DATOS PERSONALES EN LA RED

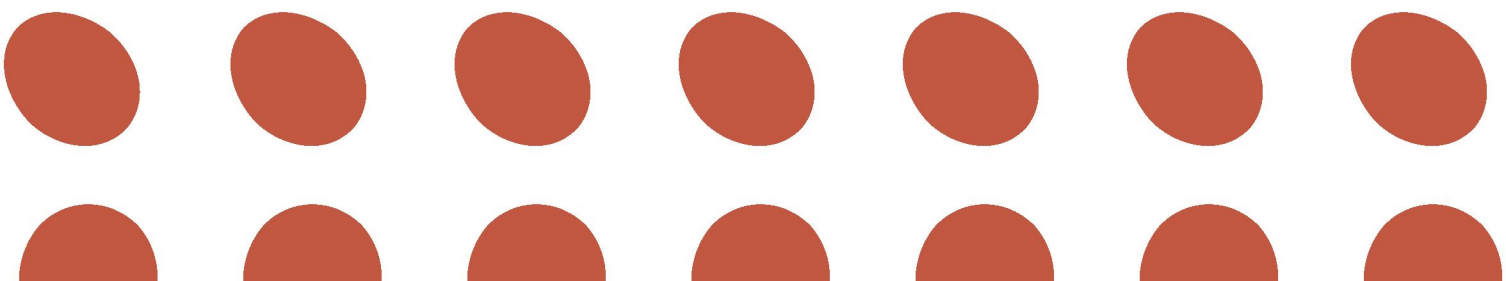
Protección de datos de carácter personal en la Sociedad Digital del Conocimiento

Junta de Castilla y León

ORSI.ES

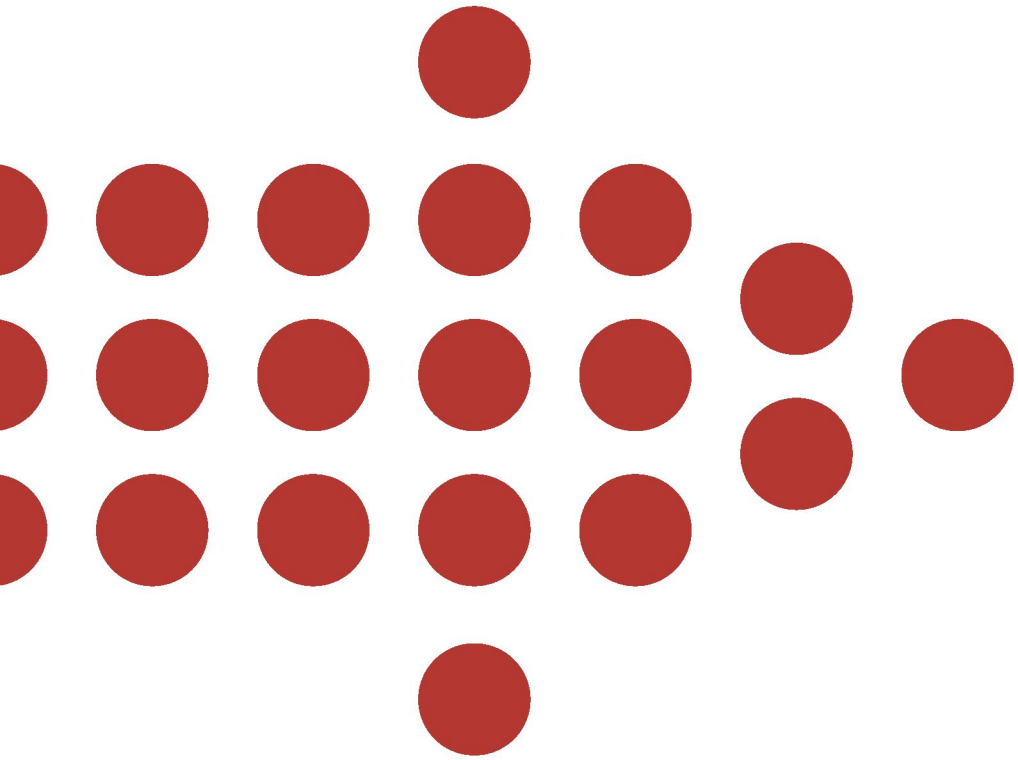
Edita: Consejería de Fomento.
Realiza: Observatorio Regional de la Sociedad de la Información. (ORSI)
Depósito Legal:

ÍNDICE



DATOS PERSONALES EN LA RED

1. INTRODUCCIÓN



1. INTRODUCCIÓN

La **privacidad personal** más honda se materializa en el ámbito íntimo del individuo. Este espacio debe mantenerse reservado y confidencial, fuera del alcance del interés y la curiosidad ajena. De esta manera, una persona mantiene su privacidad en la medida que es capaz de controlar lo que otros pueden saber sobre uno mismo, determinando las reglas de acceso a su espacio privado. La privacidad, según el diccionario de la Real Academia de la Lengua Española, es el ámbito de la vida personal de un individuo que deber ser reservado y mantenerse confidencial. Puede también definirse como el poder para controlar lo que otros pueden saber sobre uno mismo y para determinar las reglas de acceso al espacio privado.

La defensa que la norma fundamental de nuestro Estado de Derecho hace de los valores del honor y la privacidad en el *Título reservado a los derechos fundamentales* se concreta de manera muy específica en el caso del tratamiento automatizado de datos. Y si bien en su momento nuestra **Constitución**[1] fue una de las pioneras en acoger este derecho tan específico, hoy en día se entiende perfectamente el riesgo que para la privacidad personal supone el tratamiento masivo de datos por parte no sólo de las empresas privadas, sino también de las Administraciones Públicas.

La privacidad como valor dentro de los derechos civiles tiene arraigos muy diversos en cada país. De igual forma, la disponibilidad de datos personales no sólo en bases de datos, sino en ficheros en general, es creciente con el nivel de desarrollo de una economía nacional. El **objeto de este estudio** se centra precisamente en eso, en el ámbito de la privacidad que se refiere a los datos personales, en la medida en que los medios de tratamiento actuales suponen una importante innovación en la forma de entender y proteger esta privacidad, a diferencia de la más tradicional privacidad del espacio físico del entorno personal y el hogar.

Es evidente que el desarrollo de las **Tecnologías de la Información y las Comunicaciones** supone una **ventaja** ineludible, pero no hay que olvidar que también pueden convertirse en una amenaza para la privacidad en la medida en que pueden facilitar la explotación de datos personales de manera indiscriminada. Pero además de aumentar las capacidades de manejo de datos, el mundo digital conlleva todo un **nuevo reto a la gestión de la privacidad** dado que, a diferencia del papel y la palabra, las acciones son totalmente invisibles y el nivel de conciencia que el afectado tiene de la invasión de su privacidad es muy bajo o nulo. Bien es cierto que de igual manera la tecnología puede también ayudar a que este nivel de conciencia sobre la privacidad propia, así como su protección, se vea mejorado.

La preocupación por la privacidad en la Sociedad Digital del Conocimiento ha llevado a un desarrollo normativo intenso en los últimos quince años, con el establecimiento en todos los países europeos de autoridades específicas que tutelan el respeto a este derecho fundamental.

1 "Constitución Española." Ed. Boletin Oficial del Estado, 1978.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal[2] (en adelante LOPD) y el **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD[3], obligan a las empresas y Administraciones Públicas a implantar determinadas medidas técnicas y organizativas en sus Sistemas de Información. En función del tipo de datos que manejen, éstas serán más o menos restrictivas. Según la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), la innovación más importante viene de la mano de la extensión y generalización de las medidas de seguridad a los ficheros no informatizados o manuales, así como del establecimiento de nuevas reglas procedimentales para la garantía efectiva del derecho a la protección de datos[4].

Bajo la iniciativa de **apoyo al cumplimiento de normas y estándares** en el entorno empresarial digital, de la Estrategia Regional para la Sociedad Digital del Conocimiento de Castilla y León (ERSDI) 2007-2013, la Junta de Castilla y León pone de manifiesto su intención de apoyar a las empresas castellanas y leonesas para que puedan cumplir la normativa vigente en cuanto a materias como seguridad y protección de datos de carácter personal se refiere, así como los estándares relativos a la accesibilidad web, el desarrollo del software, etc. Para ello se fomenta el conocimiento de las normativas y estándares aplicables y se facilita la descarga gratuita de herramientas informáticas que permitan hacer un autodiagnóstico de la situación de la empresa en materias como protección de datos, con el fin de realizar las adaptaciones de los ficheros de datos básicos a lo establecido en la LOPD y así garantizar la seguridad de la información gestionada.

Por otro lado, las actuaciones en este ámbito dirigidas a Administraciones Locales de la Comunidad se enmarcan en la iniciativa **Red de Municipios Digitales de Castilla y León**, que promueve un marco general de interoperabilidad que garantice la transparencia de los procedimientos y la comunicación de datos entre los tres niveles de Administración existentes en España.

Es importante elevar el grado de concienciación y sensibilización en materia de seguridad de la información de ciudadanos, empresas y Administraciones. Para ello, la Junta de Castilla y León, bajo la iniciativa de **fomento de la seguridad y del uso digital inteligente** de la ERSDI, impulsa medidas para informar a los usuarios acerca de los abusos, fraudes y delitos que atentan contra su privacidad, dignidad o cualquier otro interés legítimo.

Por todo esto, la privacidad y protección de datos se configuran como elementos clave dentro de la Sociedad de la Información y el Conocimiento a los que es necesario prestar especial atención puesto que la nueva legislación impone obligaciones que deben ser conocidas y respetadas tanto por empresas como por Administraciones Públicas y otorga derechos que deben ser difundidos a todos los usuarios. Este es el principal objetivo del presente estudio.

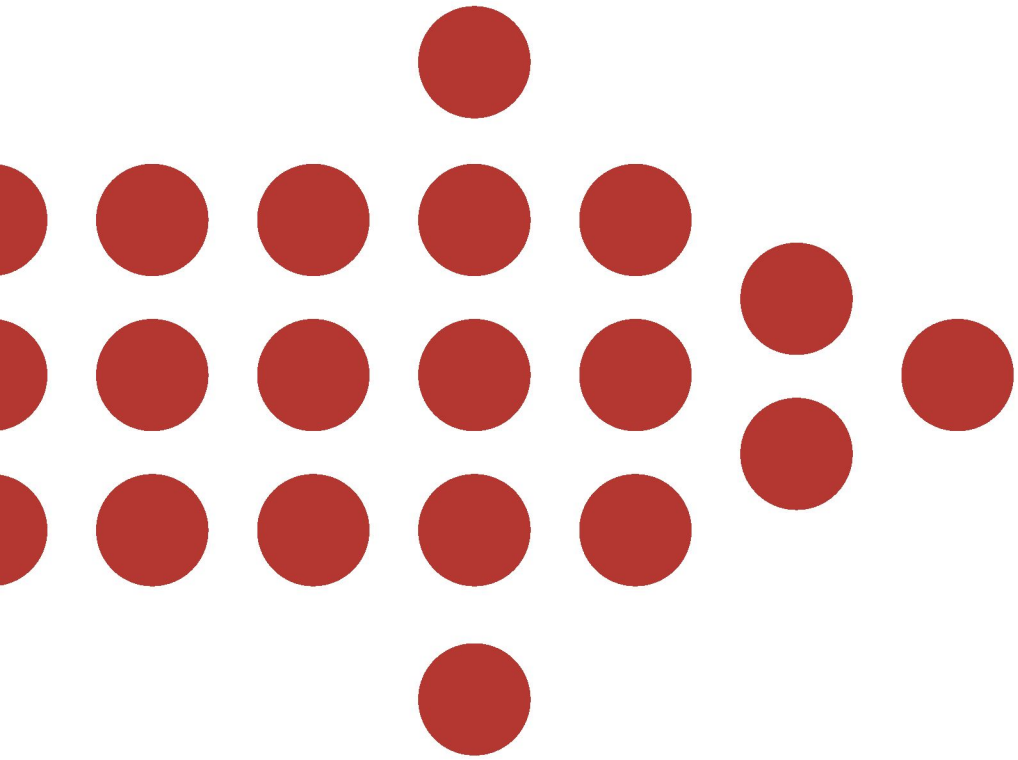
2 Jefatura del Estado. "LEY ORGÁNICA 15/1999, de 13 de diciembre, de protección de datos de carácter personal." 23750. Ed. Ministerio de la Presidencia: Boletín Oficial del Estado, 1999.

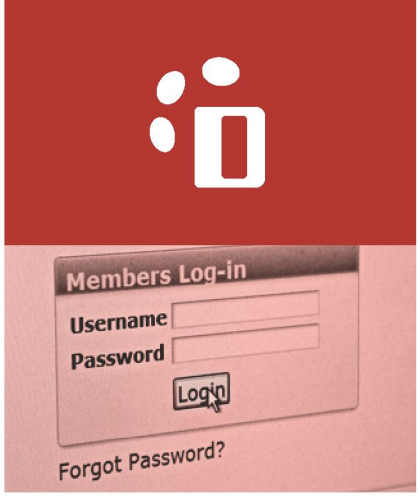
3 Ministerio de Justicia. "REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal." 979. Ed. Ministerio de la Presidencia: Boletín Oficial de Estado, 2007.

4 Entrevista realizada a D. Emilio del Val Puerto, Subdirector General de Inspección y Tutela de Derechos de la APDCM el 31 de marzo de 2008.

DATOS PERSONALES EN LA RED

2. OBJETIVOS Y ALCANCE





2. OBJETIVOS Y ALCANCE

El presente estudio se centra en **analizar la privacidad que se refiere a los datos personales**, en la medida en que los **medios de tratamiento actuales (apoyados en las TIC[5])** suponen una importante innovación en la forma de entender y proteger esta privacidad, a diferencia de la más tradicional privacidad del espacio físico del entorno personal y el hogar.

Teniendo en cuenta el alcance definido para el estudio, los principales objetivos que se pretenden son los siguientes:

- ✓ La seguridad que se debe poder ofrecer al usuario de Internet, como en el caso de la seguridad ciudadana, debe mantener un equilibrio con el respeto a su privacidad y su intimidad, derecho éste fundamental para los seres humanos. Por ello es fundamental comprender el problema de la **privacidad de los datos de carácter personal**. Dicho problema se ha incrementado con la evolución y desarrollo de las TIC.

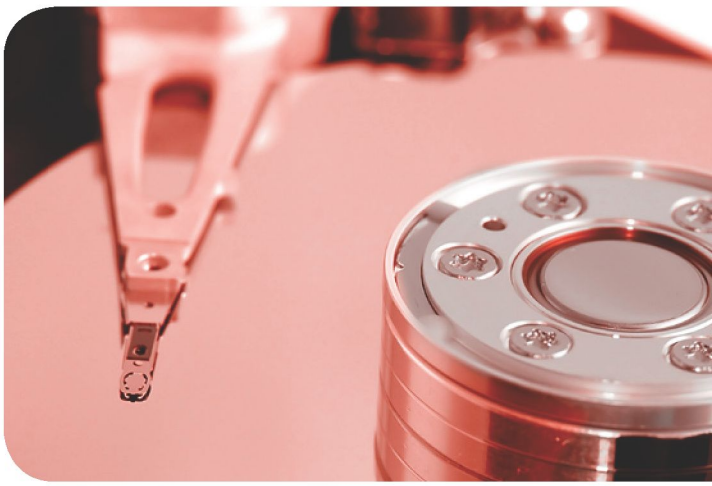
  Presentar la **perspectiva histórica** de la toma de conciencia de la protección de datos como tema merecedor de reflexión y análisis.

- ✓ Analizar el **marco normativo vigente**, así como el estado de la protección de datos de carácter personal en Castilla y León. Los marcos normativos se presentarán en un espectro restrictivo descendente, partiendo de la directiva del Parlamento Europeo y del Consejo para acabar en la aplicación normativa en el ámbito de la comunidad de Castilla y León.

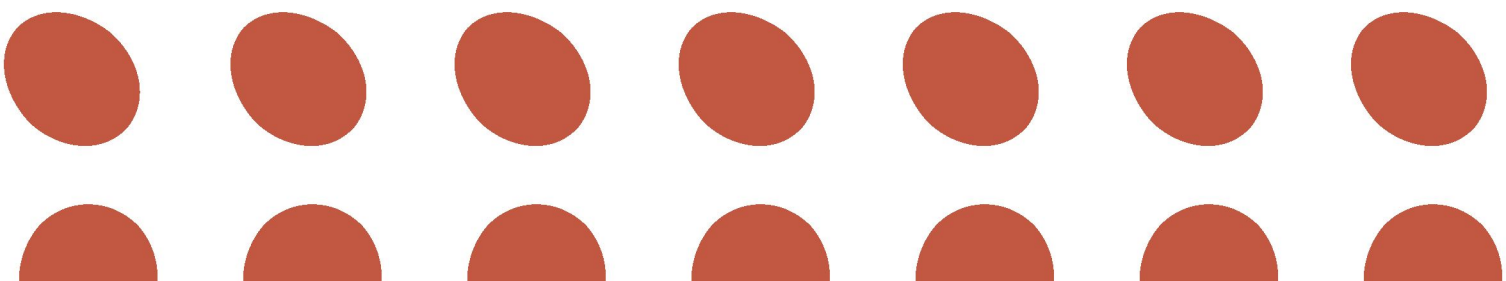
- ✓ Cómo se gestiona de la **protección de datos en las empresas y Administraciones Locales**, así como exposición de los derechos que pueden ejercer los ciudadanos y pautas de ejercicio de dichos derechos.

- ✓ Analizar las **amenazas y fortalezas** que presentan las **TIC** para la confidencialidad de los datos de carácter personal. También se hará referencia al papel que la Ingeniería Social juega como amenaza a la privacidad.

- ✓ Conocer las tecnologías existentes para la **protección de la privacidad**.

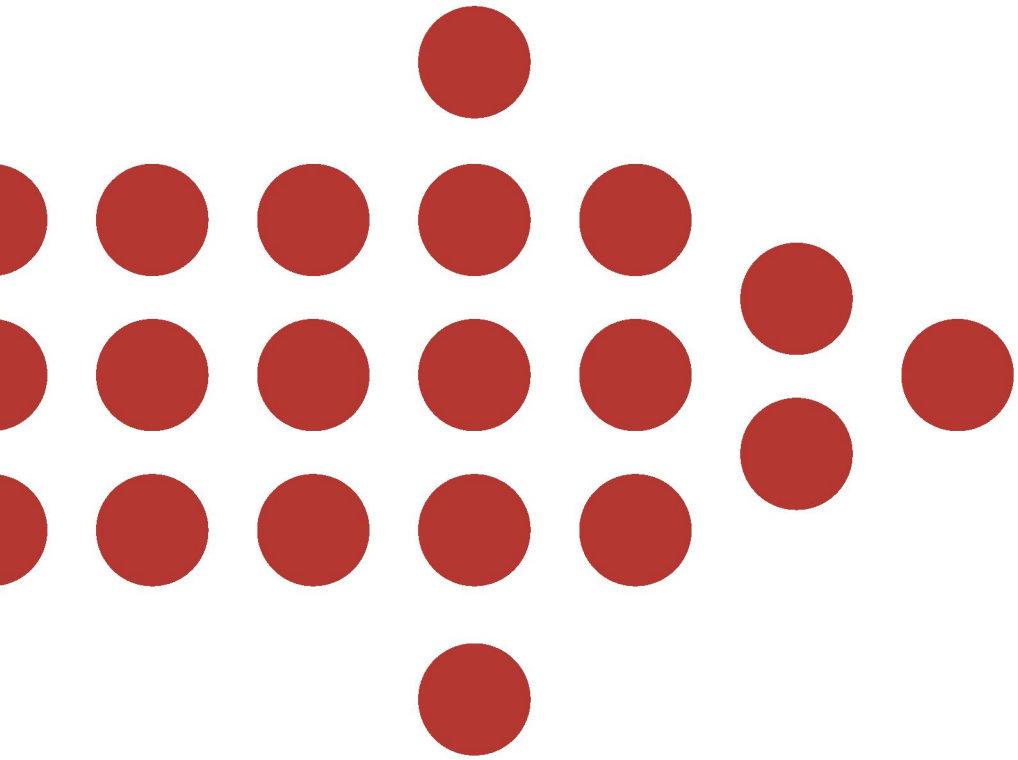


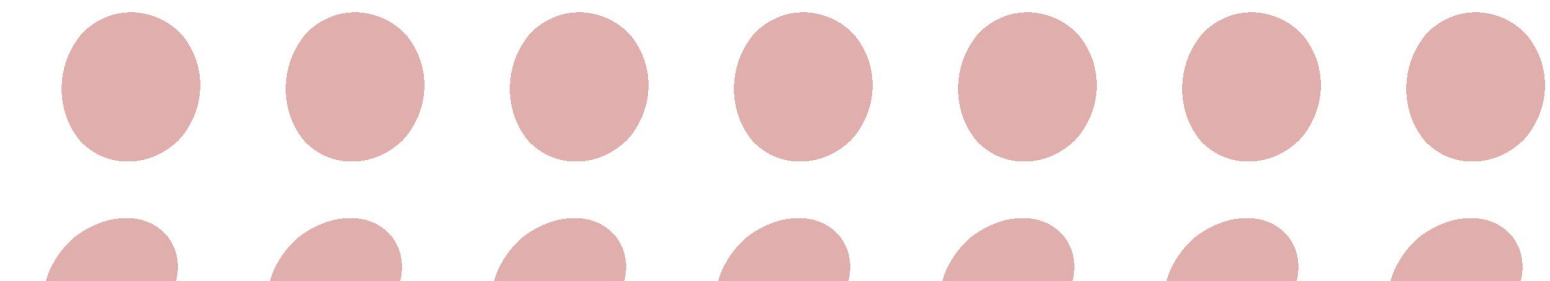
5 Tecnologías de la Información y la Comunicación.



DATOS PERSONALES EN LA RED

3. ANÁLISIS DE LA SITUACIÓN ACTUAL





3. ANÁLISIS DE LA SITUACIÓN ACTUAL

Los nuevos cambios tecnológicos y la digitalización de la información han supuesto un cambio en la forma de tratar los datos de carácter personal. De ahí la necesidad de plantearse nuevas formas de protección de datos para asegurar la privacidad de las personas. No se trata de dejar de lado las mejoras que suponen todos los avances en la vida diaria de las personas, pero hay que poner todos los medios para que los cambios que las Nuevas Tecnologías acarrean, no presenten un perjuicio para los mismos usuarios.

