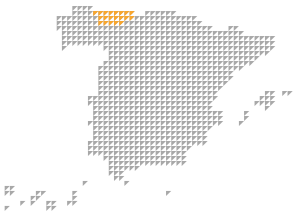
Comunidad Autónoma de Extremadura	Provincia	Nº	% relativo
	Badajoz	9	0,74%
	Cáceres	9	0,74%
	TOTAL COMUNIDAD	**18**	**1,48%**

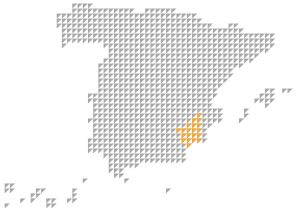
Comunidad Autónoma de Galicia	Provincia	Nº	% relativo
	A Coruña	34	2,80%
	Lugo	4	0,33%
	Ourense	3	0,25%
	Pontevedra	21	1,73%
	TOTAL COMUNIDAD	**62**	**5,10%**

Comunidad Autónoma de Illes Balears	Provincia	Nº	% relativo
	Illes Balears	15	1,23%
	TOTAL COMUNIDAD	**15**	**1,23%**

Comunidad Autónoma de La Rioja	Provincia	Nº	% relativo
	La Rioja	3	0,25%
	TOTAL COMUNIDAD	**3**	**0,25%**

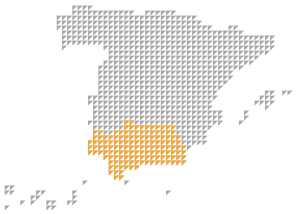
Comunidad Autónoma del País Vasco	Provincia	Nº	% relativo
	Araba/Álava	1	0,08%
	Bizkaia	18	1,48%
	Gipuzkoa	8	0,66%
	TOTAL COMUNIDAD	**27**	**2,22%**

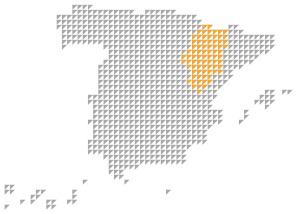
Comunidad Autónoma del Principado de Asturias	Provincia	Nº	% relativo
	Asturias	25	2,06%
	TOTAL COMUNIDAD	**25**	**2,06%**

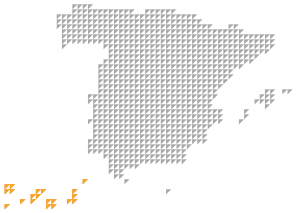
Comunidad Autónoma de la Región de Murcia	Provincia	Nº	% relativo
	Murcia	14	1,15%
	TOTAL COMUNIDAD	**14**	**1,15%**

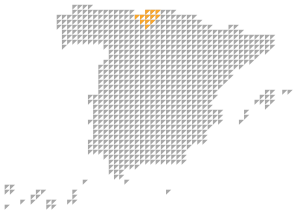
	**TOTAL**	**1.216**	**100,00%**

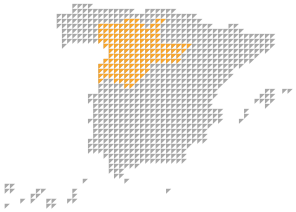
Sede de los investigados en procedimientos de infracción de las AAPP resueltos en 2017

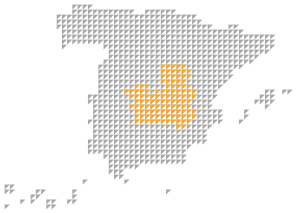
Comunidad Autónoma de Andalucía	Provincia	Nº	% relativo
	Cádiz	2	3%
	Córdoba	1	2%
	Jaén	1	2%
	Málaga	1	2%
	Sevilla	10	17%
	TOTAL COMUNIDAD	**15**	**25%**

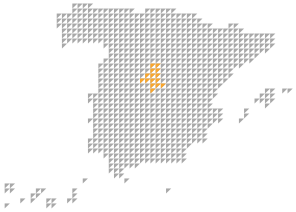
Comunidad Autónoma de Aragón	Provincia	Nº	% relativo
	Zaragoza	3	5%
	TOTAL COMUNIDAD	**3**	**5%**

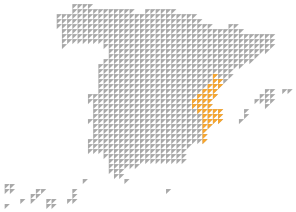
Comunidad Autónoma de Canarias	Provincia	Nº	% relativo
	Las Palmas	2	3%
	TOTAL COMUNIDAD	**2**	**3%**

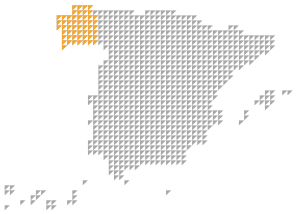
Comunidad Autónoma de Cantabria	Provincia	Nº	% relativo
	Cantabria	1	2%
	TOTAL COMUNIDAD	**1**	**2%**

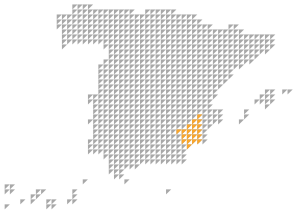
Comunidad Autónoma de Castilla y León	Provincia	Nº	% relativo
	Burgos	1	2%
	Valladolid	2	3%
	Zamora	1	2%
	TOTAL COMUNIDAD	**4**	**7%**

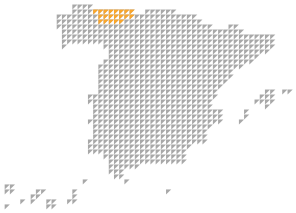
Comunidad Autónoma de Castilla-La Mancha	Provincia	Nº	% relativo
	Ciudad Real	1	2%
	Toledo	2	3%
	TOTAL COMUNIDAD	**3**	**5%**

Comunidad de Madrid	Provincia	Nº	% relativo
	Madrid	15	25%
	TOTAL COMUNIDAD	**15**	**25%**

Comunitat Valenciana	Provincia	Nº	% relativo
	Alicante / Alacant	3	5%
	Valencia / València	2	3%
	TOTAL COMUNIDAD	**5**	**8%**

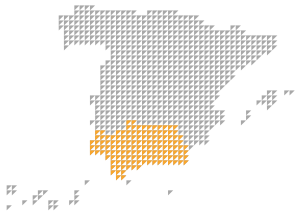
Comunidad Autónoma de Galicia	Provincia	Nº	% relativo
	A Coruña	7	12%
	Lugo	1	2%
	Pontevedra	1	2%
	TOTAL COMUNIDAD	**9**	**15%**

Comunidad Autónoma de la Región de Murcia	Provincia	Nº	% relativo
	Murcia	1	2%
	TOTAL COMUNIDAD	**1**	**2%**

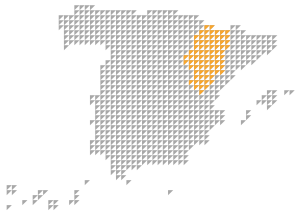
Comunidad Autónoma del Principado de Asturias	Provincia	Nº	% relativo
	Asturias	2	3%
	TOTAL COMUNIDAD	**2**	**3%**

	**TOTAL**	**60**	**100,00%**

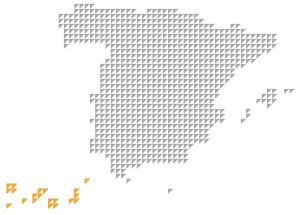
Distribución geográfica de los procedimientos de tutela de derechos iniciados en 2017 (provincia del reclamante)



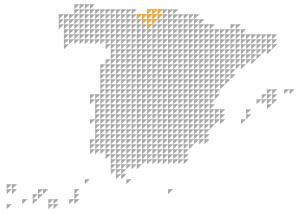
Comunidad Autónoma de Andalucía	Provincia	Nº	% Relativo
	Almería	30	1,06%
	Cádiz	76	2,70%
	Córdoba	33	1,17%
	Granada	57	2,02%
	Huelva	16	0,57%
	Jaén	33	1,17%
	Málaga	77	2,73%
	Sevilla	112	3,98%
	TOTAL COMUNIDAD	**434**	**15,41%**



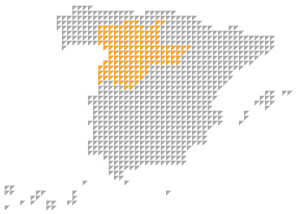
Comunidad Autónoma de Aragón	Provincia	Nº	% Relativo
	Huesca	7	0,25%
	Teruel	4	0,14%
	Zaragoza	63	2,24%
	TOTAL COMUNIDAD	**74**	**2,63%**

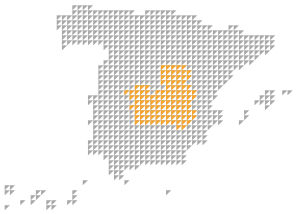


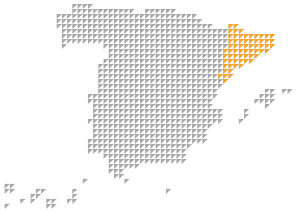
Comunidad Autónoma de Canarias	Provincia	Nº	% Relativo
	Las Palmas	82	2,91%
	Santa Cruz De Tenerife	60	2,13%
	TOTAL COMUNIDAD	**142**	**5,04%**

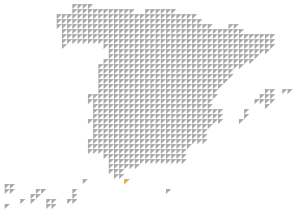


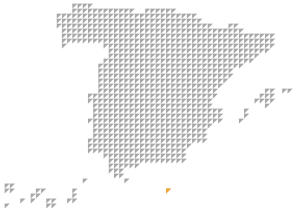
Comunidad Autónoma de Cantabria	Provincia	Nº	% Relativo
	Cantabria	38	1,35%
	TOTAL COMUNIDAD	**38**	**1,35%**

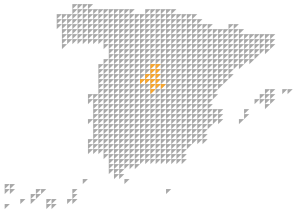
Comunidad Autónoma de Castilla y León	Provincia	Nº	% Relativo
	Ávila	8	0,28%
	Burgos	13	0,46%
	León	29	1,03%
	Palencia	7	0,25%
	Salamanca	23	0,82%
	Segovia	5	0,18%
	Soria	2	0,07%
	Valladolid	44	1,56%
	Zamora	3	0,11%
	TOTAL COMUNIDAD	**134**	**4,76%**

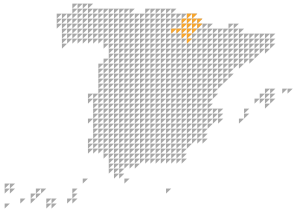
Comunidad Autónoma de Castilla-La Mancha	Provincia	Nº	% Relativo
	Albacete	10	0,35%
	Ciudad Real	19	0,67%
	Cuenca	4	0,14%
	Guadalajara	9	0,32%
	Toledo	36	1,28%
	TOTAL COMUNIDAD	**78**	**2,77%**

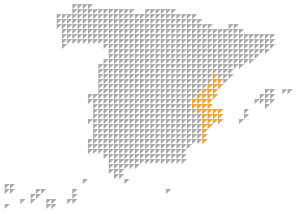
Comunidad Autónoma de Cataluña	Provincia	Nº	% Relativo
	Barcelona	246	8,73%
	Girona	22	0,78%
	Lleida	6	0,21%
	Tarragona	46	1,63%
	TOTAL COMUNIDAD	**320**	**11,36%**

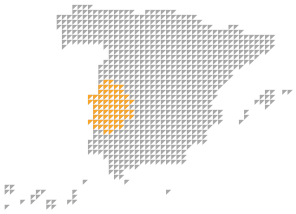
Ciudad Autónoma de Melilla	Provincia	Nº	% Relativo
	Ceuta	2	0,07%
	TOTAL COMUNIDAD	**2**	**0,07%**

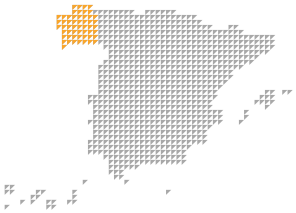
Ciudad Autónoma de Ceuta	Provincia	Nº	% Relativo
	Melilla	1	0,04%
	TOTAL COMUNIDAD	**1**	**0,04%**

Comunidad de Madrid	Provincia	Nº	% Relativo
	Madrid	655	23,25%
	TOTAL COMUNIDAD	**655**	**23,25%**

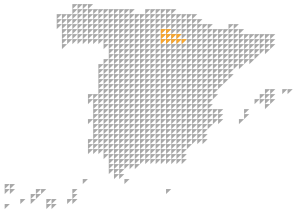
Comunidad Foral de Navarra	Provincia	Nº	% Relativo
	Navarra	18	0,64%
	TOTAL COMUNIDAD	**18**	**0,64%**

