



PLAN ESTRATÉGICO 2015-2019



Este documento tiene como objetivo sentar las bases de las líneas de actuación de la Agencia Española de Protección de Datos (AEPD) en el periodo 2015-2019, incorporando las acciones específicas que cada departamento de la AEPD ha propuesto en relación con sus respectivas materias.

La protección de datos y la privacidad se sitúan en todas las encuestas entre las preocupaciones destacadas de los ciudadanos. Teniendo en cuenta que los europeos hemos otorgado a la protección de datos el rango de derecho fundamental y que corresponde a la Agencia tanto difundir el derecho y proteger a los ciudadanos como velar por el cumplimiento de la legislación española, creemos imprescindible escuchar atentamente las necesidades que plantean todos los implicados y articular los mecanismos necesarios para fomentar las garantías necesarias. La protección de datos vive un momento determinante, por un lado, con continuos cambios tecnológicos que imponen un ritmo trepidante y que pueden tener un fuerte impacto en la vida privada de las personas y, por otro, con la próxima aprobación de un nuevo Reglamento General de Protección de Datos aplicable de forma directa en todos los países de la UE.

El **Plan Estratégico** que encontrará a continuación, aprobado mediante Resolución de la AEPD, es una iniciativa que va a permitir a la Agencia afrontar con decisión estos nuevos retos; reforzar la identidad y la cohesión interna de la institución y su imagen exterior; dar a conocer desde una perspectiva global e integradora todas las actuaciones que pretendemos poner en marcha; posibilitar la actualización de los procedimientos y sistemas de gestión interna mediante la Administración Electrónica con vistas a la mejora continua en la prestación de nuestros servicios y, como factor esencial, posibilitar la mayor participación posible de ciudadanos, responsables y profesionales de la privacidad. Se constituye así como un importante compromiso público por parte de esta institución, que marca en este documento sus líneas de trabajo prioritarias estableciendo las bases sobre las que pretende asentar su actuación en los próximos cuatro años.

Este texto es el resultado de haber sometido a consulta pública una versión borrador del mismo. En este sentido, la Agencia ha recibido casi 400 aportaciones de ciudadanos, responsables de tratamiento, expertos en protección de datos y organizaciones públicas y privadas, todas ellas de gran utilidad para la elaboración de la versión final de este Plan Estratégico. En la Agencia consideramos que la participación es un elemento esencial sin el que no puede lograrse una protección efectiva del derecho fundamental a la protección de datos y por ello queremos agradecer el esfuerzo y el interés mostrado por aquellos que han colaborado en el proceso de información pública, cuyas propuestas, aportaciones y comentarios han contribuido, sin duda, a enriquecer este documento.

Es nuestra intención afianzar a la AEPD como un organismo abierto y cercano que refuerce y amplíe las vías de comunicación con todos los implicados, dando una respuesta integral a sus necesidades. Por ello, de forma independiente al Plan, en la página web de la AEPD seguirá teniendo a su disposición un [Buzón de sugerencias](#) para hacernos llegar sus comentarios.



ÍNDICE

1. ¿POR QUÉ UN PLAN ESTRATÉGICO?	4
2. ESTRUCTURA Y CONTENIDO	9
3. DESTINATARIOS.....	13
4. MISIÓN Y VISIÓN.....	16
5. OBJETIVOS ESTRATÉGICOS.....	19
6. EJES ESTRATÉGICOS	20
7. PROGRAMAS DE ACTUACIÓN E INICIATIVAS.....	25
8. SEGUIMIENTO Y EVALUACIÓN	57



1. ¿POR QUÉ UN PLAN ESTRATÉGICO?

La Agencia Española de Protección de Datos (AEPD) es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos. Tiene como objetivos básicos, por un lado, asegurar y facilitar el cumplimiento de la normativa de protección de datos y, por otro, promover entre los ciudadanos el conocimiento de sus derechos en relación con el tratamiento de sus datos personales y apoyarles en el ejercicio de esos derechos.

En sus ya más de 20 años de existencia, la AEPD ha desempeñado un papel de primer orden en el desarrollo del derecho fundamental en España, convirtiéndose en un referente en el panorama internacional entre sus homólogas, especialmente en los ámbitos europeo e iberoamericano.

La protección de datos vive un momento decisivo, con retos constantes que obligan a escuchar atentamente las necesidades que se plantean. La digitalización de la información ha ampliado enormemente las posibilidades de recogida, almacenamiento y, sobre todo, procesado de la información, a la vez que ha crecido de forma exponencial en los últimos años la cantidad y variedad de datos personales que recogen y tratan tanto actores públicos como privados.

En España 12,6 millones de hogares (el 78,7%) tienen acceso a internet, según la encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares del Instituto Nacional de Estadística (INE) publicada en octubre de 2015. En cuanto a su uso, tres de cada cuatro personas de 16 a 74 años son usuarias frecuentes de la Red, es decir, más de 25 millones de personas. Con estas cifras, es innegable que la universalización del uso de internet y de los servicios de la sociedad de la información y la generalización de los dispositivos móviles inteligentes, entre otros factores, han conducido a un nuevo escenario en el tratamiento de los datos personales en el que no sólo aumentan las capacidades de recogida, almacenamiento y procesado de la información, sino que los costes asociados a éstas se han abaratado enormemente.

La información disponible sobre una persona ha aumentado en cantidad, pero también se ha vuelto, en cierto modo, más personal. Y en ello ha influido un cambio significativo en el papel del ciudadano, que ha pasado de ser un mero receptor de información a ser también un contribuyente activo al caudal disponible sobre él o sobre otros.

Actualmente, es posible conocer prácticamente la totalidad de los hábitos y conductas de una persona a partir de la información que sobre su localización proporcionan su teléfono móvil, las fotografías que almacena en la nube o las cámaras que graban su imagen



digitalmente en sus recorridos por la ciudad, o que respecto a su salud se transmite utilizando alguna de las aplicaciones cada vez más habituales en el entorno de la atención sanitaria, o que sobre sus principales intereses se puede deducir a través de su navegación. En este sentido, desarrollos tecnológicos como el llamado internet de las cosas o el big data están contribuyendo y van a contribuir de forma decisiva a intensificar estas tendencias.

Los datos, además, están cada vez menos circunscritos a los entornos locales o nacionales. La circulación internacional de datos, consecuencia de la globalización y del desarrollo de las tecnologías de la información y la comunicación, se ha convertido en la regla para una parte significativa de los tratamientos de datos, incluidos los vinculados con actividades tan cotidianas como la publicidad, tanto a través de los canales tradicionales (correo, teléfono) como en el entorno online; la gestión de información de empleados, clientes y terceras personas por entidades públicas o privadas; la utilización de datos biométricos por parte de entidades públicas o privadas; la videovigilancia; la prestación de servicios en internet (correo electrónico, redes sociales, motores de búsqueda...), o el uso de información personal en el ámbito de la salud (historias clínicas convencionales o electrónicas, investigación o farmacovigilancia, entre otras).

Estos desarrollos tecnológicos y sociales tienen sin duda unos efectos enormemente positivos para los ciudadanos: para el disfrute de nuevos servicios y productos, que les permiten alcanzar e interactuar con audiencias globales, para su actividad profesional, su ocio, su seguridad, su desarrollo personal o su interacción social. Pero plantean también unos riesgos adicionales desde la perspectiva de la protección de datos y la privacidad. La recogida y monetización de los datos de los usuarios son la base de los modelos de negocio de la mayoría de las empresas que operan en internet, independientemente del servicio o producto que ofrezcan. Algunas de esas compañías almacenan ingentes cantidades de datos, pudiendo crear una situación de concentración que tenga efectos no sólo en el mundo de la protección de datos, sino también en el funcionamiento de los mercados. También los poderes públicos participan de ese acceso y procesado de grandes cantidades de información, lo que suscita preocupaciones sobre los límites de su utilización. De hecho, la última Encuesta a usuarios de internet de la Asociación para la investigación de medios de comunicación (AIMC), publicada en marzo de 2015, destaca una creciente preocupación en torno a la seguridad y la privacidad. La citada encuesta refiere que existe una gran inquietud por el hecho de que las empresas o los gobiernos puedan controlar lo que se hace en internet, con un 53,8% de los usuarios que se muestran “muy preocupados” en lo que se refiere a la vigilancia que puedan hacer las empresas, una cifra similar en lo que respecta al control que puedan hacer los gobiernos (un 52,8%).

Los nuevos riesgos demandan respuestas adaptadas a las circunstancias y condicionantes actuales, que aseguren un elevado nivel de protección y que ofrezcan soluciones que faciliten la innovación y la implantación de nuevos servicios y tecnologías. La evolución de



las nuevas tecnologías y las previsiones de prosperidad económica que surgen en torno a ellas -ligadas indisolublemente a la expansión de internet- obligan a fomentar modelos de negocio que apuesten por productos y servicios innovadores a la vez que compatibles con los derechos fundamentales de los ciudadanos. Las estimaciones sobre la aportación de sector TIC al PIB español son variables. Según AMETIC, esta cifra se sitúa en 7,5%. Por otro lado, algunos estudios apuntan a que en España, los ingresos generados sólo por el internet móvil ascienden a 12.000 millones de euros, un 1,12% del PIB, y prevén que esa cifra se incrementará hasta los 34.900 millones en 2016.

En paralelo, el 17,6% de las empresas con 10 o más empleados ubicadas en España realizaron ventas mediante comercio electrónico en el año 2014, con un volumen de negocio cercano a los 200.000 millones de euros (Fuente: INE, octubre 2015). Un porcentaje importantísimo (44,8%) de los usuarios de internet que no habían comprado a través de esta vía argumentaban preocupación en torno a “la privacidad o la seguridad en el pago”.

En un contexto en el que es necesario contribuir en la medida de lo posible a generar crecimiento económico y fomento del empleo, en la Agencia estamos convencidos de que la salvaguardia de la protección de datos y la privacidad puede convertirse en un elemento diferenciador de valor añadido en los productos y servicios que se pongan en marcha, que sea compatible con el desarrollo de una economía más innovadora.

Los principios, derechos y mecanismos de garantía que recoge la legislación siguen teniendo plena vigencia, pero es necesario actualizar los instrumentos para dotarles de plena eficacia, teniendo presente la consecución de un marco europeo más armonizado.

Los modelos más tradicionales de cumplimiento, basados en la corrección de las vulneraciones de la legislación, tienen limitaciones para hacer frente a las nuevas circunstancias. El incontable número de tratamientos en los que se procesan datos de ciudadanos y la naturaleza de muchos de esos datos requieren estrategias centradas en la prevención, en el establecimiento de las condiciones que impidan que se produzcan esas vulneraciones de la ley para ofrecer una protección práctica y efectiva. Las acciones correctoras tienen un innegable valor disuasorio, especialmente cuando se manifiestan en forma de sanciones o de compensaciones económicas, y por ello deben seguir formando parte del conjunto de herramientas a disposición de una autoridad de supervisión. Pero en términos de protección directa al ciudadano consideramos que resulta más eficaz disminuir los riesgos y prevenir infracciones que repercuten negativamente en los afectados que sancionar a los responsables a posteriori por el daño cometido.

En consecuencia, el contexto actual exige que aquellos que tratan datos apuesten por la implantación de nuevas políticas y herramientas proactivas de cumplimiento. Las autoridades de protección de datos deben contribuir a promover esa implantación,



entendiendo siempre que el cumplimiento no es un fin por sí solo, sino un camino para elevar el nivel de protección y disminuir los casos en que posibles vulneraciones generen daños para los ciudadanos.

Exige, al mismo tiempo, políticas decididas que contribuyan a sensibilizar, formar y apoyar a los ciudadanos, así como la participación no sólo de instituciones, sino también que permitan avanzar en la colaboración público-privada. Estas acciones tienen también una dimensión preventiva. Los ciudadanos, los titulares de los datos, deben ser parte imprescindible de cualquier estrategia de protección. En las sociedades actuales los ciudadanos deben ser conscientes de las múltiples situaciones en que sus datos pueden ser tratados, de cómo afectan esos tratamientos a sus derechos y de cómo pueden mantener el control sobre ellos.

Existe un consenso generalizado en que los principios y derechos del actual marco normativo de protección de datos son plenamente vigentes y no deben ser cuestionados ni debilitados. Pero también hay acuerdo en que el modo en que se instrumentalizan debe ser revisado para servir mejor a sus finalidades de protección, teniendo presente también el contexto europeo y global en el que se opera.