Actualmente, la intimidad y privacidad de las personas se rigen por la LOPD y el Real Decreto 1720/2007 (RLOPD) por el que se aprueba el Reglamento de desarrollo de dicha Ley. Para velar por el cumplimiento de esta Ley y para la protección de la privacidad de todos los españoles se creó la Agencia Española de Protección de Datos[6] (AEPD); en la prensa se puede leer casi a diario sobre las actuaciones de la Agencia: "Protección de Datos multa con 6.000 euros a una empresa madrileña que tiró a la calle cartas con datos personales"[7] o "Protección de Datos recibe las primeras denuncias por inserción de imágenes en Youtube"[8].

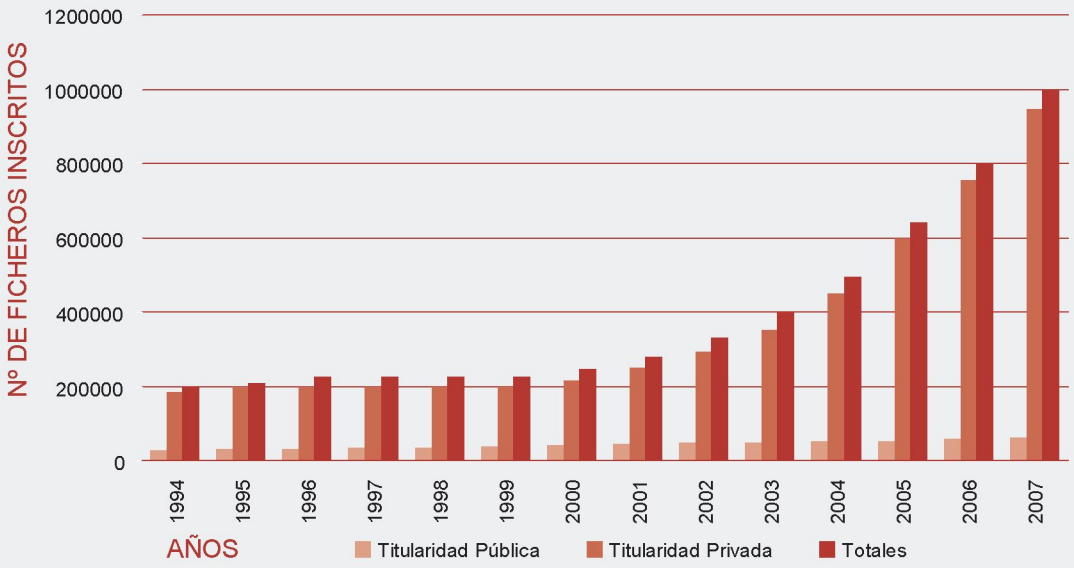


GRÁFICO 1 - EVOLUCIÓN EN LA INSCRIPCIÓN DE FICHEROS EN LA AGENCIA DE PROTECCIÓN DE DATOS
Fuente: Elaboración Propia

6 www.agpd.es.
7 Europa Press. finanzas.com 06/02/2008.
8 El Periódico.com 29/01/2008.

Una de las funciones de la Agencia es la recogida de inscripciones de ficheros de datos personales, para poder cerciorarse así, que se sigue la normativa impuesta. Si nos fijamos en las estadísticas[9], en julio de 2008 se llegó a un total de 70.790 ficheros inscritos por Entidades Públicas y 1.104.382 por el sector privado. El sector de la pequeña y mediana empresa es el que más déficit presenta en cuanto a la inscripción de ficheros de datos personales en el Registro General de Protección de Datos. Por otro lado, los ficheros relacionados con empresas de gestión de personal o que tienen a las personas como centro de su actividad son los que han representado el mayor número de registros (gestión de clientes, contable, fiscal, administrativa y Recursos Humanos) hasta 2007[10].

En cuanto a la inscripción de ficheros correspondientes a las Administraciones Autonómicas, se da una mejora en la cantidad y calidad, sobre todo en las que existe una unidad administrativa que coordina la creación e inscripción de ficheros. La administración de Castilla y León (incluyendo organismos dependientes de la misma) realizó en 2006 la inscripción de 96 ficheros, completando un total de 467[11]. La comunidad de Castilla y León ocupó en 2007 el quinto puesto entre las comunidades en recibir actuaciones previas de investigación, con un 58 de investigaciones iniciadas en 2007. Estos datos suponen una mejoría respecto a las 71 registradas el año anterior del total de España. Sólo un 1,75 % de las actuaciones posteriores a la inspección (procedimientos sancionadores) iniciadas en 2007, fueron efectuadas en Castilla y León. De hecho, los resultados obtenidos en una encuesta CATI[12] realizada a 563 empresas de Castilla y León durante los meses de junio y julio del 2007 muestran como la LOPD es la normativa aplicable a la Sociedad de la Información más conocida, un 72% de las empresas manifestaron conocer la LOPD (ver Gráfico 2).

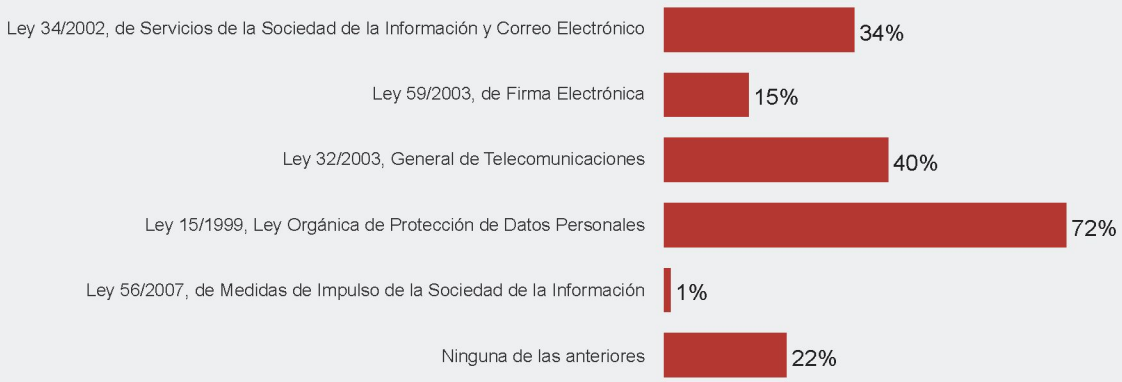


GRÁFICO 2 - GRADO DE CONOCIMIENTO DE LA NORMATIVA RELACIONADA CON LA PROTECCIÓN DE DATOS Y LA SOCIEDAD DE LA INFORMACIÓN
Fuente: Encuesta CATI. ORSI 2007

9 Agencia Española de Protección de Datos. Estadísticas mensuales del Registro General de Protección de Datos (RGPD): AGPD, Julio 2008.

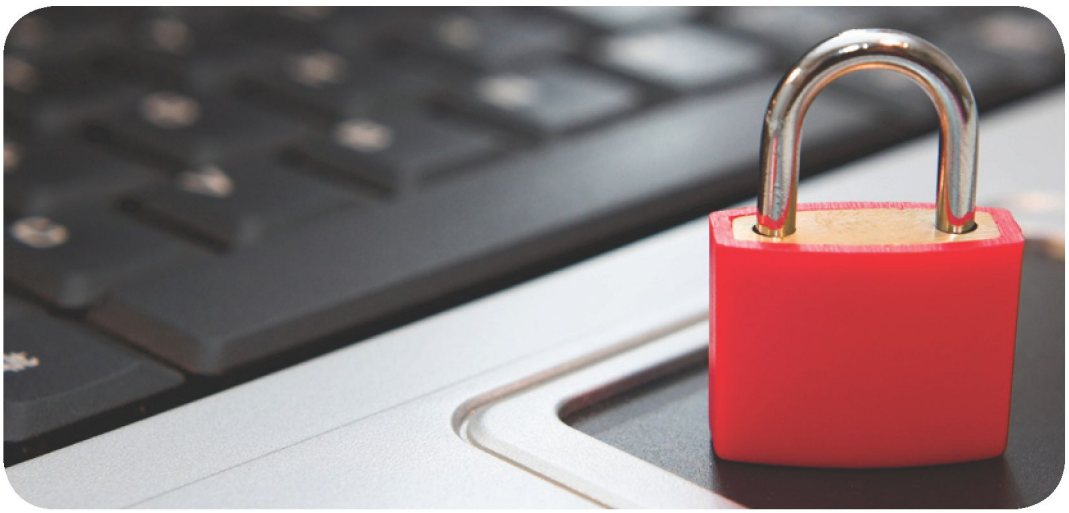
10 Agencia Española de Protección de Datos. Memoria 2007, Publicada en 2008.

11 Agencia Española de Protección de Datos. Memoria 2006, Publicada en 2007.

12 Encuesta telefónica asistida por ordenador llevada a cabo por el Observatorio Regional para la Sociedad de la Información de la Junta de Castilla y León.

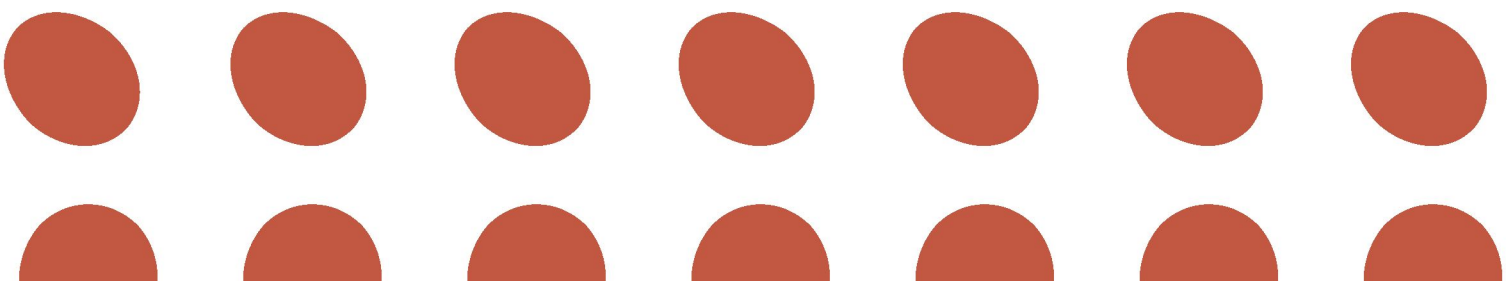
En España, de los tres millones de PYMES españolas, el 80% tienen datos de clientes, proveedores, empleados y contactos. La mayoría afirman conocer la existencia de una normativa, pero pocas la aplican[13]. Según la AEPD, sólo el 12% de las empresas cumple la normativa a rajatabla, aunque afirma que cada vez son más.

Por otro lado, más de un 70% de los ciudadanos se sienten preocupados por la protección de datos y el uso de información personal por otras personas[14], sin embargo este índice disminuye cuando se pregunta si conocen la LOPD, ya que el 57,46% desconoce su existencia. Por ello se puede decir que la situación actual en cuanto a protección de datos está en desarrollo; se está promoviendo y enfatizando la necesidad de una entidad protectora y promotora, que motive un incremento de conciencia respecto a este tema. Queda mucho por hacer, pero las bases se han establecido y se está trabajando para conseguirlo.



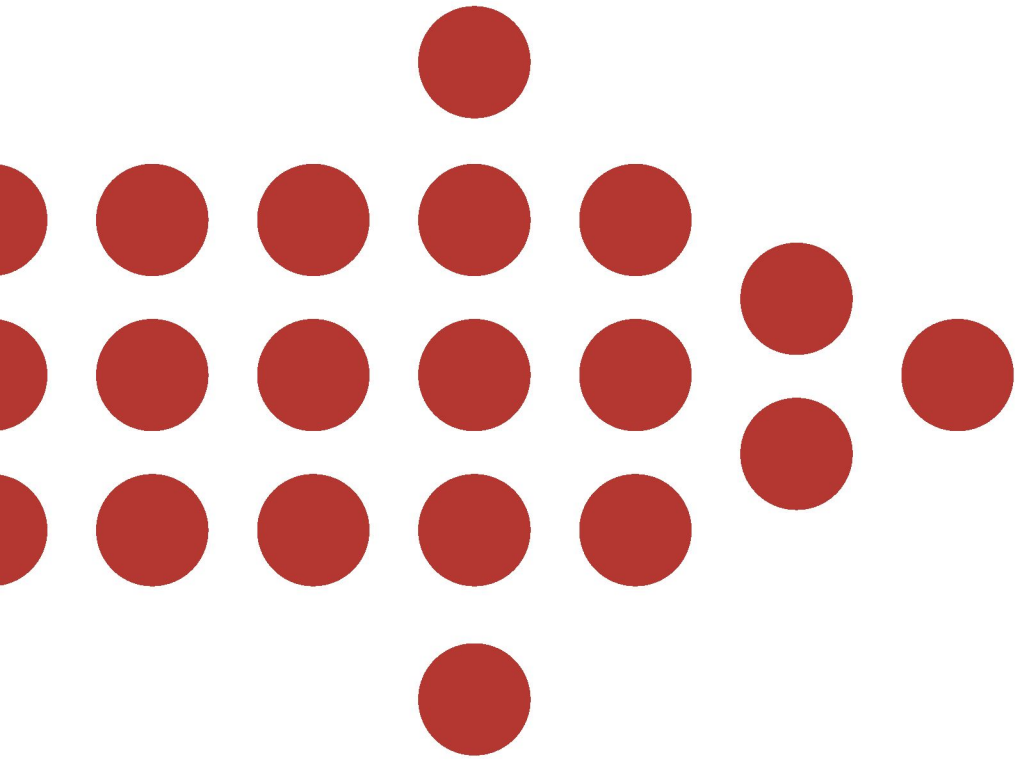
13 MM. La mayoría de las pequeñas y medianas empresas incumplen la ley de protección de datos. elpais.com. 08/5/2008.

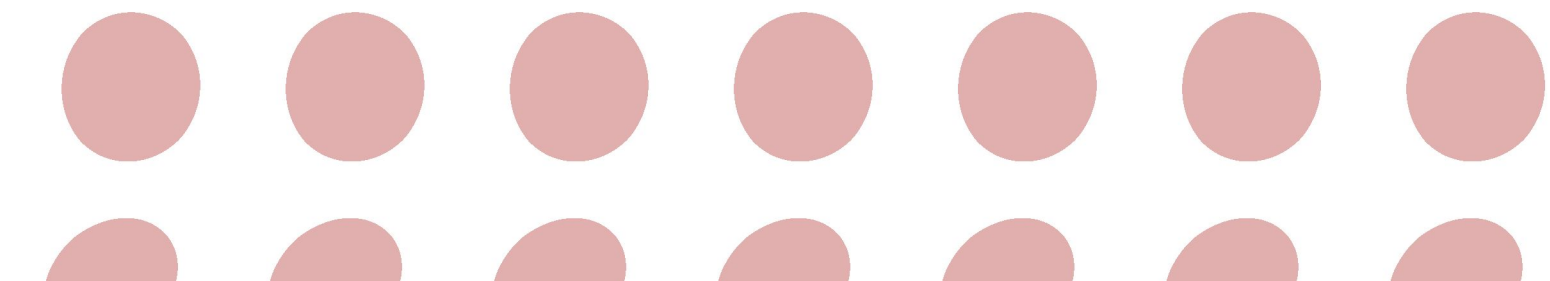
14 AEPD. Encuesta del CIS. Barómetro del Febrero de 2008, 2008.



DATOS PERSONALES EN LA RED

4. PERSPECTIVA HISTÓRICA





4. PERSPECTIVA HISTÓRICA

La Declaración Universal de los Derechos Humanos, ya en 1948, establecía el derecho a la protección de datos y la privacidad. El origen de esta Declaración se sitúa en la Carta de las Naciones Unidas: tratado constitutivo de la Organización de las Naciones Unidas[15], firmado en San Francisco en 1945. Posteriormente y en virtud del artículo 68 de dicha Carta, se creó la Comisión de los Derechos Humanos (1945), que en 2006 pasaría a llamarse el Consejo de los Derechos Humanos. La Declaración Universal de los Derechos Humanos, aunque no es un documento obligatorio o vinculante para los Estados, ha sentado las bases de la posterior legislación.

A partir de aquí, la Convención Europea para la Protección de los Derechos Humanos y Libertades Fundamentales, firmada en Roma el 4 de noviembre de 1950, recoge en su artículo 8 el derecho de toda persona al respeto de su vida privada y familiar, su casa y su correspondencia, sin interferencia del gobierno, con las excepciones de la ley acorde con las necesidades de una sociedad democrática, en pro de la seguridad nacional y bienestar económico del país, la prevención del crimen, la protección de la salud y la moral o la protección de los derechos y libertadas de otras personas. Posteriormente, el **tratado de la Unión Europea (1993)** recogería estos derechos a través del reconocimiento de la mencionada Convención en su artículo F del Título I[16].

De manera más detallada, la **Organización para la Cooperación y el Desarrollo**[17] estableció en 1980 los **principios básicos** sobre los que se debían asentar las políticas de privacidad y que venían a concretar de manera explícita el alcance del derecho a la privacidad. En este sentido los principios fueron:

1. Deben establecerse límites a la recogida de datos personales, los cuales obligan a la obtención por procedimientos justos y, cuando se requiera, con el consentimiento de la persona afectada.

2. Los datos deben ser pertinentes para el objeto que motivó su recogida y, para el mismo, deben ser precisos y mantenerse actualizados.

3. El motivo que justifica la recogida de datos debe especificarse de manera previa y el uso de los datos debe limitarse a dicho motivo.

4. Conforme al principio anterior los datos no deben ser revelados ni empleados para otro propósito con las excepciones autorizadas por la ley o salvo el consentimiento de la persona.

15 ONU: www.un.org.

16 "La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario."

5. Los datos deben protegerse con medidas razonables de seguridad contra los riesgos de pérdida, destrucción y modificación, así como de acceso, uso o revelación no autorizados.

6. Transparencia en el uso de datos personales, a través de medios que permitan conocer la existencia y naturaleza de recopilaciones de datos personales, su propósito y la identidad del responsable de dichos datos.

7. Participación de la persona a través de los derechos de:

   - Conocer la existencia de los datos referentes a ella.
   - Tener acceso en plazo y costes razonables y en formato inteligible a los mismos.
   - Conocer y poder recurrir los casos de denegación de los derechos anteriores, en su caso.
   - Corregir, completar o eliminar los datos que le afectan.

8. El responsable de los datos es el encargado de asegurar los derechos de la persona y los principios anteriores.

En torno a los Principios Básicos establecidos por la Organización para la Cooperación y el Desarrollo se ha desarrollado todo un acervo comunitario en torno a la privacidad de los datos personales y su protección, tanto en términos generales como, en particular, en los medios de comunicación electrónica, así como en los casos de obligación de retención de datos de comunicaciones por parte de los operadores, como se verá más adelante.

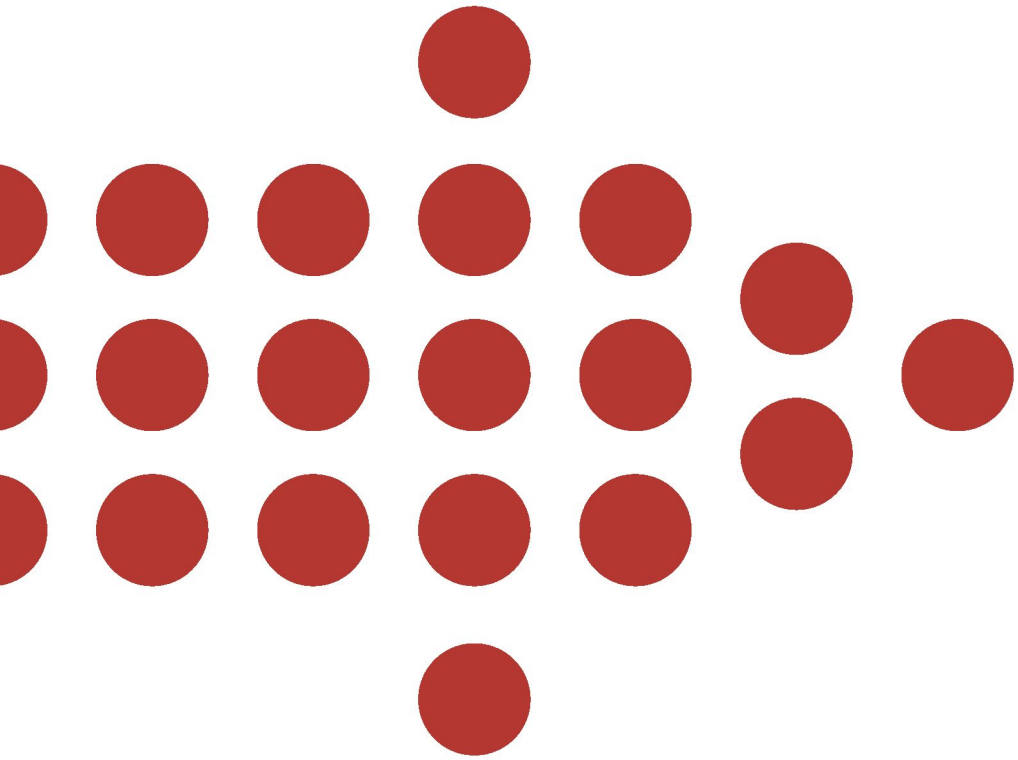
Como primer paso, el 28 de enero de 1981, se firmó en Estrasburgo el **Convenio para la Protección de las Personas con respecto al tratamiento de Datos de Carácter Personal en el marco del Consejo de Europa**. Los países firmantes se comprometían a establecer en su legislación las garantías de los derechos de sus ciudadanos en relación con el tratamiento automatizado de sus datos personales y se mencionó la conveniencia de introducir en el ámbito europeo un nivel uniforme en materia de protección de datos.