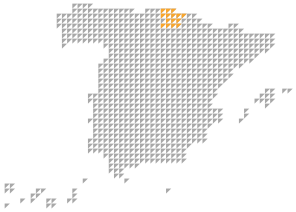
Comunitat Valenciana	Provincia	Nº	% Relativo
	Alicante / Alacant	94	3,34%
	Castellón / Castelló	103	3,66%
	Valencia / València	161	5,72%
	TOTAL COMUNIDAD	**358**	**12,71%**

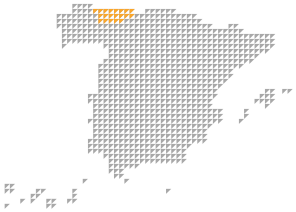
Comunidad Autónoma de Extremadura	Provincia	Nº	% Relativo
	Badajoz	62	2,20%
	Cáceres	48	1,70%
	TOTAL COMUNIDAD	**110**	**3,90%**

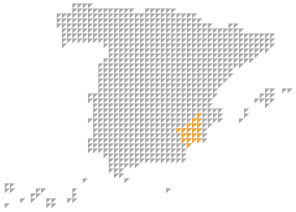
Comunidad Autónoma de Galicia	Provincia	Nº	% Relativo
	A Coruña	76	2,70%
	Lugo	7	0,25%
	Ourense	14	0,50%
	Pontevedra	45	1,60%
	TOTAL COMUNIDAD	**142**	**5,04%**

Comunidad Autónoma de Illes Balears	Provincia	Nº	% Relativo
	Illes Balears	46	1,63%
	TOTAL COMUNIDAD	**46**	**1,63%**

Comunidad Autónoma de La Rioja	Provincia	Nº	% Relativo
	La Rioja	15	0,53%
	TOTAL COMUNIDAD	**15**	**0,53%**

Comunidad Autónoma del País Vasco	Provincia	Nº	% Relativo
	Araba/Álava	17	0,60%
	Bizkaia	37	1,31%
	Gipuzkoa	12	0,43%
	TOTAL COMUNIDAD	**66**	**2,34%**

Comunidad Autónoma del Principado de Asturias	Provincia	Nº	% Relativo
	Asturias	78	2,77%
	TOTAL COMUNIDAD	**78**	**2,77%**

Comunidad Autónoma de la Región de Murcia	Provincia	Nº	% Relativo
	Murcia	106	3,76%
	TOTAL COMUNIDAD	**106**	**3,76%**

	**TOTAL**	**2817**	**100,00%**

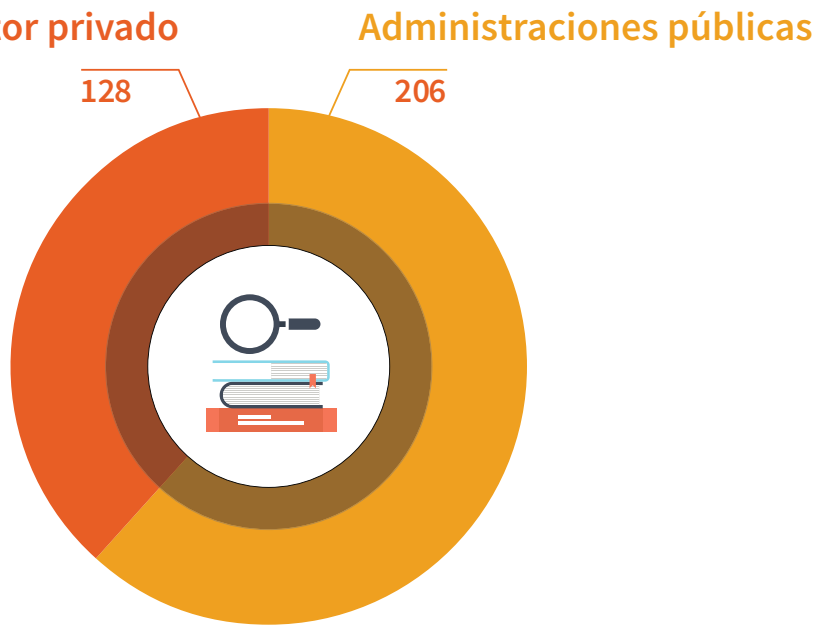
4. Gabinete jurídico

Consultas

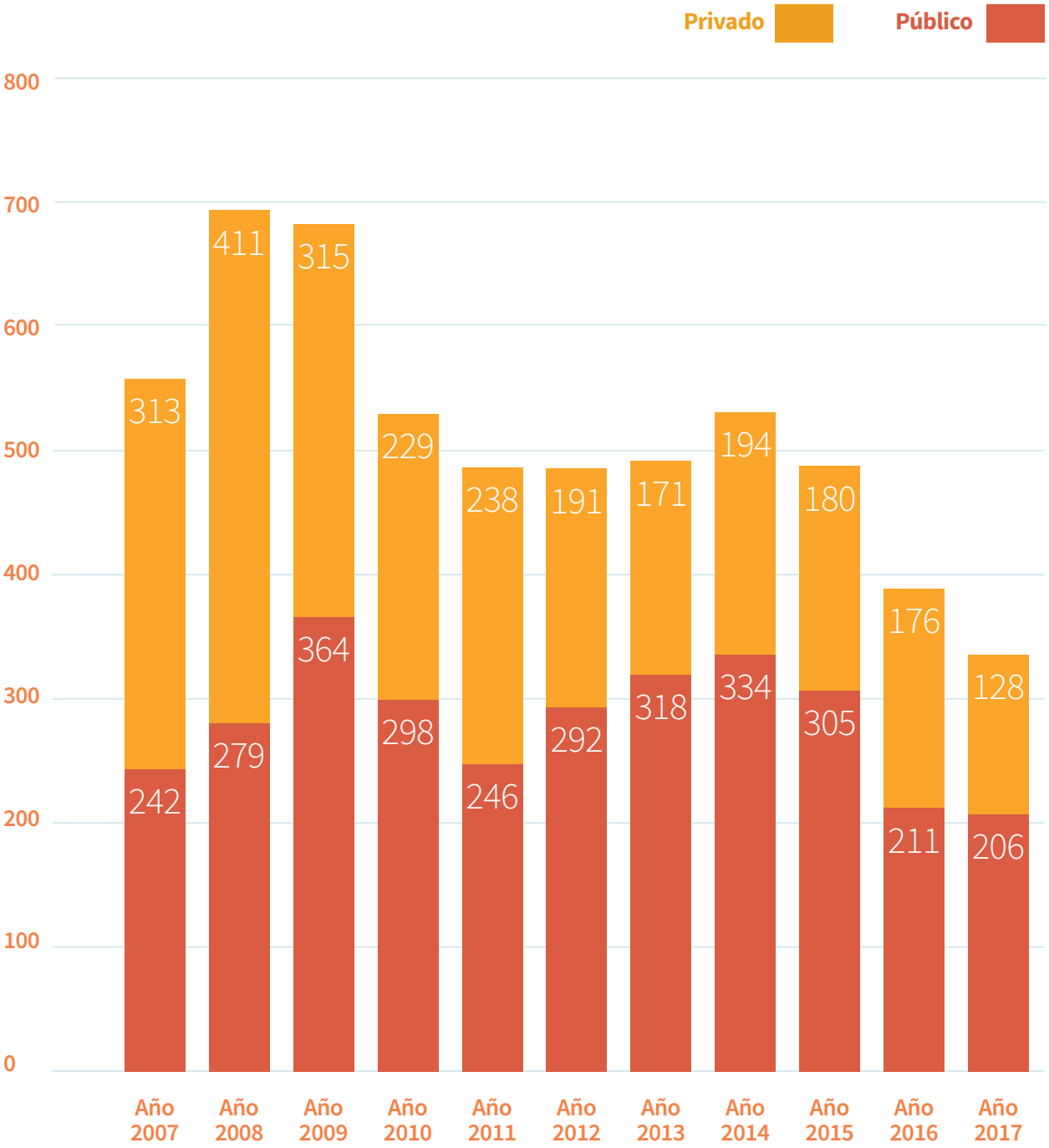
Administraciones públicas	
Administración General del Estado	85
Comunidades Autónomas	68
Entidades Locales	24
Otros Organismos	30
TOTAL	**206**

Consultas privadas	
Asociaciones y Fundaciones	14
Empresas	75
Particulares	32
Sindicatos	5
Otros	2
TOTAL	**128**

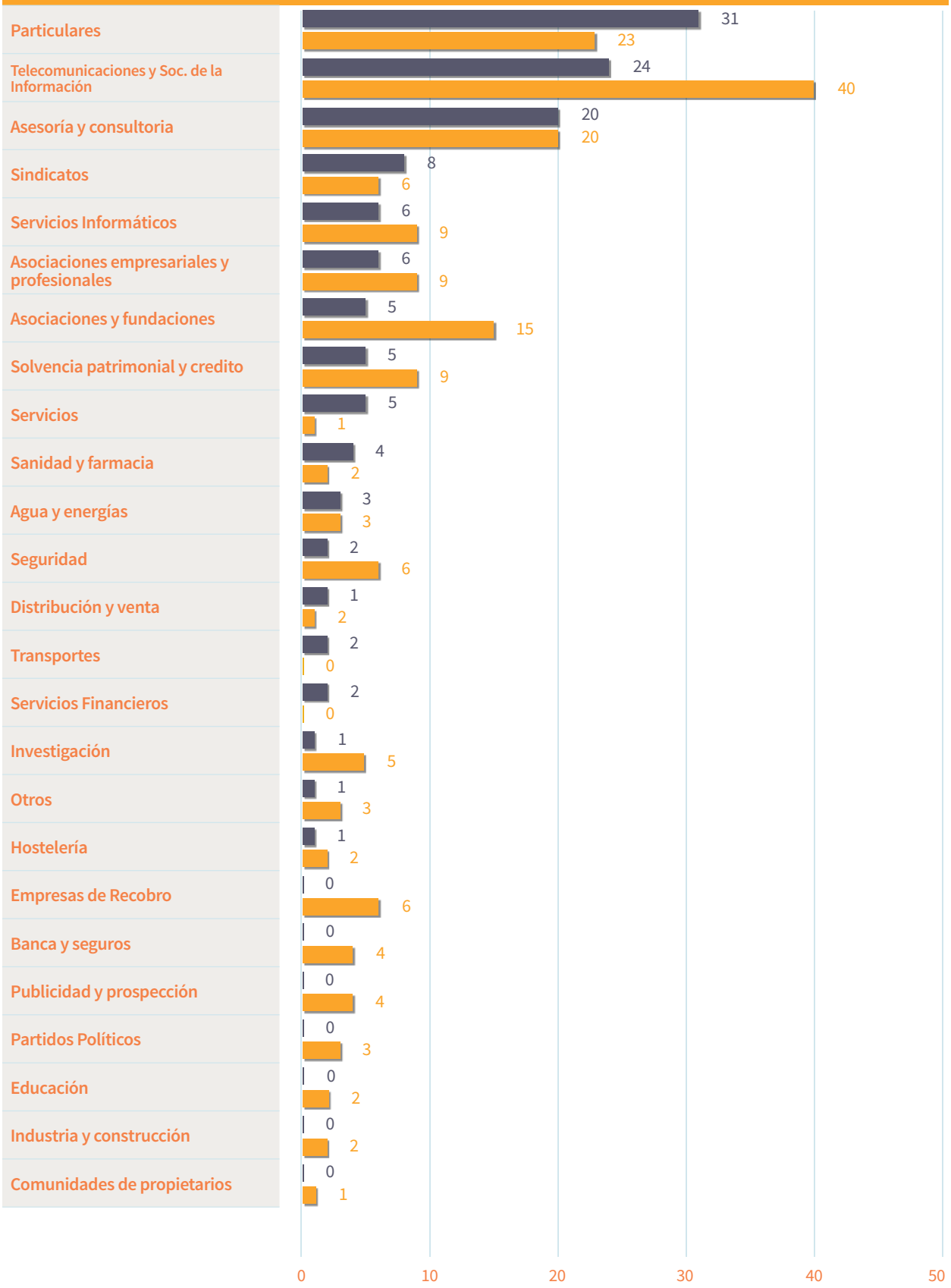
Distribución 2017 de consultas públicas/privadas