Por ello, la Unión Europea, en cuyo ordenamiento se integran las legislaciones de protección de datos de todos los Estados miembros, inició hace ya algunos años un proceso de revisión que concluirá próximamente con la aprobación de un nuevo Reglamento General de Protección de Datos, así como de una Directiva para los tratamientos en el ámbito policial y judicial penal.

Aunque todavía no se dispone del texto definitivo, todo indica que el futuro Reglamento europeo va a suponer cambios de enfoque significativos en la actividad de quienes tratan datos y de los supervisores europeos.

Desde la perspectiva de responsables y encargados de tratamiento, quizás el aspecto más relevante sea la introducción de un principio general de *accountability*, término inglés de difícil traducción pero que podría equipararse con una exigencia de responsabilidad activa. El Reglamento prevé que los responsables y encargados habrán de establecer mecanismos que les coloquen en posición de poder cumplir con los principios y derechos que en él se prevén. Deben, además, estar en condiciones de poder demostrar que disponen de esos mecanismos y que su adopción se adecúa a los riesgos que los tratamientos que realizan conllevan.

Para las autoridades de protección de datos la gran novedad del Reglamento, aparte de algunas que ya existían en nuestro ordenamiento, como la atribución de potestad sancionadora, es la intensa cooperación entre autoridades que deberá presidir el ejercicio



de sus funciones. El llamado sistema de “ventanilla única” para responsables y ciudadanos, el mecanismo de coherencia y las diversas modalidades de cooperación, que incluyen la posibilidad de realizar inspecciones conjuntas, dibujan un panorama en que muchas de las decisiones, tanto singulares respecto a casos concretos como generales en su papel de asesoramiento en la interpretación y cumplimiento de las normas, se tomarán en procesos de decisión colectivos. La mejor expresión de esta nueva orientación es el futuro Consejo Europeo de Protección de Datos, que según alguna de las propuestas que manejan los legisladores europeos podría convertirse en un organismo de la Unión Europea.

El nuevo Reglamento, y en menor medida la futura Directiva, serán determinantes en la actividad de la Agencia Española de Protección de Datos en los próximos años. Por una parte, deberá valorar los contenidos del Reglamento con vistas a sensibilizar y asesorar tanto a las autoridades con potestades normativas como a las empresas, las instituciones y los ciudadanos. En ese mismo sentido, habrá de determinar qué actuaciones propias pueden ser necesarias para una correcta aplicación del Reglamento y establecer las necesarias prioridades para su puesta en marcha. Esa tarea, por otro lado, no se limita al ámbito interno sino que debe desarrollarse también, paralelamente, en el plano europeo, donde el Grupo de Autoridades europeas de Protección de Datos tiene previsto un programa de trabajo en esa misma línea. Finalmente, la Agencia deberá analizar los cambios que será necesario introducir en su estructura y procesos para adecuarse a los nuevos métodos de funcionamiento impuestos por el Reglamento.

Para seguir evolucionando y continuar llevando a cabo esta labor desde unos parámetros que le permitan afrontar con garantías nuevas competencias y responsabilidades, la AEPD necesita afianzarse como un organismo cercano que refuerce y amplíe las vías de comunicación con el ciudadano, con las empresas y el sector de la economía digital, dando una respuesta integral a sus necesidades.

Para todo ello, la Agencia Española de Protección de Datos debe contar con instrumentos sólidos que le permitan ofrecer una respuesta adecuada, ágil y eficaz a estas nuevas exigencias. En este contexto se enmarca la elaboración de este Plan Estratégico, un documento que, aunque condicionado a la disponibilidad de los correspondientes medios personales y presupuestarios, va a permitir a la Agencia afrontar con decisión los nuevos retos y, en especial, los derivados del próximo marco regulatorio europeo; reforzar la identidad y la cohesión interna de la institución y su imagen exterior; dar a conocer desde una perspectiva global e integradora todas las iniciativas y actuaciones que pretendemos poner en marcha; posibilitar la actualización de los procedimientos y sistemas de gestión interna mediante la Administración Electrónica con vistas a la mejora continua en la prestación de nuestros servicios, y, como factor esencial, posibilitar la mayor participación posible de ciudadanos, responsables y profesionales de la privacidad en las decisiones estratégicas.



2. ESTRUCTURA Y CONTENIDO

La sistemática aplicada en la elaboración de este Plan Estratégico ha partido de la fijación de la misión y visión de la Agencia Española de Protección de Datos como institución y, a partir de las mismas, de la concreción de los grandes objetivos que quieren alcanzarse mediante el desarrollo del Plan.

Para la realización de estos objetivos se plantean una serie de iniciativas estructuradas en cinco grandes ejes estratégicos, que a su vez se encuentran desarrollados a través de diferentes programas específicos.

Cada uno de estos ejes será objeto de un adecuado seguimiento y control que permita retroalimentar el Plan y, en consecuencia, hacer los ajustes y modificaciones que se consideren necesarios.

Los **cinco ejes** estratégicos del Plan son los siguientes:

- **Eje estratégico 1:** Prevención para una protección más eficaz.
- **Eje estratégico 2:** Innovación y protección de datos: factor de confianza y garantía de calidad.
- **Eje estratégico 3:** Una Agencia colaboradora, transparente y participativa.
- **Eje estratégico 4:** Una Agencia cercana a los responsables y a los profesionales de la privacidad.
- **Eje estratégico 5:** Una Agencia más ágil y eficiente.



Los **programas** integrados en cada uno de los ejes estratégicos son los siguientes:

Eje estratégico 1. Prevención para una protección más eficaz

- 1.1. Protección de los ciudadanos
- 1.2. Protección de los menores y educación
- 1.3. Sanidad
- 1.4. Acciones en relación con las Instituciones Públicas
- 1.5. Certificación, acreditación y auditoría
- 1.6. Otras actuaciones de prevención

Eje estratégico 2. Innovación y protección de datos: factor de confianza y garantía de calidad

- 2.1. Creación de la Unidad de Evaluación y Estudios Tecnológicos
- 2.2. Establecimiento de canales de colaboración tecnológica con universidades y grupos de investigación
- 2.3. Colaboración con la universidad en proyectos de innovación interdisciplinares.



- 2.4. Colaboración con la industria, los profesionales y las Administraciones Públicas para la mejora de la competitividad y el fomento de la economía digital
- 2.5. Estudios e informes sobre iniciativas y proyectos de carácter tecnológico
- 2.6. Promoción de la seguridad en el tratamiento de los datos personales.
- 2.7. Espacio web para desarrolladores

Eje estratégico 3. Una Agencia colaboradora, transparente y participativa

- 3.1. Fomento de una cultura de protección de datos
- 3.2. Herramientas de comunicación
- 3.3. Página web
- 3.4. Divulgación

Eje estratégico 4. Una Agencia cercana a los responsables y a los profesionales de la privacidad

- 4.1. Relación con los responsables
- 4.2. Pymes
- 4.3. Profesionales de la privacidad, profesionales TIC y delegados de protección de datos

Eje estratégico 5. Una Agencia más ágil y eficiente

- 5.1. Respuesta a los retos internacionales
- 5.2. Simplificación y mejora de la gestión
- 5.3. AEPD digital
- 5.4. Estatuto y competencias de la Agencia

De cara a la consecución de las iniciativas que componen el Plan, cada programa contará con un **responsable** identificable que coordinará el desarrollo y la ejecución de todas las iniciativas contenidas en el mismo. Con esta atribución la Agencia persigue que la planificación temporal de las iniciativas recogidas en el documento pueda cumplirse, organizando los recursos humanos y materiales precisos para alcanzar los resultados fijados.



<p><u>Eje estratégico 1</u></p> <p>Prevención para una protección más eficaz</p>	<p><u>Eje estratégico 2</u></p> <p>Innovación y protección de datos: factor de confianza y garantía de calidad</p>	<p><u>Eje estratégico 3</u></p> <p>Un Agencia colaboradora, transparente y participativa</p>	<p><u>Eje estratégico 4</u></p> <p>Una Agencia cercana a los responsables y a los profesionales de la privacidad</p>	<p><u>Eje estratégico 5</u></p> <p>Una Agencia más ágil y eficiente</p>
<ul style="list-style-type: none"> - Protección de los ciudadanos - Protección de los menores y educación - Sanidad - Instituciones Públicas - Certificación y acreditación y auditoría - Otras actuaciones de prevención 	<ul style="list-style-type: none"> - Creación de la Unidad de Evaluación y Estudios Tecnológicos - Establecimiento de canales de colaboración tecnológica con universidades y con grupos de investigación - Colaboración con la Universidad en proyectos de innovación interdisciplinares - Colaboración con la industrias, los profesionales y las administraciones públicas - Estudios e informes sobre iniciativas y proyectos tecnológicos - Promoción de la seguridad en el tratamiento de los datos personales. - Espacio Web para desarrolladores 	<ul style="list-style-type: none"> - Fomento de una cultura de protección de datos - Herramientas de comunicación - Página web - Divulgación 	<ul style="list-style-type: none"> - Relación con los responsables - Pymes - Profesionales de la privacidad, profesionales TIC y delegados de protección de datos 	<ul style="list-style-type: none"> - Respuesta a los retos internacionales - Simplificación y mejora de la gestión - AEPD digital - Estatuto y competencias de la AEPD



3. DESTINATARIOS

El presente Plan Estratégico se ha elaborado teniendo en cuenta los destinatarios a los que va dirigido:

- 1) **Ciudadanos.** El pilar fundamental de la protección de datos son los ciudadanos por cuyo derecho fundamental debe velar esta Agencia. Para contribuir a esa protección de forma efectiva es imprescindible la realización de una labor de difusión preventiva, que los ciudadanos conozcan cuáles son sus derechos en materia de protección de datos, qué pueden hacer para protegerlos y cómo exigirlos en caso de que fuera necesario, teniendo en cuenta además un contexto tecnológico en continuo cambio que, en ocasiones, puede tener un fuerte impacto en la esfera privada. Por ello, muchas de las iniciativas de la Agencia contenidas en este Plan están centradas en desarrollar esa labor preventiva de concienciación en diferentes niveles y con especial atención a los colectivos más vulnerables, como los menores.
- 2) **Responsables.** La Agencia va a centrar buena parte de su trabajo en colaborar con las empresas y autónomos que en el desarrollo de su actividad comercial o empresarial se convierten en los principales obligados al cumplimiento de la legislación de protección de datos, ya sea como responsables o encargados del tratamiento. Ello sin perjuicio de otros ámbitos que, por la naturaleza de los datos que tratan, requieren de un tratamiento específico (partidos políticos, sindicatos, confesiones religiosas, etc.). La Agencia quiere contribuir a que el sector empresarial consiga un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico de España. Las iniciativas incluidas en el Plan están dirigidas a poner en marcha las herramientas y canales de cooperación necesarios para lograr que el desarrollo de la actividad tanto de pequeñas empresas como de grandes grupos respete de forma activa este derecho fundamental. Al mismo tiempo, a través de la Unidad de Evaluación y Estudios Tecnológicos, se prevé la colaboración con los responsables y empresas para garantizar la privacidad y la competitividad empresarial desde el diseño del producto o proceso tecnológico. Se trata, en definitiva, de que la institución facilite el cumplimiento y sea receptiva a las sugerencias que nos dirijan con el fin de mejorar los instrumentos de los que disponemos para hacer efectiva esa colaboración.
- 3) **Instituciones Públicas.** Las instituciones públicas, en el ejercicio de sus funciones y en la prestación de los diferentes servicios que ofrecen, tratan una gran cantidad de datos personales. Mediante diferentes iniciativas se busca poner en marcha proyectos que generen estrechos lazos de colaboración entre las diferentes



entidades públicas y la Agencia con el fin de lograr también su estrecha implicación en el cumplimiento y fomento del derecho a la protección de datos. Por ello, se van a desarrollar iniciativas en ámbitos administrativos sectoriales como educación y sanidad. Al mismo tiempo, se va a reforzar la colaboración con otras Autoridades de Protección de Datos, el Defensor del Pueblo, el Consejo de Transparencia y Buen Gobierno, las Fuerzas y Cuerpos de Seguridad, la Fiscalía, el Consejo General del Poder Judicial, la Administración General del Estado, las Comunidades Autónomas y la Federación Española de Municipios y Provincias como algunos de los principales implicados en la protección de este derecho. No podemos olvidar en este Plan el importante papel que juegan las diferentes instituciones públicas para promover y difundir el respeto a la protección de datos.