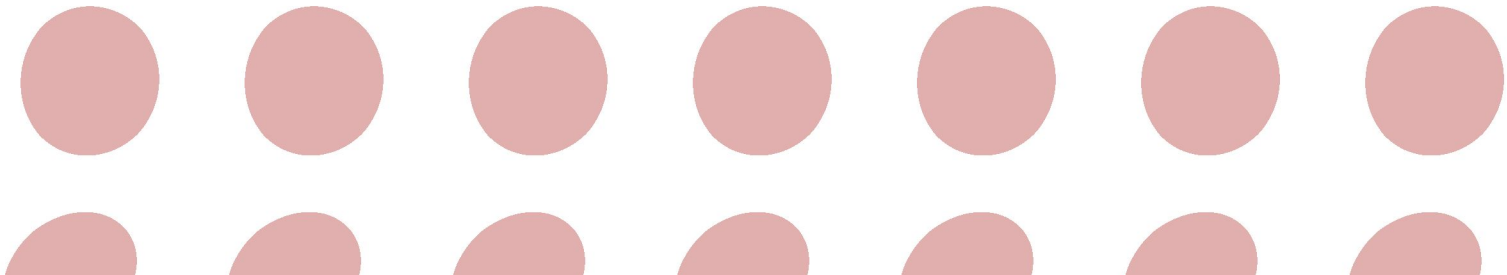
Posteriormente se firma el **Acuerdo de Schengen** el 14 de junio de 1985, referido a la libre circulación de personas en el llamado espacio Schengen. El Acuerdo de Schengen constituye uno de los pasos más importantes en la historia de la construcción de la Unión Europea (UE). El acuerdo tiene como objetivo finalizar con los controles fronterizos dentro del Espacio Schengen y armonizar los controles fronterizos externos. España se incorpora al Acuerdo Schengen en 1991. El Acuerdo de Schengen supuso la creación del **Sistema de Información Schengen**[18] y para poder utilizarlo, los Estados miembros debían garantizar un nivel adecuado de protección de datos personales en su derecho interno. El Convenio de Schengen, firmado el 19 de junio de 1990, completa el Acuerdo y define las condiciones y las garantías de aplicación de esta libre circulación. El Acuerdo y el Convenio, la normativa adoptada sobre la base de ambos textos y los acuerdos conexos conforman el "acervo de Schengen". Desde 1999, el acervo de Schengen está integrado en el marco institucional y jurídico de la Unión Europea.

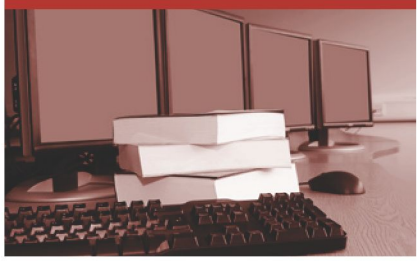
18 Un sistema o base de datos que permite a las autoridades competentes de los Estados miembros *disponer de información* relativa a algunas categorías de personas y objetos.

DATOS PERSONALES EN LA RED

5. ESTADO NORMATIVO







5. ESTADO NORMATIVO

5.1 ESTADO NORMATIVO EUROPEO

Desde que la Convención Europea de Derechos Humanos y Libertades Fundamentales de 1950 recogiera el derecho a la privacidad, el proceso de conformación del marco normativo referente a estos derechos se ha ido construyendo y concretando paulatinamente.

La Directiva 95/46/CE es la referencia normativa de protección de estos derechos. Esta directiva creó el grupo de trabajo formado por las autoridades nacionales de protección de datos, conocido por Grupo de Trabajo del Artículo 29, por ser éste el que declara su creación.

La Directiva 97/66/CE sobre protección de la privacidad y el procesamiento de datos personales en el sector de las telecomunicaciones, concreta de manera específica la Directiva 95/46/CE en su aplicación al sector de las redes y servicios de telecomunicaciones.

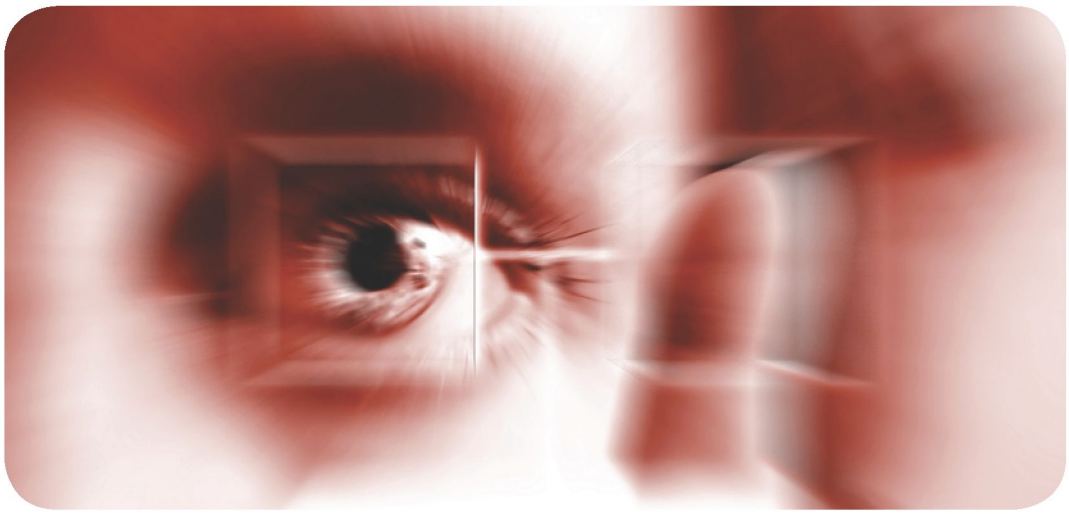
Posteriormente, en 2002, la Directiva 2002/58/CE sobre el procesamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas, generaliza la Directiva 97/66/CE para cualquier red de comunicaciones pública, independientemente de la tecnología que emplee. Además aumenta el alcance de la protección y regulación más allá de la confidencialidad de las comunicaciones, a la información guardada en los terminales, el tráfico generado, la ubicación del usuario, los directorios públicos (listines) y las comunicaciones comerciales no deseadas. La Directiva sobre protección de datos es, por lo tanto, tecnológicamente neutral: se aplicará, con independencia de los medios tecnológicos empleados en el tratamiento de datos personales, siempre que el responsable del tratamiento esté establecido en el territorio de un Estado miembro de la UE o emplee equipos situados en la UE.

El Parlamento Europeo aprobó el 15 de marzo de 2006 la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[19].

Dos Directivas completan el ámbito normativo de las comunicaciones y el comercio on-line: la Directiva 1999/93/CE estableció el marco comunitario para la firma electrónica y la 2000/31/CE el referente al comercio electrónico y los servicios de la Sociedad Digital del Conocimiento.

19 La polémica en este caso no viene exclusivamente por la vía del respeto a la privacidad de las comunicaciones personales sino también por el impacto que el sobrecoste de la captura y almacenamiento de estos datos causará a la industria de telecomunicaciones, que finalmente, acabará pagando el consumidor.

El derecho a la protección de datos es un derecho en constante evolución. Esta normativa provee al ciudadano europeo de elementos para ejercer su derecho a la protección de datos de carácter personal de forma más tácita y efectiva, posicionándolo de tal manera que podrá exigir su cumplimiento con más frecuencia y fuerza ante los responsables de los ficheros o tratamientos que son cualquier organización (empresa, comerciante, profesional liberal, asociación, corporación, fundación...) de carácter público o privado que en el ejercicio de su actividad someta dichos datos a tratamiento informático o manual.



5.2 ESTADO NORMATIVO ESPAÑOL

La Constitución Española (1978) en el Artículo 18.4 dispone que la ley limitará el uso de la informática para garantizar el honor a la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. En desarrollo del citado artículo 18.4, fue aprobada la Ley Orgánica 5/1992 de 29 de octubre de 1992 de regulación del tratamiento automatizado de datos de carácter personal (LORTAD). Esta ley entró en vigor el 31 de enero de 1993 y a partir de la misma se creó la Agencia de Protección de Datos. El Estatuto de la Agencia de Protección de Datos fue aprobado por el Real Decreto 42/93, de 26 de marzo.

Además, la Directiva Europea en materia de protección de datos otorga a las autoridades nacionales de protección de datos personales capacidad para la determinación de los requisitos técnicos precisos, entre ellos, la orientación a los responsables del tratamiento de datos, el examen de los sistemas implantados y la formulación de instrucciones técnicas.

La entrada en vigor de la Directiva 95/46/CE obligó a elaborar la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), derogando la LORTAD. La LOPD garantiza una serie de derechos a las personas físicas, titulares de los datos, tales como el derecho a ser informado de cuándo y por qué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la modificación o supresión de los datos o el derecho de oposición al tratamiento de los mismos.

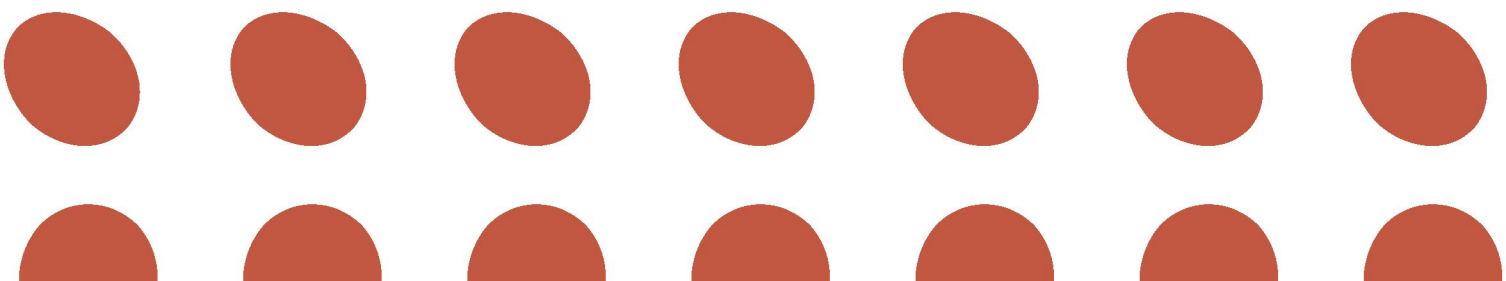
El Real Decreto 1720/2007 aprobado el 21 de diciembre de 2007 por el que se aprueba el Reglamento que desarrolla la LOPD, vigente desde el 19 de abril de 2008, hace especial referencia a la gran importancia de implantar las medidas de seguridad necesarias para garantizar la protección de la privacidad en los datos de carácter personal. De hecho, se incrementan los niveles y medidas de seguridad a implementar sobre los datos de carácter personal. La norma incluye expresamente en su ámbito de aplicación a los ficheros y tratamientos de datos no automatizados (en papel) y fija criterios específicos sobre medidas de seguridad de los mismos. Además, regula todo un procedimiento para garantizar que cualquiera pueda tener pleno conocimiento de la utilización de sus datos, antes de que éstos sean recogidos y tratados. Para garantizar este derecho, se exige de manera expresa al responsable de esos ficheros de datos que conceda al interesado un medio sencillo y gratuito para permitir el derecho de acceso, rectificación, cancelación y oposición.

5.3 ESTADO NORMATIVO EN CASTILLA Y LEÓN

La LOPD establece la posibilidad de que las Comunidades Autónomas creen sus propios organismos de protección de datos para gestionar los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial. Estos organismos tendrán la consideración de autoridades de control, lo que garantiza plena independencia y objetividad en el ejercicio de su cometido.

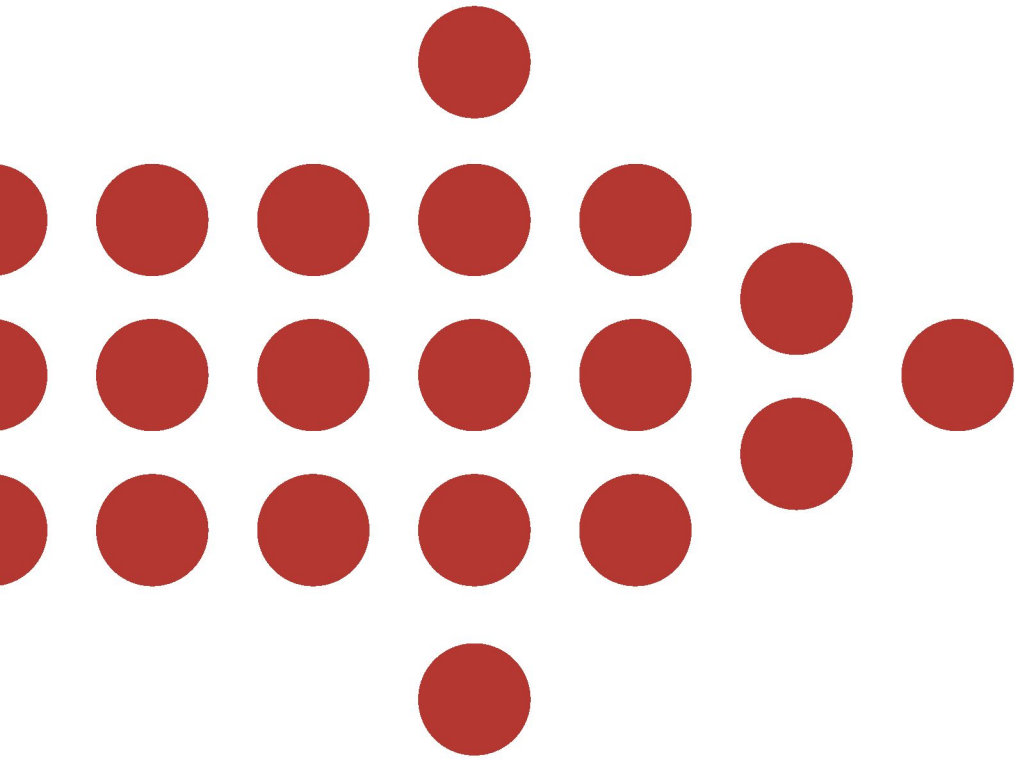
Diversas Comunidades Autónomas han creado sus propias autoridades independientes en la materia. Así lo han hecho la Comunidad de Madrid en el año 2001, la Comunidad de Cataluña en el año 2002 y la Comunidad del País Vasco en el año 2004. Por su parte, la Junta de Castilla y León, en su Estrategia Regional para la Sociedad Digital del Conocimiento 2007-2013, evalúa la posible creación de una Agencia Regional de Protección de Datos en la región para que vele por la protección de los derechos de los ciudadanos consagrados por la normativa de Protección de Datos de Carácter Personal, coordinándose con la Agencia Española de Protección de Datos en las labores de inspección y sanción.

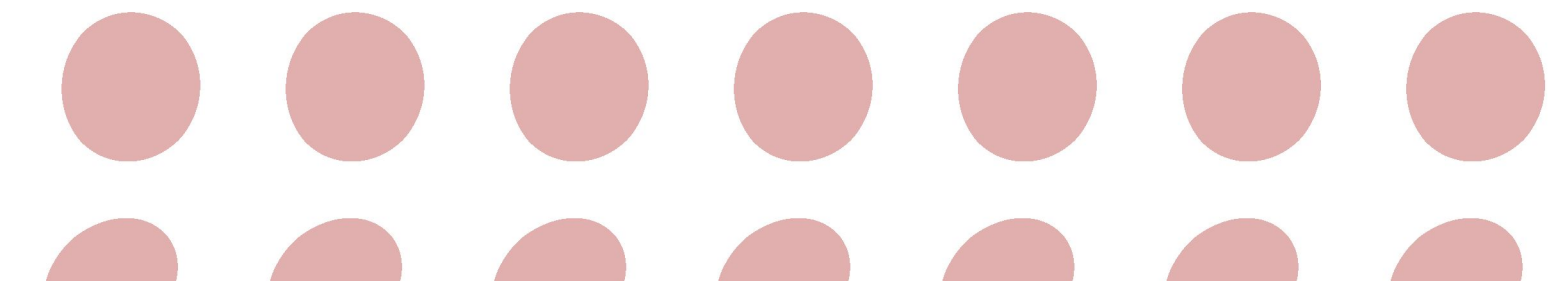
D. Emilio del Val Puerto, Subdirector General de Inspección y Tutela de Derechos de la Agencia de Protección de Datos de la Comunidad de Madrid, considera que las Autoridades de Control autonómicas juegan un papel relevante tanto en gestión de Registro de los Ficheros de Datos de Carácter Personal de titularidad pública de la Comunidad Autónoma correspondiente, como en el desarrollo de trabajos de consultoría y asesoramiento para los responsables de tales ficheros de "titularidad pública".



DATOS PERSONALES EN LA RED

6. APLICACIÓN DE LA LOPD EN PYMES Y ADMINISTRACIONES PÚBLICAS





6. APLICACIÓN DE LA LOPD EN PYMES Y ADMINISTRACIONES PÚBLICAS

La LOPD se presenta como una obligación para las entidades y organismos a la hora de mejorar los procedimientos e implementar la seguridad de la información que manejan. Según la Agencia Española de Protección de Datos (AEPD), el desarrollo de nuevas tecnologías utilizadas en el entorno laboral como la videovigilancia, el uso de datos biométricos, el correo electrónico o el acceso a Internet, entre otros, han intensificado el debate entre los límites y garantías que deben acompañar al ejercicio de aquellas facultades de control.

6.1 RECOMENDACIONES GENERALES PARA EL CUMPLIMIENTO DE LA LOPD

El cumplimiento de la LOPD incide directamente en la imagen de empresas y Entidades Públicas. Por ello, a continuación se incluyen unas recomendaciones generales para cumplir con los requisitos que marca la LOPD:

- Informar a las personas físicas cuando la entidad recoja sus datos y obtener el consentimiento expreso del afectado y por escrito, cuando corresponda (como el caso de los datos sensibles).
- Identificar los ficheros de carácter personal.
- Designar los responsables de la organización en materia de protección de datos de carácter personal.
- Dar de alta los ficheros en el Registro General de Protección de Datos de la AEPD (notificando posteriormente cualquier modificación o cancelación de los datos si fuera pertinente). Las administraciones públicas, además tendrán que publicar la creación, modificación o supresión de sus ficheros de datos en el Boletín Oficial correspondiente.

- Implantar las medidas de seguridad expuestas en el Reglamento de la LOPD (Real Decreto 1720/2007), en los sistemas de información y ficheros que traten datos de carácter personal (automatizados o en formato papel), diferenciando los tres niveles de seguridad dependiendo el tipo de datos (nivel alto, medio y bajo). Ver ANEXO I y ANEXO II para más información.

- Implantar y concienciar a todos los empleados de los procedimientos dirigidos al cumplimiento de la normativa de la empresa.

- Elaborar un Documento de Seguridad, obligatorio por ley, que contenga el ámbito de aplicación de la LOPD, normas, medidas y procedimientos de actuación, las funciones del personal que trata los datos personales y las obligaciones del Responsable de Seguridad. Además tiene que contener la estructura de los ficheros de datos de carácter personal, los procedimientos de notificación y respuesta ante incidencias, así como las medidas técnicas y organizativas para las copias de respaldo y la gestión de soportes.

- Realizar auditorias con una periodicidad bienal para datos de nivel medio o alto.

- Permitir a las personas ejercer los derechos de acceso, rectificación, cancelación y oposición que se extraen de la aplicación de la LOPD, respetando los plazos marcados por la ley.

- Firmar un contrato específico con las empresas a las que sea vaya a ceder los datos personales, siempre y cuando vayan a ser utilizados para el mismo fin con el que fueron recogidos y un contrato de confidencialidad con las empresas que subcontrate y el servicio que presten conlleve tratamiento de datos en nombre del cliente.

- Si se precisa realizar una transferencia de datos a otra empresa fuera de la Unión Europea, es necesario solicitar la autorización de la Agencia Española de Protección de Datos.

Cualquiera que analice la normativa de protección de datos personales comprenderá enseguida que el cumplimiento de la misma es la principal herramienta para la obtención de un grado de seguridad cierto en las empresas y Entidades Públicas, dado que su cumplimiento nos va a llevar a analizar e integrar los Procesos, las Personas y las Medidas Técnicas.

6.2 NOVEDADES DEL REGLAMENTO DE DESARROLLO DE LA LOPD (RD 1720/2007)

La necesidad de aprobar el Reglamento de desarrollo de la LOPD como instrumento dirigido a obtener mayores niveles de seguridad en la aplicación de dicha norma ha culminado con la publicación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

A continuación se mencionan los principales cambios que introduce el Reglamento:

- El reglamento se aplica también a los **ficheros y tratamientos no automatizados (en papel)** y se fijan **criterios específicos** sobre las medidas de seguridad de los mismos. También incluye cambios en las medidas a adoptar en los ficheros automatizados.

- Se garantiza que las personas, antes de consentir que sus datos sean recogidos y tratados, puedan tener **pleno conocimiento de la utilización** que se vaya hacer de estos datos.

- El interesado dispondrá de un **medio sencillo y gratuito para ejercitar su derecho** de acceso, rectificación, cancelación y oposición, sin tener que usar correo certificado ni otros medios que le supongan un gasto adicional.

- Todos los datos derivados de la **violencia de género** pasan a un nivel alto de seguridad.

- Permite que **los ficheros de nóminas sean considerados como Básicos** en lugar de como nivel alto, como sucedía hasta ahora.

- Especificaciones sobre protección de datos de los **menores de edad**.

- Especificaciones sobre la solvencia patrimonial y crédito.

- Especificaciones sobre la Tarjeta Sanitaria.

El Reglamento responde a los siguientes fines: objetivar los criterios en la aplicación de la LOPD, dar respuesta a las inquietudes de la Comisión Europea, incorporar criterios legislativos y completar el desarrollo reglamentario de las novedades introducidas en la LOPD.

6.3 CONSIDERACIONES ESPECIALES PARA LA EMPRESA PRIVADA

Las empresas realizan tratamiento de datos personales en su actividad diaria: gestión de pedidos, datos de contacto de clientes, facturas que se emiten, publicidad directa, nóminas del personal, recepción de currículos por aspirantes a un puesto, etc. Por lo tanto, la normativa aplicable en materia de Protección de Datos de Carácter Personal es aplicable a las PYMES y su infracción puede suponer graves sanciones económicas que van de los 600 a los 600.000 euros.

La inclusión de formularios de contacto (en papel y *on-line*) que no respetan el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los datos de los usuarios registrados, páginas web que no hacen referencia a la política de privacidad o de prestación de servicios de la Sociedad de la Información aplicada por la empresa, la no inscripción de los ficheros de datos de la empresa en el Registro de la AEPD, la inexistencia de Documentos de Seguridad o el incumplimiento de las obligaciones en relación a las cámaras de seguridad, son algunos de los incumplimientos más frecuentes en los que incurren las empresas con respecto a la normativa de Protección de Datos.

Una de las novedades que incorpora el Reglamento de Desarrollo de la LOPD (RD 1720/2007) es que para la implantación de la exigencias en materia de protección de datos, las empresas se podrán centrar en los datos referentes a empleados y clientes particulares, y podrán exceptuar, los datos de profesionales puesto que quedan fuera del ámbito de esta Ley.

Según palabras del propio Director de la Agencia de Protección de Datos, Artemi Rallo Lombarte, en una entrevista para la Cadena Ser, a raíz de la reciente publicación del Reglamento se ha pretendido desarrollar una normativa que permita convivir dos conceptos: por un lado, el derecho a la intimidad y privacidad de las personas y por otro, el desarrollo de la actividad económica.