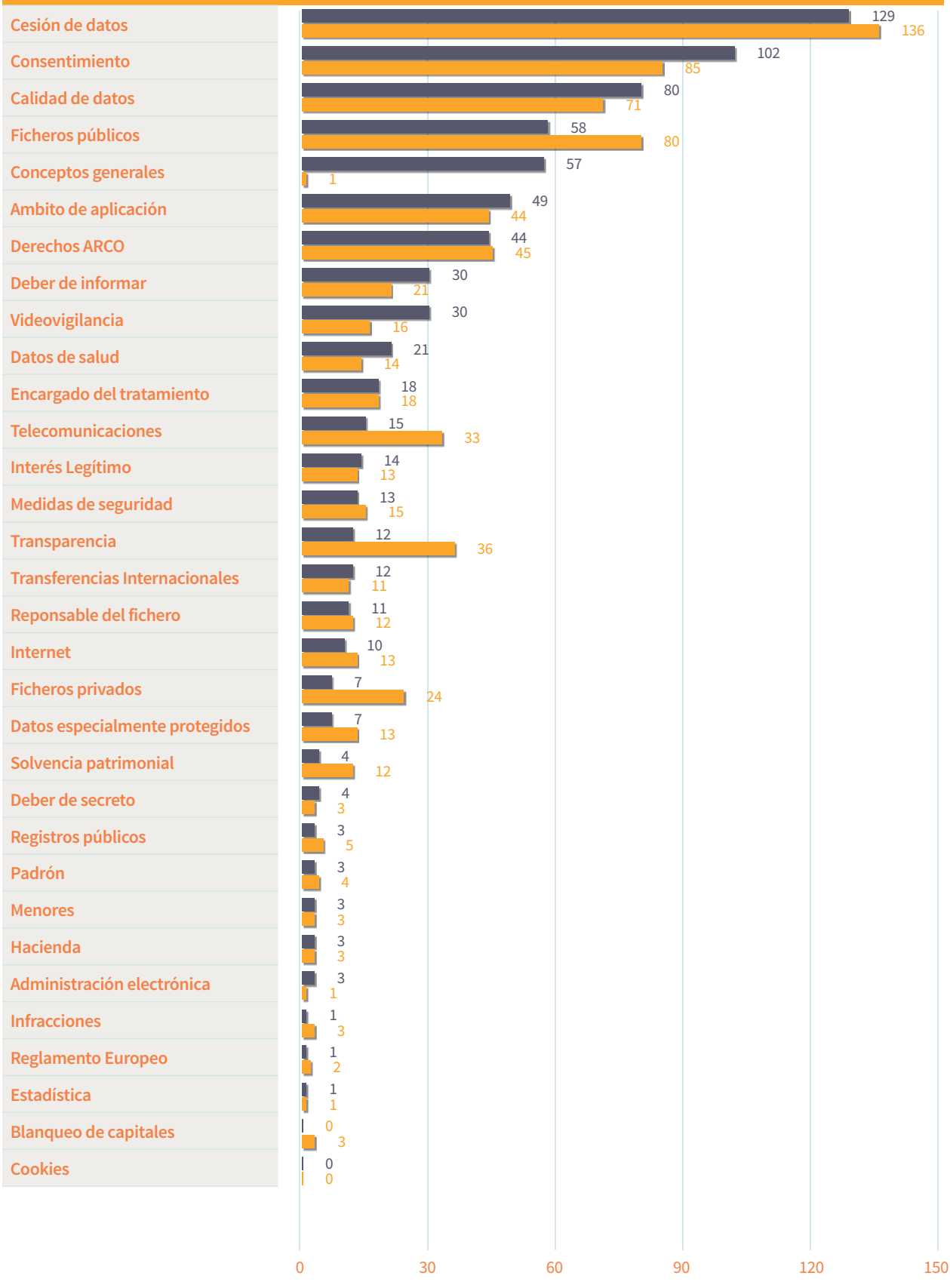
Evolución de las consultas (2007-2017)



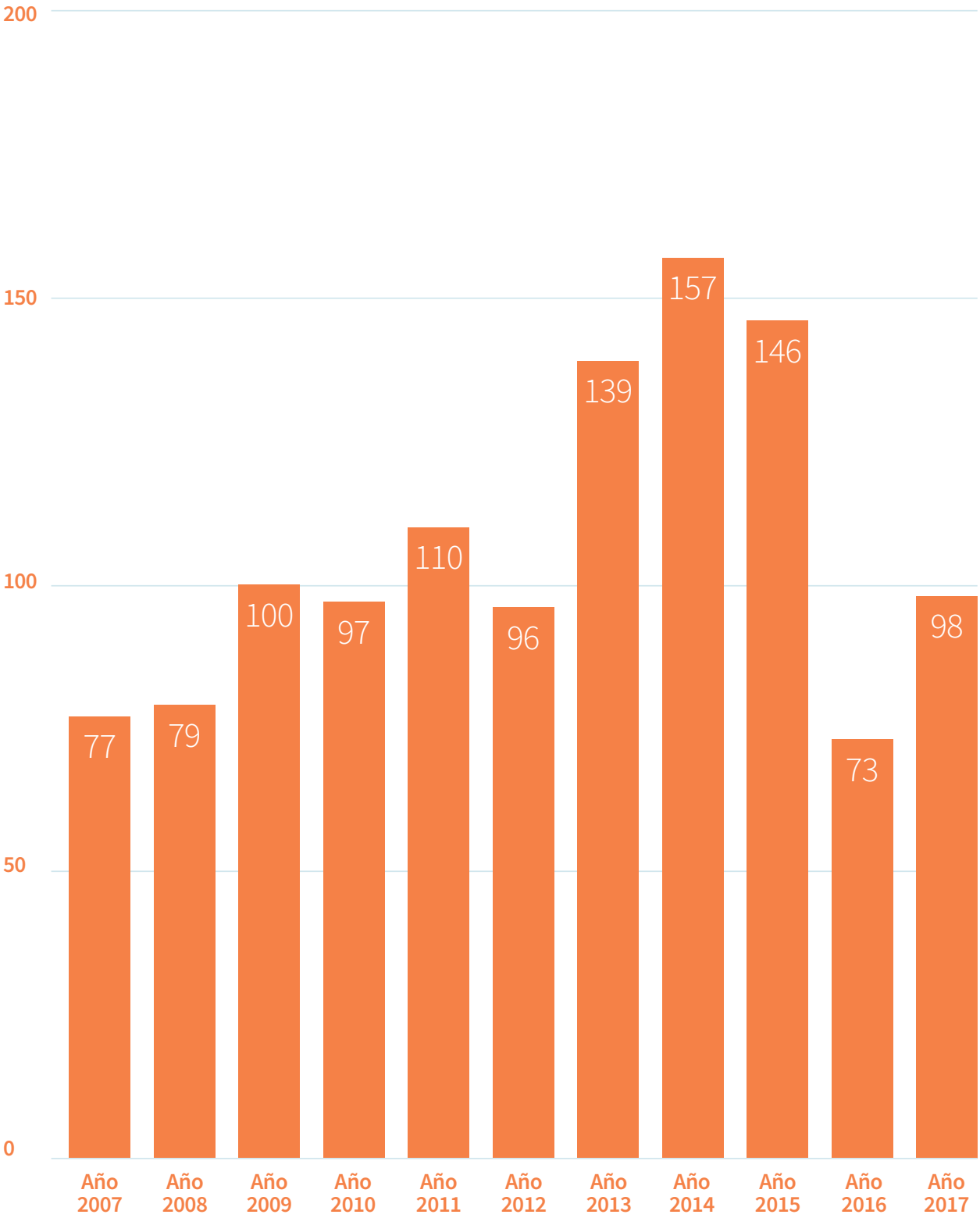
Evolución de consultas por sectores (2017 ■ 2016 □)



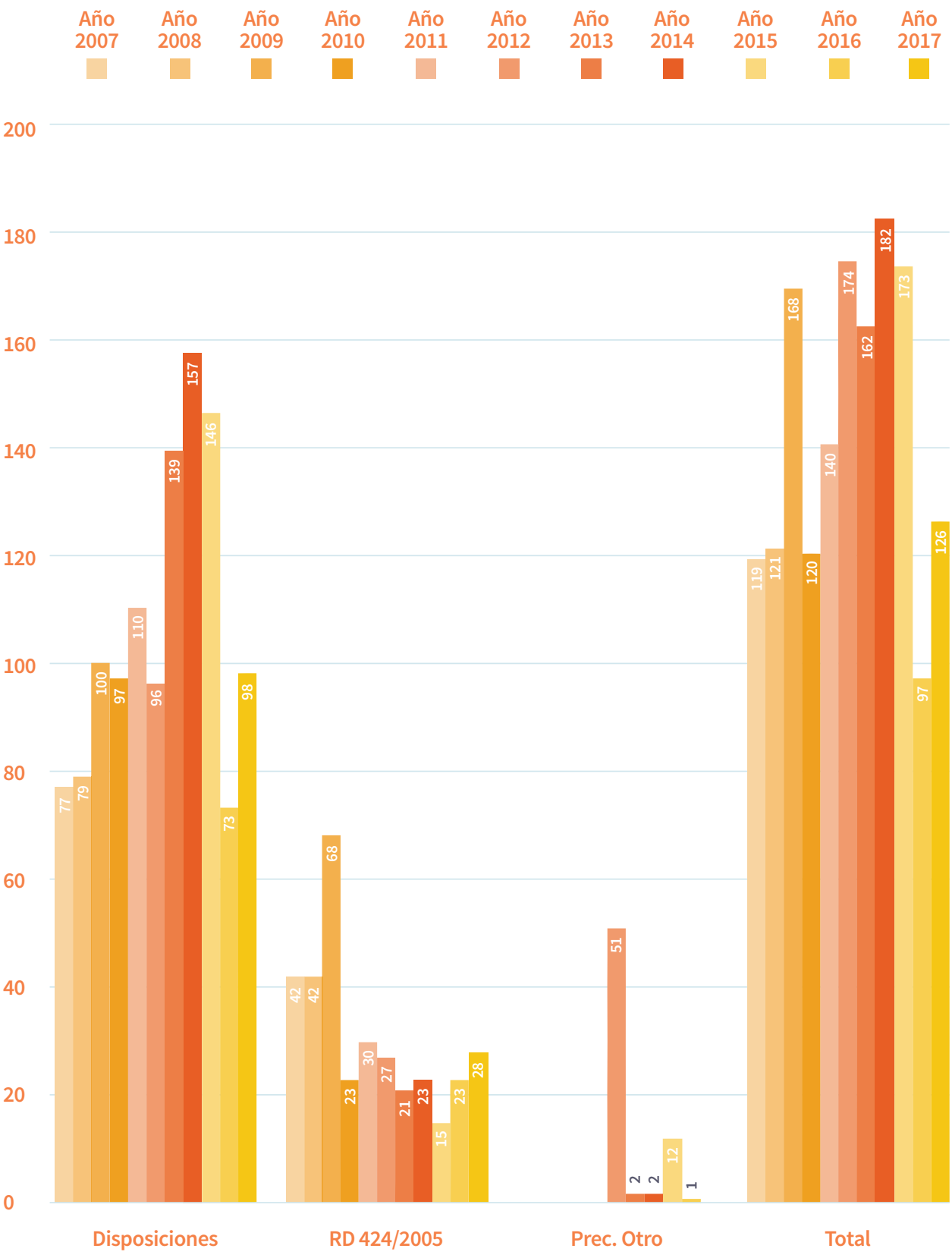
Evolución de consultas por materias (2017 ■ 2016 □)



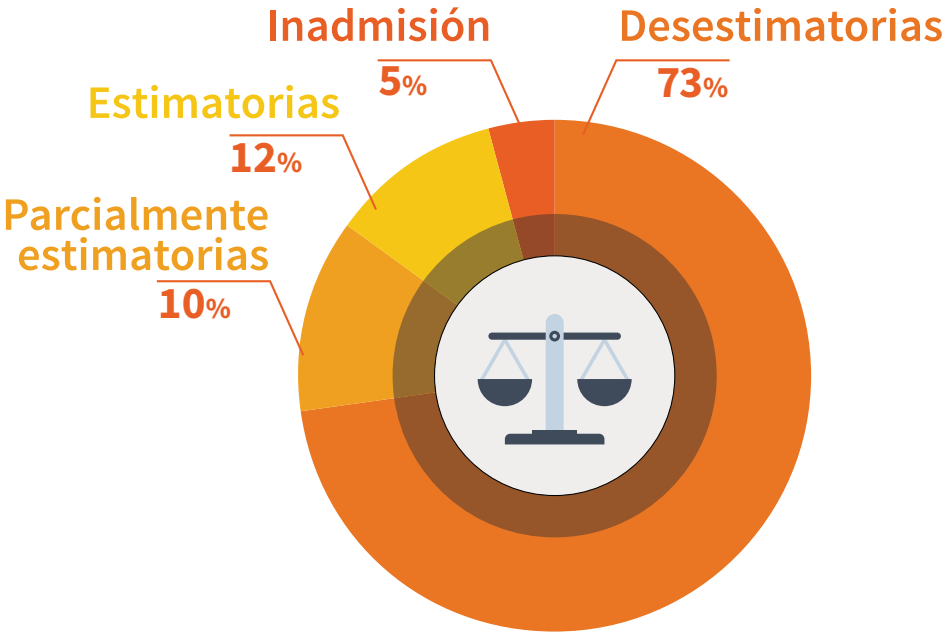
Evolución de informes preceptivos a disposiciones generales (2007-2017)