- 4) **Profesionales de la privacidad y delegados de protección de datos.** Los profesionales de la privacidad desarrollan una labor muy relevante en el asesoramiento que realizan a los responsables y encargados de tratamiento. Igualmente, con independencia de cuál sean las previsiones definitivas que finalmente se establezcan en el futuro Reglamento europeo de protección de datos, la figura del delegado de protección de datos tiene, para la Agencia, una función fundamental como interlocutor para facilitar la adopción de las correspondientes medidas protectoras en el seno de las entidades responsables, desarrollando así la labor proactiva que la Agencia quiere impulsar.
- 5) **Personal de la Agencia Española de Protección de Datos.** Este Plan Estratégico va dirigido también al personal que presta sus servicios en la Agencia Española de Protección de Datos como un elemento fundamental a la hora de llevar a cabo las tareas que se derivan del mismo. El desempeño de las funciones que la Agencia tiene actualmente encomendadas, así como la asunción de las nuevas tareas y responsabilidades que recoge este Plan, requerirá de su compromiso y de la necesaria formación para alcanzar el más efectivo cumplimiento de los objetivos propuestos.





4. MISIÓN Y VISIÓN

MISIÓN

La misión de la Agencia Española de Protección de Datos deriva de las funciones que la normativa le confiere, en concreto en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal; su Reglamento de desarrollo, aprobado mediante RD 1720/2007, de 21 de diciembre; el Estatuto de la Agencia, aprobado mediante RD 428/1993, de 26 de marzo; la Ley 34/2012, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico; y la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Difundir y proteger los derechos de los ciudadanos, promoviendo entre la ciudadanía y las organizaciones el valor de la privacidad

Velar por el cumplimiento de la legislación sobre protección de datos, promoviendo medidas preventivas y ejerciendo la potestad sancionadora

Impulsar una labor proactiva que permita detectar el impacto que los nuevos desarrollos tecnológicos pueden tener en la privacidad de los ciudadanos, promoviendo una concepción de la privacidad como activo de las organizaciones públicas y privadas, y como elemento distintivo de la competitividad en el mercado



VISIÓN

La visión de la Agencia representa el lugar donde la Agencia quiere llegar y la forma en la que quiere verse reconocida por los destinatarios de sus servicios al finalizar el presente Plan Estratégico.

Una Agencia cercana, proactiva y colaboradora, que ofrezca una respuesta eficaz tanto a los ciudadanos como a los sujetos obligados y que responda a las nuevas demandas, retos y oportunidades para profundizar en la garantía efectiva del derecho fundamental a la protección de datos



A modo de representación esquemática, a continuación se muestra un mapa que trata de representar las relaciones causa-efecto entre los distintos elementos que conforman el presente Plan Estratégico desde las distintas perspectivas que se han determinado como relevantes: misión y visión, objetivos, ejes estratégicos, programas e iniciativas:

- La capacidad organizativa de la Agencia
- Los procesos internos y,
- La dimensión o perspectiva externa de la Agencia.





4. OBJETIVOS ESTRATÉGICOS

En el marco de las competencias y funciones de la Agencia, y de acuerdo con las previsiones legales y presupuestarias que rigen su actividad, se han establecido los siguientes **objetivos estratégicos**:

- 1) Fomentar las actuaciones de **prevención** para un cumplimiento más eficaz del derecho, especialmente en ámbitos con un gran impacto ciudadano como la educación y la protección de los menores, la sanidad o la contratación irregular.
- 2) Apoyar aquellas iniciativas que contribuyan a generar un clima de confianza en el ámbito de la **economía digital**, y en los usos de la tecnología por los sectores público y privado, favoreciendo la competitividad de las empresas de contenidos digitales, el desarrollo y la innovación de las industrias TIC y creando un ambiente propicio de cumplimiento normativo en materia de privacidad.
- 3) Impulsar una **labor proactiva** en la Agencia que permita detectar el impacto que los **nuevos desarrollos tecnológicos** pueden tener en la privacidad de los ciudadanos, favoreciendo la introducción, desde las primeras fases de desarrollo de sus nuevos productos y servicios, de los requerimientos que la legislación española y europea establece en materia de protección de datos. Esta actividad deberá tomar en consideración las orientaciones recogidas en la Agenda Digital para Europa y para España, así como las que aparecen en los planes de creación del Mercado Único Digital.
- 4) Promover una Agencia más **transparente, abierta, accesible y participativa**, que favorezca la **comunicación** con la sociedad y establezca relaciones estables de colaboración con los responsables y encargados del tratamiento y con los profesionales de la privacidad, facilitando su acceso a los servicios de la Agencia mediante el uso de herramientas y mecanismos adecuados a sus necesidades.
- 5) Fomentar una Agencia más **ágil y eficiente** mediante la mejora continua de la calidad de los servicios que presta, con especial atención a la simplificación de los procedimientos, la reducción de los tiempos de tramitación, la optimización de recursos y el uso intensivo de las herramientas de la Administración electrónica.
- 6) Reforzar la posición de la Agencia para responder con éxito a los **retos internacionales**, afianzándola como una Autoridad de referencia en el contexto europeo e iberoamericano, especialmente ante la próxima aprobación del nuevo Reglamento Europeo de Protección de Datos, que va a requerir un profundo proceso de adaptación de su organización y de los recursos con los que cuenta.



5. EJES ESTRATÉGICOS

Los objetivos señalados anteriormente se han agrupado en cinco ejes estratégicos en los que se enmarcan, a su vez, distintos programas de actuación e iniciativas.



EJE ESTRATÉGICO 1: PREVENCIÓN PARA UNA PROTECCIÓN MÁS EFICAZ

Las principales líneas de trabajo que la Agencia pretende impulsar en este Eje están centradas en el desarrollo de herramientas y contenidos que promuevan la concienciación ciudadana sobre los derechos y las garantías que les asisten en materia de protección de datos, con especial atención a la protección de los ciudadanos con respecto a las actividades que desarrollan en internet, así como una línea específica para la protección de la privacidad en el colectivo de los menores de edad, el desarrollo de programas de intervención en los sectores educativo y sanitario y la actuación con las principales



empresas de los sectores que tradicionalmente acumulan un mayor número de reclamaciones (telecomunicaciones, agua, energía y banca).

Dentro de este mismo eje estratégico se pretenden llevar a cabo diversas iniciativas en el terreno de los dispositivos de almacenamiento y recuperación de datos, así como en la evaluación del impacto sobre protección de datos en relación con la instalación de los contadores inteligentes, líneas definidas por el fuerte impacto que el desarrollo de estas tecnologías puede tener en el derecho fundamental.

También se va a acometer el estudio y evaluación de los modelos de certificación y acreditación en materia de cumplimiento normativo de protección de datos existentes, en relación con la previsión incluida en los borradores de Reglamento europeo de protección de datos que se encuentran en fase de discusión.

Por último, en este mismo apartado se tiene previsto promover acciones de distinta índole en relación con los tratamientos de datos por parte de las Administraciones Públicas.

EJE ESTRATÉGICO 2: INNOVACIÓN Y PROTECCIÓN DE DATOS: FACTOR DE CONFIANZA Y GARANTÍA DE CALIDAD

La protección de datos es un factor crítico para conseguir un correcto afianzamiento de la Sociedad de la Información, pues es determinante para proporcionar productos y servicios de calidad y, especialmente, para generar confianza entre los ciudadanos en relación al respeto de sus derechos y, en particular, de su privacidad.

Desde esta perspectiva de apoyo a la innovación respetuosa con los derechos de las personas, la AEPD tiene que estar preparada para detectar el impacto que los nuevos desarrollos tecnológicos pueden tener en la privacidad de los ciudadanos, buscando mitigar los riesgos sin que, en ningún caso, haya que renunciar a las funcionalidades y beneficios que pueden aportar a los usuarios o a las ventajas competitivas que estos nuevos desarrollos pueden proporcionar a las empresas españolas.

Con este objetivo, la Agencia desarrollará una labor proactiva entre los responsables de estos productos y servicios para que introduzcan, desde las primeras fases de desarrollo, los requerimientos que la legislación española y europea establecen en materia de protección de datos. Esta actividad deberá tomar en consideración las orientaciones recogidas en la Agenda Digital para Europa y para España, así como las que aparecen en los planes de creación del Mercado Único Digital.

Por todo ello, ha de tener también la capacidad de realizar estudios prospectivos y de análisis de los productos y servicios que ya están en el mercado, de forma que pueda conocer de primera mano sus funcionalidades y la forma en que almacenan, tratan y



comunican las categorías de datos personales que recogen, así como la transparencia con la que se producen estos tratamientos, contando con la colaboración de empresas, administraciones públicas y ciudadanos.

EJE ESTRATÉGICO 3: UNA AGENCIA COLABORADORA, TRANSPARENTE Y PARTICIPATIVA

La Agencia quiere impulsar la mejora de los servicios de información y de asesoramiento a los ciudadanos y a los responsables que resultan obligados por la normativa de protección de datos tanto a través de la revisión de los canales de información existentes como mediante la creación de nuevas vías de comunicación.

Este apartado incluye la puesta en marcha de un servicio específico de atención a menores, docentes y padres, a pymes y a responsables de ficheros, así como novedosos canales de información (apps para móviles, redes sociales, etc.)

Asimismo, se pretende facilitar la relación de los ciudadanos y de las entidades con la Agencia, a través de su modernización y el uso de la Administración Electrónica, e intensificando las labores de divulgación y formación mediante Jornadas y otros medios. Un 62% de los ciudadanos que utilizan internet ha contactado o interactuado con las administraciones o servicios públicos a través de Internet por motivos particulares, según datos del INE. En el terreno empresarial, el 93,0% de las empresas interactuó con las Administraciones Públicas a través de internet en el año 2014.

EJE ESTRATÉGICO 4: UNA AGENCIA CERCANA A LOS RESPONSABLES Y A LOS PROFESIONALES DE LA PRIVACIDAD

Desde la Agencia se ha prestado una atención especial a facilitar a responsables y encargados del tratamiento el cumplimiento de las obligaciones que impone la normativa de protección de datos. Para ello, se han puesto a su disposición distintas herramientas tendentes a facilitar la inscripción de ficheros, la comunicación mediante aplicativos de protección de datos desarrollados por terceros, las herramientas para la autoevaluación, la elaboración de disposiciones para las Administraciones Públicas, las medidas de seguridad, las transferencias internacionales de datos, etc.

Al mismo tiempo que se llevan a cabo estas tareas, y con la mirada puesta en el nuevo escenario que se abre con la adopción del Reglamento europeo, la Agencia quiere ofrecer un servicio más cercano a los responsables, encargados y profesionales de la privacidad que sea de utilidad para la adopción de las medidas a las que éstos resulten obligados en el nuevo marco regulatorio. La Agencia valora el papel de los profesionales de la privacidad como interlocutores en esta materia, manteniendo con ellos una relación fluida y ágil.



En este sentido, la Agencia promoverá la figura de los delegados de protección de datos (DPO), que tienen una labor proactiva fundamental de cara a implantar las medidas protectoras y de evaluación de impacto en el seno de las entidades responsables, por lo que se quiere establecer una estrecha colaboración con estos agentes.

Además, se pretende incrementar los medios y las vías para atender las cuestiones que tanto los responsables como los encargados del tratamiento puedan plantear en relación al cumplimiento de las obligaciones que la normativa de protección de datos les atribuye, estableciendo un canal específico dirigido a las pymes y micropymes. Este canal se constituye como un medio de gran importancia dado que, según el 'Retrato de las pyme 2014', con cifras del Directorio Central de Empresas (DIRCE), el 99,88% del tejido empresarial en España está constituido por pymes (entre 0 y 249 asalariados).

EJE ESTRATÉGICO 5: UNA AGENCIA MÁS ÁGIL Y EFICIENTE

Este eje integra un conjunto de programas e iniciativas que tienen en común la optimización de los recursos de la Agencia para poder afrontar en las mejores condiciones posibles los nuevos retos, en especial con la inminente reforma del marco normativo europeo de protección de datos, que va a tener un notable impacto, además de en la normativa interna, en la organización y funcionamiento de la propia Agencia que, en esa medida, deberá adaptar su estructura y sistemas de trabajo a este nuevo escenario con vistas a seguir garantizando los mejores estándares de calidad en sus servicios.

Se pretende así promover un conjunto amplio de iniciativas encaminadas a simplificar y reducir las cargas burocráticas y los tiempos de tramitación de los procedimientos que son competencia de la Agencia, en especial las consultas, los procedimientos de tutela de derechos, los sancionadores y los recursos, llevando a cabo un seguimiento continuo de las medidas que se vayan adoptando y una evaluación de sus resultados.