En esta línea está definido el ámbito de aplicación del RD 1720/2007, en el que se excluyen los tratamientos de datos de personas en ejercicio de una actividad profesional. Desde el 19 de abril de 2008, fecha en la que entró en vigor este Real Decreto, podemos dirigirnos a una persona miembro de una organización, o en ejercicio de una actividad económica, sin necesidad de tener que pedirle consentimiento expreso para el envío de publicidad, o informarle acerca de la organización. Por tanto, podremos hacer envíos comerciales, *mailings, emailings*, dirigidos a profesionales, siempre y cuando la información que remitamos esté dirigida al aprovechamiento por parte la organización.

Algunos de los contenidos de la LOPD y del nuevo Reglamento inciden directamente en el día a día de las empresas. Estos son algunos elementos esenciales a tener en cuenta por las empresas a la hora de cumplir la Ley:

- Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta ley establece para la protección de las personas.

- Toda persona, empresa o entidad privada que proceda a la creación de ficheros de carácter personal, lo notificará previamente a la Agencia de Protección de Datos.
  Las empresas deben comunicar a la AEPD los cambios que se produzcan en la finalidad del fichero, en su responsable y en la dirección de su ubicación.

- El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir a la empresa privada, o entidad que se completen los datos que falten o se proceda a su subsanación. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la AEPD hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

- El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

Aún así, las empresas no deberían descuidar la información que se proporcione a sus clientes en cuanto a los tratamientos que se vayan a realizar, ni tampoco la implantación de una serie de medidas de seguridad que les permita conservar la información tal y como la recaban, impidiendo el acceso por parte de terceros no autorizados, y evitando incidencias en los sistemas de información.

Por ello, todas las empresas deben ser conscientes de las obligaciones en materia de protección de datos y aplicarlas adaptándolas a las particularidades y requerimientos de la actividad que desempeñan.

El nuevo Reglamento propone una herramienta para conseguir éste objetivo de cumplimiento legal, adaptado a las particularidades de la actividad, que son los **Códigos Tipo**[20]. Este instrumento ya estaba recogido en la Ley Orgánica 15/1999, y ahora el RD 1720/2007 lo desarrolla para que las empresas puedan beneficiarse de ello. Los Códigos Tipo pueden ser elaborados bien por una empresa, bien por órganos representativos de empresas o bien por una Administración Pública. Contendrán los procedimientos y requisitos para cumplir con la legislación en materia de protección de datos, adaptados a la actividad correspondiente.

Son la propuesta por parte de la Agencia Española de Protección de Datos, para alcanzar el mayor cumplimiento por parte de las empresas Españolas. La apuesta tanto por parte de asociaciones empresariales, como de Administraciones Públicas, debería ser la de fomentar y promover el mayor número de inscripciones de Códigos Tipo en los próximos años.

20 Ver punto 6.6 del presente estudio.

La Agencia de Inversiones y Servicios de Castilla y León (ADE) puso en marcha un nuevo servicio destinado a ayudar a las PYMES de Castilla y León a asegurar la información que manejan y a adaptarse a la Ley Orgánica de Protección de Datos y la Seguridad de la Información. Actualmente, este servicio de adaptación se ofrece a través de FEPECYL (Federación de Polígonos Empresariales de Castilla y León: www.fepecyl.com) en tres fases:

1. Posibilidad de asistir a talleres formativos en materia de LOPD. En los talleres se explica los riesgos de las PYMES por incumplimiento de la LOPD, actuaciones para la implantación de la Ley y mantenimiento del sistema de protección de datos.

2. Descarga gratuita de la Herramienta "Ayúdate" de adaptación básica a la LOPD[21] que permitirá a las empresas hacer un **autodiagnóstico** de la situación de los ficheros de datos de la empresa para la adaptación de los mismos a la LOPD (Ley Orgánica de Protección de Datos). Para aquellas empresas que manejen ficheros de datos de Nivel Básico (según la Ley), la herramienta además permite **adaptar** los mismos de acuerdo con los procesos de gestión excelentes.

3. Consultoría Individualizada en la que se ofrece una auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) actual, recomendaciones de mejora, formación sobre el SGSI de la empresa y creación del documento de seguridad de la empresa con la consecuente adaptación a las disposiciones de la LOPD.

6.4 CONSIDERACIONES ESPECIALES PARA LAS ADMINISTRACIONES PÚBLICAS

Para las Administraciones Públicas el cumplimiento de la LOPD conlleva generalmente una mejora de la organización de la seguridad, desde la asignación de responsabilidades, hasta la aplicación de las medidas de seguridad a todos los niveles de las personas. Al igual que las empresas, las Administraciones Públicas han de tener en cuenta algunos de los contenidos de la LOPD y del Reglamento que más afectan a su funcionamiento:

- ✓ La creación, modificación y supresión de ficheros de titularidad pública y en la Administración Pública sólo podrá hacerse por medio de una disposición general publicada en el Boletín Oficial de Estado o diario oficial correspondiente. Las disposiciones de creación o de modificación de ficheros en la Administración Pública deberán indicar la siguiente información:

21 http://www.fepecyl.com/ayudate/herramienta.asp.

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y en su caso las transferencias de los datos que se prevean a terceros.
- Los órganos de las Administraciones responsables de los ficheros.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación u oposición.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

✓ La LOPD restringe el tratamiento de datos de carácter personal sin el consentimiento del interesado al ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario. Asimismo, la cesión de datos personales entre Administraciones Públicas sin el consentimiento del interesado, cuando el fin del mismo es histórico, estadístico o científico, cuando hayan sido recogidos por una Administración con destino a otra o cuando la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias, sí podrán llevarse a cabo.

Según los expertos consultados, el problema con el que se encuentran la mayoría de Administraciones Públicas es la falta de una estructura formal de responsabilidades sobre Seguridad de la Información. Las Relaciones de Puestos de Trabajo, más conocidas como RPT, de las Administraciones públicas no prevén la existencia de un Responsable de Seguridad, tal y como define el RD 1720/2007, ni están especificadas sus funciones. Por otra parte, la compleja estructura funcional de estas organizaciones, hace difícil la toma de decisiones que se puedan desplegar a toda la organización. Al igual que ocurría con las empresas privadas, también se propone los Códigos Tipo para las Administraciones Públicas, como instrumento para la **sistematización del cumplimiento de la legislación en materia de protección de datos**. Esta herramienta permite la mejora de los procesos existentes en las Administraciones Públicas, adecuando los procedimientos a la legislación, e incluso definiendo las obligaciones propias en ésta materia.

De esta manera, la idiosincrasia de la legislación vigente en materia de protección de datos hace que adecuar los sistemas de información de las organizaciones pueda parecer complejo. La Ley recoge determinados requerimientos que se prestan a diferentes planteamientos a la hora de implantarlos. Por ello, se hace necesaria la intervención de un ente que

interprete la legislación y determine las diferentes vías aceptadas para la implantación de los requerimientos. En el ámbito estatal, esta función la desempeña la Agencia Española de Protección de Datos, que es quien a través de sus resoluciones, acepta o rechaza determinadas formas de tratamiento de la información. En el ámbito regional, es frecuente que se produzcan vacíos interpretativos, es decir, hay determinadas exigencias legales que afectan a las relaciones con la Administración Pública regional, o en la que intervienen otras legislaciones de ámbito regional, en las que no hay interpretación a la hora de la implantación. La Agencia estatal en este sentido no cubre la necesidad de respuesta que requieren las organizaciones y por tanto se genera un volumen elevado de incumplimientos involuntarios, debidos al desconocimiento.

Como evidencia D. Emilio del Val: "Las agencias autonómicas tienen competencia sobre la disciplina y control de los tratamientos de datos de carácter personal en el ámbito de actuación de las AAPP a las que se dirigen su acción de control, tramitando reclamaciones y denuncias de los ciudadanos para la protección de sus derechos y siendo responsable de la persecución de las infracciones de dichas Administraciones a lo dispuesto en la LOPD".

La **Red de Municipios Digitales de Castilla y León (RMD)** es una iniciativa de la Consejería de Fomento de la Junta de Castilla y León, enmarcada en la **Estrategia Regional para la Sociedad Digital del Conocimiento (ERSDI) 2007-2013**, que pretende ayudar y coordinar a las Entidades Locales en el desarrollo de los Servicios Públicos Digitales en su entorno local.

La Red de Municipios Digitales ha publicado una **Guía de adaptación a la LOPD para Entidades Locales** con el objetivo de proporcionar una metodología de aplicación en ayuntamientos y diputaciones de Castilla y León, así como una serie de recomendaciones a tener en cuenta a la hora de su cumplimiento. Esta guía está disponible a través de su página web, así como también un servicio de información y plantillas tipo para la adecuación de las Entidades Locales de Castilla y León a la LOPD.
Para acceder a toda la información: www.jcyl.es > Sociedad de la Información > Red de Municipios Digitales > Gestión Municipal Interna > Protección de Datos.

Las **plantillas** disponibles son:

- Modelo de Acuerdo de Confidencialidad.
- Modelos Cláusula de Recogida de Datos (con y sin cesión).
- Modelo Contrato de Confidencialidad.
- Modelos de Respuesta al derecho de acceso, cancelación y rectificación.
- Modelos de Ejercicio del derecho de Acceso, Cancelación, Rectificación u Oposición.

6.5 DIFERENCIAS EN LA GESTIÓN DE DATOS DE CARÁCTER PERSONAL PARA EL CUMPLIMIENTO DE LA LOPD EN EMPRESAS Y ENTIDADES PÚBLICAS.

A continuación se presenta un breve resumen de las principales diferencias entre empresas y Entidades Públicas respecto a la implantación de la LOPD.

EMPRESA PRIVADA	EMPRESA PÚBLICA
El responsable del fichero es la sociedad, comunidad de bienes, fundación, etc.	El responsable del fichero es la Entidad Pública, pero más en concreto, la Dirección General o dependencia que en última instancia decide sobre el destino y condiciones del tratamiento de datos.
La declaración de los ficheros se simplifica, salvo en grandes corporaciones, pues las dinámicas de tratamiento de datos son semejantes y todos los ficheros dependen del mismo responsable.	La declaración de ficheros exige además la publicación en diario oficial de los ficheros que se pretende declarar y de sus contenidos. Esta tarea es lenta y produce un estancamiento de los proyectos de las Entidades Pública.
Los ficheros son sólo de titularidad privada, lo que simplifica el proceso.	Pueden disponer de ficheros de naturaleza privada y pública, por lo que hay que hacer un ejercicio de discernimiento de los ficheros según la tipología de su naturaleza.
Declaran sus ficheros ante la AEPD.	Deben declarar sus ficheros ante la APD autonómica y en su defecto ante la nacional.
Las relaciones con terceros se complican (sobre todo en el caso de las multinacionales) por la gran cantidad de relaciones externas y por la existencia habitual de servicios centralizados corporativos en otros países (a veces con nivel de protección no equiparable al español).	La transmisión de datos a nivel internacional es reducida comparada con el ámbito privado.
Disponen de un abanico más amplio de aplicaciones adaptadas a su problemática.	Problemática muy aislada y una oferta comercial de sistemas mucho más restringida y específica.
El Documento de Seguridad depende mucho del desarrollo que haya alcanzando el departamento de Tecnologías de la Información (TI) de la compañía, pues debe armonizar con los procedimientos desarrollados para la producción, desarrollo y continuidad del negocio.	El Documento de Seguridad debe ser debidamente integrado en las políticas existentes en la entidad y son fuertemente influidos por la organización particular de cada administración.
Pueden recibir sanciones económicas de hasta 600.000€.	No reciben sanciones económicas, sino que sus motivaciones son orientadas al mantenimiento de una buena imagen y el peso del costo político.
El grado de complejidad de adaptación es menor.	Las Entidades Públicas se someten a unos procedimientos de adaptación a la LOPD que presentan un grado de complejidad y dedicación superior a las empresas privadas.

6.6 CERTIFICACIONES RELACIONADAS CON LA PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN PERSONAL

Códigos Tipo

Los códigos tipo son documento que recogen los criterios y condiciones que han de permitir la elaboración de unas normas de buenas prácticas, orientadas a garantizar unos estándares de referencia en estricto cumplimento de la ley en el tratamiento de datos de carácter personal.

Dichos códigos hacen alusión a la política concreta de la entidad en cuanto a cómo llevará a cabo lo establecido por la ley, pero con el matiz de establecer en ellos un plus adicional a la hora de instaurar dichas prácticas. Según lo dispuesto en el Artículo 32 de la LOPD:

- ✓ Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

- ✓ Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

- ✓ Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados e inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el Artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas[22].

Proyecto Europrise

Además de los códigos tipo como mecanismo promotor de la adecuación a la LOPD, el proyecto Europrise es un proyecto de validación de mercado cofinanciado por la Comisión Europea a través del programa eTEN[23], que pretende establecer un mecanismo en toda Europa para evaluar la adecuación de los productos y servicios de Tecnologías de la Información a los requisitos que establece la legislación en materia de privacidad y protección de datos.

22 Información disponible en la página web de la Agencia de Protección de Datos: www.agpd.es.

23 Formalmente «TEN-Telecom», abreviatura inglesa de Trans-european Telecomunication Networks.

El establecimiento de este Sello de Privacidad supondrá la existencia de un certificado europeo que promueve la protección del consumidor, los derechos civiles y la aceptación de las normas de privacidad mediante mecanismos transparentes que darán lugar a nuevas posibilidades de introducción de las Tecnologías de Protección de la Privacidad y un incremento en la confianza en las Tecnologías de la Información.

El mecanismo de certificación que propone Europrise se basa en dos niveles: El primer nivel consistiría en el procedimiento de acreditación de expertos que realicen las evaluaciones de productos y servicios. Una vez realizado el informe por dichos expertos, éste es remitido a la autoridad de certificación para su revisión.

En la fecha de publicación de este estudio se está finalizando la fase de acreditación de expertos para el proyecto y a continuación se aprobarán los proyectos que formarán parte de las pruebas piloto, la subsiguiente evaluación de resultados y finalización de estudios referentes al tema.

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El objeto de la LOPD es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente su honor e intimidad personal y familiar, pero las organizaciones suelen debatir entre sólo cumplir con la LOPD o implantar las medidas necesarias para no tener incidentes.

La legislación establece unas medidas de seguridad concretas, pero deja claro que la organización debe hacer lo necesario para proteger los datos personales y los **Sistemas de Gestión de la Seguridad de la Información (SGSI)**.

El Sistema de Gestión de la Seguridad de la Información es el concepto central sobre el que se construye la ISO 27000[24], donde se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de su fecha de elaboración.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- ✓ Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

24 Conjunto de estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

- ✓ Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de la Seguridad de la Información.

Un SGSI contempla los controles necesarios para:

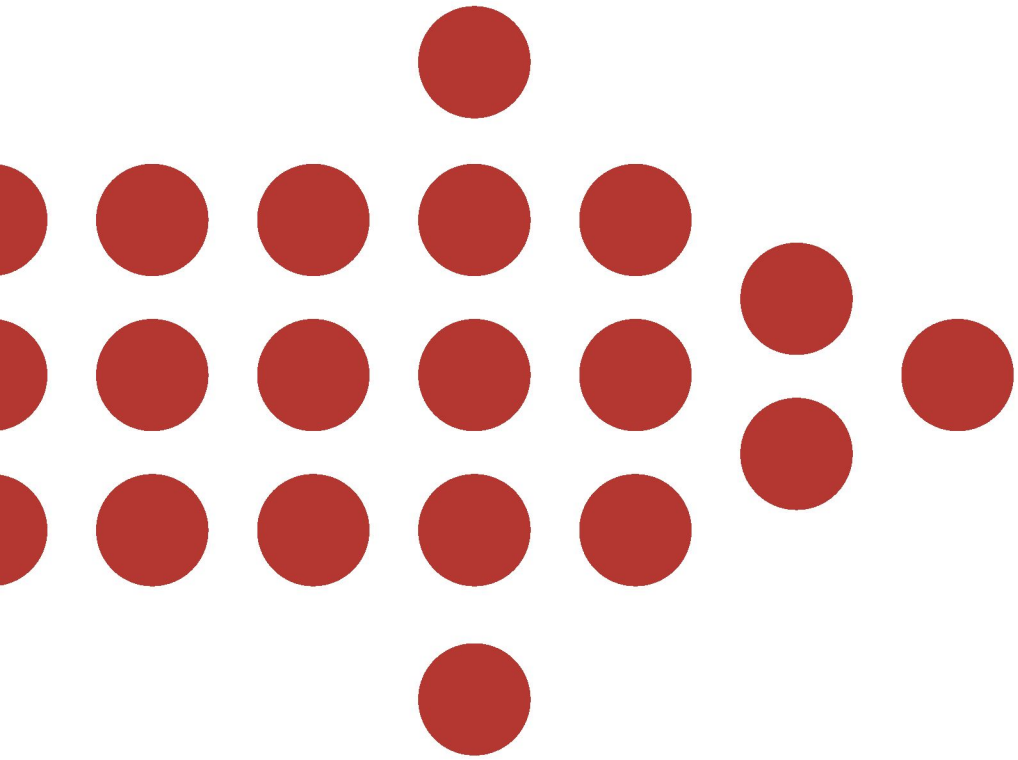
- ✓ Evitar accidentes en la medida de lo posible.
- ✓ Detectarlos rápidamente si se producen.
- ✓ Darles una respuesta rápida, eficaz y ordenada.
- ✓ Adoptar las medidas para que se vuelva a repetir.

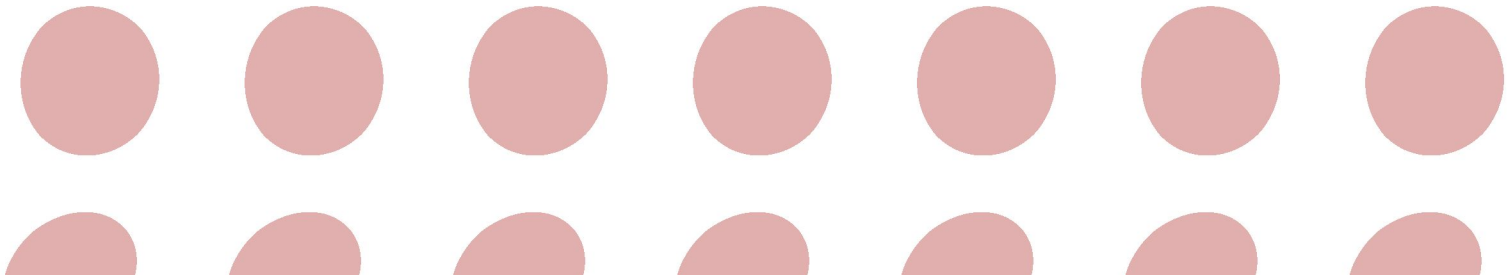
La implantación de un SGSI no implica el cumplimiento de la LOPD, pero ayuda a mejorar los procesos de Seguridad de la Información que están íntimamente relacionados con el cumplimiento de algunos de los aspectos de la LOPD respecto a medidas de seguridad.

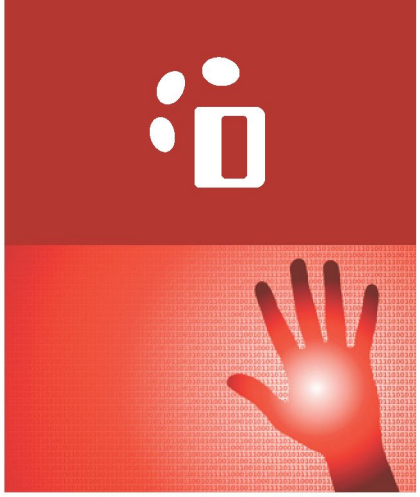
El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos para asegurar el máximo beneficio y el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

DATOS PERSONALES EN LA RED

7. LOS CONSUMIDORES







7. LOS CONSUMIDORES

Los ciudadanos y consumidores tienen una serie de derechos en relación con el tratamiento de datos de carácter personal. En síntesis serían los siguientes:

✓ Cuando se recaben sus datos tienen derecho a recibir información sobre:

- La existencia del fichero o tratamiento de datos, finalidad de la recogida y destinatarios.
- El carácter optativo u obligatorio de las preguntas.
- Las consecuencias sobre la obtención de los de los datos, así como la negativa a suministrarlos.
- La posibilidad de ejercer los derechos de acceso, rectificación, cancelación u oposición.
- La identidad y dirección del responsable del tratamiento o su representante.

✓ En el uso de los datos tienen derecho a que sólo se empleen para la finalidad que le han notificado. Pudiendo denunciar ante la AEPD los usos que no se correspondan con esa finalidad.

- ✓ Derecho a consultar el Registro General de Protección de Datos de la Agencia que es un registro de consulta pública y gratuita. Incluso este derecho se puede ejercer a través de Internet.

- ✓ Derecho de acceso a los datos. El afectado puede recabar información de sus datos de carácter personal sometidos a tratamiento, el origen de los mismos y las cesiones o comunicaciones realizadas o que se prevean realizar. La información deberá ser legible e inteligible si utilizar claves o códigos cualquiera que sea el medio utilizado.

- ✓ Derechos de rectificación y cancelación. El interesado puede instar al responsable del fichero, a cumplir la obligación de mantener la exactitud de los datos, rectificando o cancelando los datos de carácter personal cuando resulten incompletos o inexactos, o bien sean inadecuados o excesivos para la finalidad de recogida, en su caso, o cuyo tratamiento no se ajuste a la ley.

- ✓ Derecho de oposición. Cuando no es necesario prestar consentimiento para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga de lo contrario, el interesado podrá oponerse a su tratamiento cuando existan motivos fundados o legítimos relativos a una concreta situación personal.