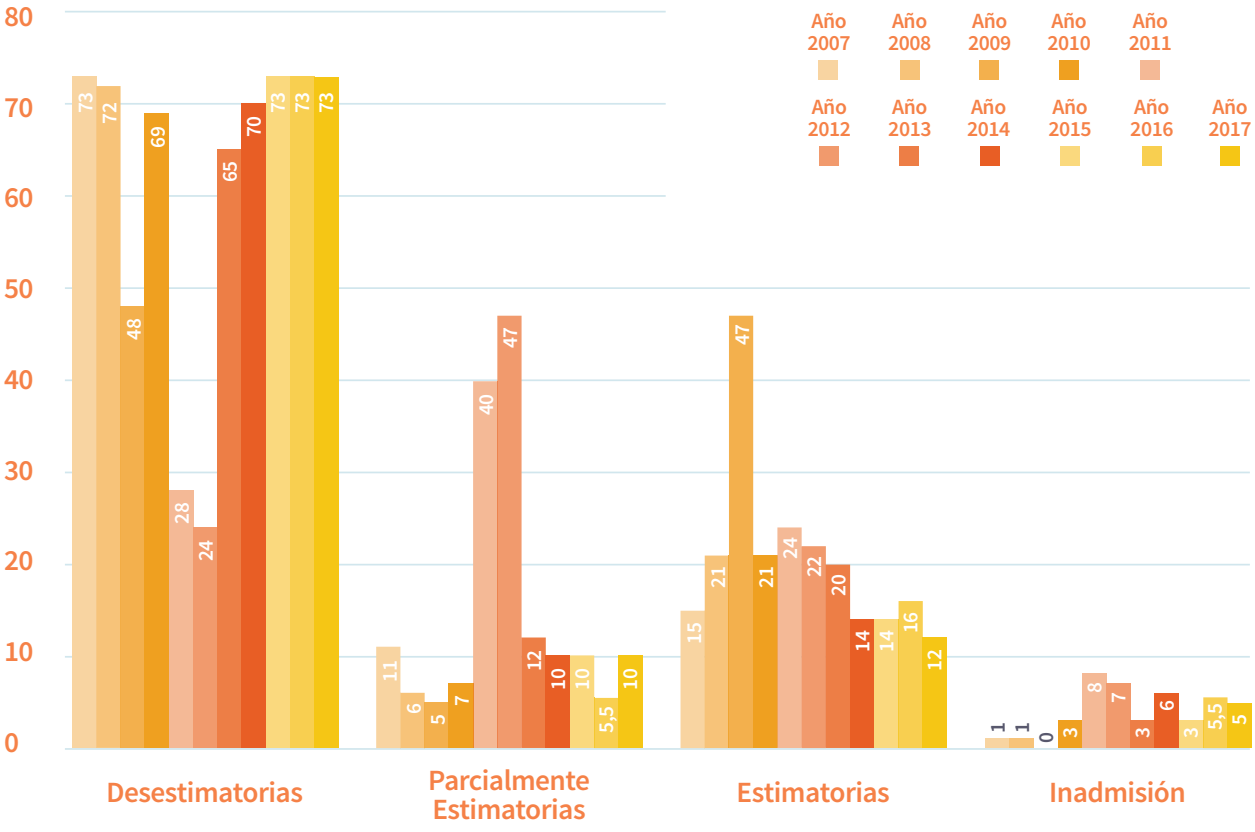
Evolución de informes preceptivos (2007-2017)



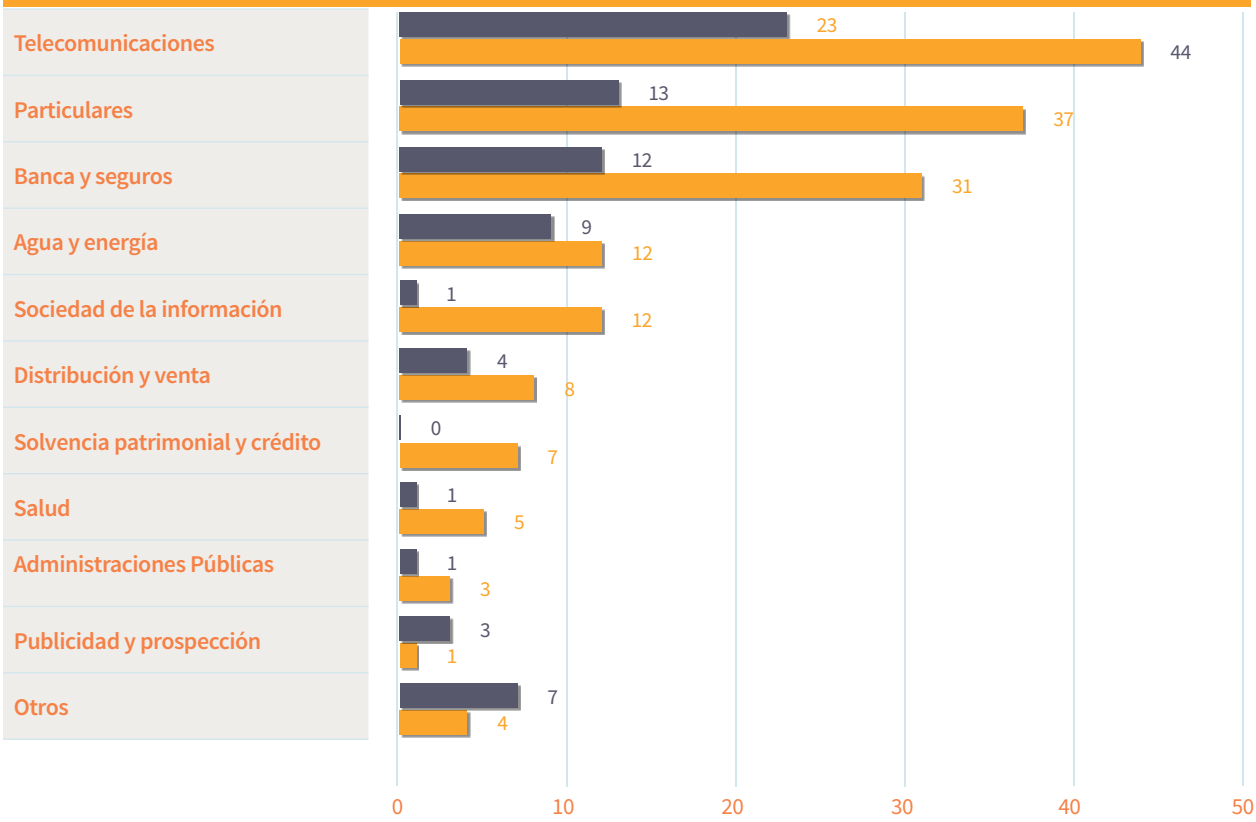
Sentencias Audiencia Nacional en 2017



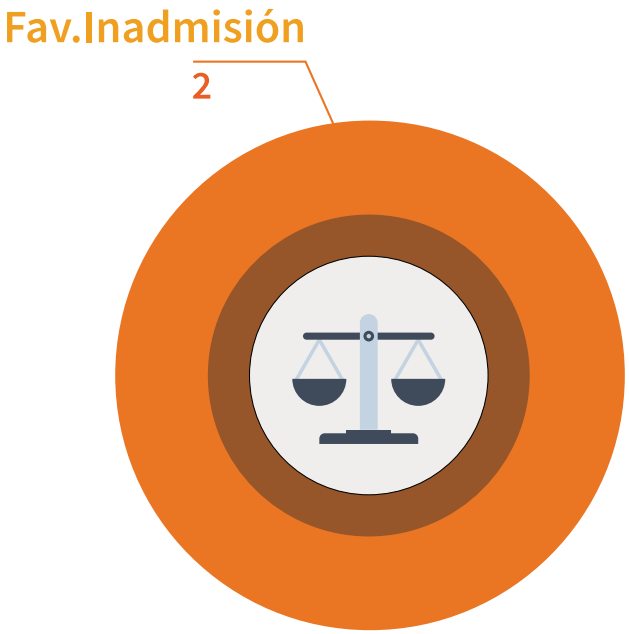
Evolución por sentido del fallo en porcentajes (2007-2017)



Comparativa por sector del recurrente (2017 ☐ 2016 ■)



Comparativa por sector del recurrente (2017-2016)



5. Atención al ciudadano

Consultas totales planteadas ante el área de Atención al Ciudadano						
	Atención presencial	Teléfono	Por escrito	Sede electrónica	Respuesta automática FAQs	TOTAL
AÑO 2015	3.767	74.260	550	7.054	132.704	218.335
AÑO 2016	4.183	76.869	552	8.054	147.297	236.955
AÑO 2017	3.699	73.501	516	7.438	170.754	255.908
% 2016-2017	**-11,57**	**-4,38**	**-6,52**	**-7,65**	**15,92**	**8,00**

Comparativa de visitas a la web (www.agpd.es)			
AÑO	2015	2016	2017
Visitas	4.952.945	5.534.282	6.724.113
Incremento% 2016-2017	21,49		

Accesos al portal de videos 'Protege tus datos en internet'	
Accesos al canal	29.672
Visualizaciones de vídeos	33.283*

*Se puede acceder a los vídeos directamente sin pasar por el canal, entrando desde la web www.tudecideseninternet.es.

Accesos a la web www.tudecideseninternet.es	
Visitantes distintos [1]	Número de visitas [2]
66.810	101.500

[1] Visitantes distintos: visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo contará como una.
[2] Visitas: número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.

Temas más consultados en el catálogo de preguntas frecuentes		
ORDEN	TEMA DE CONSULTA	ACCESOS
1	Ficheros de solvencia patrimonial	19.950
2	Videovigilancia	13.796
3	Obligaciones de los responsables de los ficheros	12.637
4	Comunidades de vecinos	11.715
5	En qué te podemos ayudar y en qué no	10.693
6	Reglamento General de Protección de Datos	10.500
7	Inscripción de ficheros	10.306

Temas más consultados en la atención presencial y telefónica	
TEMAS DE CONSULTA	%
Denuncias	17,43
Inscripción de ficheros	15,08
Derechos ARCO y Olvido	10,59
Videovigilancia	7,09
Ficheros de morosidad	5,07
Reglamento General de Protección de Datos	5,04
Cesión de datos	3,80
Comunidades de vecinos	2,47
Otros(*)	33,39

(*) Incluye temas como cumplimiento de la LOPD, transferencias internacionales, medidas de seguridad, etc.

Análisis de consultas telefónicas y presenciales sobre Derechos ARCO

DERECHOS	%
Cancelación	43,34
Acceso	31,36
Olvido	12,38
Oposición	8,73
Rectificación	4,16

Consultas especializadas sobre el tratamiento de datos de menores

CONSULTAS	2017
Teléfono	178
WhatsApp	247
Canal Joven	246
Sede electrónica	224

Evolución del registro de entrada/salida de documentos

	2015	2016	2017	% 2016-2017
Entrada	506.670	433.484	404.429	-6,70
Salida	328.830	369.794	362.773	-1,90
TOTAL	**835.500**	**803.278**	**767.202**	**-4,49**

Distribución de los documentos registrados en 2017 según el medio utilizado

REGISTRO DE ENTRADAS	2017	%
Por medios electrónicos	385.162	95,24
· Con certificado electrónico	267.082	
· Sin certificado electrónico	118.080	
Por otros medios *	19.267	4,76
TOTAL ENTRADAS	**404.429**	**100,00**

REGISTRO DE SALIDAS	2017	%
Por medios electrónicos	103.553	28,55
· Comparecencia en sede	47.694	
· Dirección Electrónica Habilitada	55.859	
Por otros medios*	259.220	71,45
TOTAL SALIDAS	**362.773**	**100,00**

* Correo electrónico, correo postal, en mano, mensajería…

Solicitudes de acceso a información pública

Recibidas	Inadmitidas*	Concedidas	Desistimiento	Consultas**	Denegadas
59	13	33	1	6	6