Para llevar a cabo esas iniciativas será preciso acometer un profundo proceso de digitalización y automatización de los procesos internos de gestión y de las herramientas de comunicación con nuestros destinatarios, buscando mejorar de forma significativa los ratios de accesibilidad, rapidez y simplicidad de nuestros servicios.

Todo ello sólo será posible con la implicación activa del personal de la Agencia, para lo cual se impulsarán iniciativas orientadas a incentivar su productividad y la calidad de su trabajo, estableciendo sistemas de evaluación objetiva de su rendimiento, junto con las necesarias acciones de formación para garantizar su mejor adaptación a los objetivos de este Plan.

El cumplimiento de estas medidas va a poder lograrse no sólo mediante la movilización de recursos de la Agencia en el ámbito interno, sino también, y no por ello menos relevante, reforzando su proyección internacional, posibilitando su presencia en aquellos foros que



promuevan una cooperación internacional efectiva y garanticen un valor añadido en las iniciativas que se promuevan en ejecución del presente Plan Estratégico.

En último término, las acciones propuestas conllevan que la estructura derivada del Estatuto de la Agencia, que data de 1993, deba ser objeto de una revisión profunda que sólo podrá llevarse a efecto mediante la aprobación de un nuevo Estatuto.



6. PROGRAMAS DE ACTUACIÓN E INICIATIVAS

Los distintos programas de actuación e iniciativas que se desarrollan a continuación se han agrupado en cada uno de los cinco ejes estratégicos citados anteriormente.

EJE ESTRATÉGICO 1. Prevención para una protección más eficaz

<u>Eje estratégico 1</u> Prevención para una protección más eficaz	<u>Eje estratégico 2</u> Innovación y protección de datos: factor de confianza y garantía de calidad	<u>Eje estratégico 3</u> Un Agencia colaboradora, transparente y participativa	<u>Eje estratégico 4</u> Una Agencia cercana a los responsables y a los profesionales de la privacidad	<u>Eje estratégico 5</u> Una Agencia más ágil y eficiente
- Protección de los ciudadanos - Protección de los menores y educación - Sanidad - Instituciones Públicas - Certificación, acreditación y auditoría - Otras actuaciones de prevención				

PROGRAMA 1.1. Protección de los ciudadanos

En el marco de la protección del derecho fundamental a la protección de datos de los ciudadanos, la Agencia quiere desarrollar una labor preventiva de concienciación con carácter general y, además, quiere centrarse en algunos ámbitos en los que dicha labor puede requerir una especial atención.

Actuación 1.1.1. Protección de los derechos en internet.

- Se elaborará una Guía general sobre los derechos de los ciudadanos, de la que se extraerán materiales adicionales (fichas) para su divulgación.
- Se elaborará una Guía para la configuración de las políticas de privacidad.



- Se elaborará una Guía para usuarios de internet, teniendo en cuenta el análisis de riesgos y las políticas y herramientas desarrolladas para que estos puedan gestionar su privacidad.

Actuación 1.1.2. Garantizar la privacidad en la prestación de servicios en internet.

La prestación de servicios en internet debe ir acompañada de políticas de privacidad que permitan garantizar los derechos de los usuarios, cuya tutela corresponde a las Autoridades de protección de datos.

La naturaleza global de estos servicios hace necesaria una actuación coordinada de estas Autoridades. Para ello, se desarrollarán las siguientes acciones:

- Mantener un contacto periódico con los prestadores de servicios.
- Auditar las políticas de privacidad en la prestación de servicios.
- Llevar a cabo acciones coordinadas con otras Autoridades.

Actuación 1.1.3. Contratación irregular y morosidad.

La contratación irregular de servicios constituye una de las principales fuentes de reclamaciones ante la Agencia, especialmente en los sectores de telecomunicaciones y suministros de agua y energía. El importe de las sanciones en 2014 ha sido de casi 11 millones de euros en telecomunicaciones y 2 millones en energía, lo que supone el 74% del total de las sanciones impuestas. Otros sectores afectados son el financiero. Para hacer frente a esta situación, se impulsarán las siguientes actuaciones:

- Analizar con las principales empresas afectadas las deficiencias constatadas por la Agencia, intercambiar criterios para su resolución y auditar su implantación posterior. Se pondrá especial atención a la inclusión de los datos en ficheros comunes de morosidad.
- Actualización del plan sectorial de oficio sobre control de datos en contratación telefónica y a través de internet.
- Elaboración de una Guía para la presentación de quejas y reclamaciones en el ámbito de las telecomunicaciones, partiendo de los trabajos que ya se han llevado a cabo conjuntamente con el Instituto Nacional de Consumo y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI).



- Colaboración con otras Administraciones y con las organizaciones sociales orientadas a la protección de los consumidores y usuarios y, en particular, con el Consejo de Consumidores y Usuarios.
- Elaboración de materiales prácticos, así como la creación de una sección de preguntas frecuentes (FAQs) por temática.

Actuación 1.1.4. Tratamiento de datos con fines de publicidad.

Elaboración de un espacio web sobre privacidad en el ámbito de los tratamientos de datos con fines de publicidad.

La Agencia impulsará la colaboración con aquellas entidades que promueven esquemas de autorregulación en esta materia.

Actuación 1.1.5. Protección de la privacidad de las víctimas de violencia de género.

La Agencia promoverá la protección de la privacidad de las víctimas de los delitos de violencia de género y la colaboración con la Fiscalía General del Estado y las unidades especializadas de la Guardia Civil y del Cuerpo Nacional de Policía, especialmente en el ámbito de internet y las nuevas tecnologías.

PROGRAMA 1.2. Protección de los menores y educación

El tratamiento de datos de y por los menores de edad aconseja la puesta en marcha de diversas iniciativas que refuercen la concienciación y la protección de un colectivo especialmente expuesto a los riesgos relacionados con su privacidad. La encuesta del Instituto Nacional de Estadística (INE) publicada en octubre de 2015 muestra que el uso de Internet y, sobre todo, del ordenador, es una práctica mayoritaria en edades anteriores a los 10 años. El uso del ordenador y de internet en los jóvenes de 10 a 15 años es prácticamente universal, con una media del 95,1% y un 93,6% respectivamente. Por su parte, la disposición de teléfono móvil se incrementa significativamente a partir de los 10 años hasta alcanzar el 90,4% en la población de 14 años.

El 39,6% cree que el riesgo más habitual al que están expuestos los menores en internet es la difusión de fotos y vídeos comprometidos, seguido de dar demasiada información sobre ellos mismos a gente que no conocen (22,9%) y ser acosado u hostigado con el fin de obtener concesiones sexuales (17,1%), según datos del CIS.



Actuación 1.2.1. Canal de comunicación con centros educativos, docentes, monitores, padres y menores.

Incluye la puesta en marcha de un teléfono específico de información dirigido a menores, padres y docentes, así como un canal de comunicación a través de WhatsApp.

Se impulsará un canal más activo de comunicación con otras administraciones y entidades con el fin de dar a conocer también las iniciativas que desde diferentes ámbitos se vienen trabajando con el fin de fomentar un uso responsable de las nuevas tecnologías.

Actuación 1.2.2. Plan de inspección sectorial de oficio sobre servicios cloud en el ámbito educativo.

El objetivo de esta actuación es recabar información sobre las medidas que deben adoptarse para la aplicación de las recomendaciones contenidas en la inspección sectorial de oficio y ofrecer a las entidades implicadas la colaboración de la Agencia.

En tal sentido, se prevén actuaciones en relación con los distintos sectores afectados:

- Consejerías autonómicas.
- Asociaciones de centros privados.
- Plataformas educativas.
- Editoriales de libros digitales.

Actuación 1.2.3. Colaboración con las administraciones educativas.

Se impulsarán las siguientes líneas de actuación:

- Formación de docentes. En colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), las Comunidades Autónomas y el sector privado, a través de cursos virtuales para educadores, MOOC, jornadas sectoriales de formación de formadores, materiales, etc.
- Formación de alumnos. En especial, mediante el apoyo a la elaboración de los contenidos de la materia como integrante del curricular básico de la ESO y Bachiller.
- Formación de padres.

Actuación 1.2.4. Colaboración con la Fiscalía y las Fuerzas y Cuerpos de Seguridad.

Se impulsará la colaboración con la Fiscalía de Menores y la Fiscal de Sala de Criminalidad Informática, en los siguientes ámbitos:



- Elaboración de materiales que ayuden a prevenir delitos cometidos contra menores y mujeres víctimas de violencia de género en internet, así como los realizados por menores.
- Dar traslado a la Fiscalía de aquellas actuaciones de las que la AEPD tenga conocimiento con ocasión de los procedimientos de su competencia que puedan ser constitutivos de delitos en el campo de la criminalidad informática.
- Participación de la AEPD en jornadas de formación conjuntas.

Asimismo, se promoverá la colaboración con las Unidades Tecnológicas de la Policía y la Guardia Civil, a través de un convenio con el Ministerio del Interior, y con las restantes Fuerzas y Cuerpos de Seguridad para el desarrollo de acciones formativas y de herramientas de información que garanticen una navegación segura por parte del menor y de las familias en internet.

Actuación 1.2.5. Políticas de privacidad en redes sociales y móviles.

Se promoverá la supervisión por parte de la Agencia de las políticas de privacidad en las redes sociales y dispositivos móviles, y especialmente del control de su uso por menores de 14 años, teniendo en cuenta las conclusiones de la Subcomisión para el estudio de las Redes Sociales de la Comisión de Interior en el Congreso de los Diputados.

Se fomentará una mayor educación digital de los menores a través de la elaboración de fichas prácticas para que estos configuren sus políticas de privacidad en las redes sociales e internet, en colaboración con el Ministerio de Educación y las Comunidades Autónomas.

Actuación 1.2.6. Revisión y actualización de materiales y herramientas prácticas.

Se revisarán los recursos que ofrece la Agencia para que el material y las herramientas que se ofrecen sean útiles, comprensibles y accesibles para todas las personas, en especial para aquellas con discapacidad. En particular:

- Se elaborarán fichas didácticas dirigidas a los menores, padres y profesores.
- Se revisará la página web de la Agencia destinada a menores y su funcionamiento.
- Elaboración de una Guía para centros docentes que proporcione los criterios generales que estos deben seguir en el tratamiento de los datos personales que realizan de sus alumnos, a fin de que dispongan de una herramienta de fácil acceso que posibilite su adecuación a la normativa de protección de datos.



- Elaboración de una Guía para Universidades.
- Elaboración de una Guía sobre la videovigilancia en los centros escolares, que se integraría posteriormente en la Guía para centros docentes.

Actuación 1.2.7. Premios y concursos.

Inclusión en la convocatoria de los Premios de Protección de Datos de la Agencia de un premio específico en este ámbito, así como la convocatoria de un concurso escolar que recoja la experiencia llevada a cabo con la iniciativa Pandijuegos.

PROGRAMA 1.3. Sanidad

Se prevén diversas actuaciones en relación con los tratamientos llevados a cabo en el sector sanitario.

Actuación 1.3.1. Plan de inspección sectorial de oficio de sanidad.

Se llevará a cabo la actualización del Plan de inspección sectorial de oficio de sanidad que se llevó a cabo en 1997, en la que se incluirán todos los niveles asistenciales, tanto públicos como privados, las labores de investigación, la actividad farmacéutica, los componentes de salud electrónica y salud móvil, etc.

A tal fin, se estudiará la posibilidad de establecer un convenio de colaboración con el Ministerio de Sanidad.

Actuación 1.3.2. Plan de inspección sectorial de oficio del sector sociosanitario.

Su objetivo es detectar los tratamientos y cesiones de datos que se llevan a cabo entre ambos sectores, social y sanitario, buscando su adecuación a la legislación de protección de datos y de acuerdo con la información que suministren los sectores afectados.

Actuación 1.3.3. Guía para instituciones y profesionales sanitarios.

Esta guía recogerá de una forma práctica las obligaciones y buenas prácticas más relevantes en relación con aquellas materias que hayan sido objeto del plan de inspección sectorial de oficio.

Actuación 1.3.4. Guía para pacientes y usuarios de la sanidad.

Esta guía abordará de una forma práctica y básica los derechos y buenas prácticas más relevantes que sean de interés para los pacientes y usuarios de la sanidad.

Actuación 1.3.5. Herramientas adaptadas.