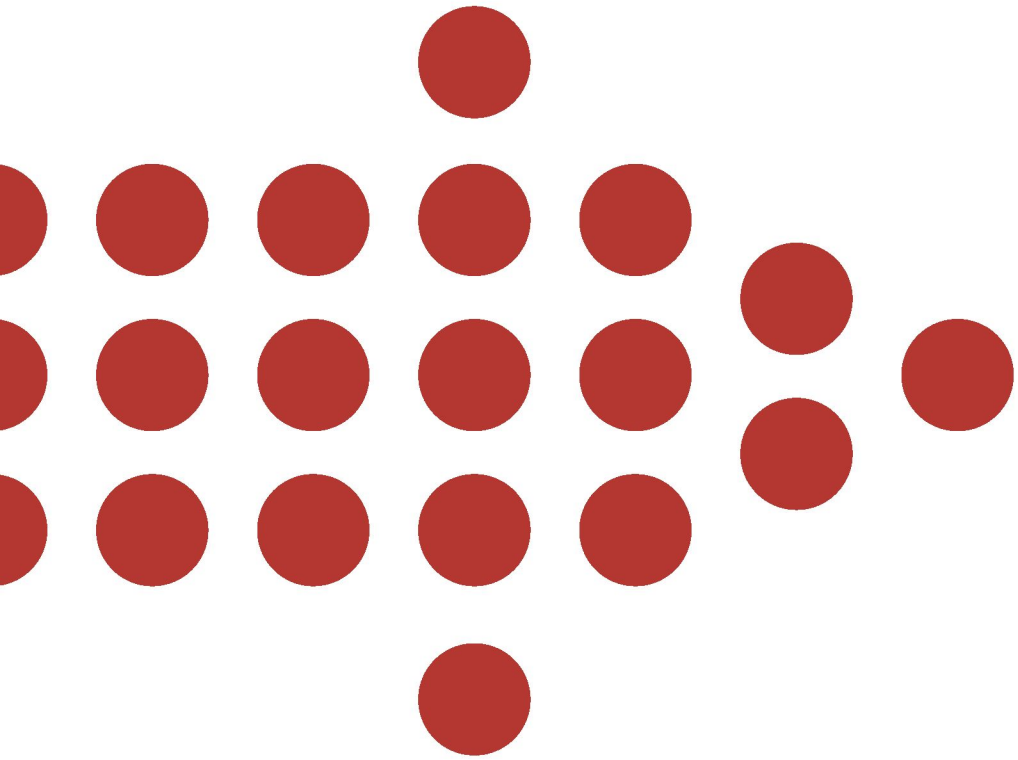
- ✓ Derecho de impugnación. El interesado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

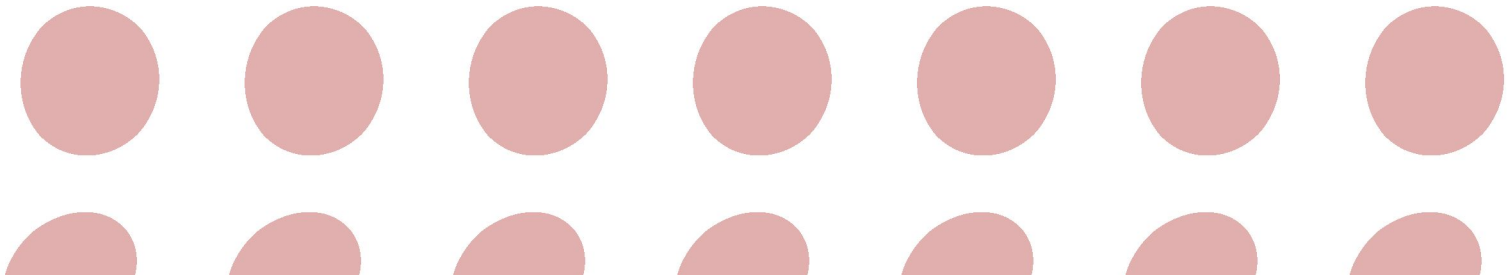
El ejercicio de los mismos es personalísimo, por lo tanto debe ser ejercido directamente por los interesados ante cada uno de los responsables de ficheros, empresa u organismo público, solicitando información sobre qué datos tienen y cómo dichos datos fueron obtenidos, la rectificación de los mismos, o en su caso, la cancelación de los datos.

Para facilitar al ciudadano el ejercicio de estos derechos, la AEPD pone a disposición del consumidor varios modelos tipo en su página web: www.agpd.es.

DATOS PERSONALES EN LA RED

8. AMENAZAS DE LAS TIC EN LA PRIVACIDAD DE LOS DATOS PERSONALES





8. AMENAZAS DE LAS TIC EN LA PRIVACIDAD DE LOS DATOS PERSONALES

El carácter universal de la Red nos convierte en ciudadanos del mundo, pero también puede dejar expuesta, ante ese mismo mundo, nuestra privacidad.

Todo esto hace necesario que exista una regulación equilibrada acompañada de planes de formación e información a los usuarios, entidades públicas y empresas, que nos permita disfrutar de las ventajas de la Sociedad Digital del Conocimiento, y que nos proteja al mismo tiempo de sus peligros.

A continuación analizaremos las principales amenazas a las que se enfrentan los usuarios TIC en relación a la privacidad de sus datos personales:

8.1 ARCHIVOS DE REGISTRO (LOG FILES)

Cada vez que un cibernauta visita un sitio web, se registra un dato en un archivo *log*[25] del servidor. Se va configurando, de este modo, una especie de cuaderno de bitácora del navegante[26]. Los servidores tienen programas para transformar esa cantidad de archivos en una información clara, analizando, por ejemplo, el orden por el cual las páginas web han sido visitadas, dando cuenta así de los intereses y decisiones adoptadas durante las visitas.

Esta acción puede no perjudicar a la privacidad en la medida en que se utilicen los datos disociadamente, es decir, no pueden asociarse a una persona determinada o determinable. Sin embargo, en otras ocasiones, lo que realmente interesa es conocer la identificación de quiénes acceden, por ejemplo, para marketing directo, y es ahí donde se necesita aplicar un sistema de protección de datos nominativos.

8.2 SPAM

Actualmente se denomina *Spam* o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica.

De este modo, se entiende por *Spam* cualquier mensaje no solicitado y que, normalmente, tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es el correo electrónico.

El *Spam* evidencia la violación de los derechos de protección de datos en tanto en cuanto, la temática de los contenidos se selecciona principalmente a través de los archivos de registro.

25 *Log file*: archivo que registra las acciones del usuario.
26 Denominado en inglés *clickstream data*.

Si por ejemplo visitamos una página web sobre Italia, el *Spam* recibido en los siguientes días incluiría ofertas sobre viajes a Italia, comida italiana o ropa italiana. Los proveedores de Internet solían vender este tipo de información a agencias de publicidad, pero esta práctica se está persiguiendo[27]. Asimismo, el envío de correos cadena y hoax (bulos) es una práctica común utilizada para recopilar direcciones de correo electrónico sin el consentimiento de los usuarios. Utilizan correos de contenidos llamativos como la religión, virus incurables, cadenas de buena suerte, leyendas urbanas, métodos para hacerse millonarios o regalos de grandes compañias, que motivan al receptor al reenvío de dichos mensajes y lo convierten en participante del proceso de captación de direcciones de correo.

El bajo coste de los envíos vía Internet (mediante el correo electrónico), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades en el volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada. Además, en muchas ocasiones los contenidos rozan la ilegalidad, si es que no son manifiestamente ilegales, como la pornografía infantil.

Otra modalidad de *Spam* es mediante mensajes de texto en el móvil, que principalmente son publicidad de los operadores móviles. Este tipo de *Spam* no está muy difundido debido al coste del envío de los mensajes.

La recopilación de datos personales con fines comerciales a través de medios electrónicos se regula mediante la Ley 34/2002 de servicios de la Sociedad de la Información y de comercio electrónico, donde se establece que las comunicaciones comerciales deben identificarse como tales y prohíbe su envío por correo electrónico u otras vías de comunicación equivalente, salvo que el destinatario haya prestado su consentimiento.

8.3 VIRUS INFORMÁTICOS: SPYWARE

Los virus informáticos se trasmiten de muchas formas, en la actualidad la más común es mediante correo electrónico, pero los virus pueden trasmitirse mediante CDs, memorias USB o cualquier dispositivo de almacenamiento de datos que sea conectado a nuestro ordenador.

Los virus se pueden utilizar para robar datos personales ajenos, como cuentas de usuario, números de cuenta de la banca *on-line*, incluso pueden infectar teléfonos móviles y recopilar los números de contacto del usuario. Un ejemplo es el virus *CommWarrior*, que tras infectar un teléfono usa la agenda de contactos para reenviarse a todos los números de la agenda del usuario.

Un tipo de virus que afecta directamente a la privacidad de los datos personales es el ***Spyware***. Se conoce como *Spyware* a las aplicaciones de *software* que son instaladas en los ordenadores de los usuarios, la mayoría de las veces sin su conocimiento o autorización, y que al ejecutarse utilizan la conexión a Internet para extraer datos e información sobre el contenido del ordenador en el cual residen.

27 AOL (American Online, proveedor estadounidense de medios y servicios de acceso a Internet) reveló en el 2006 atos de 36 millones de búsquedas en muchas de las cuales se lograba descifrar el nombre, dirección y otros datos personales de los usuarios.

El *Spyware* normalmente registra y envía información sobre hábitos de navegación en la Red, las páginas web que más frecuentemente se visitan, el tiempo de conexión a Internet, etc. No provocan ningún efecto visible en el ordenador, ni cuando son instalados, ni cuando se encuentran en plena acción. Por ello, precisamente, los usuarios no suelen preocuparse de si algún programa de este tipo se encuentra instalado en su sistema. La forma de eliminarlo es instalándose un programa antispyware en el ordenador.

Un antispyware es un programa informático específicamente **diseñado para detectar y eliminar programas espías**. Tienen un funcionamiento similar a los programas antivirus. Estos programas no son incompatibles con los programas antivirus, sino que son complementarios y muchas veces se comercializan en un solo paquete. Teniendo ambos instalados en nuestro ordenador estaremos mejor protegidos contra posibles intrusiones en nuestro sistema.

Cookies

Las *cookies* son pequeños ficheros que se almacenan en el disco duro del ordenador del usuario. Normalmente se utilizan para beneficio del usuario. Mediante el uso de cookies se permite al servidor web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc. Al permitir que los sitios web "recuerden" a los visitantes, se les puede ofrecer un servicio individualizado, informando de las novedades y liberándolos de ciertas tareas engorrosas de identificación. Algo parecido a entrar en un restaurante y que el camarero nos llame por nuestro nombre.

Sin embargo, las cookies no son un buen elemento de seguridad, ya que cualquiera que conozca mínimamente su funcionamiento podría acceder físicamente a ellas, tal vez a través de red local, a los datos guardados en las mismas dentro de un ordenador, y utilizar todos los servicios a los que permiten acceder los nombres y contraseñas en ellas almacenados.

Por otro lado, sí que es cierto que lo que inicialmente se creó como un mecanismo para beneficiar al usuario ha sido pervertido para beneficiar al anunciante, que husmea nuestras idas y venidas y almacena perfiles de usuario para luego dirigirnos su propaganda personalizada. Esta posibilidad abre las puertas a especulaciones acerca de su venta a terceros o su análisis, y ése es el riesgo real de las cookies.

Según la LOPD, los datos recogidos de las cookies deben almacenarse en un fichero y notificarlo a la Agencia de Protección de Datos, sin olvidar el previo permiso del usuario.

8.4 LOS SERVICIOS WEB 2.0

La Web 2.0 ofrece servicios de interacción con otros internautas, como son los foros, blogs, redes sociales, mundos virtuales, etc., donde pueden transmitirse opiniones y preferencias. Estos datos se almacenan en servidores web sin dificultad durante varios años por lo que cualquier persona puede capturar, copiar y almacenar todo lo que se escriba.

Un rastreo permitiría recopilar, sin que el usuario lo sepa, una cantidad de información suficiente para recomponer su perfil.

En este sentido, tanto la Agencia Española de Protección de Datos, como el Consejo de Europa, aconsejan ser conscientes de que los datos personales que damos en la red y las opiniones vertidas en dichos foros son públicas y pueden ser malinterpretadas o utilizadas con fines que atenten a la privacidad de los usuarios. Se aconseja utilizar todos los mecanismos posibles para preservar el anonimato en la Red.

Actualmente, la Unión Europea planea modificar la legislación sobre blogs y redes sociales. El pasado mes de septiembre de 2008 el pleno del Parlamento Europeo aprobó un informe que regulará el respeto de la privacidad y la protección de datos en webs sociales y que se enmarca dentro del paquete de reformas de la legislación europea sobre Telecomunicaciones que la UE tramita actualmente.

De esta forma, las normas comunitarias de protección de datos se extenderán a las redes privadas de comunicación en Internet, como Facebook o Myspace, y no sólo a las públicas. Asimismo, siempre que surja un peligro inminente y directo para los intereses de los consumidores (como el acceso no autorizado al contenido de mensajes electrónicos, a datos relativos a transacciones con tarjetas de crédito, etc.), los proveedores deberán informar inmediatamente, además de a las autoridades nacionales, a los usuarios afectados.

A esto se le suman las distintas enmiendas aprobadas que aumentarán la protección contra el correo basura, las cookies, los virus informáticos, los troyanos o programas espía, y los afectados tendrán la posibilidad de emprender acciones legales contra los remitentes.

8.5 LA INGENIERÍA SOCIAL

La mayoría de las amenazas a la privacidad personal, hacen uso de métodos automatizados que explotan alguna vulnerabilidad suficientemente generalizada para que baste lanzar las redes en lugar oportuno para recoger una buena pesca de datos. A partir de esa captura de datos pueden derivarse nuevas acciones que, según el caso, causarán un mayor o menor daño. Sin embargo, en otras ocasiones, los métodos de ataque son tan antiguos como la propia civilización y hacen uso de técnicas de Ingeniería Social para alcanzar un objetivo ya predeterminado.

El ingeniero social aplica técnicas de persuasión, adquiriendo normas de conducta, ganando credibilidad, exigiendo relaciones recíprocas, pero las aplica de manera manipuladora, engañosa y carente de ética, con unos resultados potencialmente devastadores.

Hay diversos hechos[28] que hacen de la Ingeniería Social un método a menudo exitoso. Además de una sistemática de nuestra credibilidad, la tendencia natural a asumir determinados roles, los prejuicios aceptados categóricamente sobre otras personas cuando las enmarcamos en un rol, la entrada en juego del pensamiento heurístico sobre el sistemático cuando se nos somete al más mínimo estrés o cuando entran en juego nuestros miedos, la inclinación hacia la conformidad, son algunos de los casos que pueden ponerse como ejemplos para entender el funcionamiento de la ingeniería social.

Para ponerse a la altura de las circunstancias, las organizaciones (y también los individuos en su ámbito personal) pueden establecer una serie de contramedidas que minimicen el potencial impacto de la ingeniería social en sus intereses, sean estos su beneficio económico, la reputación de sus marcas o la calidad de servicio percibida por los ciudadanos.

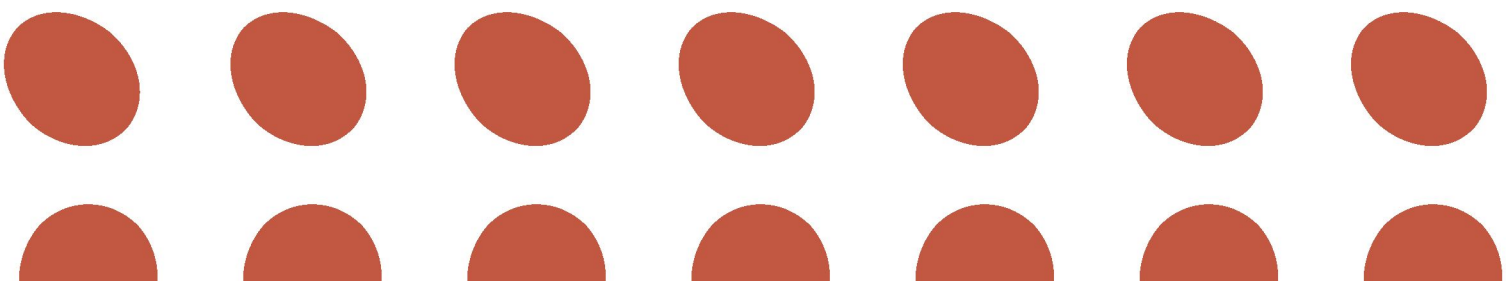
Algunos ejemplos de contramedidas de éxito son los planes de concienciación sobre la seguridad y, en especial, sobre la relevancia de la privacidad de los datos de carácter personal, el establecimiento de normas sencillas sobre los niveles de confidencialidad de cada tipo de información, y la necesidad de los procedimientos de control de identidad en los accesos.

La mayoría de los expertos están de acuerdo en que la Ingeniería Social es la asignatura pendiente de la seguridad de los sistemas de información y que en un futuro próximo las mayores innovaciones en los ataques de seguridad se van a producir con la sofisticación de los burdos métodos de ataque mediante Ingeniería Social que ahora se presentan en forma de toscos mensajes de *phising*. El *Phising* consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales con el fin de obtener datos personales y bancarios de los usuarios para hacerse pasar por ellos en diversas operaciones *on-line*.

Algunas recomendaciones básicas para minimizar los ataques basados en la Ingeniería Social en empresas y Administraciones Públicas son:

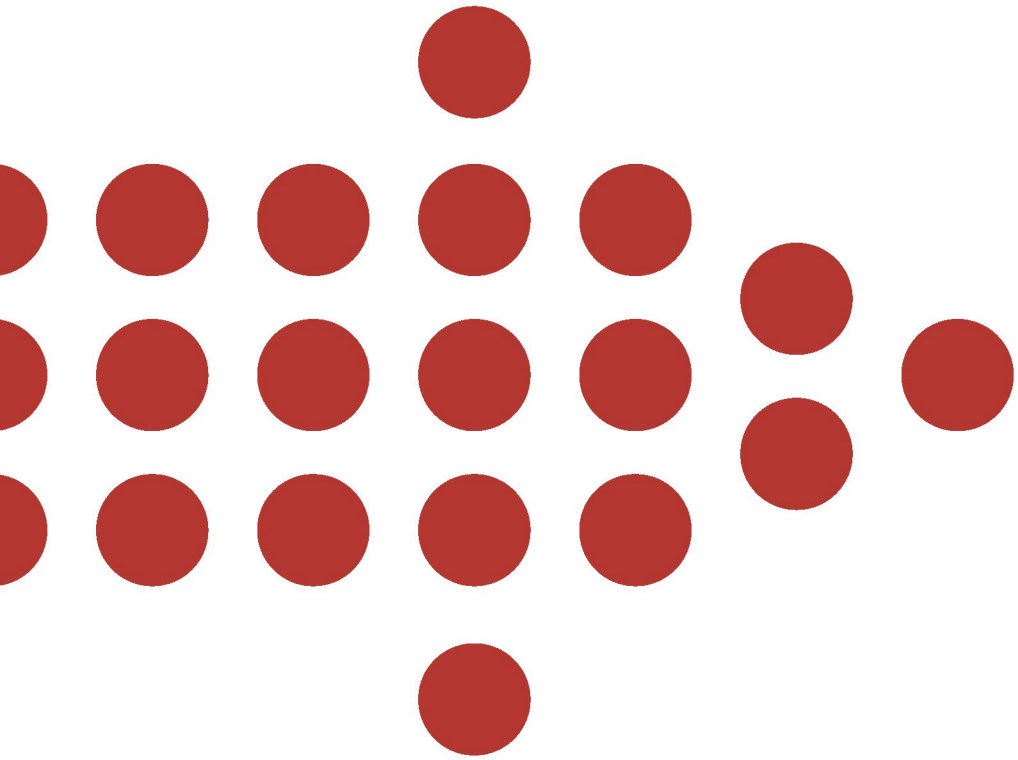
- ✓ Respetar el acuerdo de confidencialidad.
- ✓ Verificar la dirección de origen del mail.
- ✓ Informar de posibles violaciones de seguridad.
- ✓ Respetar los procedimientos internos de la organización.

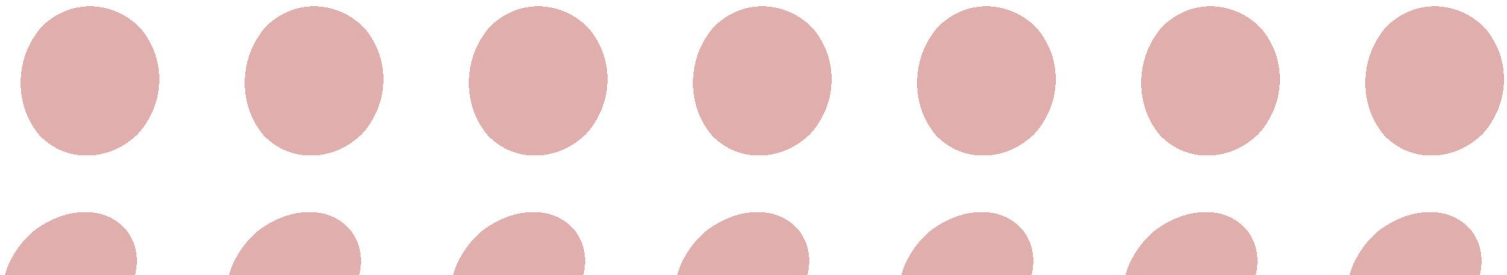
28 "El arte de la intrusión". Kevin Mitnick.



DATOS PERSONALES EN LA RED

9. TECNOLOGÍAS PARA LA PROTECCIÓN DE LA PRIVACIDAD





9. TECNOLOGÍAS PARA LA PROTECCIÓN DE LA PRIVACIDAD

El desarrollo y generalización del uso de las Tecnologías de la Información y Comunicaciones (TIC) aplicado a los ámbitos personales, empresariales y administrativos está provocando una serie de cambios, donde las TIC se configuran como motores de desarrollo en la Sociedad de la Información. Las TIC intervienen de forma directa en la privacidad de los datos de carácter personal. En algunos casos, como ya hemos visto, como fuentes de amenazas, que utilizadas de forma incauta atentan contra la privacidad de las personas. Sin embargo, las TIC suponen a su vez la principal herramienta de protección y prevención por un lado, y de diagnóstico por otro. Es por eso que en este capítulo analizaremos las fortalezas que suponen las TIC en el ámbito de protección de datos de carácter personal.

Las TIC bien utilizadas pueden generar nuevas oportunidades de acceso a la información, promover capacidades y mejorar la productividad. Sin embargo, se debe insistir una y otra vez en el hecho de que las TIC deben ser vistas sólo como herramientas que deben estar al servicio del ser humano y, por tanto, son un medio y no un fin en sí mismas.

Por todo ello, las TIC también pueden considerarse como una herramienta para favorecer el cumplimiento de la legislación y, en particular, las normas de protección de datos. La Directiva 2002/58/EC sobre la privacidad y las comunicaciones electrónicas ya contempla en cierta medida la utilización de tecnología con este fin. Las denominadas Tecnologías para la protección de la intimidad (PET[29]) pueden servir para la protección de datos personales. Algunos ejemplos de PET son[30]:

- ✓ Herramientas que permiten el anonimato automático de los datos tras un lapso determinado de tiempo. Obedece al principio de que los datos tratados deben guardarse en una forma que permita identificar al interesado únicamente durante el tiempo necesario dependiendo de los fines iniciales para los cuales se facilitan los datos. Es decir los datos solamente pueden estar identificados durante el tiempo preciso dependiendo del propósito que motivó su recogida.

- ✓ Los instrumentos de cifrado que impiden el pirateo de la información transmitida por Internet. Responden a la obligación del responsable del tratamiento de datos de adoptar medidas adecuadas para proteger los datos personales frente al tratamiento ilícito. Algunos ejemplos son la firma electrónica[31] y los certificados digitales[32].