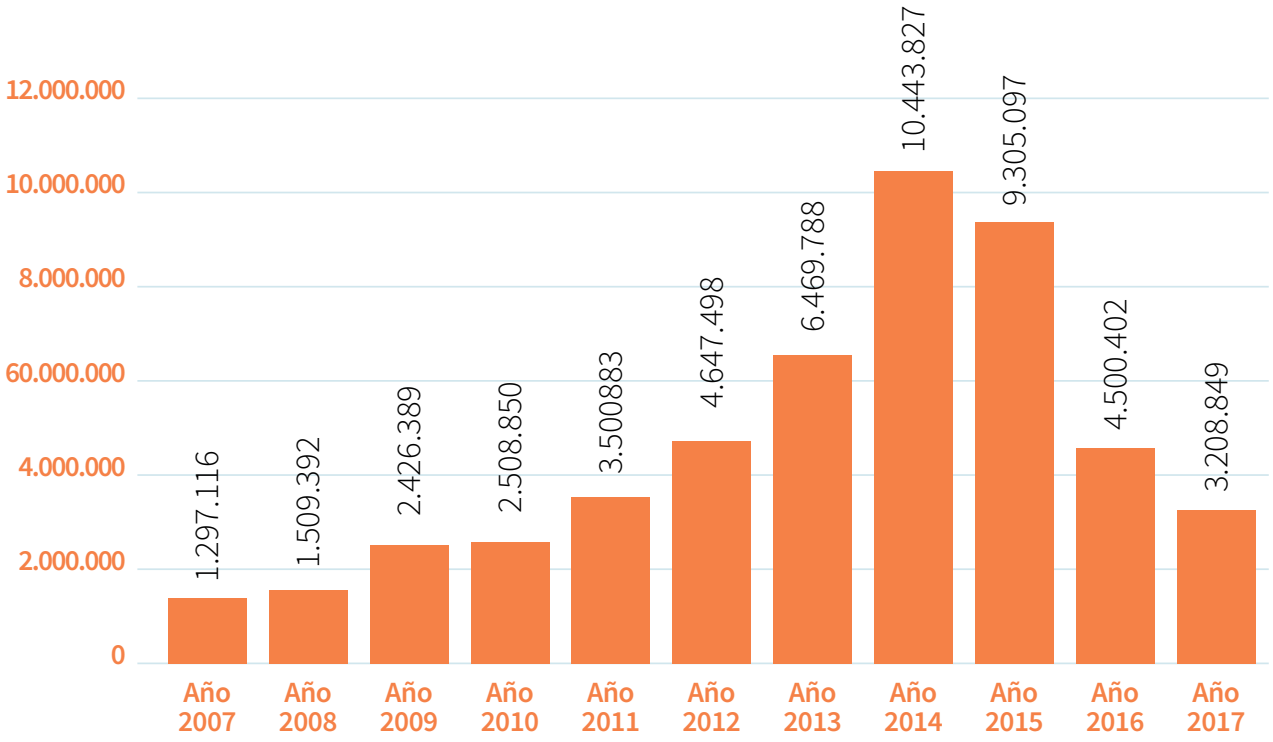
*Causas de inadmisión (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno): abuso de derecho; reelaboración y peticiones repetidas (art. 18 Ley de Transparencia) Disposición adicional 1ª de la citada ley.

**No se trataba de peticiones de acceso la información sino de consultas sobre protección de datos.

Accesos a contenidos electrónicos	
2017	
Accesos web	6.724.113
Página de transparencia	856.245
Consultas FAQs	170.754
Consultas electrónicas de ciudadanos	7.438
Acceso Facilita_RGPD (publicada en septiembre 2017)	29.009
Herramienta EVALÚA	12.061
Herramienta DISPONE	4.563
Herramienta NOTA	352.525
Guía de seguridad y privacidad en Internet	120.974
Orientaciones sobre protección de datos en la reutilización de la información del sector público	4.137
Orientaciones y garantías en los procedimientos de anonimización	14.620
Cómo gestionar una fuga de información en un despacho de abogados	6.615
Guía para centros educativos (publicada el 19 de octubre 2017)	31.113
Guía de Compra segura en Internet (publicada el 18 de diciembre 2017)	5.147
Plan de inspección sectorial realizado a hospitales públicos	34.585
Decálogo de protección de datos para el personal sanitario y administrativos	35.964

6. Registro General de Protección de Datos

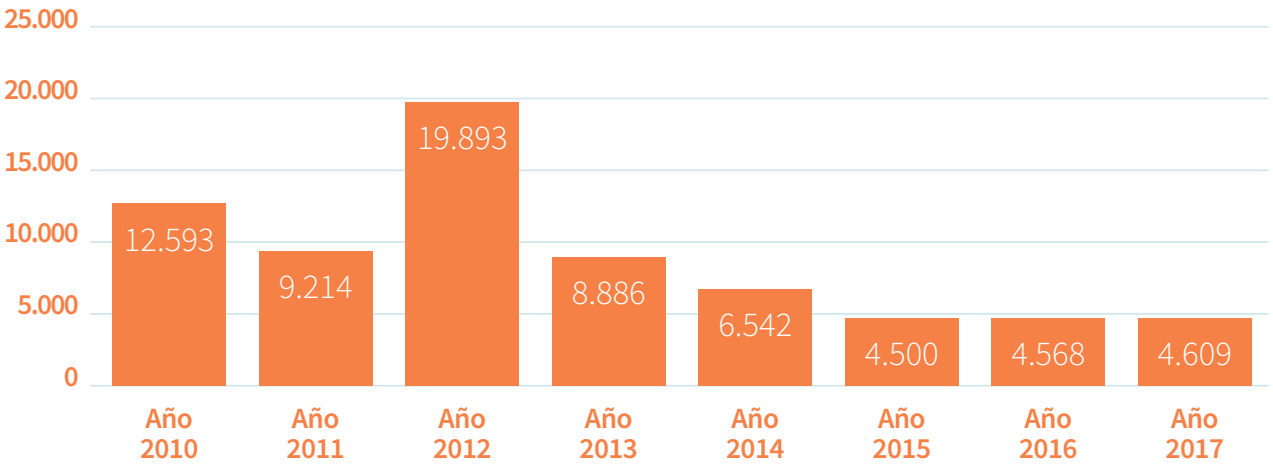
Derecho de consulta al Registro		
Titularidad	**2016**	**2017**
Privada	2.733.169	2.341.761
Pública	1.767.233	867.088
TOTAL	**4.500.402**	**3.208.849**



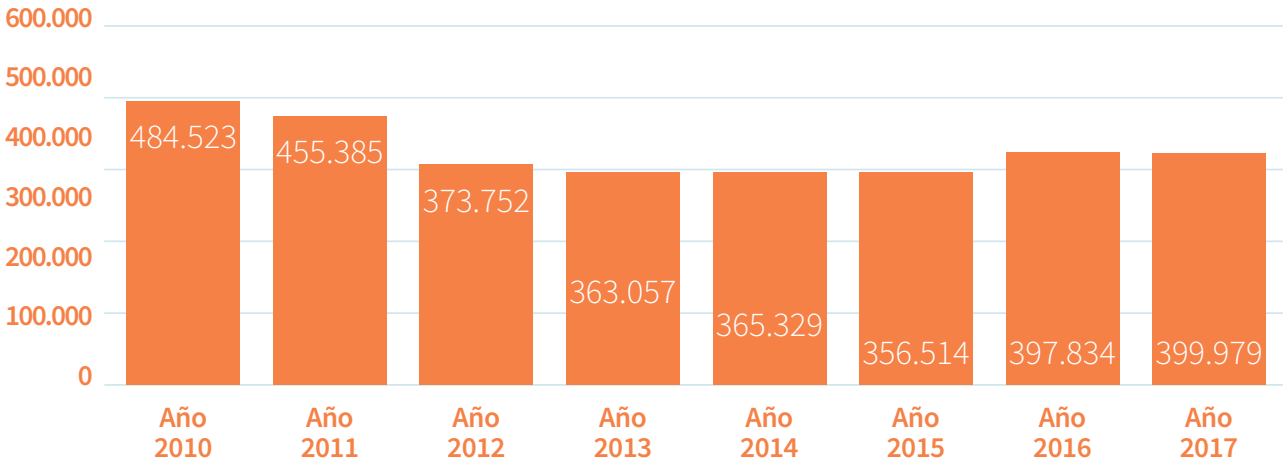
Evolución de la inscripción de ficheros en el RGPD

A 31 de dic.	2010	2011	2012	2013	2014	2015	2016	2017
Tit. Pública	108.289	117.503	137.396	146.282	152.824	157.324	161.892	166.501
Tit. Privada	2.036.583	2.491.968	2.865.720	3.228.777	3.594.106	3.950.620	4.348.454	4.748.433
TOTAL	**2.144.872**	**2.609.471**	**3.003.116**	**3.375.059**	**3.746.930**	**4.107.944**	**4.510.346**	**4.914.934**

Incremento anual de ficheros de titularidad pública



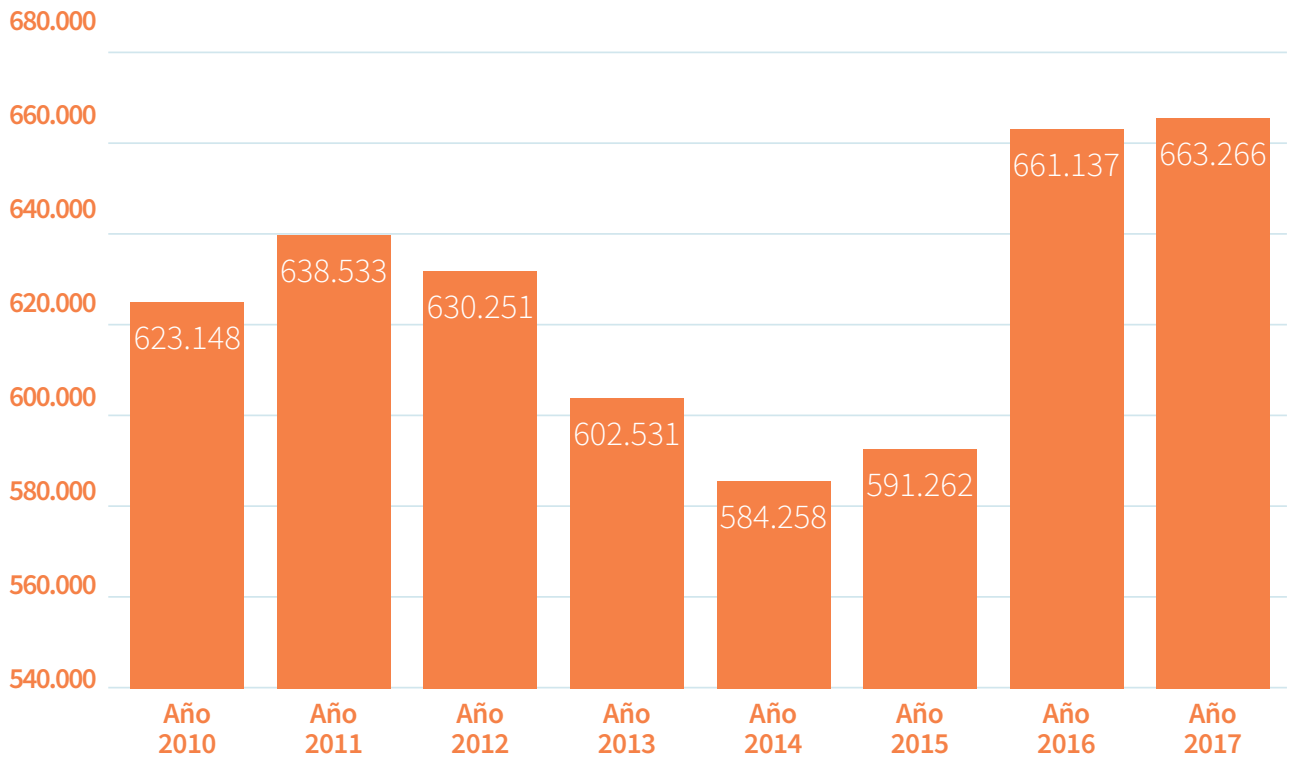
Incremento anual de ficheros de titularidad privada



Operaciones de inscripción

	2016	2017	% Variación 2016/2017	Media diaria en 2016	Media diaria en 2017
Operaciones de inscripción	661.137	663.266	+0,3	2.755	2.764
Total de ficheros inscritos	4.510.346	4.914.934	+9	1.677	1.686

Evolución anual de las operaciones de inscripción



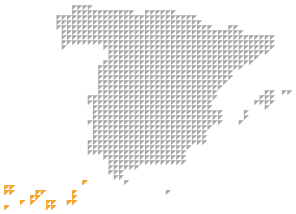
Inscripción de titularidad privada

Distribución territorial de ficheros

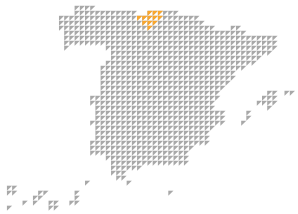
Comunidad Autónoma de Andalucía	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Almería	3.853	**22.600**	9.387	**74.748**
Cádiz	5.252	**31.155**	13.287	**99.174**
Córdoba	3.765	**22.661**	10.470	**73.227**
Granada	4.756	**31.853**	12.143	**104.271**
Huelva	1.284	**10.332**	3.278	**31.113**
Jaén	2.825	**18.000**	6.755	**61.566**
Málaga	8.550	**55.000**	23.603	**176.751**
Sevilla	7.574	**51.665**	17.193	**145.155**
TOTAL COMUNIDAD	37.827	**242.328**	96.116	**766.005**