Se impulsará el desarrollo de herramientas específicas adaptadas a las especiales características de los distintos ámbitos del entorno sanitario.

PROGRAMA 1.4. Acciones en relación con las Instituciones Públicas

En este programa se pretende promover acciones de distinta índole tendentes a mejorar las medidas de prevención en relación con los tratamientos de datos que llevan a cabo las Administraciones Públicas.

Actuación 1.4.1. Orientaciones de protección de datos en la reutilización de información del sector público y en la anonimización.

Esta actuación se enmarca en la línea de impulsar la reutilización de la información del sector público, favoreciendo el desarrollo de nuevas actividades económicas y ofreciendo procedimientos que garanticen la anonimización de los datos personales.

Actuación 1.4.2. Guía de protección de datos en la Administración Electrónica.

Esta guía estaría destinada a establecer criterios de actuación en materia de protección de datos en relación con los procedimientos y demás instrumentos propios de la Administración electrónica, tanto para las Administraciones Públicas como para los ciudadanos, a fin de que conozcan sus derechos y obligaciones respectivas en estos entornos.

Actuación 1.4.3. Fomentar las buenas prácticas en materia de privacidad.

Se pretende evaluar las distintas opciones para fomentar las buenas prácticas administrativas y promover su difusión. Entre ellas, mediante la formación de los empleados públicos en materia de protección de datos, manteniendo los cursos online que se imparten en colaboración con el Instituto Nacional de Administración Pública (INAP).

Actuación 1.4.4. Promover la seguridad jurídica mediante la emisión de informes preceptivos de los proyectos normativos.

Con esta actuación se busca reforzar el ejercicio realizado por la Agencia en la emisión de informes preceptivos como instrumento preventivo que posibilita la adecuación de los proyectos normativos a las exigencias de la legislación de protección de datos, evitando conflictos en la aplicación posterior de las normas.

Actuación 1.4.5. Colaboración con las Autoridades autonómicas de protección de datos



La Agencia seguirá impulsando los órganos e instrumentos de colaboración ya establecidos y promoverá otros nuevos con las Autoridades de Protección de Datos de País Vasco, Cataluña y Andalucía.

Actuación 1.4.6. Colaboración con el Defensor del Pueblo.

Se impulsará la colaboración con el Defensor del Pueblo a través de los instrumentos que se consideren más adecuados para las necesidades de ambas instituciones con el objetivo de potenciar la garantía del derecho fundamental a la protección de datos.

Actuación 1.4.7. Colaboración con el Consejo de Transparencia y Buen Gobierno.

Se establecerán criterios conjuntos de interpretación para ponderar la aplicación de la normativa de transparencia y acceso a la información pública con el ejercicio del derecho fundamental a la protección de los datos personales.

Actuación 1.4.8. Colaboración con el Consejo General del Poder Judicial.

Con la entrada en vigor de la reforma de la Ley Orgánica del Poder Judicial se delimitan con mayor claridad las competencias del Consejo General del Poder Judicial (CGPJ) como Autoridad de Control en materia de Protección de Datos, atribuyéndole la competencia sobre los tratamientos efectuados con fines jurisdiccionales y los ficheros jurisdiccionales, siendo competencia de la AEPD los de naturaleza no jurisdiccional.

Esto obliga a establecer relaciones de colaboración estrechas y eficaces entre ambas autoridades de control, así como con el Ministerio de Justicia, para lo que se mantendrán reuniones con el fin de fijar unos criterios comunes y claros de delimitación competencial que eviten conflictos de competencias y confusión a los ciudadanos a la hora de dirigirse a la Autoridad de Control correspondiente.

En especial, se impulsarán esas relaciones a través del Convenio suscrito con el Centro de Documentación Judicial (CENDOJ).

Asimismo, se realizará una Evaluación de Impacto en la Protección de Datos Personales sobre el proceso de anonimización y publicación de sentencias del CENDOJ.

Actuación 1.4.9. Colaboración con la Fiscalía General del Estado.

Se impulsará la colaboración con la Fiscalía General del Estado en los siguientes ámbitos:



- Traslado de información sobre cualquier actividad delictiva de la que la Agencia tenga conocimiento en el ejercicio de sus competencias, en especial los delitos de descubrimiento y revelación de secretos o de acceso ilegal a sistemas informáticos, así como los relativos a la violencia de género, especialmente a través de internet y las nuevas tecnologías.
- Realización de actividades formativas conjuntas para mejorar y potenciar la respectiva actuación en defensa del derecho a la protección de datos, cualquiera que sea el ámbito jurisdiccional en que se plantee el conflicto.
- Establecer contactos para facilitar la gestión en relación con los ficheros declarados por la Fiscalía General del Estado.

Actuación 1.4.10. Colaboración con la Administración General del Estado.

Se reforzarán las relaciones con la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), Red.es, el Ministerio de Hacienda y Administraciones Públicas, a través de la Dirección de Tecnologías de la Información y las Comunicaciones, la Oficina para la Ejecución de la Reforma de la Administración (OPERA) y el Ministerio de Fomento, en relación con los drones.

Asimismo, la AEPD solicitará colaborar en los trabajos del Comité de Dirección TIC y el Foro de Transformación Digital para facilitar el cumplimiento de la normativa de protección de datos, en especial en ámbitos como la seguridad, el fomento de buenas prácticas para mitigar el impacto de las TIC en relación con el tratamiento de datos personales, la formación de empleados, o como punto de encuentro entre la Agencia y los responsables de seguridad y protección de datos de las Administraciones Públicas.

Se elaborará una Guía para empleados públicos.

Actuación 1.4.11. Colaboración con las Comunidades Autónomas y las Entidades Locales.

Se impulsarán las relaciones con las Comunidades Autónomas en aquellos ámbitos que puedan requerir su colaboración para un ejercicio más efectivo de las competencias de la Agencia.

Asimismo, se reforzarán las relaciones con las Entidades Locales a través de la Federación Española de Municipios y Provincias en ámbitos como videovigilancia, publicación de actos en webs municipales, uso de cloud, redes sociales, etc.

Actuación 1.4.12. Colaboración con las Universidades.



Se promoverán acciones de colaboración con las Universidades en aquellas cuestiones que puedan contribuir al conocimiento y difusión del derecho a la protección de los datos personales, especialmente en el ámbito de la investigación.

PROGRAMA 1.5. Certificación, acreditación y auditoría

Los esquemas de certificación se presentan cada vez más como herramientas útiles para conseguir en la práctica mayores niveles de protección. El futuro Reglamento europeo reconoce esta importancia creciente y prevé que los Estados, las Autoridades de Protección de Datos y las instituciones europeas promuevan su implantación.

Actuación 1.5.1. Evaluación de los modelos de certificación y acreditación del cumplimiento de la normativa de protección de datos.

Estudiar y evaluar los diversos modelos de certificación y acreditación existentes o futuros para verificar su adecuación como instrumentos de mejora de la privacidad de las personas.

Actuación 1.5.2. Auditorías de protección de datos y de seguridad.

Asimismo, la Agencia promoverá la realización de auditorías periódicas de seguridad y de protección de datos como elementos decisivos de comprobación del cumplimiento de las obligaciones legales de las organizaciones.

PROGRAMA 1.6. Otras actuaciones de prevención

Actuación 1.6.1. Guía sobre cookies.

El 52% de los usuarios de internet declara conocer qué son las cookies y el 24% indica haber realizado modificaciones en la configuración del navegador para prevenir o limitar las cookies, según cifras de INE de octubre de 2015. Estas cifras ponen de manifiesto que en los últimos años se ha mejorado la información que las páginas web ofrecen a sus usuarios, pero aún queda mucho trabajo por hacer. La Agencia llevará a cabo diversas actuaciones con representantes del sector del comercio electrónico y la publicidad online (Adigital, IAB y Autocontrol de la Publicidad) para la evaluación de la Guía sobre el uso de las cookies que se elaboró con estas entidades en 2013 y, en función de los resultados, se procedería a su actualización.

Actuación 1.6.2. Contadores inteligentes.



El despliegue de los contadores inteligentes en España, en particular, para implantar la tarificación eléctrica horaria ha tenido como resultado que haya varios millones de contadores instalados.

Se promoverá la colaboración de la Agencia respecto a la necesidad de que los responsables que utilicen contadores inteligentes realicen una evaluación de impacto en la protección de datos de estos sistemas, de conformidad con la Recomendación de la Comisión Europea de 9 de marzo de 2012 (DOUE 13.3.2012) relativa a los preparativos para el despliegue de los sistemas de contador inteligente.

Actuación 1.6.3. Inspecciones sectoriales de oficio.

Además de los planes de inspección sectorial de oficio mencionados específicamente en este Plan, la Agencia abordará otras iniciativas en este campo derivadas de las necesidades detectadas en el desarrollo del presente Plan Estratégico o de las eventuales circunstancias que aconsejen una revisión en profundidad de un sector determinado.



EJE ESTRATÉGICO 2: Innovación y protección de datos: factor de confianza y garantía de calidad

<p><u>Eje estratégico 1</u></p> <p>Prevención para una protección más eficaz</p>	<p><u>Eje estratégico 2</u></p> <p>Innovación y protección de datos: factor de confianza y garantía de calidad</p>	<p><u>Eje estratégico 3</u></p> <p>Un Agencia colaboradora, transparente y participativa</p>	<p><u>Eje estratégico 4</u></p> <p>Una Agencia cercana a los responsables y a los profesionales de la privacidad</p>	<p><u>Eje estratégico 5</u></p> <p>Una Agencia más ágil y eficiente</p>
	<ul style="list-style-type: none"> - Creación de la Unidad de Evaluación y Estudios Tecnológicos - Establecimiento de canales de colaboración tecnológica con universidades y grupos de investigación - Colaboración con la universidad en proyectos de innovación interdisciplinares - Colaboración con la industrias, los profesionales y las administraciones públicas - Estudios e informes sobre iniciativas y proyectos tecnológicos - Promoción de la seguridad en el tratamiento de datos personales - Espacio web para desarrolladores 			



Actuación 2.1. Creación de la Unidad de Evaluación y Estudios Tecnológicos (UEET).

Se promoverá la creación de una Unidad especializada que evalúe las implicaciones para la privacidad de las nuevas tecnologías, realizando estudios prospectivos y análisis de los productos y servicios que ya están en el mercado para conocer de primera mano sus funcionalidades y la forma en que almacenan, tratan y comunican las categorías de datos personales que recogen, así como la transparencia con la que se llevan a cabo estos tratamientos.

Actuación 2.2. Establecimiento de canales de colaboración tecnológica con universidades y grupos de investigación.

La UEET necesitará contar con especialistas muy cualificados en los últimos avances y desarrollos de ingeniería informática e ingeniería de las telecomunicaciones para poder examinar los productos y servicios que integran las nuevas propuestas tecnológicas, debido a la necesidad de analizar en profundidad los sistemas operativos, programas y dispositivos para conocer qué datos personales se almacenan, tratan y comunican a terceros y verificar que dichos tratamientos se ajustan a lo establecido en sus especificaciones y a la normativa de protección de datos.

Por este motivo, sin perjuicio de los acuerdos y convenios específicos que se puedan alcanzar con diferentes universidades para acoger alumnos de grado o postgrado en prácticas, se convocarán, por parte de la AEPD, becas para graduados en materias tales como matemáticas, física, ingeniería informática e ingeniería de telecomunicaciones, lo que redundará, en el futuro, en que existan profesionales TIC que conozcan estas materias y reconozcan la necesidad de que los desarrollos tecnológicos que realicen en su vida profesional respeten los derechos de los ciudadanos.

Del mismo modo, se establecerán contactos con grupos de investigación tecnológica con vistas a establecer convenios de colaboración que permitan una colaboración continuada de sus miembros apoyando a la AEPD en las labores descritas en este apartado y, al mismo tiempo, poder tener un canal de comunicación para plantear a la Agencia las inquietudes que en materia de protección de datos aparezcan en sus investigaciones.

Finalmente, se propondrá la incorporación de la materia de protección de datos en la formación de estudios universitarios y, en particular, en los de carácter técnico y científico.

Actuación 2.3. Colaboración con la universidad en proyectos de innovación interdisciplinares.



La innovación no sólo se produce en el ámbito tecnológico sino que los cambios jurídicos, sociales, económicos, de modelo de negocio, etc. influyen también en gran manera en la forma en que se percibe la protección de datos personales y en cómo se deben implantar las garantías que salvaguarden los derechos de los ciudadanos.