29 PET: Privacy Enhancing Technologies.

30 COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, 2007.

31 La criptografía sirve para proteger el contenido de los correos electrónicos y resuelve, entre otros, el problema de garantizar que un mensaje ha sido escrito realmente por la persona que posee la dirección de correo electrónico desde la que nos ha llegado el mensaje.

32 Un certificado digital es un fichero digital que es intransferible y no es modificable, emitido por una tercera parte de confianza (Entidad Certificadora), que se asocia a una persona o entidad una clave pública. La misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de ello.

- ✓ Los anuladores de *cookies*[33] , que bloquean las cookies introducidas en un ordenador para que lleve a cabo determinadas instrucciones sin que el usuario tenga conocimiento de ello. Responden al principio de que los datos deben tratarse de forma lícita y transparente y que ha de informarse al interesado del tratamiento que se realice.

- ✓ La Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios de Internet analizar la política de los sitios web en lo que se refiere a la intimidad y compararla con las preferencias del usuario en relación con la información que desee facilitar. Contribuye a garantizar que el interesado autoriza el tratamiento de sus datos con conocimiento de causa.

Las PET dependen del desarrollo de las Nuevas Tecnologías. Una vez se detectan los peligros que suponen ciertos procesos tecnológicos, hay que desarrollar las herramientas para luchar contra dichos peligros. La evolución de la tecnología, detectar los riesgos que plantea en relación con los derechos fundamentales y la protección de datos personales y definir los requisitos técnicos para hacerles frente mediante las PET (afinar las medidas tecnológicas conforme a los distintos riesgos y datos de que se trate, tener presente la necesidad de salvaguardar intereses como la seguridad pública, etc.) son los pilares básicos del proceso de seguridad de las tecnologías de protección. No hay que olvidar que la eficacia de las PET depende de la tipología de las mismas y de su mantenimiento y desarrollo diacrónico.

El uso de las PET no debe impedir que los organismos responsables del cumplimiento de las leyes relativas a la protección de datos personales y otras autoridades competentes ejerzan sus funciones. Desde el punto de vista social y ético, estas responsabilidades recaen también en quienes elaboran las especificaciones técnicas y quienes desarrollan o ejecutan programas o sistemas operativos. D. Emilio del Val[34] asevera que la constante evolución tecnológica y la relativización de los conceptos de tiempo y espacio, se han revelado en la sociedad actual como aliados "ilegitimos" de una amenaza constante para la privacidad y la protección de los datos de carácter personal. Así, en un mundo globalizado, las posibilidades coercitivas del Estado se minimizan ostensiblemente y, en consecuencia, el recurso normativo resulta claramente insuficiente para disciplinar conductas y atajar la potencialidad vulneradora de los derechos, inherente al uso de las Nuevas Tecnologías.

Los consumidores son los más interesados en las PET y que las normas de protección de datos se apliquen correctamente. Se debe sensibilizar a los consumidores acerca de los riesgos del tratamiento de datos y de las soluciones que las PET pueden aportar como complemento a los sistemas actuales en tema de protección de datos. Según Martín Pérez, presidente de ASIMELEC[35]: "Hay que desarrollar una cultura de la seguridad en el uso de las Nuevas Tecnologías, con acciones de divulgación y difusión orientadas a dar a conocer a los ciudadanos los problemas de seguridad asociados al uso de los servicios de la Sociedad de la Información, y las herramientas y buenas prácticas disponibles para mitigar estos problemas y potenciar el uso seguro y confiable de estos servicios".

33 Las *cookies* son pequeños ficheros que se almacenan en el disco duro del ordenador y que sirven para recabar preferencias seleccionadas por el usuario.

34 Subdirector General de Inspección y Tutela de Derechos de la Agencia de Protección de Datos de la Comunidad de Madrid.

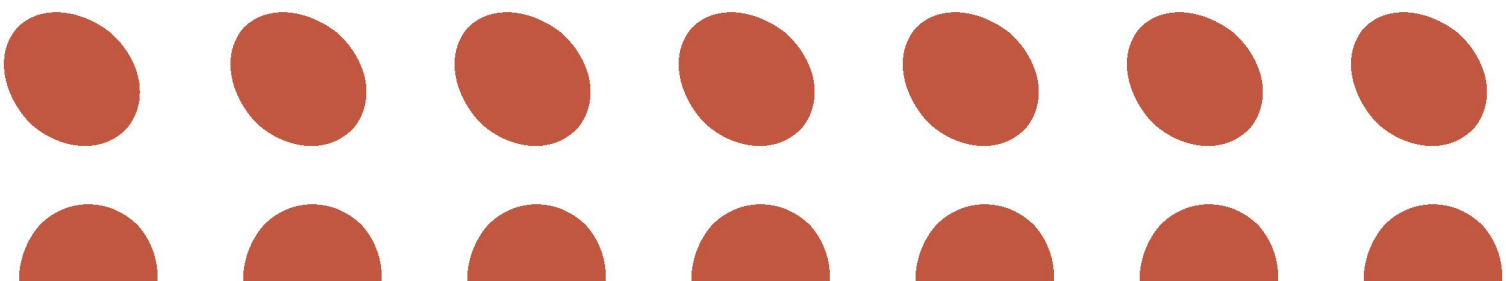
35 Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones.

Cada vez que alguien utiliza el correo electrónico, navega por la Web o interviene en los foros de conversación está revelando datos sensibles acerca de sí mismo. La mayoría de los usuarios no es consciente de la cantidad de información privada que de forma inadvertida e involuntaria está revelando a terceros.

Estas, y otras muchas cuestiones motivan que para sacar un provecho seguro de Internet, los usuarios deban mantenerse informados sobre los riesgos existentes en cada momento y conocer la forma de evitarlos.

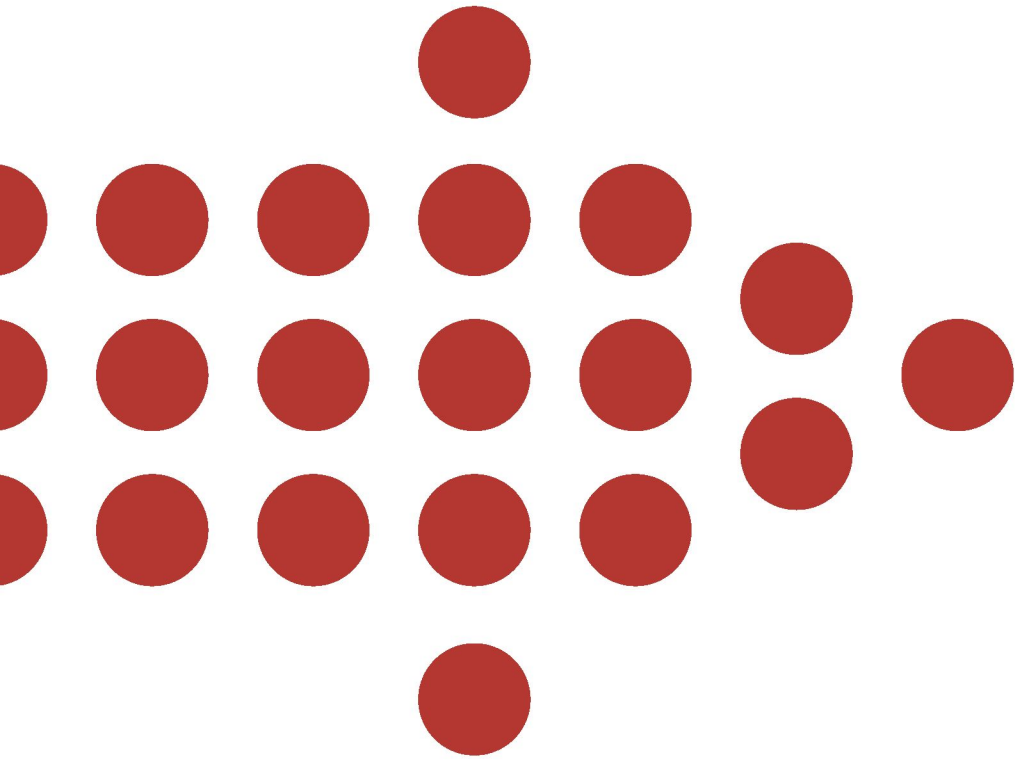
Es por ello que la Junta de Castilla y León, a través del Programa Aprende[36], pone en marcha un conjunto de proyectos para promover el **uso inteligente de las Nuevas Tecnologías**, facilitando una integración segura de los ciudadanos de Castilla y León en la Sociedad Digital del Conocimiento. Además, todos los castellanos y leoneses tendrán la oportunidad de conocer las nuevas herramientas tecnológicas y la importancia de su uso adecuado a través de la Web Seguridad y Privacidad (www.iniciate.es/seguridad), para aprovechar al máximo las ventajas que las TIC reportan en cuanto a protección de datos personales y evitar así sus riesgos.

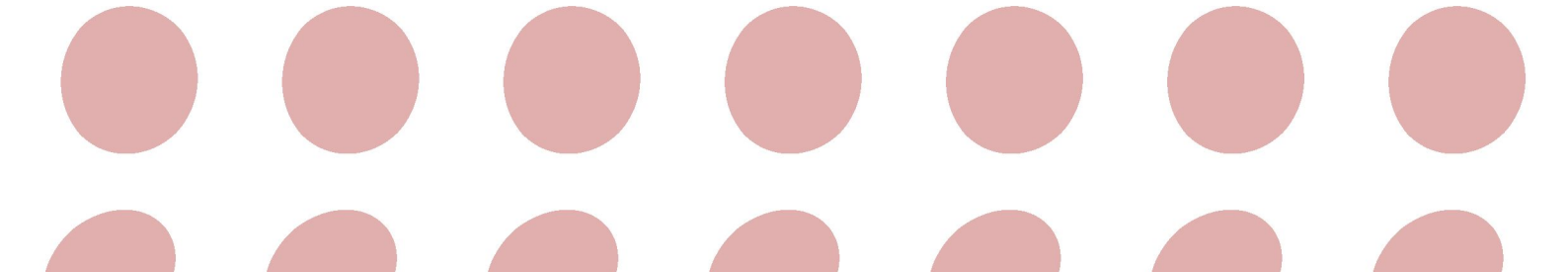
36 www.jcyl.es > Sociedad de la Información > Promoción > Programa Aprende.



DATOS PERSONALES EN LA RED

10. SEGURIDAD VS PRIVACIDAD: EL "GRAN HERMANO"





10. SEGURIDAD VS PRIVACIDAD: EL "GRAN HERMANO"

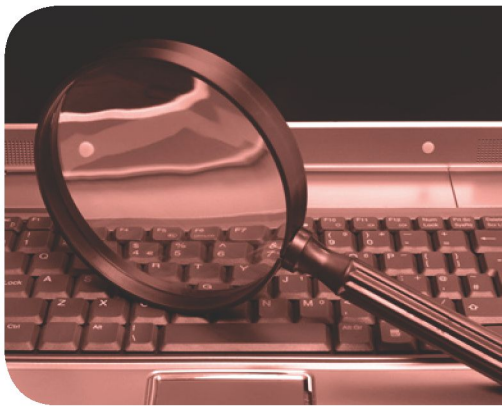
El término "Gran Hermano" tomado de la novela de Orwell 1984 en la que el dictador *"Big Brother"* (Gran Hermano) es omnipresente y su servicio secreto controla hasta las esferas más íntimas de sus ciudadanos, fue publicada en 1949, años después de que la vigilancia llevada a cabo sobre el autor por Scotland Yard terminase. Posteriormente el término "Gran Hermano" se convirtió en sinónimo de vigilancia total por parte del Estado.

En la actualidad se ha implantado un modelo social en el que la vigilancia y la tele-vigilancia están absolutamente presentes en la vida ciudadana. Vivimos en una sociedad que se convierte en un magnífico escenario para el desarrollo e implantación de las más modernas tecnologías de la vigilancia, que se suman sin ningún problema a las utilizadas tradicionalmente. Y es por ello que hay que estar alerta ante esta realidad de control tan altamente desarrollado.

La vigilancia se nos presenta como una manta protectora contra el frío de la inseguridad, pero tras esta confortable metáfora se esconde la certeza de un mundo cada vez más controlado y un poder cada vez más represivo. Corremos el riesgo, por tanto, de interiorizar la vigilancia de tal manera que no lleguemos a ser conscientes del nivel de control, inspección, examen, vigilancia, intervención, revisión, registro e investigación al que se nos somete diariamente[37].

En nuestra sociedad abundan las nuevas tecnologías de la seguridad. Estamos ante una sociedad vigilada. Existen gran variedad de estas tecnologías y continuamente se incorporan otras nuevas: circuitos cerrados de televisión (CCTV), programas de reconocimiento facial, sensores de proximidad, detectores de movimiento, cámaras infrarrojas, cámaras robots, secuenciadores de vídeo, sensores de humo, contactos magnéticos, cámaras con radiofrecuencia, cámaras de baja iluminación, cámaras acuáticas, cámaras visibles u ocultas...

Es en este contexto donde surge el debate de si es más importante la privacidad o la seguridad. Sin duda nuestra primera respuesta a dicha pregunta sería: "ambas". El problema es que la privacidad y la seguridad son inversamente proporcionales ya que el aumento de una de ellas supone el descenso de la otra. La aparición y desarrollo de las Nuevas Tecnologías ha influido en la aparición de estos dilemas y ha hecho que la preocupación de la sociedad en materia de privacidad y seguridad sea mayor. Sin duda un hecho es claro, la inclinación de la balanza hacia uno de los lados depende de las experiencias de la sociedad en cada momento. Si la sociedad se ve amenazada en su seguridad, por ejemplo con los ataques terroristas del 11 de septiembre del 2001, ven justificadas cualquier tipo de medidas que garanticen su salvaguarda. Pero ¿hasta que punto?.



37 (Capmany Sans, Dani).

En EEUU, ingenieros del FBI crearon *"Omnivore"* (1997), que traspasaba el concepto de "pinchar" las líneas telefónicas a Internet. Los ingenieros del departamento federal se basaron en una antigua legislación que permite, en ciertas circunstancias, intervenir conversaciones telefónicas. En 1999 *"Omnivore"* habría mutado a *"Carnivore"* y oficialmente se llamó "DCS1000". *"Carnivore"* no sólo rastrea mensajes a través de correo electrónico, sino que también la participación en foros, grupos de discusión, conversaciones en chat y cualquier otra actividad de interacción en la Red. *"Carnivore"* funciona como una caja negra de muy fácil instalación que se coloca en el proveedor de acceso a Internet (ISP). A través de los ISPs, *"Carnivore"* tiene acceso a toda la información que llega o recibe el usuario. La operatoria exacta de *"Carnivore"* es una incógnita. Los grupos de defensa de las libertades civiles y muchos otros grupos políticos y sociales de EE.UU. han pedido al FBI que publique el código fuente del programa para conocer su verdadero impacto en la privacidad de los individuos (El "código fuente" son las líneas de programación del software). El FBI se ha negado a entregar el código, argumentando que los criminales pueden utilizarlo para neutralizar a *"Carnivore"*. Este software ha sido utilizado en 25 ocasiones, según fuentes ligadas al FBI y en 10 de ellas se instaló para investigar grupos que estaban atentando en contra de la seguridad.

Las reacciones de la sociedad civil frente a la sensación de "Gran Hermano" se materializan en los movimientos *Ciberpunk*, *Crypto Anarchy* o *Anti-Rfid*, entre otros. El movimiento *Ciberpunk* tiene una visión negativa del impacto de la tecnología en la humanidad que se está desarrollando de forma desenfrenada y manipula la mayor parte de las interacciones sociales. Las Nuevas Tecnologías si bien proporcionan mayores niveles de comodidad, también alienan al individuo y ayudan a controlarlo. En este sentido surge el *Crypto Anarchism* que ensalza la ausencia de gobierno, líderes o leyes en Internet. La criptografía permite esta anarquía, reforzar la privacidad y consecuentemente la libertad. En sus comunidades creen que es donde pueden ser totalmente libres, decir lo que se piensa y mostrarse uno mismo como realmente es. Otra de las corrientes que surgen a partir de tecnologías que pueden atentar contra la privacidad es el movimiento *Anti-Rfid*, bajo el argumento de que esta tecnología Rfid (que a continuación explicamos) goza ya de gran difusión y es potencialmente posible seguir y recopilar los hábitos de un individuo.

10.1 RFID SPYCHIPS

La tecnología de identificación por radiofrecuencia RFid *(Radio Frequency IDentification)* es una tecnología de captura de datos que utiliza diminutos chips rastreadores adheridos a los productos a cierta distancia.

En España estas etiquetas, principalmente son usadas para el control antirrobo en los supermercados y tiendas. También se emplean para realizar inventarios de forma rápida y en la gestión de la cadena de suministro.

Aunque esta tecnología no es en absoluto novedosa, el oscurantismo en torno a las circunstancias de su más que previsible despliegue, reside en que esta tecnología atenta contra la privacidad, motivo por el cual recientemente se está creando un movimiento anti RFid[38]. Las razones principales por las que RFID resulta preocupante en lo que a refiere a la privacidad son:

38 Como el patrocinado por diversos movimientos de derechos civiles en http://www.spychips.com.

1. El comprador de un artículo puede no saber de la presencia de la etiqueta o ser incapaz de eliminarla.

2. La etiqueta puede ser leída a cierta distancia sin conocimiento por parte del individuo.

3. Si un artículo etiquetado es pagado mediante tarjeta de crédito o conjuntamente con el uso de una tarjeta de fidelidad, entonces sería posible enlazar la ID única de ese artículo con la identidad del comprador.

La mayoría de las preocupaciones giran alrededor del hecho de que las etiquetas RFid puestas en los productos siguen siendo funcionales incluso después de que se hayan comprado los productos y se hayan llevado a casa, y esto puede utilizarse para vigilancia, y otros propósitos sin relación alguna con sus funciones de inventario en la cadena de suministro.

A pesar de esta creciente preocupación por garantizar la privacidad en el uso de sistemas RFid, existen numerosos mecanismos que permiten evitar la utilización inadecuada de las ventajas que ofrece esta tecnología. A continuación se discuten las propuestas más relevantes:

- ✓ **El comando "Kill":** Estipular que todas las etiquetas deben tener la capacidad de poder ser inutilizadas a través de un comando especial conocido como comando "kill", de manera que la etiqueta está realmente "muerta" y no puede volver a ser reactivada. La finalidad que se persigue con ello es impedir que alguien pueda reactivar una etiqueta permitiendo el seguimiento de una persona sin su consentimiento.

- ✓ **La jaula de Faraday:** la introducción de chips RFid en el pasaporte o DNI ya ha sido motivo de polémica, pues existe el riesgo de que cualquier persona provista de un lector RFid pudiera leer todos nuestros datos personales. Se puede evitar con lo que se conoce como "Jaula de Faraday": un envase (cartera, funda, etc.) hecho con una hoja o malla de metal impenetrable para las señales de radio.

- ✓ **Etiquetas RFid inteligentes** de manera que reaccionen protegiendo la privacidad pero proporcionando la funcionalidad deseada. Esto normalmente implicaría el uso de métodos criptográficos.

- ✓ **"Blocker tag":** consiste en realizar un bloqueo selectivo de lectores RFid mediante etiquetas o tags que se encargan de ello.

RFid es una tecnología en claro auge y con unas perspectivas de crecimiento futuro bastante optimistas. Sin embargo, según los expertos, la preocupación de los ciudadanos por la privacidad y la protección de datos es uno de los obstáculos que dificultan que su expansión se produzca de una manera más rápida[39].

39 Más información sobre RFID en el estudio "RFID: Identificación por Radiofrecuencia", publicado por el ORSI 2007 y disponible en www.orsi.es.

10.2 VIDEOVIGILANCIA

Es un hecho constatado por la AEPD que la videovigilancia (tanto la pública como la privada) continúa en aumento[40]. Lo que está claro es que las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el Artículo 3 de la LOPD. Artemi Rallo, Director de la Agencia de Protección de Datos, afirma que los sistemas instalados y comunicados a la Agencia han pasado de 10 en 2003 a 3.500 en 2007. Algunos de ellos, como el del metro de Madrid, suponen más de 3.000 cámaras instaladas. En cualquier gran avenida del centro de una ciudad se pueden contar por centenares. Todo parece indicar, en palabras de Rallo, «que somos los propios ciudadanos los que estamos dispuestos a convertirnos en nuestro propio Gran Hermano».

Según la Instrucción 1/2006 del 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, siempre que resulte posible, deben adoptarse otros medios menos intrusivos para asegurar la protección de las personas y en el caso de que se implante la videovigilancia deben seguirse tres juicios: el de idoneidad, necesidad y proporcionalidad.

Asimismo, al considerarse las imágenes un dato de carácter personal el tratamiento no exige su conservación sino que basta con su recogida o grabación, excepto cuando es para uso personal o se realiza por parte de las Fuerzas y Cuerpos de Seguridad del Estado[41]. Como cualquier dato de carácter personal, deben poder ejercerse los derechos de acceso, rectificación y cancelación por parte de los usuarios, así como el deber de información por parte de la empresa o Entidad que use este tipo de mecanismo. Por ello, es imprescindible colocar al menos un distintivo informativo ubicado en un lugar visible, en zonas videovigiladas (tanto en espacios abiertos como cerrados) y no olvidar poner a disposición de los interesados los impresos en los que se les informe de esta práctica según el Artículo 5.1 de la LOPD[42]. Por último los datos deben cancelarse en un mes como máximo desde su captación.

No se puede negar la evidencia del uso de las videocámaras para la protección ciudadana, pero conforme se extiende su uso, aumentan los casos de personas que ven violados sus derechos a la intimidad, el honor, etc., el eterno debate, seguridad o privacidad.