Comunidad Autónoma de Aragón	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Huesca	1.351	**9.967**	2.734	**25.027**
Teruel	356	**4.541**	954	**12.601**
Zaragoza	4.360	**37.120**	9.375	**95.101**
TOTAL COMUNIDAD	6.066	**51.561**	13.063	**132.729**

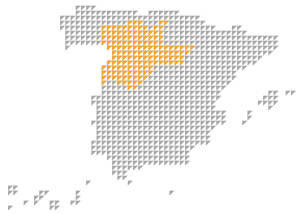
Comunidad Autónoma del Principado de Asturias	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	6.270	**47.062**	15.737	**143.510**



Comunidad Autónoma de Canarias	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Las Palmas	3.594	**24.952**	9.587	**82.586**
Santa Cruz de Tenerife	3.317	**27.159**	8.540	**86.609**
TOTAL COMUNIDAD	6.908	**52.012**	18.127	**169.195**



Comunidad Autónoma de Cantabria	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	3.097	**19.683**	7.091	**53.360**



Comunidad Autónoma de Castilla y León	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Ávila	750	**5.273**	1.581	**13.617**
Burgos	1.599	**12.187**	3.427	**30.857**
León	1.848	**14.989**	4.246	**42.086**
Palencia	708	**5.692**	1.533	**17.063**
Salamanca	991	**9.858**	2.602	**27.523**
Segovia	772	**6.685**	2.314	**22.127**
Soria	473	**3.429**	1.119	**9.730**
Valladolid	2.160	**16.747**	5.053	**48.177**
Zamora	489	**5.003**	1.434	**15.673**
TOTAL COMUNIDAD	9.778	**79.684**	23.309	**226.853**

Comunidad Autónoma de Castilla-La Mancha	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Albacete	2.189	**15.371**	5.022	**48.147**
Ciudad Real	2.008	**13.765**	5.238	**42.375**
Cuenca	648	**5.854**	1.691	**16.850**
Guadalajara	984	**6.593**	2.256	**18.125**
Toledo	2.009	**17.738**	5.573	**53.282**
TOTAL COMUNIDAD	7.835	**59.216**	19.780	**178.779**

Comunidad Autónoma de Cataluña	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Barcelona	28.657	**218.519**	66.906	**592.415**
Girona	2.732	**32.428**	7.724	**92.643**
Lleida	1.494	**14.817**	3.824	**39.755**
Tarragona	3.999	**25.873**	9.526	**78.272**
TOTAL COMUNIDAD	36.867	**291.140**	87.980	**803.085**

Comunidad de Madrid	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	41.984	**273.346**	95.510	**738.479**

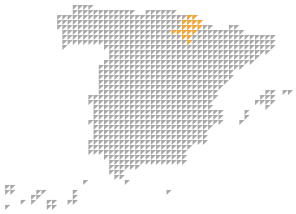
Comunitat Valenciana	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Alicante / Alacant	10.759	**68.965**	24.307	**190.763**
Castellón / Castelló	3.324	**21.976**	6.725	**62.938**
Valencia / València	14.206	**99.950**	30.731	**280.963**
TOTAL COMUNIDAD	28.280	**190.686**	61.763	**534.664**

Comunidad Autónoma de Extremadura	RESPONSABLES		FICHEROS	
Badajoz	2.616	**18.110**	6.477	**54.065**
Cáceres	1.234	**10.889**	3.604	**33.049**
TOTAL COMUNIDAD	3.847	**28.956**	10.081	**87.114**

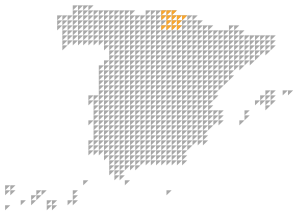
Comunidad Autónoma de Galicia	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
A Coruña	8.348	**50.466**	19.753	**145.476**
Lugo	1.991	**14.183**	4.158	**39.247**
Ourense	1.570	**12.331**	3.400	**33.314**
Pontevedra	5.673	**38.174**	12.876	**112.238**
TOTAL COMUNIDAD	17.565	**114.869**	40.187	**330.275**

Comunidad Autónoma de las Illes Balears	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	6.440	**39.228**	19.628	**145.692**

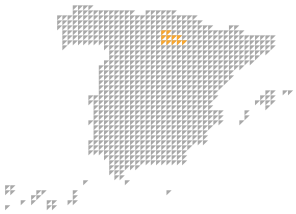
Comunidad Foral de Navarra	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	2.304	**17.664**	7.695	**54.534**



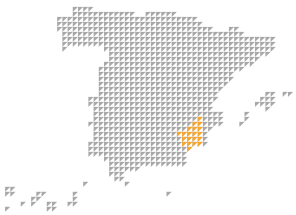
Comunidad Autónoma del País Vasco	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
Araba / Álava	1.472	**9.919**	2.995	**25.642**
Gipuzkoa	4.737	**22.814**	12.248	**69.356**
Bizkaia	6.862	**38.421**	14.444	**103.740**
TOTAL COMUNIDAD	13.066	**71.029**	29.687	**198.738**



Comunidad Autónoma de La Rioja	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	1.272	**13.298**	2.783	**34.665**



Comunidad Autónoma de la Región de Murcia	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	6.938	**49.325**	15.111	**141.870**



Ciudad Autónoma de Ceuta	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	218	**1.082**	425	**2.976**

Ciudad Autónoma de Melilla	RESPONSABLES		FICHEROS	
	2017	TOTAL	2017	TOTAL
TOTAL COMUNIDAD	231	**1.174**	685	**5.437**

Distribución de ficheros según tipos de datos

	2017	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	5.446	95.849
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	32.022	484.501
Datos de carácter identificativo	462.219	4.748.433
Datos de características personales	194.895	2.103.217
Datos de circunstancias sociales	135.768	1.281.126
Datos académicos y profesionales	106.860	1.178.257
Detalles de empleo y carrera administrativa	115.397	1.394.919
Datos de información comercial	142.923	1.368.166
Datos económico-financieros	245.885	2.657.973
Datos de transacciones	195.342	2.018.917
Otros tipos de datos	23.875	234.654

Distribución de ficheros según su finalidad

	2017	TOTAL	% Variación 2017-Total
Gestión de clientes, contable, fiscal y administrativa	237.420	2.717.584	+8,74
Recursos humanos	91.630	1.041.181	+8,80
Gestión de nóminas	62.550	759.145	+8,24
Publicidad y prospección comercial	58.493	472.427	+12,38
Videovigilancia	52.657	339.053	+15,53
Prevención de riesgos laborales	46.267	436.325	+10,60
Comercio electrónico	28.953	181.456	+15,96
Seguridad y control de acceso a edificios	16.162	92.645	+17,45
Gestión y control sanitario	13.047	175.382	+7,44
Análisis de perfiles	10.158	77.721	+13,07
Historial clínico	10.013	127.896	+7,83
Seguridad privada	5.956	36.019	+16,54
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	5.752	66.375	+8,67
Educación	4.872	56.389	+8,64
Prestación de servicios de comunicaciones electrónicas	4.488	32.354	+13,87
Cumplimiento/incumplimiento de obligaciones dinerarias	4.328	57.942	+7,47
Servicios económicos-financieros y seguros	3.674	76.513	+4,80
Fines estadísticos, históricos o científicos	2.894	94.458	+3,06
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical	2.556	24.680	+10,36
Guías/repertorios de servicios de comunicaciones electrónicas	2.332	21.547	+10,82
Gestión de asistencia social	990	16.992	+5,83
Prestación de servicios de solvencia patrimonial y crédito	769	10.162	+7,57
Investigación epidemiológica y actividades análogas	578	10.257	+5,64
Prestación de servicios de certificación electrónica	504	4.625	+10,90
Otras finalidades	98.939	803.058	+12,32

Distribución de ficheros según el sector de actividad (1/2)

	2017	TOTAL	% variación 2017-Total
Comunidades de propietarios	82.195	653.986	+12,57
Comercio	47.010	551.010	+8,53
Sanidad	31.916	347.882	+9,17
Turismo y hostelería	27.449	249.161	+11,02
Actividades inmobiliarias	13.540	140.576	+9,63
Asociaciones y clubes	10.485	102.253	+10,25
Educación	10.346	115.938	+8,92
Contabilidad, auditoria y asesoría fiscal	9.813	177.870	+5,52
Construcción	9.671	157.591	+6,14
Actividades jurídicas, notarios y registradores	8.081	109.031	+7,41
Transporte	6.674	97.992	+6,81
Comercio y servicios electrónicos	5.140	34.279	+14,99
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	5.060	56.752	+8,92
Servicios informáticos	4.543	63.815	+7,12
Activ. de organizaciones empresariales, profesionales y patronales	4.328	32.138	+13,47
Actividades diversas de servicios personales	4.293	47.040	+9,13
Agricultura, ganadería, explotación forestal, caza, pesca	3.584	50.559	+7,09
Industria química y farmacéutica	3.345	59.076	+5,66
Seguros privados	2.517	38.174	+6,59
Maquinaria y medios de transporte	2.233	50.076	+4,46
Actividades de servicios sociales	2.207	33.478	+6,59
Producción de bienes de consumo	1.592	31.796	+5,01
Sector energético	1.583	26.919	+5,88
Servicios de telecomunicaciones	1.366	19.290	+7,08
Actividades políticas, sindicales o religiosas	1.115	23.275	+4,79

Continúa en página siguiente

Distribución de ficheros según el sector de actividad (2/2)			
Actividades relacionadas con los juegos de azar y apuestas	957	11.541	+8,29
Publicidad directa	784	13.929	+5,63
Seguridad	749	9.990	+7,50
Entidades bancarias y financieras	723	14.371	+5,03
Inspección técnica de vehículos y otros análisis técnicos	494	5.121	+9,65
Organización de ferias, exhibiciones, congresos y otras actividades relacionadas	482	5.683	+8,48
Investigación y desarrollo (i+d)	410	5.691	+7,20
Selección de personal	278	5.417	+5,13
Activ. postales y de correo (oper. postales, serv. post., transport.)	247	3.922	+6,30
Solvencia patrimonial y crédito	34	1.202	+2,83
Mutualidades colaboradoras de los organismos de la seguridad social	9	841	+1,07
Otras actividades	156.966	1.369.778	+11,46

Inscripción de titularidad pública

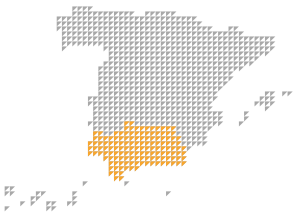
Distribución de ficheros por tipo de administración		
	2017	TOTAL
Administración General	230	9.137
Administración CC.AA	453	30.476
Administración Local	4.403	98.132
Otras personas jurídico-públicas	591	28.756
TOTAL	**5.677**	**166.501**

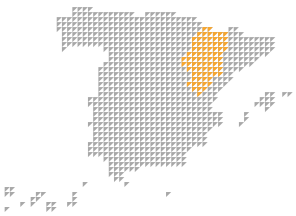
Distribución de ficheros de la Administración General	
	Ficheros
Presidencia del Gobierno	13
Ministerio de Asuntos Exteriores y de Cooperación	556
Ministerio de Justicia	152
Ministerio de Defensa	2.277
Ministerio de Hacienda y Función Pública	479
Ministerio del Interior	242
Ministerio de Fomento	601
Ministerio de Educación, Cultura y Deporte	314
Ministerio de Empleo y Seguridad Social	2.037
Ministerio de Energía, Turismo y Agenda Digital	185
Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente	450
Ministerio de la Presidencia y para las Administraciones Territoriales	665
Ministerio de Economía, Industria y Competitividad	551
Ministerio de Sanidad, Servicios Sociales e Igualdad	615
TOTAL	**9.137**

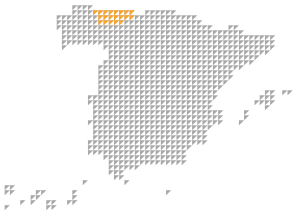
Distribución de ficheros de titularidad pública - CCAA