Por ello, es necesario que la Agencia establezca los cauces de colaboración necesarios con el ámbito académico para el establecimiento de grupos de trabajo interdisciplinares que valoren todas estas innovaciones y nuevos desarrollos y el apoyo a los proyectos de investigación que tengan como objetivo la promoción y la defensa del derecho a la protección de datos personales ante las nuevas realidades que aparecen constantemente.

En este empeño, se deberá prestar especial atención a los proyectos e iniciativas amparados por el programa Horizonte 2020 de la Unión Europea, que financia proyectos de investigación e innovación de diversas áreas temáticas en el contexto europeo en el periodo.

Actuación 2.4. Colaboración con la industria, los profesionales y las Administraciones Públicas para la mejora de la competitividad y el fomento de la economía digital.

Celebración de encuentros o seminarios periódicos con expertos de las empresas o asociaciones tecnológicas más relevantes de España para conocer los desarrollos que están llevando a cabo, sus opiniones en relación con la implantación de los requerimientos de protección de datos en los productos que desarrollan o comercializan y promover políticas adecuadas de protección de datos (en particular, la Protección de Datos desde el Diseño y las Evaluaciones de Impacto).

Asimismo, se impulsarán vías de colaboración con organismos públicos encargados de la promoción de las TIC y de la ciberseguridad como, por ejemplo, la SETSI, Red.es, el Instituto Nacional de Ciberseguridad (INCIBE), el Centro para el Desarrollo Tecnológico Industrial (CDTI), y el Centro Criptológico Nacional (CCN) para buscar las posibles sinergias y puntos comunes de interés y aunar esfuerzos para mejorar las garantías de protección de datos de los ciudadanos.

Estas actuaciones deberán enmarcarse dentro de los objetivos establecidos en la Agenda Digital para Europa y para España y, en lo que se afecta a la protección de datos personales la Agencia se centrará especialmente en el impulso y apoyo de las siguientes iniciativas:

- Iniciativas en relación con las TIC en las pymes y el comercio electrónico.
- Iniciativas en relación con la industria de contenidos digitales.
- Iniciativas que favorezcan un clima de confianza en el ámbito digital.



- Iniciativas de desarrollo e innovación del sector TIC como generador de empleo.

Actuación 2.5. Estudios e informes sobre iniciativas y proyectos de carácter tecnológico.

Diversos estudios prospectivos señalan que la sensorización de las personas y el internet de las cosas van a experimentar un crecimiento exponencial en los próximos años con el consiguiente impacto en la privacidad. La AEPD debe estar preparada para conocer los caminos de esta evolución, las tecnologías utilizadas y su transcendencia para los derechos de los ciudadanos, tanto en el plano teórico general como en el de la situación en España.

Por ello, se realizarán estudios sobre diversos aspectos de la llamada sociedad conectada, que cubrirían temas como big data, internet de las cosas, device fingerprinting, smart cities, smart cars, smart homes (tv inteligentes, contadores inteligentes...), aplicaciones móviles, drones y otras tecnologías de vigilancia inteligente, smart workplaces, seguros basados en el comportamiento, etc.

Además, por su especial sensibilidad, se llevará a cabo un estudio específico sobre el uso de estas tecnologías en el ámbito sanitario, donde esta tendencia se está expandiendo rápidamente, con un gran impacto en la privacidad de las personas. Ello también permitiría transmitir conocimiento y experiencia a la realización del estudio general antes mencionado.

Actuación 2.6. Promoción de la seguridad en el tratamiento de datos personales.

Con especial orientación a los ciudadanos y a las pymes, se estudiará y se pondrán en marcha iniciativas que permitan conocer el estado de la seguridad de los distintos dispositivos fijos y móviles en aras a una mejor protección de los datos personales tratados en los mismos y, en su caso, facilitar herramientas que ayuden a los usuarios a mejorar la privacidad de sus dispositivos. Para ello se colaborará con el INCIBE para aunar esfuerzos y buscar sinergias entre ambas instituciones.

Asimismo, se llevará a cabo un estudio sobre la utilización de herramientas tales como Big Data en la lucha contra las ciberamenazas para conjugar este objetivo imprescindible para el desarrollo de la sociedad de la información y el conocimiento y la economía digital con las garantías de los derechos de las personas. Para ello, se buscará la colaboración de instituciones públicas con competencias en la materia como el INCIBE, el CCN-CERT o la Comisión de Estrategia TIC, así como de entidades privadas como desarrolladores de soluciones de seguridad y organizaciones de promoción de la seguridad de los sistemas de información.



Se prestará especial atención a los tratamientos que deben llevar a cabo los CERT para responder proactivamente y con la presteza requerida a estas ciberamenazas para los sistemas de tratamiento de información públicos, privados y personales o domésticos.

Actuación 2.7. Espacio web para desarrolladores.

Las personas y organizaciones que diseñan, desarrollan y programan productos y servicios TIC son el primer eslabón de una cadena en la que resulta especialmente importante la adecuación a la normativa de protección de datos y los principios y derechos que consagra.

Además, desde la perspectiva de la protección de datos desde el diseño y las evaluaciones de impacto (EIPD) su concienciación y formación en estas materias es imprescindible.

Por ello, el microsite propuesto resumiría y presentaría estos temas y materias poniendo el foco en la terminología, los conocimientos y las labores realizadas por estos profesionales.



EJE ESTRATÉGICO 3. Una Agencia colaboradora, transparente y participativa

<u>Eje estratégico 1</u> Prevención para una protección más eficaz	<u>Eje estratégico 2</u> Innovación y protección de datos: factor de confianza y garantía de calidad	<u>Eje estratégico 3</u> Un Agencia colaboradora, transparente y participativa	<u>Eje estratégico 4</u> Una Agencia cercana a los responsables y a los profesionales de la privacidad	<u>Eje estratégico 5</u> Una Agencia más ágil y eficiente
		<ul style="list-style-type: none"> - Fomento de una cultura de protección de datos - Herramientas de comunicación - Página web - Divulgación 		

PROGRAMA 3.1. Fomento de una cultura de protección de datos

Con el desarrollo de este programa la Agencia pretende promover diversas acciones e iniciativas tendentes a mejorar la atención a los ciudadanos en el ejercicio de sus derechos.

Actuación 3.1.1. Ampliación de los servicios de atención al público.

Se ampliarán las funciones de información y asesoramiento de la Agencia, en especial, independizando las líneas telefónicas por materias o sectores (ciudadanos, pymes, responsables, y menores, padres y docentes), lo que requerirá la necesaria adaptación del personal que presta estos servicios.

Actuación 3.1.2. Edición y difusión de materiales para que los ciudadanos conozcan sus derechos.

Revisión de los materiales actuales y, en su caso, actualización y creación de nuevas herramientas (guías, vídeos, fichas prácticas) o nuevos contenidos digitales para ayudar a los ciudadanos a conocer sus derechos y presentar reclamaciones.

Elaboración de guías y herramientas multimedia de autoaprendizaje y ayuda.

Actualización de la Guía de videovigilancia.



Actuación 3.1.3. Canales de participación ciudadana.

Se valorarán, para su implantación posterior cuáles de los posibles mecanismos de participación, como buzones de sugerencias o foros, se adaptan mejor a la labor desarrollada por la Agencia.

Actuación 3.1.4. Evaluación de los servicios.

Se reforzará la evaluación anual de los servicios que presta la Agencia, diseñando e implantando sistemas de medición adecuados a sus características y necesidades, especialmente aquellos que evalúen el nivel de satisfacción y la calidad de la atención prestada a los ciudadanos.

Actuación 3.1.5. Actualización de la Carta de Servicios.

Actualización de la Carta de Servicios en sintonía con los objetivos del Plan Estratégico.

PROGRAMA 3.2. Herramientas de comunicación

El objetivo del programa será promover diversas acciones e iniciativas tendentes a impulsar la comunicación y presencia de la Agencia en diferentes entornos.

Actuación 3.2.1. Presencia de la Agencia en las redes sociales.

Más del 80% de los usuarios de internet utiliza las redes sociales. Los organismos públicos tienen la obligación de estar en contacto con los ciudadanos, ya sea para dar difusión a las iniciativas realizadas y que estos puedan conocer las novedades que les afectan como para escuchar sus comentarios. La presencia en las redes sociales es un instrumento idóneo para tomar el pulso de ciudadanos, empresas y profesionales y dar respuesta, ya sea de forma interna o externa, a sus demandas. El objetivo final es la construcción de un organismo público que difunde, escucha y da respuesta.

Actuación 3.2.2. Blog de la Agencia.

En esta labor de dar a conocer el derecho fundamental a la protección de datos cobra también una especial relevancia tanto la difusión de las iniciativas puestas en marcha como el tratamiento de los diferentes temas que pueden tener una incidencia destacada en la protección de datos. Para ello, la Agencia quiere trabajar en la construcción de un altavoz que recoja la visión y postura del organismo en diferentes ámbitos, una visión cercana al ciudadano y alejada, en la medida de lo posible, de los tecnicismos. La construcción de un blog que analice de forma sencilla la evolución de las iniciativas en desarrollo, que promocióne los proyectos puestas en marcha o que recoja la posición de la Agencia sobre



temas de actualidad puede suponer una oportunidad para acercarse tanto al ciudadano como al responsable y plasmar, de forma práctica, comprensible y accesible para todas las personas el trabajo realizado por este organismo.

Actuación 3.2.3. Aplicaciones móviles.

Las aplicaciones en los teléfonos móviles juegan un papel fundamental a la hora de acceder a internet: más de la mitad de los individuos (58%) accede mayoritariamente mediante apps, según datos de la AIMC. Para dar un paso adicional en la interacción con los ciudadanos, responsables y profesionales, la Agencia quiere poner en marcha el desarrollo de aplicaciones móviles que permitan un acceso más cómodo, flexible y estructurado a la información disponible en un entorno multiplataforma y, al mismo tiempo, para aportar funcionalidades que permitan a las personas tener un mayor y mejor control sobre su privacidad.

Actuación 3.2.4. Relaciones con los medios.

La difusión que realizan los medios de comunicación del derecho a la protección de datos es un elemento esencial tanto para fomentar la sensibilización y el conocimiento de los ciudadanos en esta materia como para que los responsables cumplan con sus obligaciones legales. La Agencia quiere profundizar en la atención personalizada a los medios de comunicación, que han contribuido de forma imprescindible en los últimos años a divulgar la labor realizada por ella. Para ello, además de mantener la respuesta personalizada a las demandas de información, fomentará reuniones periódicas organizadas en torno a diferentes temáticas o asuntos de interés.

Actuación 3.2.5. Agenda institucional.

En aras a reforzar la transparencia y de que tanto ciudadanos como responsables puedan conocer las actividades en las que participa la Agencia, este organismo quiere fomentar la publicación de su agenda institucional, ampliando los contenidos de la sección ya existente.

Actuación 3.2.6. Memoria anual de la Agencia.

La AEPD elabora y difunde anualmente su Memoria, un documento exhaustivo que recoge un informe detallado de las actividades realizadas por este organismo, una exposición de las novedades legislativas y jurisprudenciales más relevantes y un análisis de los principales retos que afronta el derecho fundamental a la protección de los datos personales. La Agencia elaborará esta Memoria anual teniendo en cuenta los objetivos e iniciativas recogidas en este Plan Estratégico.



Actuación 3.2.7. Encuestas.

Se promoverá la realización de encuestas con otras entidades para conocer cuál es la percepción que tienen actualmente los ciudadanos españoles en materia de privacidad y protección de datos.

Asimismo, para disponer de información permanente, se promoverán desde la [página web de la Agencia](#) encuestas dirigidas a ciudadanos, responsables y profesionales de la privacidad sobre aquellos ámbitos o temas que se consideren de interés.

PROGRAMA 3.3. Página web

La Agencia impulsará la revisión de su web para reforzar su información y la consulta de sus contenidos por parte de los usuarios de la misma.

Actuación 3.3.1. Actualización de la web. Nuevos contenidos.

Se promoverá la revisión de la estructura de la web para incorporar nuevas herramientas de información y de consulta (microsites sectoriales por temas de interés, fichas prácticas, etc.), y todo ello de una forma comprensible y accesible, en especial para las personas con discapacidad.

Se elaborará un tesoro de protección de datos para facilitar la búsqueda por los ciudadanos y responsables de la información disponible en la web de la Agencia.

Actuación 3.3.2. Canal de transparencia de la Agencia.