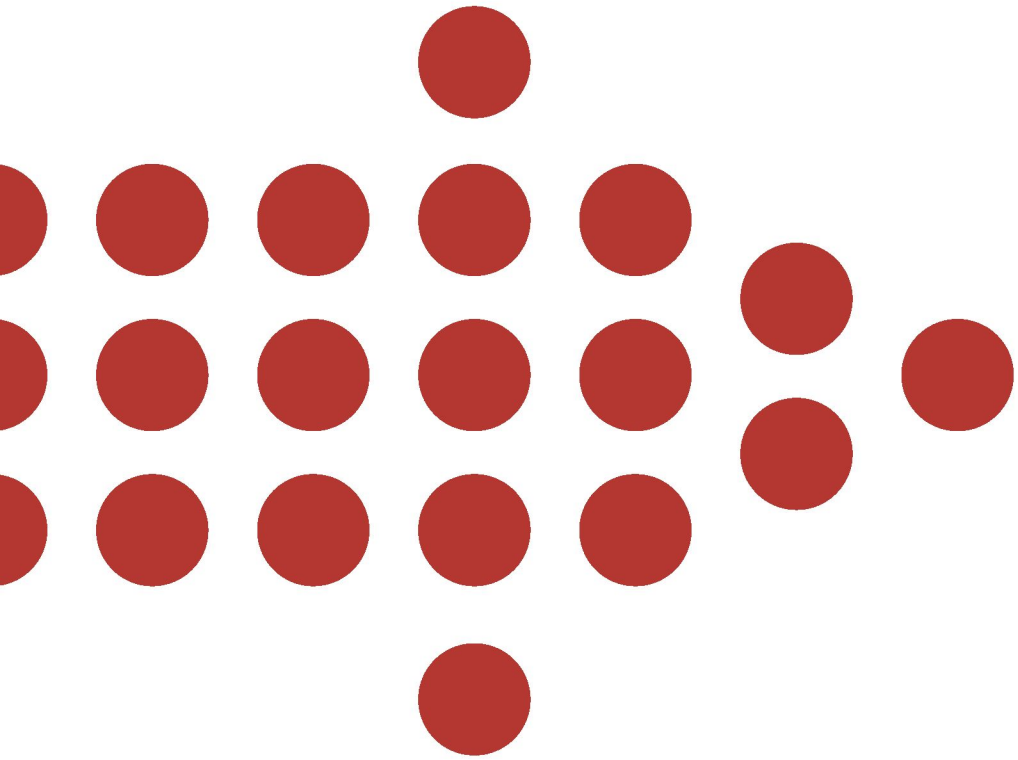
40 Belaza, Mónica C. “Ciudadanos espiados por los ojos de las cerraduras”. Elpais.com. 09/12/2007.

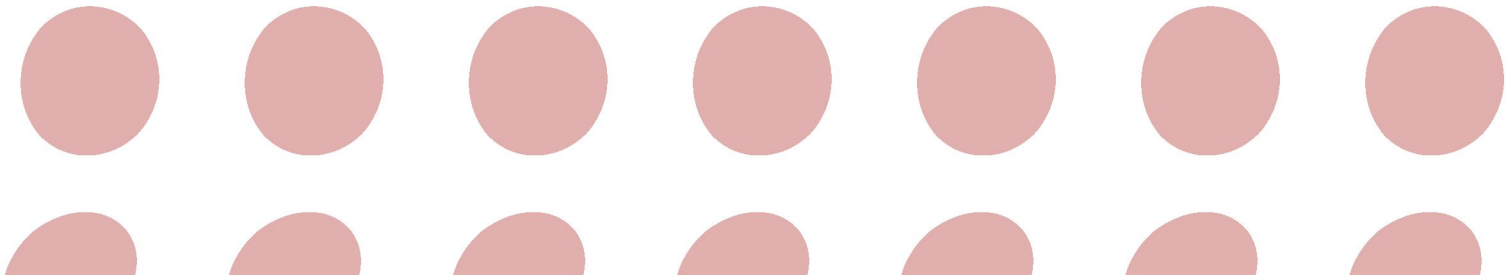
41 La Ley Orgánica 4/1997, del 4 de agosto, regula la utilización de videocámaras por las Fuerzas de Seguridad en lugares públicos ya sean abiertos o cerrados.

42 Los interesados deben ser informados de la existencia de un fichero, de la finalidad de los datos recogidos y de los destinatarios de la información, así como de las consecuencias de la obtención de los dato, la posibilidad de ejercer sus derechos y de identificar al responsable.

DATOS PERSONALES EN LA RED

11. CONCLUSIONES





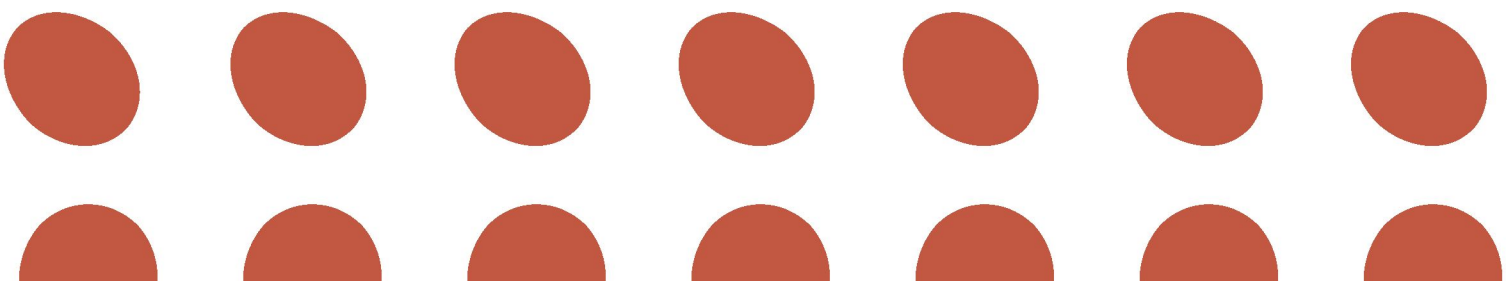
11. CONCLUSIONES

Para D. Emilio del Val[43] "la constante evolución tecnológica y la relativización de los conceptos de tiempo y espacio, se ha revelado en las sociedad actual como aliados «ilegítimos» de una amenaza constante para la privacidad y la protección de datos de carácter personal. Así en un mundo globalizado, las posibilidades coercitivas del Estado se minimizan ostensiblemente y, en consecuencia, el recuso normativo resulta claramente insuficiente para disciplinar conductas y atajar la potencialidad vulneradora de los derechos, inherente al uso de las nuevas tecnologías". De ahí la labor informativa e impulsora de los Organismos de Control.

El cumplimiento de la LOPD deriva en beneficios y ventajas para la empresa y Administraciones Públicas. Por un lado tenemos el beneficio interno que supone la implantación de protocolos de actuación ante las problemáticas habituales que ayuden a la mejora y rapidez en la respuesta ante las mismas. Además, el cumplimiento de la ley deriva en un beneficio externo producto de la imagen que se ofrece a los ciudadanos, una imagen de control, eficacia y orden de los documentos y datos que maneja la entidad en cuestión. El rol de las Agencias de Protección de Datos autonómicas es esencial en este sentido.

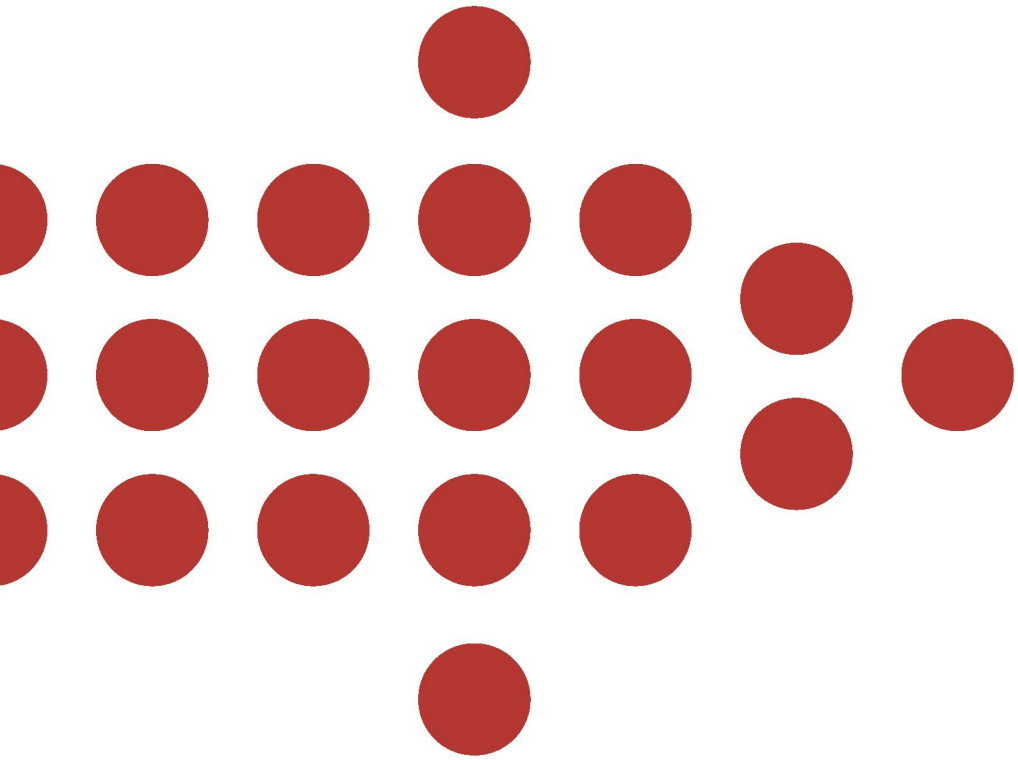
La privacidad por lo tanto, es un derecho fundamental de las personas, el cuál debe ser respetado y protegido. Protegido por medio de las leyes y Organismos de Control y respetado por las empresas y Entidades Públicas.

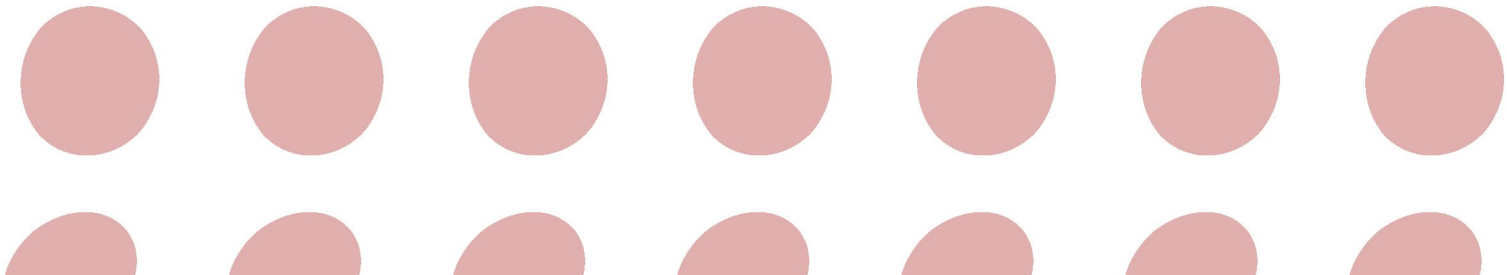
43 Subdirector General de Inspección y Tutela de Derechos de la Agencia de Protección de Datos de la Comunidad de Madrid.

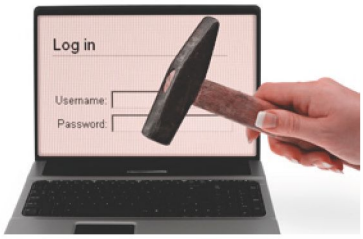


DATOS PERSONALES EN LA RED

ANEXO I: NIVELES DE SEGURIDAD SEGÚN LA NATURALEZA DE LOS DATOS



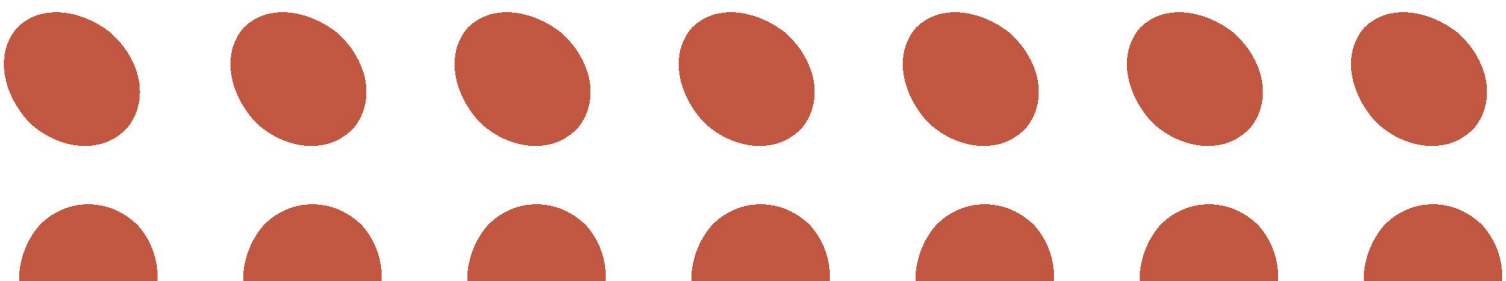




ANEXO I: NIVELES DE SEGURIDAD SEGÚN LA NATURALEZA DE LOS DATOS

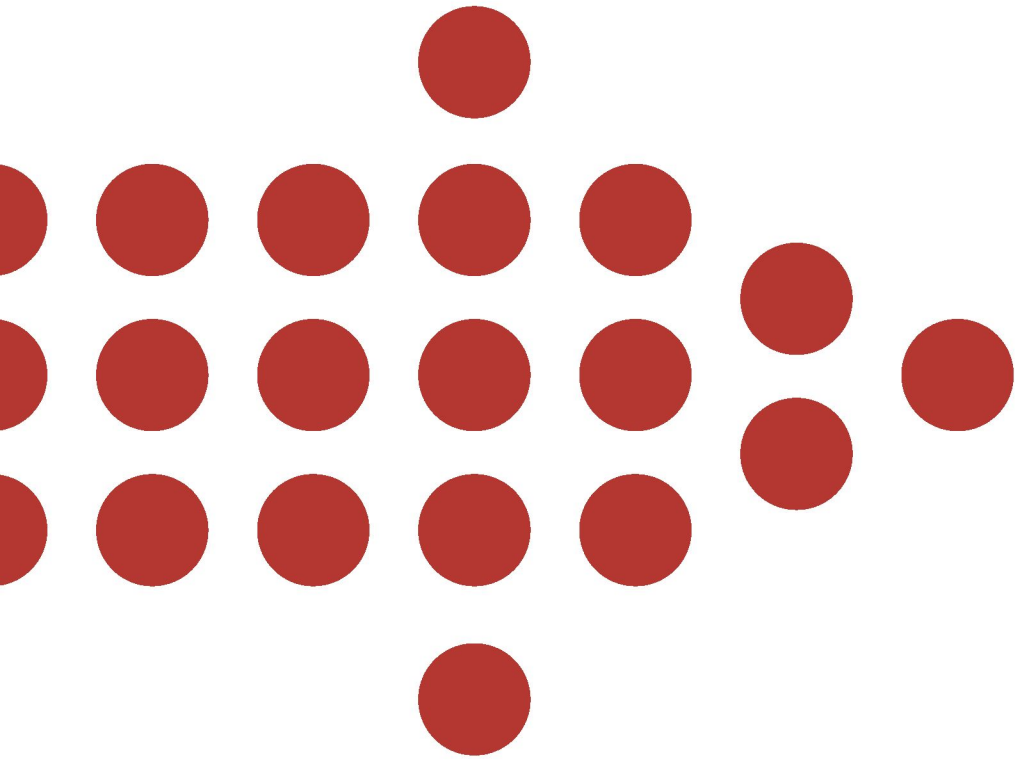
Los datos de carácter personal se pueden clasificar en tres niveles dependiendo de la naturaleza de los datos en sí, como puede verse en la siguiente tabla:

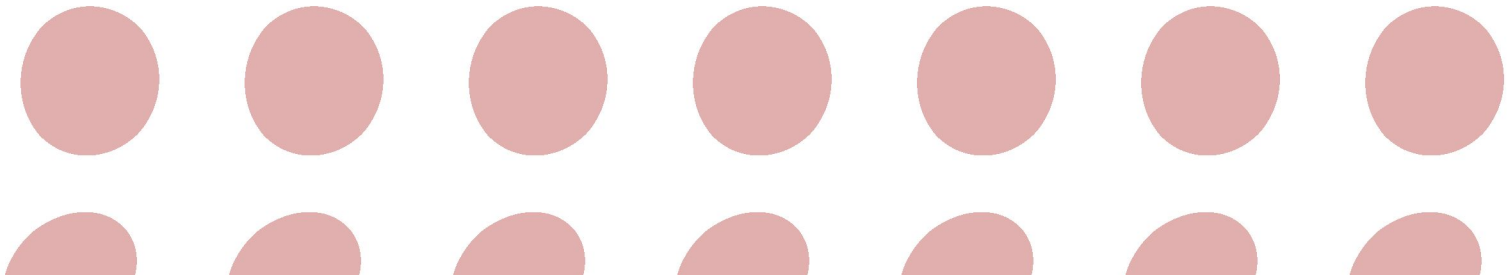
TODO TIPO DE FICHEROS	
NIVELES	NATURALEZA DE LOS DATOS
NIVEL BÁSICO	• Todos los ficheros que contengan datos de carácter personal.
NIVEL MEDIO	• Comisión de infracciones administrativas o penales. • Servicios financieros. • Hacienda pública. • Entidades Gestoras y Servicios Comunes de la Seguridad Social. • Datos que ofrezcan una definición de características o de la personalidad de los ciudadanos y que permita evaluar determinados aspectos de la personalidad o el comportamiento de los mismos.
NIVEL ALTO	• Ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual. • Datos recabados para fines policiales sin consentimiento de las personas afectadas. • Datos derivados de actos de violencia de género. • Datos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas.



DATOS PERSONALES EN LA RED

ANEXO II: MEDIDAS DE SEGURIDAD DEPENDIENDO DE LOS NIVELES





ANEXO II: MEDIDAS DE SEGURIDAD DEPENDIENDO DE LOS NIVELES

Las medidas de seguridad exigibles a los ficheros y tratamiento de datos se clasifican en tres niveles dependiendo de la naturaleza de la información tratada y del grado de necesidad de garantizar la confidencialidad e integridad de la información:

<table>
<tr><th colspan="3">MEDIDAS DE SEGURIDAD PARA FICHEROS AUTOMATIZADOS</th></tr>
<tr><th colspan="3">NIVEL ALTO</th></tr>
<tr><th colspan="2">NIVEL MEDIO</th><th></th></tr>
<tr><th>NIVEL BÁSICO</th><th colspan="2"></th></tr>
<tr>
<td>✓ Documento de Seguridad:
• Debe existir un documento de seguridad donde queden reflejados los tratamientos de datos.

✓ Funciones y obligaciones del personal:
• Se deben definir las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

✓ Control de acceso:
• Los usuarios deben tener acceso sólo a los datos que necesitan por lo que han de implantarse mecanismos que impidan el acceso a datos no autorizados.
• El responsable del fichero debe asegurarse de que exista una relación actualizada de usuarios y perfiles de usuarios.
• Únicamente el personal autorizado puede conceder y modificar los derechos de acceso.
• Todo aquel que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones que el personal de seguridad.</td>
<td>✓ Responsable de seguridad:
• Deberá de existir esta figura que será especificada en el Documento de Seguridad.

✓ Auditoría:
• Realización de Auditorías cada 2 años.
• Debe realizarse extraordinariamente tras modificaciones que puedan repercutir en el cumplimiento de las medidas de seguridad, iniciando el cómputo de dos años.

✓ Control de acceso físico:
• Deberá establecerse un control de acceso a los locales donde están ubicados todos los sistemas de información (no sólo los que contengan datos de carácter personal.

✓ Gestión de soporte y documentos:
• Debe registrarse la información del tipo fecha, origen, información, destinatario, etc., en la entrada y salida de soportes con datos de nivel medio.</td>
<td>✓ Gestión de soporte y documentos:
• Los datos de nivel alto contenidos en soportes para ser distribuidos, deberán ser cifrados o bien se deberá emplear cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.
• Etiquetado de los soportes para que las personas autorizadas identifiquen su contenido de forma comprensible y que se dificulte para el resto de personas.

✓ Registro de acceso:
• Se deberá registrar: usuario, fecha, hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado.
• Revisión de los registros de acceso mensualmente.
• Los datos registrados se deben conservar como mínimo 2 años.
• El responsable de seguridad deberá tener control directo de los mecanismos de registro, revisar los registros periódicamente y elaborar un informe de problemas detectados en las revisiones.</td>
</tr>
</table>

<table>
<tr><th colspan="3">MEDIDAS DE SEGURIDAD PARA FICHEROS AUTOMATIZADOS</th></tr>
<tr><th colspan="3">NIVEL ALTO</th></tr>
<tr><th colspan="2">NIVEL MEDIO</th><th></th></tr>
<tr><th>NIVEL BÁSICO</th><th colspan="2"></th></tr>
<tr>
<td>✓ Gestión de Soportes y documentos:
• La salida de correos electrónicos y sus anexos fuera de los locales también deberá ser autorizada por el responsable del fichero.
• Etiquetado comprensible para identificar su contenido a los usuarios que tengan acceso a soportes con datos sensibles y que dificulten la identificación para el resto de las personas.
✓ Registro de incidencias:
• Deberá constar: el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
✓ Copias de respaldo y recuperación:
• Deberán realizarse copias de respaldo, como mínimo, semanalmente.
• Verificar copias y procedimientos de recuperación cada 6 meses.
• En caso de pérdida de ficheros parcialmente automatizados, se permitirá grabar manualmente los datos, reflejándolo en el documento de seguridad.
• No se pueden realizar pruebas de desarrollo con datos reales.
✓ Identificación y autenticación inequívoca:
• Se podrán utilizar mecanismos basados en certificados digitales.
• Periodicidad cambio contraseña no superior a un año.</td>
<td>✓ Registro de incidencias:
• Deberán incluirse los procedimientos de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de dichos procedimiento. La autorización no debe ser obligatoriamente por escrito.</td>
<td>✓ Copias de seguridad y recuperación:
• Deberán almacenarse en un lugar diferente al lugar donde se encuentran los equipos Informáticos.
✓ Telecomunicaciones:
• La transmisión de datos personales a través de redes públicas o inalámbricas de Tele-comunicaciones debe realizarse de forma cifrada.</td>
</tr>
</table>

MEDIDAS DE SEGURIDAD PARA FICHEROS NO AUTOMATIZADOS

NIVEL ALTO

NIVEL MEDIO

NIVEL BÁSICO

- Las medidas dispuestas para los ficheros automatizados de nivel básico.

✓ **Criterios de archivo:**

- Se debe garantizar la correcta conservación, localización y consulta de la información, posibilitando el ejercicio de los derechos de acceso, rectificación, modificación y oposición de acuerdo con la legislación aplicable.
- En caso de no existir una norma aplicable, el responsable del fichero deberá establecer los criterios procedimientos de actuación.

✓ **Dispositivos de almacenamiento:**

- Deben disponer de mecanismos que obstaculicen su apertura, o se deberán aplicar medidas en caso de que sus características físicas no lo permitan.

✓ **Custodia de soportes:**

- Mientras la documentación no se encuentre archivada en los dispositivos de almacenamiento, la persona que se encuentre a su cargo debe custodiarla e impedir que pueda ser accedida por personas no autorizadas.