	2017	Ficheros
Comunidad Autónoma de Andalucía	39	1.954
Comunidad Autónoma de Aragón	7	421
Comunidad Autónoma del Principado de Asturias	23	554
Comunidad Autónoma de Canarias	21	413
Comunidad Autónoma de Cantabria	11	248
Comunidad Autónoma de Castilla y León	24	874
Comunidad Autónoma de Castilla-La Mancha	63	961
Comunidad Autónoma de Cataluña	73	10.359
Comunidad de Madrid	33	9.965
Comunitat Valenciana	37	601
Comunidad Autónoma de Extremadura	3	524
Comunidad Autónoma de Galicia	4	339
Comunidad Autónoma de las Illes Balears	30	719
Comunidad Foral de Navarra	29	205
Comunidad Autónoma del País Vasco	39	1.330
Comunidad Autónoma de La Rioja	2	371
Comunidad Autónoma de la Región de Murcia	2	455
Ciudad Autónoma de Ceuta	10	81
Ciudad Autónoma de Melilla	3	102
TOTAL	**453**	**30.476**

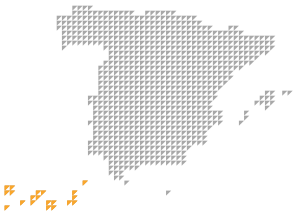
Distribución territorial de ficheros

Comunidad Autónoma de Andalucía	RESPONSABLES	FICHEROS
		
Almería	111	1.279
Cádiz	50	932
Córdoba	96	1.010
Granada	196	1.725
Huelva	88	1.293
Jaén	92	972
Málaga	117	2.534
Sevilla	129	2.142
TOTAL COMUNIDAD	**879**	**11.887**

Comunidad Autónoma de Aragón	RESPONSABLES	FICHEROS
		
Huesca	206	2.013
Teruel	80	580
Zaragoza	312	3.615
TOTAL COMUNIDAD	**598**	**6.208**

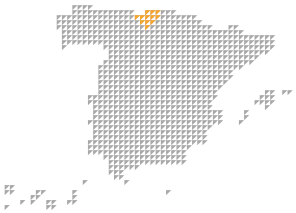
Comunidad Autónoma del Principado de Asturias	RESPONSABLES	FICHEROS
		
TOTAL COMUNIDAD	**97**	**1.836**

Comunidad Autónoma de Canarias



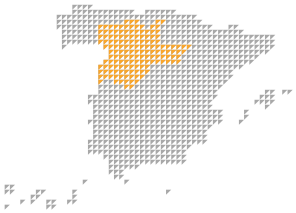
	RESPONSABLES	FICHEROS
Las Palmas	54	1.072
Santa Cruz de Tenerife	67	1.063
TOTAL COMUNIDAD	**121**	**2.135**

Comunidad Autónoma de Cantabria

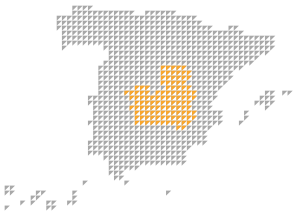


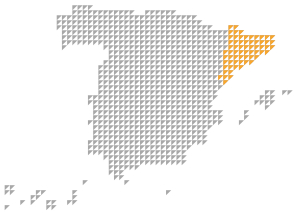
	RESPONSABLES	FICHEROS
TOTAL COMUNIDAD	**80**	**1.089**

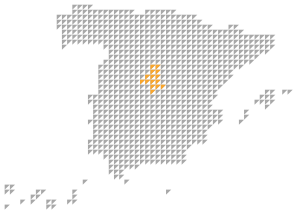
Comunidad Autónoma de Castilla y León

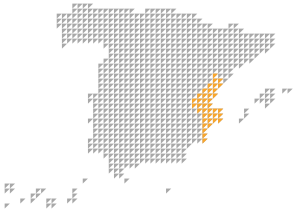


	RESPONSABLES	FICHEROS
Ávila	121	1.466
Burgos	348	2.607
León	210	1.378
Palencia	125	1.349
Salamanca	94	613
Segovia	71	873
Soria	19	166
Valladolid	209	2.512
Zamora	54	346
TOTAL COMUNIDAD	**1.251**	**11.310**

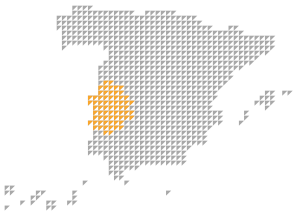
Comunidad Autónoma de Castilla-La Mancha	RESPONSABLES	FICHEROS
		
Albacete	101	3.435
Ciudad Real	110	991
Cuenca	210	1.832
Guadalajara	51	782
Toledo	137	1.592
TOTAL COMUNIDAD	**609**	**8.632**

Comunidad Autónoma de Cataluña	RESPONSABLES	FICHEROS
		
Barcelona	455	6.217
Girona	236	3.108
Lleida	223	2.271
Tarragona	183	2.074
TOTAL COMUNIDAD	**1.096**	**13.670**

Comunidad de Madrid	RESPONSABLES	FICHEROS
		
TOTAL COMUNIDAD	**238**	**4.812**

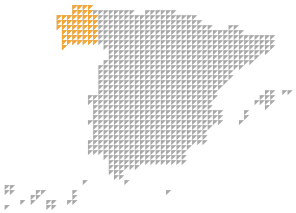
Comunitat Valenciana	RESPONSABLES	FICHEROS
		
Alicante / Alacant	166	2.587
Castellón / Castelló	113	1.226
Valencia / València	264	4.130
TOTAL COMUNIDAD	**542**	**7.943**

Comunidad Autónoma de Extremadura



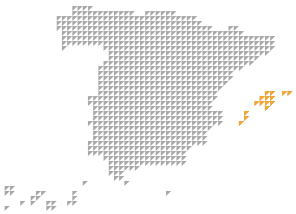
	RESPONSABLES	FICHEROS
Badajoz	199	6.224
Cáceres	159	2.437
TOTAL COMUNIDAD	**358**	**8.661**

Comunidad Autónoma de Galicia



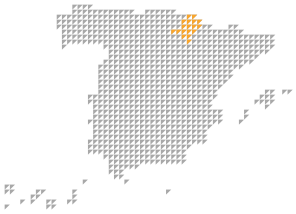
	RESPONSABLES	FICHEROS
A Coruña	102	2.005
Lugo	71	1.056
Ourense	91	1.056
Pontevedra	71	1.099
TOTAL COMUNIDAD	**335**	**5.216**

Comunidad Autónoma de las Illes Balears



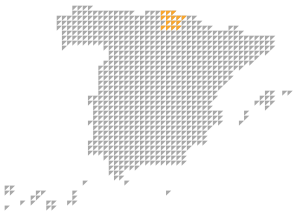
	RESPONSABLES	FICHEROS
TOTAL COMUNIDAD	**86**	**1.755**

Comunidad Foral de Navarra



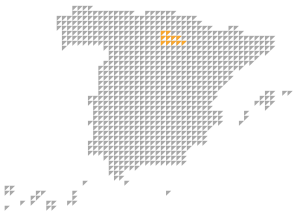
	RESPONSABLES	FICHEROS
TOTAL COMUNIDAD	**268**	**3.242**

Comunidad Autónoma del País Vasco



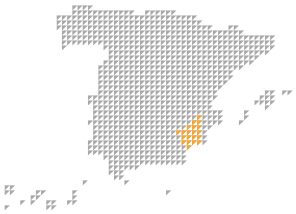
	RESPONSABLES	FICHEROS
Araba / Álava	66	776
Gipuzkoa	123	2.234
Bizkaia	171	4.839
TOTAL COMUNIDAD	**360**	**7.849**

Comunidad Autónoma de La Rioja



	RESPONSABLES	FICHEROS
TOTAL COMUNIDAD	**44**	**458**

Comunidad Autónoma de la Región de Murcia



	RESPONSABLES	FICHEROS
TOTAL COMUNIDAD	**56**	**1.429**

Distribución de ficheros de titularidad pública – Otras personas jurídico-públicas

	TOTAL
Cámaras Oficiales de Comercio e Industria	496
Notariado	8.404
Universidades	1.617
Colegios Profesionales	2.974
Otros	15.265
TOTAL	**28.756**

Distribución de ficheros según tipos de datos

	2017	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	311	20.167
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	1.096	40.373
Datos relativos a infracciones	895	28.766
Datos de carácter identificativo	5.677	166.501
Datos de características personales	2.930	86.355
Datos de circunstancias sociales	1.881	46.298
Datos académicos y profesionales	1.842	55.644
Detalles de empleo y carrera administrativa	1.455	49.326
Datos de información comercial	945	21.631
Datos económico-financieros	2.622	73.819
Datos de transacciones	781	31.449
Otros tipos de datos	618	25.017

Distribución de ficheros con datos sensibles

		2017	TOTAL
Datos especialmente protegidos		**311**	**20.167**
	Ideología	172	9.767
	Creencias	95	8.818
	Religión	99	9.226
	Afiliación Sindical	192	18.347
Otros datos especialmente protegidos		**1.096**	**40.373**
	Origen Racial	219	12.657
	Salud	1.083	40.182
	Sexual	150	9.880
Datos relativos a infracciones		**895**	**28.766**
	Infracciones Penales	455	19.014
	Infracciones Administrativas	809	27.756

Distribución de ficheros según su finalidad

	2017	TOTAL	% 2017/total
Procedimiento administrativo	1.740	53.759	+3,24
Gestión contable, fiscal y administrativa	746	23.896	+3,12
Recursos humanos	616	28.389	+2,17
Educación y cultura	596	18.784	+3,17
Servicios sociales	378	10.444	+3,62
Gestión de nómina	294	13.835	+2,13
Gestión sancionadora	293	6.482	+4,52
Fines históricos, estadísticos o científicos	269	19.934	+1,35
Hacienda pública y gestión de administración tributaria	247	10.782	+2,29
Gestión económica-financiera pública	227	7.211	+3,15
Trabajo y gestión de empleo	224	5.945	+3,77
Videovigilancia	224	3.343	+6,70
Función estadística pública	221	12.916	+1,71
Prevención de riesgos laborales	212	4.112	+5,16
Seguridad y control de acceso a edificios	174	4.189	+4,15
Publicaciones	170	3.015	+5,64
Seguridad pública y defensa	167	4.223	+3,95
Padrón de habitantes	162	6.922	+2,34
Gestión y control sanitario	103	3.853	+2,67
Justicia	102	10.738	+0,95
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	80	2.681	+2,98
Prestación de servicios de certificación electrónica	67	1.798	+3,73
Historial clínico	64	2.108	+3,04
Investigación epidemiológica y actividades análogas	38	1.530	+2,48
Gestión de censo promocional	32	1.105	+2,90
Otras finalidades	2.464	49.257	+5,00

Transferencias internacionales de datos

Resoluciones de autorización (1/3)

	2000-2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total Aut.
Estados Unidos											**944**
EEUU	124	28	25	40	62	47	51	30	404	133	**944**
Iberoamérica											**564**
Panamá	2	-	-	-	-	1	3	2	1	-	**9**
Colombia	18	12	22	23	17	21	23	10	9	14	**169**
Chile	18	8	9	7	1	-	-	2	2	-	**47**
Uruguay	7	3	13	-	2	-	-	-	-	-	**25**
Perú	13	19	20	30	23	23	5	5	6	8	**152**
Guatemala	2	1	-	-	2	1	-	-	-	-	**6**
Paraguay	6	4	1	4	2	-	-	-	-	-	**17**
Brasil	4	-	1	2	2	3	1	1	5	3	**22**
El Salvador	1	-	-	-	-	-	-	-	1	-	**2**
Costa Rica	2	-	1	1	2	1	-	3	1	6	**17**
Nicaragua	1	-	-	-	-	-	-	-	-	-	**1**
México	3	8	20	12	14	7	2	6	9	14	**95**
Ecuador	0	-	1	-	-	-	-	-	-	-	**1**
Venezuela	0	-	-	-	-	-	1	-	-	-	**1**
India											**342**
India	39	28	14	29	27	42	53	39	39	32	**342**

Continúa en página siguiente

Resoluciones de autorización (2/3)