Se reforzará el Canal de transparencia mediante la actualización de la información publicada en el mismo, la publicación de los informes preceptivos y las sentencias, la accesibilidad al mismo a través del Portal de Transparencia de la AGE, y la difusión de los criterios establecidos de forma conjunta entre el Consejo de Transparencia y Buen Gobierno y la AEPD en aplicación de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

PROGRAMA 3.4. Divulgación

Impulso de iniciativas de divulgación de las actividades de la Agencia dirigidas a ciudadanos, empresas y profesionales.

Actuación 3.4.1. Sesión abierta anual.



Celebración de la Sesión anual Abierta de la Agencia dirigida a ciudadanos, empresas y profesionales de la privacidad. Esta iniciativa, que ha celebrado en 2015 su séptima edición, tiene como objetivo servir como punto de encuentro entre la Agencia y múltiples sectores empresariales y sociales para dar respuesta a sus inquietudes.

Actuación 3.4.2. Jornada del Día Europeo de la Protección de Datos.

Celebración de una Jornada anual conmemorativa del Día Europeo de la Protección de Datos, una efeméride que tiene lugar el 28 de enero.

Actuación 3.4.3. Jornadas sectoriales.

Se pretende intensificar las actividades de divulgación de la Agencia con jornadas conmemorativas o sectoriales dedicadas a temas de actualidad, a colectivos que demandan información de la Agencia de forma especializada -delegados de protección de datos, profesionales de la privacidad...- o de aquellos a los que es la Agencia la que requiere información -educadores, prestadores de servicios...-. Los formatos de estas sesiones variarán en función de la temática y de los colectivos y sectores afectados. Se promoverá la opción de retransmitirlas en formato abierto atendiendo a las circunstancias particulares de cada evento.

Se promoverá una Jornada para responsables de protección de datos de Comunidades Autónomas y de Entidades Locales.



EJE ESTRATÉGICO 4.

Una Agencia cercana a los responsables y a los profesionales de la privacidad

<u>Eje estratégico 1</u> Prevención para una protección más eficaz	<u>Eje estratégico 2</u> Innovación y protección de datos: factor de confianza y garantía de calidad	<u>Eje estratégico 3</u> Un Agencia colaboradora, transparente y participativa	<u>Eje estratégico 4</u> Una Agencia cercana a los responsables y a los profesionales de la privacidad	<u>Eje estratégico 5</u> Una Agencia más ágil y eficiente
			<ul style="list-style-type: none"> - Relación con los responsables - Pymes - Profesionales de la privacidad, profesionales TIC y delegados de protección de datos 	

PROGRAMA 4.1. Relación con los responsables

La normativa de protección de datos impone a los responsables de su tratamiento una serie de obligaciones que deben observar para respetar los derechos de los ciudadanos, lo que constituye una de las garantías establecidas en el sistema. El cumplimiento de estas obligaciones, por sus características, genera dudas en ocasiones en los responsables. La Agencia debe contribuir a resolverlas, de manera que las garantías que representan sean realmente efectivas para los ciudadanos. En este sentido, uno de los indicadores utilizados habitualmente para evaluar el nivel de conocimiento de la LOPD ha sido la inscripción de ficheros en el Registro General de Protección de Datos (RGPD). La Agencia no desconoce que, dependiendo de la forma jurídica de la empresa, el porcentaje de cumplimiento con el RGPD varía enormemente y, por ello, centrará buena parte de las medidas recogidas en este programa en la divulgación de la protección de datos entre las pequeñas y medianas empresas.

El objetivo de este programa es el impulso de iniciativas dirigidas, por una parte, a atender las cuestiones planteadas por los responsables del tratamiento en materias relacionadas con la inscripción, modificación o supresión de ficheros, tratamientos de datos como cesiones, transferencias internacionales, la conservación por razones históricas, estadísticas o científicas, así como sobre códigos tipo o códigos de conducta y su seguimiento. Y, por otra, para que los responsables del tratamiento y los profesionales del sector puedan



trasladar a la Agencia aquellas cuestiones que de manera general se vayan suscitando en la aplicación de la normativa.

Actuación 4.1.1. Unidad de atención a los responsables.

Con el fin de mantener una relación ágil y fluida con los responsables y encargados del tratamiento, y poder canalizar de forma eficiente las consultas que puedan plantear acerca del cumplimiento de sus obligaciones en materia de protección de datos, tanto en el marco normativo actual como en el que se desarrolle a partir de la entrada en vigor del Reglamento europeo, la Agencia pondrá en marcha una unidad de atención a los responsables, de forma que sea posible atender y asistir, mediante correo electrónico y por teléfono, a los responsables y encargados del tratamiento en aquellas cuestiones que planteen.

Se promoverá una sistematización del conjunto de informes y resoluciones de la AEPD que facilite su público conocimiento y utilización.

Actuación 4.1.2. Edición y difusión de materiales y herramientas prácticas.

Elaboración de guías, fichas, recomendaciones, herramientas y otros materiales prácticos sobre cumplimiento de las obligaciones de los responsables en materia de:

- Elaboración de políticas de privacidad y aviso legal.
- Elaboración de cláusulas informativas y de consentimiento.
- Elaboración del documento de seguridad.
- Medidas de seguridad.
- Transferencias internacionales.
- Códigos tipo.
- Conservación de datos para fines históricos, estadísticos y científicos.

Se elaborará una Guía para el responsable y se actualizará la Guía sobre protección de datos personales en el ámbito de las relaciones laborales.

PROGRAMA 4.2. PYMES

Este programa pretende desarrollar distintas iniciativas de apoyo a las pymes y micropymes en las que el tratamiento de datos no constituye una ocupación esencial de su actividad. Es necesario subrayar que este segmento empresarial tiene una particular importancia por su volumen de tratamiento de datos y por su contribución a la generación de empleo, ocupando cerca del 63% del total de trabajadores, según datos del Ministerio de Empleo y Seguridad Social.

Actuación 4.2.1. Canal específico para atención personalizada.



El tejido económico español está formado fundamentalmente por pymes y micropymes en las que el cumplimiento de las obligaciones que impone la legislación aplicable puede presentar especiales dificultades. El 99,88% del tejido empresarial español está constituido por pymes y micropymes y la persona física (autónomo) es la forma predominante en la constitución de una empresa seguida de la sociedad limitada, según datos recogidos en el 'Retrato de las pymes 2014' del Ministerio de Industria, Energía y Turismo. Para estos colectivos se hace preciso establecer un canal de atención personalizada que les ayude a cumplir con las obligaciones que impone la LOPD y, para ello, se promoverá la puesta en marcha de mecanismos de información específica online y telefónica.

Actuación 4.2.2. Herramientas para facilitar el cumplimiento de la LOPD.

La Agencia ofrece distintas herramientas para facilitar el cumplimiento de la normativa de protección de datos a través de su web. Sería preciso conocer la valoración que hacen de las mismas las organizaciones representativas de las pymes y obtener información tanto sobre posibles mejoras para su actualización como sobre la creación de nuevas herramientas. Este contacto se articulará a través de las asociaciones más representativas de las pymes y de las empresas digitales.

En especial se promoverá el diseño y elaboración de una herramienta que permita a las empresas de menos de 50 empleados conocer qué obligaciones tienen que cumplir atendiendo a sus especiales características.

Actuación 4.2.3. Sesión abierta para pymes.

Celebración de una Jornada dedicada a aquellas cuestiones de su interés relacionadas con la privacidad.

Actuación 4.2.4. Fraccionamiento del pago de sanciones.

Se favorecerá el fraccionamiento del pago de las sanciones para las pequeñas y medianas empresas.

Actuación 4.2.5. Formación para emprendedores.

Se impulsarán acciones de formación de emprendedores en colaboración con las asociaciones más representativas.



PROGRAMA 4.3. Profesionales de la privacidad, profesionales TIC y delegados de protección de datos

El rol del delegado de protección de datos no se encuentra recogido en la actual normativa española, si bien es una figura ampliamente desarrollada en otros Estados miembros. A falta de saber los requisitos concretos que se establecerán al respecto en el futuro Reglamento europeo, y teniendo en cuenta que la notificación de los ficheros a la Agencia para su inscripción en el Registro General de Protección de Datos dejará de ser una obligación, la figura del delegado de protección de datos contará con un papel destacado a la hora de atender los derechos de los ciudadanos dentro de las entidades responsables.

Por ello, la Agencia quiere prestar una especial atención a esta figura con el fin de que pueda disponer de toda la información necesaria para desarrollar su labor, convirtiéndose en un cauce idóneo para la interlocución entre la Agencia y los responsables.

También contribuyen al cumplimiento de las obligaciones de los responsables los profesionales del sector de la privacidad, que desempeñan un relevante papel en la efectiva aplicación de la normativa de protección de datos mediante la labor de asesoramiento que prestan. Por tanto, sería muy útil que, en su contacto con la Agencia, transmitan las preocupaciones o dificultades que encuentren en la aplicación de la legislación. A la vez, la Agencia quiere posibilitar que este colectivo conozca las líneas de actuación de este organismo, lo que redundará en la calidad de su asistencia y consejo y, por tanto, en el mayor y mejor cumplimiento de la legislación por parte de los responsables del tratamiento.

Finalmente, hay que tener en consideración la necesidad de apoyar y formar adecuadamente a los profesionales TIC y, en particular, a los especializados en seguridad. Estos profesionales son los encargados de diseñar, desarrollar y mantener los sistemas de información, productos y servicios que tratan datos personales y, por ello, es de capital importancia concienciarles en la necesidad de implantar los requerimientos de protección de datos en los sistemas que diseñen mediante el impulso de políticas de protección de datos desde el diseño y por defecto, y para que aboguen por la realización de evaluaciones de impacto en la protección de datos en los proyectos que desarrollan.

Actuación 4.3.1. Canal específico para atención personalizada.

Se habilitará un canal para atender las cuestiones planteadas por los delegados de protección de datos y los profesionales de la privacidad, con arreglo a los sectores de actividad que desempeñen.

Actuación 4.3.2. Diseño de formación específica.



Se desarrollarán jornadas de formación sobre temas concretos orientadas a ambos colectivos.

Actuación 4.3.3. Guía para Delegados de Protección de Datos.

Se elaborará una Guía para delegados de protección de datos (DPO) que atienda a las características propias de esta figura.

Actuación 4.3.4. Colaboración con asociaciones de profesionales de protección de datos.

Se promoverá la colaboración con asociaciones de profesionales de la privacidad y de la consultoría, y, en particular, en los ámbitos de la formación y la divulgación. A este fin, se mantendrán reuniones periódicas con dichas asociaciones.

Actuación 4.3.5. Colaboración con asociaciones profesionales y colegios TIC.

Se promoverá, a través de las organizaciones representativas del sector, la formación de los profesionales TIC en los estándares de protección de datos y su concienciación como actores clave en el éxito de estrategias de protección de datos desde el diseño.

Además, la Agencia desarrollará políticas de colaboración con los profesionales TIC para mejorar su conocimiento de las novedades tecnológicas que se produzcan y su impacto en la protección de datos y, en particular, para promover la mejora de la seguridad de los sistemas de información.



EJE ESTRATÉGICO 5: Una Agencia más ágil y eficiente

<p><u>Eje estratégico 1</u></p> <p>Prevención para una protección más eficaz</p>	<p><u>Eje estratégico 2</u></p> <p>Innovación y protección de datos: factor de confianza y garantía de calidad</p>	<p><u>Eje estratégico 3</u></p> <p>Un Agencia colaboradora, transparente y participativa</p>	<p><u>Eje estratégico 4</u></p> <p>Una Agencia cercana a los responsables y a los profesionales de la privacidad</p>	<p><u>Eje estratégico 5</u></p> <p>Una Agencia más ágil y eficiente</p> <ul style="list-style-type: none"> - Respuesta a los retos internacionales - Simplificación y mejora de la gestión - AEPD digital - Estatuto y competencias de la AEPD

PROGRAMA 5.1. Respuesta a los retos internacionales

Los efectos de la globalización y del desarrollo de las tecnologías de la información y la comunicación sobre los tratamientos de información personal han impulsado una cada vez más intensa cooperación internacional. Es necesario buscar soluciones comunes a los retos de unos servicios universales, establecer mecanismos que faciliten los flujos internacionales de datos al tiempo que se salvaguarda el derecho a la protección de datos, y desarrollar herramientas que permitan hacer frente a vulneraciones de las legislaciones de protección de datos de carácter transfronterizo. La AEPD debe estar presente en estos procesos para poder contribuir eficazmente a la preparación y adopción de las decisiones que puedan posteriormente tener repercusiones en el ámbito interno.