	2000-2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total Aut.
Otros países											**461**
Marruecos	11	8	7	4	10	13	9	7	7	7	**83**
Singapur	4	-	1	2	4	1	6	3	7	9	**37**
Japón	2	1	1	3	4	7	7	1	7	4	**37**
Malasia	3	3	-	-	2	1	5	2	4	2	**22**
Tailandia	2	-	-	-	1	-	-	-	-	4	**7**
Filipinas	9	4	3	5	9	8	5	6	5	8	**62**
China	5	3	1	14	4	6	-	2	8	3	**46**
Hong Kong	1	1	1	-	1	2	-	2	5	2	**15**
Egipto	1	-	-	-	1	1	-	1	-	-	**4**
Nigeria	1	-	-	-	-	-	-	-	-	-	**1**
Túnez	1	-	2	-	3	-	-	2	1	-	**9**
Sudáfrica	3	-	-	-	3	-	1	1	-	3	**11**
Australia	1	7	-	-	3	4	3	1	8	4	**31**
Canadá	1	-	-	-	1	-	2	-	2	3	**9**
Rep. Bielorrusa	3	-	-	-	-	-	-	-	-	-	**3**
Mónaco	-	1	-	-	-	-	-	-	-	-	**1**
Israel	-	1	6	2	-	-	-	-	-	-	**9**
Vietnam	-	-	3	-	1	-	-	-	-	-	**4**
Barbados	-	-	3	-	-	-	-	-	-	-	**3**
Andorra	-	-	1	-	-	-	-	-	-	-	**1**
Mauricio	-	-	-	1	-	-	-	-	-	1	**2**
Kenia	-	-	-	-	1	-	-	-	-	-	**1**
Serbia	-	-	-	-	1	-	-	1	-	9	**11**
Taiwán	-	-	-	-	2	-	1	-	1	-	**4**
Croacia	-	-	-	-	1	-	-	-	-	-	**1**
Turquía	-	-	-	-	1	-	-	-	1	1	**3**
Ucrania	-	-	-	-	1	-	-	-	-	2	**3**
Bermudas	-	-	1	-	1	-	-	-	-	1	**3**
Nueva Zelanda	-	-	-	-	1	-	1	-	-	-	**2**

Continúa en página siguiente

Resoluciones de autorización (3/3)

	2000-2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total Aut.
Rep. de Corea	-	-	-	-	1	-	1	-	-	2	**4**
Federación Rusa	-	-	-	-	1	1	-	-	1	6	**9**
Emiratos Árabes	-	-	-	-	-	1	-	-	2	1	**4**
Arabia Saudí	-	-	-	-	-	-	-	1	4	1	**6**
Indonesia	-	-	-	-	-	-	-	-	1	1	**2**
Puerto Rico	-	-	-	-	-	-	-	-	2	-	**2**
Irán	-	-	-	-	-	-	-	-	-	1	**1**
Qatar	-	-	-	-	-	-	-	-	-	1	**1**
Camboya	-	-	-	-	-	-	-	-	-	1	**1**
Myanmar	-	-	-	-	-	-	-	-	-	1	**1**
Botswana	-	-	-	-	-	-	-	-	-	1	**1**
Madagascar	-	-	-	-	-	-	-	-	-	1	**1**
Republica de Moldova	-	-	-	-	-	-	-	-	-	2	**2**
Rep. Dem. Pop. De Laos	-	-	-	-	-	-	-	-	-	1	**1**
Internacional											**65**
Internacional	-	-	3	1	3	8	2	8	20	20	**65**
Solicitudes Presentadas	451	166	197	201	224	192	187	128	737	325	2.808
Archivadas	162	24	31	16	52	15	26	29	91	76	522
Total Autorizaciones	276	128	155	175	177	170	150	108	499	253	**2.091**

Ficheros inscritos con transferencias internacionales según titularidad

	Ficheros
Titularidad Privada	20.157
Titularidad Pública	8.436
TOTAL	**25.593**

Evolución de las autorizaciones de transferencias internacionales según las garantías aportadas (tipo de contrato y normas corporativas vinculantes –BCR-)

	2010	2011	2012	2013	2014	2015	2016	2017
2001/497/CE (1)	80	112	167	195	226	246	379	434
2002/16/CE (2) - 2010/87/UE (3)	475	619	735	861	966	1037	1.364	1.527
BCR	-	1	8	17	23	34	61	83
Cláusulas Encargado-Subencargado (4)	-		2	9	16	22	32	43
Contrato “ad hoc”	-		-	-	1	1	2	3

(1) DECISIÓN DE LA COMISIÓN, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE

(2) DECISIÓN DE LA COMISIÓN, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (derogada desde 15 de mayo de 2010)

(3) DECISIÓN DE LA COMISIÓN, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo

(4) RESOLUCIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS de 16 de octubre de 2012

Transferencias internacionales de datos amparadas en las autorizaciones de movimientos de datos entre encargados y subencargados del tratamiento

	2012	2013	2014	2015	2016	2017	Total
Ficheros	1	1.561	1.625	20	32	-	**2.771**
Responsables	1	454	437	8	26	8	**814**

Transferencias internacionales de datos amparadas en la autorización de transferencias internacionales basadas en contrato “ad hoc”

	2014	2015	2016	2017	Total
Ficheros	59	27	543	409	**1.038**
Responsables	14	9	146	129	**298**

Actuaciones como autoridad correvisora de normas corporativas vinculantes (BCR)									
	2010	2011	2012	2013	2014	2015	2016	2017	Total
Revisión BCR'S	1	4	7	3	9	10	8	7	**49**

Evolución de la inscripción de los ficheros de videovigilancia*		
Año de Inscripción	Titularidad Privada	Titularidad Pública
1994 – 2010	61.834	1.250
2011	33.437	433
2012	33.131	529
2013	36.099	417
2014	37.402	456
2015	40.558	438
2016	49.943	328
2017	53.259	286
TOTAL	**345.663**	**4.137**

* Incluye, además de los ficheros que tienen declarada la videovigilancia como finalidad tipificada, aquellos otros en los que se desprende de su denominación o descripción. Por ejemplo, ficheros cuya finalidad tipificada es la de seguridad privada y su denominación es la de "videovigilancia" o "CCTV".

Ficheros de videovigilancia de titularidad privada (1/2)

SECTOR DE ACTIVIDAD PRINCIPAL	2016	2017	% variación 2016-2017
Otras actividades	88.074	104.909	+19,11
Comercio	66.918	76.043	+13,64
Turismo y hostelería	35.033	40.307	+15,05
Comunidades de propietarios	27.009	33.601	+24,41
Sanidad	16.583	19.287	+16,31
Activ. Relacionadas con los productos alimenticios, bebidas y tabacos	6.025	7.161	+18,85
Construcción	5.457	6.060	+11,05
Transporte	4.878	5.611	+15,03
Actividades inmobiliarias	3.925	4.729	+20,48
Industria química y farmacéutica	4.172	4.622	+10,79
Educación	3.773	4.337	+14,95
Contabilidad, auditoria y asesoría fiscal	2.788	3.230	+15,85
Maquinaria y medios de transporte	2.880	3.191	+10,80
Agricultura, ganadería, explotación forestal, caza, pesca	2.736	3.182	+16,30
Servicios informáticos	2.727	3.016	+10,60
Asociaciones y clubes	2.483	2.841	+14,42
Actividades relacionadas con los juegos de azar y apuestas	2.305	2.503	+8,59
Sector energético	2.127	2.271	+6,77
Seguridad	1.937	2.151	+11,05
Actividades diversas de servicios personales	1.777	2.140	+20,43
Producción de bienes de consumo	1.853	2.038	+9,98
Actividades jurídicas, notarios y registradores	1.552	1.845	+18,88
Comercio y servicios electrónicos	1.400	1.734	+23,86
Servicios de telecomunicaciones	1.467	1.595	+8,73
Actividades de servicios sociales	1.410	1.576	+11,77

Continúa en página siguiente

Ficheros de videovigilancia de titularidad privada (2/2)			
SECTOR DE ACTIVIDAD PRINCIPAL	2016	2017	% variación 2016-2017
Activ. De organizaciones empresariales, profesionales y patronales	1.172	1.457	+24,32
Entidades bancarias y financieras	983	1.097	+11,60
Seguros privados	632	753	+19,15
Actividades políticas, sindicales o religiosas	594	700	+17,85
Inspección técnica de vehículos y otros análisis técnicos	390	451	+15,64
Publicidad directa	293	334	+13,99
Organización de ferias, exhibiciones, congresos y otras activ. Relac.	232	281	+21,12
Activ. Postales y de correo (oper. Postales, serv. Post., transport.	214	252	+17,76
Investigación y desarrollo (i+d)	216	237	+9,72
Selección de personal	65	70	+7,69
Mutualidades colaboradoras de los organismos de la seguridad social	30	30	+0,00
Solvencia patrimonial y crédito	22	21	-4,55
TOTAL	**296.132**	**345.663**	**+16,73**

7. Presencia internacional de la AEPD en 2017

Reunión	Fecha	Lugar
Sesiones Plenarias del Grupo de Trabajo del Artículo 29 (GT29)	7 y 8 de febrero 4 y 5 de abril 7 y 8 de junio 3 y 4 de octubre 28 y 29 de noviembre	Bruselas (Bélgica)
Reuniones de subgrupos del GT29		
Reunión de coordinación de subgrupos	10 de enero	Bruselas (Bélgica)
Futuro de la privacidad (FoP)	27 de enero 17 de marzo 23 de mayo 12 de septiembre 7 de noviembre	
Enforcement	24 de enero 15 de marzo 21 de abril 28 de junio 27 de octubre	
Cooperación	11 de enero 3 de mayo 4 de julio	
Financial matters	1 de febrero 16 de marzo 5 de julio 17 de octubre	
Borders, Travelers & Law Enforcement (BTLE)	17 de enero 9 de marzo 16 de mayo 6 de septiembre 26 de octubre	Bruselas (Bélgica)
Key Provisions	23 de febrero 4 de mayo 27 de junio 19 de octubre	
E-Government	2 de febrero 27 de febrero 17 de mayo 24 de octubre	
Tecnología (TS)	18 y 19 de enero 9 de marzo 16 de mayo 6 y 7 de septiembre 25 y 26 de octubre	

Control de Agencias y Grandes Sistemas de Información UE		
Comité de apelaciones JSB Europol	19 de abril	Bruselas (Bélgica)
Europol cooperation board	14 de junio 16 de noviembre	
Grupos de Supervisión Coordinada de los sistemas VIS, SIS II y EURODAC	13 y 14 de junio 14 y 15 de noviembre	
JSA Customs	20 de abril	
Grupo de trabajo del Consejo para asuntos Schengen (Acervo)	8 de febrero 6 y 7 de marzo 3 de mayo 15 y 16 de mayo	
EUROJUST: Plenario	9 de junio	La Haya (P. Bajos)

Otras reuniones		
Reunión con la Agencia Holandesa PD sobre Microsoft	17 de enero	La Haya (Países Bajos)
Reuniones Grupo de Expertos de la Comisión para la implantación del RGPD	14 de febrero 27 de abril 16 de junio	Bruselas (Bélgica)
EDPB IT Systems	1 de marzo	Bruselas (Bélgica)
Taller sobre certificación (París)	30 de marzo	París (Francia)
Reuniones "Grupo de Telecomunicaciones de Berlín"	24 y 25 de abril 27 de noviembre	Washington DC (EEUU) París (Francia)
Conferencia de primavera de Autoridades europeas de Protección de Datos	27 y 28 de abril	Limassol (Chipre)
Taller interactivo RGPD miembros APPA	18 de mayo	París (Francia)
Reuniones Grupo de redacción de las Reglas de Procedimiento del Comité Europeo de Protección de Datos	10 de mayo 5 de septiembre 16 de octubre 31 de octubre 6 de diciembre	Bruselas (Bélgica)
Communication workshop	1 de junio	Bruselas (Bélgica)
Whatsapp Taskforce	12 de julio	Bruselas (Bélgica)
Reunión con la Comisión Europea sobre el Anteproyecto LOPD	22 de septiembre	Bruselas (Bélgica)
39ª Conferencia Internacional de Autoridades de Protección de Datos	25 al 29 de septiembre	Hong Kong (China)
Ampliación del acceso de las fuerzas del orden público a registros centralizados de cuentas bancarias	25 de octubre	Bruselas (Bélgica)
IMI-GDPR Users Workshop	7 y 8 de diciembre	Bruselas (Bélgica)

8. Secretaría General

Gestión de Recursos Humanos

	DOTACIÓN	CUBIERTOS*
Funcionarios	174	150
Laborales	4	4
Laborales fuera de Convenio	2	2
Alto cargo	1	1
TOTAL	**181**	**157**

*Parte de los puestos vacantes han sido creados en julio de 2017 y los concursos para su cobertura se resolverán en enero de 2018

Mujeres	82
Hombres	75

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	7	3	25	51	-	17	2	12	2	4	12	15

GRUPO	A1	A2	C1	C2
Efectivos	39	47	21	43

Evolución del presupuesto

	CRÉDITO EJERCICIO 2015	CRÉDITO EJERCICIO 2016	CRÉDITO EJERCICIO 2017
CAPITULO I	7.295.520	7.305.820	7.360.820
CAPITULO II	5.224.000	4.896.060	4.956.060
CAPITULO III	232.450	232.450	160.950
CAPITULO IV	-	267.940	284.440
CAPITULO VI	1.316.000	1.316.000	1.316.000
CAPITULO VIII	22.800	22.800	22.800
TOTAL	**14.090.770**	**14.101.070**	**14.101.070**

Los datos de todos los capítulos son siempre referidos a créditos definitivos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es