Actuación 5.1.1. Estudio de los efectos de la adopción del reglamento europeo.

La inminente aprobación del Reglamento General de Protección de Datos de la UE supondrá modificaciones sustanciales en la legislación y la práctica de protección de datos tanto en los Estados miembros como en el conjunto de la Unión. La AEPD debe abordar el análisis de los contenidos del Reglamento y su impacto en la vigente normativa de protección de datos, comenzando por la LOPD y su Reglamento de desarrollo, con la finalidad de asesorar a las diversas autoridades del Estado y Comunidades Autónomas que



puedan verse afectadas y cooperar con ellas en la identificación de disposiciones que serán desplazadas por el Reglamento, en la identificación y desarrollo de posibles modificaciones o adaptaciones que deban llevar a cabo los Estados miembros, y en la identificación y preparación de las medidas interpretativas, directrices o buenas prácticas que la AEPD debiera aprobar. En esta tarea, la Agencia debe además analizar impactos sectoriales y sobre colectivos de interesados, en colaboración con entidades representativas de sectores empresariales, organizaciones ciudadanas y profesionales de la privacidad.

Asimismo, la AEPD debe evaluar los efectos del Reglamento sobre sus distintas actividades y diseñar y poner en práctica las necesarias adaptaciones estructurales y procedimentales.

Finalmente, la Agencia debe desarrollar las actuaciones necesarias para participar eficazmente en los trabajos orientados a la aplicación del Reglamento a nivel europeo, en particular dentro del Grupo de Autoridades del Artículo 29, cuyo programa de trabajo 2016-2018 está centrado en el proceso de transición al futuro Consejo Europeo de Protección de Datos y en la preparación de las primeras directrices o criterios que el Reglamento atribuye al futuro Consejo.

Actuación 5.1.2. Estudio de los efectos de la adopción de la Directiva europea sobre protección de datos en el ámbito policial y judicial penal.

Se promoverá un estudio en el que se analizarán los contenidos de la Directiva y su impacto en la vigente normativa de protección de datos a los efectos de asesorar y sensibilizar a las autoridades con competencias legislativas sobre las medidas a adoptar, con especial referencia a la posible vigencia de determinadas previsiones de la LOPD.

Actuación 5.1.3. Cooperación con Iberoamérica.

La AEPD, en su condición de Secretaría Permanente de la Red Iberoamericana de Protección de Datos, reforzará la colaboración con las Autoridades nacionales de protección de datos en las actuaciones que se impulsen en el ámbito de dicha Red, así como en la edición de materiales de divulgación y difusión del derecho, entre otras iniciativas.

PROGRAMA 5.2: Simplificación y mejora de la gestión

Impulso de diversas iniciativas para la mejora de la gestión de los procedimientos y de los sistemas de trabajo de la Agencia.

Actuación 5.2.1. Simplificación de los procedimientos.



Se promoverán las acciones necesarias para conseguir una simplificación de los procedimientos de la Agencia, especialmente mediante la reducción de trámites y la digitalización de expedientes. Se promoverá la elaboración de un manual de procedimientos.

Actuación 5.2.2. Reducción de los tiempos de tramitación.

Se adoptarán acciones específicas encaminadas a conseguir una reducción significativa de los tiempos de gestión en los procedimientos relativos a las consultas, los procedimientos de tutela de derechos, los sancionadores y los de recursos, incluyendo una verificación de su cumplimiento mediante auditorías de mejora.

Actuación 5.2.3. Análisis de los recursos personales y materiales, evaluación del desempeño y productividad por objetivos.

Para la mejora y simplificación de los procedimientos y sistemas de trabajo resulta necesario optimizar los recursos disponibles por la Agencia. Sólo así será posible acometer nuevas competencias con los recursos existentes. Para ello, se recabará información de la situación de la plantilla y de sus necesidades, y se adoptará un sistema de evaluación del desempeño y productividad por objetivos que tenga en cuenta la especial dedicación y el cumplimiento horario, el cumplimiento por objetivos y el reconocimiento de esfuerzos especiales.

Se llevarán a cabo acciones de formación específica del personal de la Agencia para su adecuada adaptación a los objetivos y fines recogidos en este Plan Estratégico.

PROGRAMA 5.3. AEPD digital

Este programa desarrollará diversas iniciativas tendentes a completar la digitalización y automatización de los procedimientos y sistemas de gestión de la Agencia.

Actuación 5.3.1. Plan de digitalización.

Se creará un grupo de trabajo que diseñe y ponga en marcha un plan de implantación gradual de procedimientos electrónicos a fin de completar la digitalización de la Agencia. Estos trabajos se desarrollarán en el marco de la colaboración prevista con la Comisión de Estrategia TIC y con otros organismos de la Administración General del Estado que desempeñan funciones en este ámbito.

Actuación 5.3.2. Mejora del sistema de consultas de la Sede electrónica a través de las preguntas frecuentes (FAQs).



Actualmente, se encuentra publicado en la Sede electrónica un catálogo de preguntas frecuentes (FAQs) mediante las que el ciudadano puede encontrar una primera respuesta a sus consultas. Este sistema debe mejorarse, añadiendo, por ejemplo, un sistema automático interactivo de personalización de consultas. Además, se promoverá el diseño de unas FAQs temáticas sobre aquellas materias o sectores de mayor incidencia o interés para la Agencia (educación, salud, fraude, pymes, etc.).

Actuación 5.3.3. Utilización del CL@VE como medio de identificación en la Sede electrónica.

La plataforma común de identificación, autenticación y firma electrónica de las Administraciones Públicas “Cl@ve” permite a los ciudadanos identificarse de la misma forma ante todos los organismos de la Administración, admitiendo certificados electrónicos, claves permanentes y claves temporales para aquellos interesados que acceden esporádicamente a los servicios. La Agencia se incorporará a este sistema, que gestiona de forma centralizada el Ministerio de Hacienda y Administraciones Públicas, simplificando así la relación con los ciudadanos.

En estos momentos se admiten como formas de identificación el certificado electrónico para realizar el trámite completo en formato digital y la preinscripción, que recibe los datos pero no inicia el trámite hasta que no se recibe la confirmación en papel con la firma hológrafa. La Agencia prevé aumentar los medios de identificación y firma con el sistema “Cl@ve”.

Actuación 5.3.4. Uso del Registro Electrónico como canal de comunicación con la Agencia.

La Sede electrónica de la Agencia contiene un registro electrónico para que ciudadanos y empresas puedan relacionarse con la Agencia en este formato para iniciar ciertos trámites, como la inscripción de un fichero, la presentación de una denuncia o una reclamación. Para la recepción de cualquier otra información existe un registro electrónico genérico donde los interesados pueden aportar documentos en formato libre.

Se impulsará el registro electrónico como canal de presentación de documentos ante la Agencia. Siete de cada 10 empresas utilizan la firma digital en alguna comunicación con agentes externos. De ellas, el 98,9% la emplea para relacionarse con las Administraciones Públicas, según datos del INE.

Actuación 5.3.5. Integración en el Sistema de Interconexión de Registros (SIR).

Se procederá a la integración del registro de entrada/salida de documentos de la Agencia en el Sistema de Interconexión de Registros de las Administraciones Públicas (SIR).



Actuación 5.3.6. Generalización de la firma electrónica en todos los documentos -internos y externos- de la Agencia.

La firma electrónica con el certificado de la Sede permite firmar documentos de forma automática. Ya se está utilizando para la notificación de las inadmisiones a trámite y se va a ampliar al resto de las resoluciones, salvo en el caso de los procedimientos sancionadores. Se estudiará en qué otros flujos de información se puede emplear.

Actuación 5.3.7. Extensión de la notificación por comparecencia en Sede electrónica a todos los procedimientos de la AEPD.

Actualmente se utiliza la dirección electrónica habilitada y la notificación por comparecencia para la notificación de las resoluciones del Registro General de Protección de Datos. Una vez que esté disponible CI@ve, se puede ampliar esta forma de notificación a todos los procedimientos que se tramitan o presentan por la Sede electrónica.

Se impulsará la notificación por comparecencia en Sede electrónica a las personas físicas y se establecerá la notificación electrónica obligatoria a las personas jurídicas a las que tenga que dirigirse la Agencia.

Actuación 5.3.8. Proyecto ARCHIVE (Archivo digital)

Se valorará con el Ministerio de Hacienda y Administraciones Públicas la participación de la AEPD en la puesta en marcha del proyecto ARCHIVE (archivo digital).

Actuación 5.3.9. Impulso de la plataforma intermediadora de la AGE.

Se promoverá la utilización de la plataforma de intermediación de la Administración General del Estado (AGE) para facilitar el acceso de los ciudadanos a los servicios que presta la Agencia.

PROGRAMA 5.4. Estatuto y competencias de la AEPD.

El Estatuto de la AEPD se aprobó hace más de veinte años, cuando la sociedad de la información se encontraba en un incipiente grado de desarrollo. Ello por sí solo justificaría la aprobación de un nuevo Estatuto. Pero a esta situación se añade la inminente aprobación del Reglamento europeo de protección de datos, que introduce importantes novedades en el régimen de obligaciones de los sujetos regulados por esa norma y, lo que es más importante, de las competencias que habrán de asumir las Autoridades de protección de datos. Así, desaparecen algunas de las obligaciones hasta ahora recogidas en la normativa de la Unión, tales como la de registro de los ficheros, mientras que surgen otras nuevas como, entre otras, las de control previo de determinados tratamientos, la posibilidad de



certificaciones en materia de protección de datos, o un desarrollo de la necesaria coordinación internacional entre autoridades de control a través del denominado “procedimiento de coherencia” y las importantes competencias otorgadas al Consejo Europeo de Protección de Datos, del que formaría parte la Agencia como Autoridad de control española.

Actuación 5.4.1. Revisión del Estatuto orgánico de la Agencia.

Promover la modificación del Estatuto orgánico de la Agencia de 1993 a efectos de posibilitar la adaptación de su estructura y funcionamiento al grado de desarrollo alcanzado por la Agencia y al nuevo marco normativo establecido por el próximo Reglamento europeo de protección de datos.



7. SEGUIMIENTO Y EVALUACIÓN

Para el seguimiento del Plan Estratégico de la Agencia Española de Protección de Datos se prevé un mecanismo de seguimiento continuo.

La coordinación del seguimiento y evaluación del Plan y de las respectivas iniciativas puestas en marcha corresponde a la Unidad de Apoyo de la Agencia, bajo la directa supervisión y control de su Directora. Los responsables de los respectivos programas reportarán trimestralmente a la Unidad de Apoyo la información correspondiente a las distintas iniciativas y acciones promovidas durante ese período en cumplimiento del Plan Estratégico.

La Unidad de Apoyo adoptará las herramientas necesarias para que esta información se recabe de la forma más adecuada posible y con la menor interferencia en la gestión ordinaria de las unidades y servicios de la Agencia.

La Unidad de Apoyo elaborará un informe anual dando cuenta del grado de cumplimiento del Plan Estratégico, las nuevas propuestas al mismo y, en su caso, las eventuales medidas correctoras a adoptar en caso de incumplimiento. Este Plan se configura como un documento vivo, de forma que se puedan incorporar nuevas actuaciones o adaptar las previstas a la vista del diagnóstico realizado y los medios disponibles.

El informe anual de evaluación se remitirá a la Comisión Constitucional del Congreso y se hará público en la [web de la Agencia](#).

Asimismo, en la página web de la Agencia se creará un microsite con toda la información relativa al Plan Estratégico, incorporando un buzón para que los ciudadanos, responsables y profesionales puedan remitir sus opiniones, sugerencias y nuevas propuestas de actuación de la Agencia para su eventual incorporación al mismo. En ese mismo microsite se podrán consultar de forma sistematizada las actuaciones que la Agencia pretende poner en marcha para el cumplimiento del Plan y el cronograma previsto para la ejecución de cada una de ellas.

Este documento supone un paso adelante para trabajar en afianzar un organismo eficaz, participativo y transparente, marcando un compromiso a través de unas líneas de trabajo prioritarias que pretenden establecer la base sobre la que la AEPD quiere construir su actuación durante los próximos cuatro años. Las medidas recogidas en el presente Plan, así como las actuaciones concretas que la Agencia pueda poner en marcha para llevarlas a cabo, son únicamente medios orientados a la consecución de un fin: la protección efectiva del derecho fundamental a la protección de datos.