✓ **Tratamiento de archivos:**

- Deberán establecer unos procedimientos que estarán dirigidos a garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, oposición, rectificación y cancelación.

✓ **Responsable de seguridad:**

- Se designará uno o varios responsables de seguridad, tal y como se especificaba para los ficheros automatizados.

✓ **Auditoría:**

- Debe realizarse una auditoría, interna o externa, al menos cada dos años.

✓ **Almacenamiento de la información:**

- Los dispositivos de almacenamiento deben encontrarse en salas de acceso restringido mediante puertas con llave o equivalente. Dichas áreas deben permanecer cerradas si no es preciso acceder a los documentos.
- En caso de que esto no se pueda cumplir, el responsable del fichero debe adoptar medidas alternativas adecuadamente recogidas en el documento de seguridad.

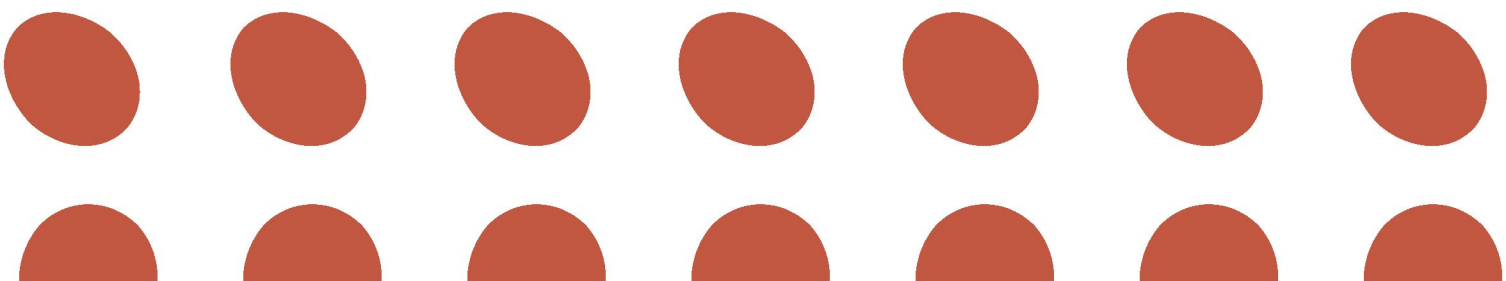
✓ **Copia o reproducción:**

- La generación de copias sólo se puede hacer bajo el control del personal autorizado en el documento de seguridad.
- Se deben destruir las copias desechadas, evitando su recuperación o acceso posterior.

✓ **Acceso a la documentación:**

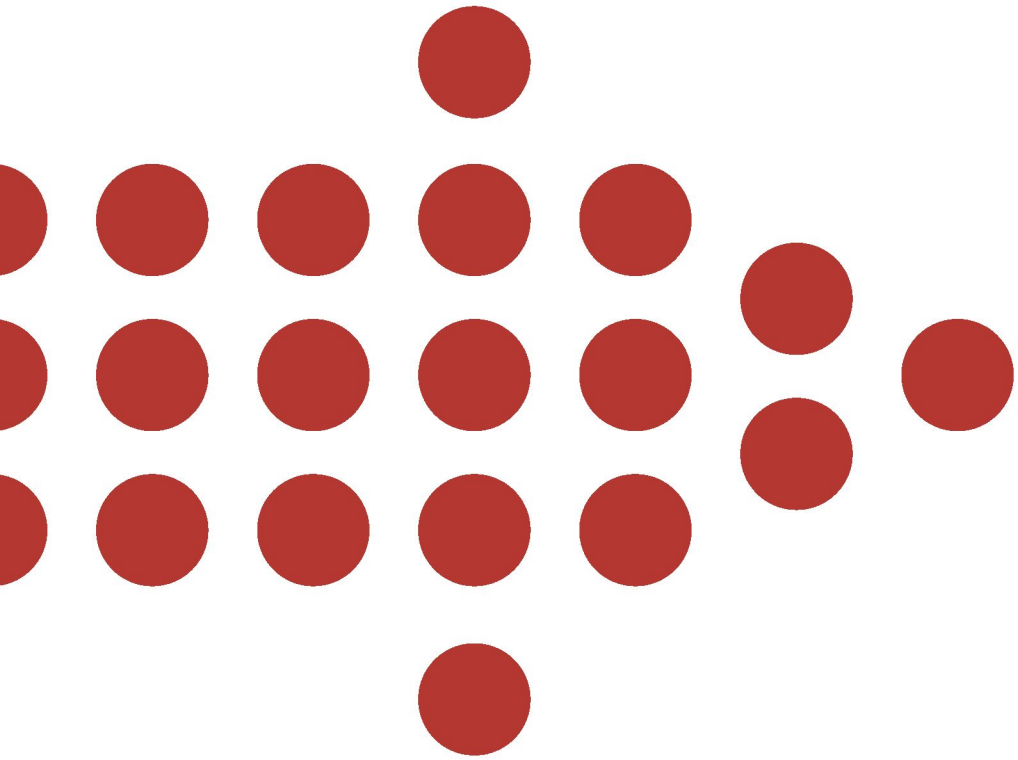
- El acceso a la documentación se limitará exclusivamente al personal autorizado.
- Establecer mecanismos que permitan identificar los accesos realizados para documentos con múltiples usuarios.
- El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado en el documento de seguridad.

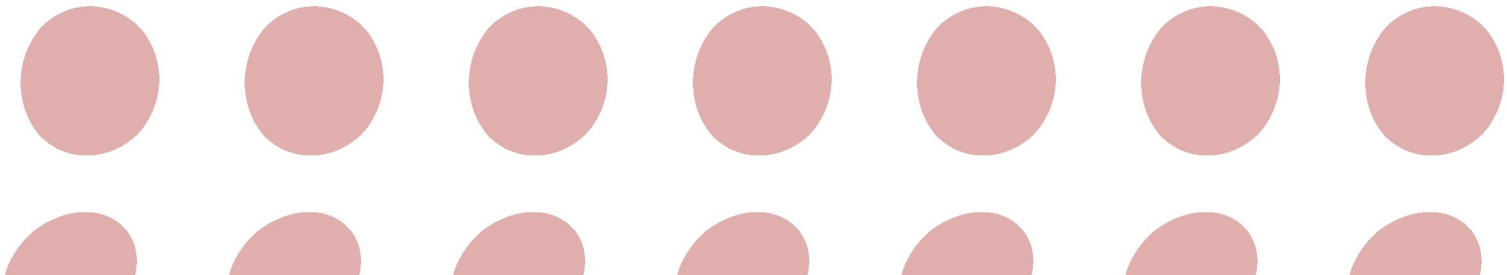
✓ **Traslado de documentación:** Al realizar el traslado físico de la documentación deben adoptarse las medidas que impidan el acceso o manipulación de la información.



DATOS PERSONALES EN LA RED

ANEXO III: COLABORACIONES



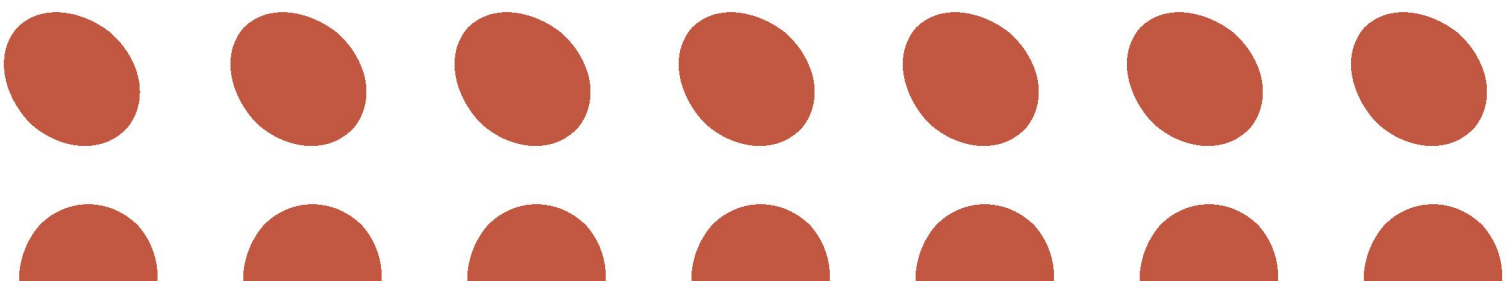


ANEXO III: COLABORACIONES

Para la elaboración del presente estudio han intervenido los siguientes expertos en la materia, a los que agradecemos su colaboración:

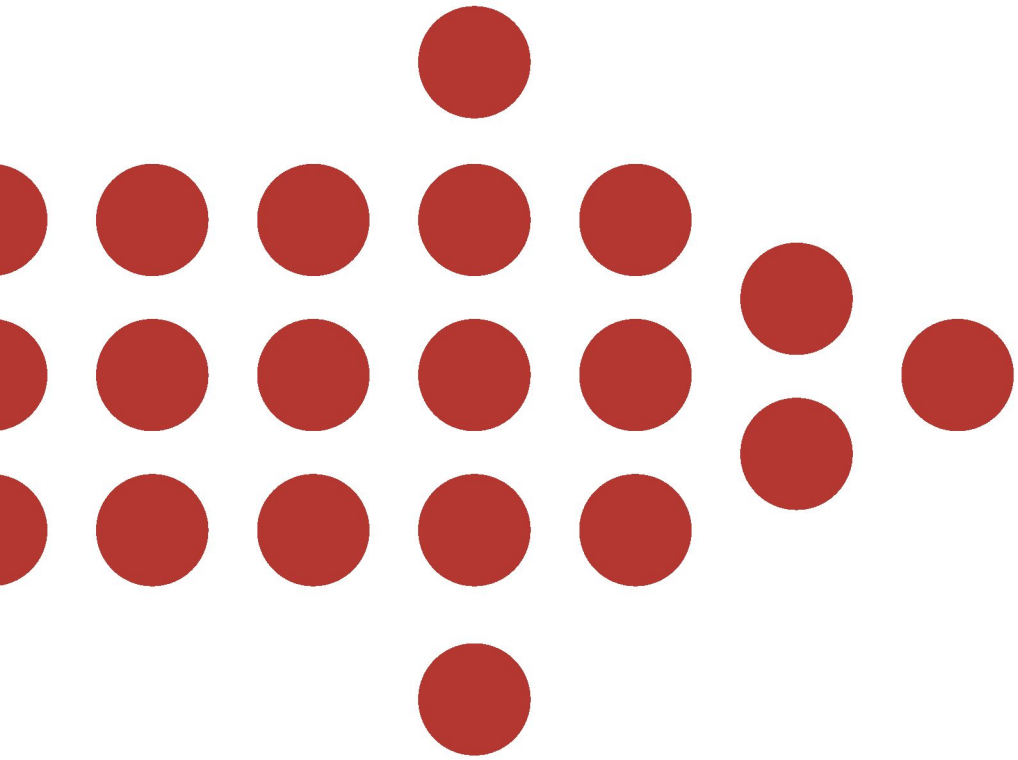
- ✓ **D. Emilio del Val Puerto**, Subdirector General de Inspección y Tutela de Derechos de la Agencia de Protección de Datos de la Comunidad de Madrid.

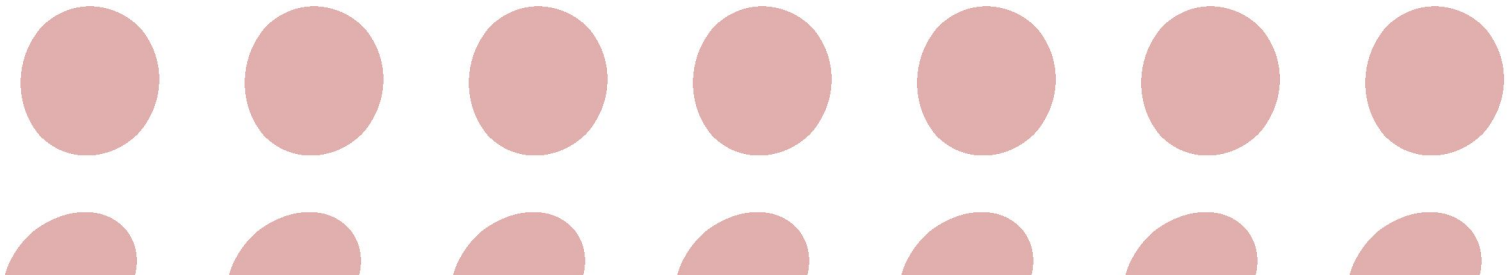
- ✓ **Esther Arenales Gómez y María Lanao García-Abril**, CISA, especialistas en Seguridad de la Información y LOPD, lead auditor ISO 27000.



DATOS PERSONALES EN LA RED

ANEXO IV: SITIOS DE INTERÉS EN INTERNET





ANEXO IV: SITIOS DE INTERÉS EN INTERNET

REFERENCIAS WEB DE LAS AGENCIAS DE PROTECCIÓN DE DATOS ESPAÑOLAS

ORGANISMO	LOCALIZACIÓN DE LA INFORMACIÓN	COMENTARIOS
Agencia Española de Protección de Datos	**www.agpd.es**	Es un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Sus funciones consisten en velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
Agencia de Protección de Datos de la Comunidad de Madrid	**www.madrid.org**	La Agencia de Protección de Datos de la Comunidad de Madrid tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales. Sus competencias versan sobre los ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, entes que integran la Administración Local de su ámbito territorial, Universidades públicas y Corporaciones de derecho público representativas de intereses económicos y profesionales de la misma.
Agencia Catalana de Protección de Datos	**www.apdcat.es**	Tiene como principal función las competencias de registro, control, inspección, sanción y resolución, así como la adopción de posturas e instrucciones en la comunidad autónoma catalana.
Agencia Vasca de Protección de Datos	**www.avpd.euskadi.net**	La Agencia Vasca de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones.

REFERENCIAS WEB DE LOS OBSERVATORIOS DE LA SOCIEDAD DE LA INFORMACIÓN REGIONALES

ORGANISMO	LOCALIZACIÓN DE LA INFORMACIÓN	COMENTARIOS
Observatorio Regional de la Sociedad de la Información en Castilla y León	**www.orsi.es**	El Observatorio de la Sociedad de la Información en Castilla y León tiene como misión identificar y generar conocimiento sobre el estado de la Sociedad Digital del Conocimiento en Castilla y León de forma cualitativa y cuantitativa para poder comparar con otros ámbitos territoriales de su entorno.
Observatorio Aragonés de la Sociedad de la Información	**www.observatorioaragones.org**	Su objetivo fundamental es servir como instrumento de información y formación sobre el impacto de las nuevas tecnologías en Aragón, su uso y su evolución a lo largo de estos últimos años. También se pretende divulgar el potencial de las TIC en el territorio aragonés mediante elementos que recojan la evolución de la sociedad de la información en Aragón, así como atraer y agrupar fuerzas y opiniones en torno a las TIC.
Observatorio de Guipuzkoa	**www.egipuzkoa.net**	La Diputación Foral de Gipuzkoa ha asumido un firme compromiso para impulsar de manera prioritaria y acelerada la plena incorporación de Gipuzkoa a la Sociedad de la Información.
Observatorio de la Sociedad de la Información en Navarra	**www.cfnavarra.es/ObservatorioSi**	El Observatorio para la Sociedad de la Información en Navarra es un instrumento que permite obtener y analizar información sobre el grado de desarrollo y utilización de las Tecnologías de la Información y la Comunicación en la Sociedad Navarra, de forma sistemática.
Observatorio Extremeño de Sociedad de la Información	**www.juntaex.es/consejerias/infraestructuras-desarrollo-tecnologico/dg-sociedad-informacion/Observatorio-ides-idweb.html**	El Observatorio Extremeño de Sociedad de la Información es un instrumento de la Junta de Extremadura que tiene como función realizar el seguimiento y análisis de la evolución de la Sociedad del Conocimiento en la Región, realizando estudios, encuestas y otras actividades que permitan conocer la situación actual y el impacto de la incorporación de las tecnologías de la información y la comunicación a los distintos sectores de la sociedad.
Observatorio para la Sociedad de la Información de la Generalitat de Cataluña	**www10.gencat.net/dursi/es/si/observatori.htm**	El objetivo del Observatorio para la Sociedad de la Información (OBSI) es ofrecer información coyuntural de los principales indicadores referentes a la implantación de la SI en Cataluña.

ORGANISMO	LOCALIZACIÓN DE LA INFORMACIÓN	COMENTARIOS
Asturias Sociedad de la Información	**www.asturiasenred.com/easturias/portal/contenidos/observatorio**	Su objetivo es promover y estimular actividades relacionadas con el desarrollo de la Sociedad de la Información y Tecnologías de la Información orientadas al desarrollo regional. Además, se encarga de analizar y disponer de datos para evaluar el grado de implantación de la Sociedad de la Información en nuestra región.
Oficina Valenciana para la Sociedad de la Información	**www.ovsi.com**	Oficina valenciana, creada en 1996 dentro de una Red Europea de Oficinas, con el objetivo de lograr ventajas y beneficios conjuntos procedentes de la Sociedad de la Información. Dentro de la OVSI se encuentra el Cevalsi (Observatorio de la Sociedad Tecnológica) con publicaciones de infobarómetros sociales y empresariales de la Comunidad Valenciana.

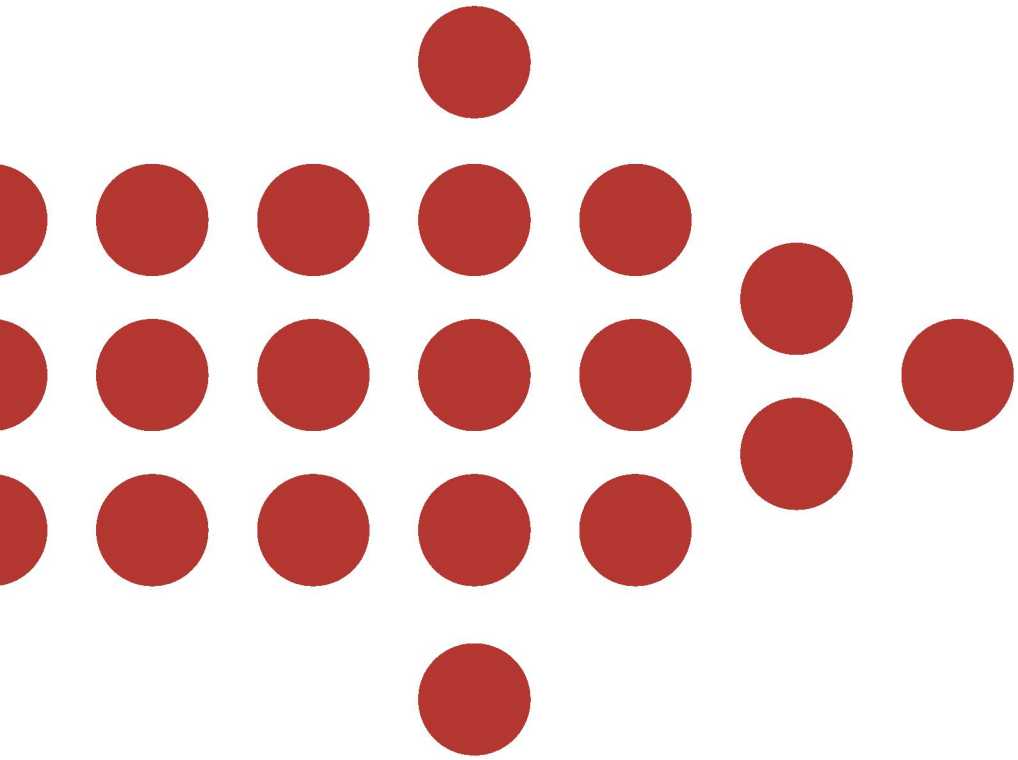
REFERENCIAS WEB DE PUBLICACIONES ESPECIALIZADAS

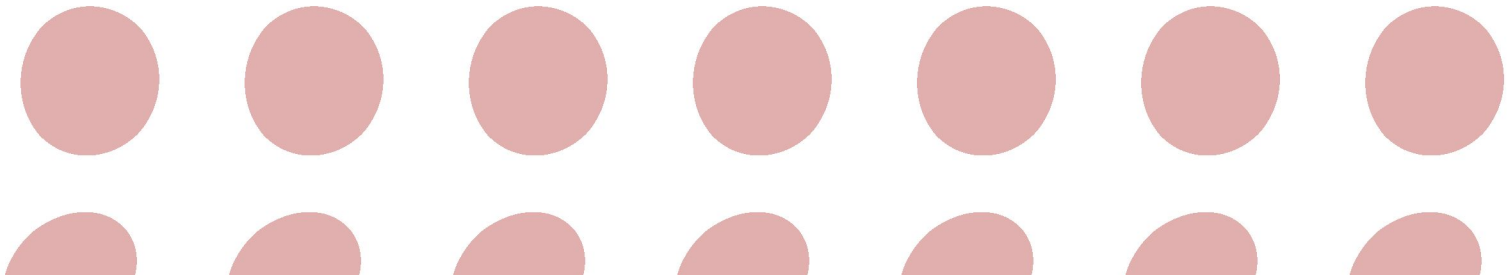
ORGANISMO	LOCALIZACIÓN DE LA INFORMACIÓN	COMENTARIOS
Lex Nova: La Revista	**www.lexnova.es**	Lex Nova ofrece una revista de contenido jurídico con las últimas novedades sobre legislación, proyectos de ley, resoluciones judiciales y práctica jurídica, incluyendo artículos de actualidad sobre los temas más candentes de la realidad jurídica.
Ars Technica	**www.arstechnica.com**	Revista especializada en noticias y artículos novedosos, análisis de tendencias tecnológicas y consejo de expertos en temas que van desde los aspectos tecnológicos fundamentales a los diferentes modos en los que la tecnología nos ayuda a disfrutar del mundo que nos rodea.
Baquia Magazine	**www.baquia.com**	Emprendedores, personas interesadas en los negocios y los directivos de empresas son el público que configura la comunidad de www.baquia.com, gracias a ellos y a multitud de colaboradores actualmente Baquia se ha convertido en una plataforma de generación de contenidos multimedia especializados en las TIC.
IDP: Revista de Internet, Derecho y Política	**www.ouc.edu/idp**	Revista de Internet, Derecho y Política que pretende ser una plataforma de reflexión y discusión sobre el contenido y alcance de los cambios que las tecnologías de la información y la comunicación -y, en particular, el fenómeno de Internet- conllevan en los campos del derecho, la política y la Administración pública.

ORGANISMO	LOCALIZACIÓN DE LA INFORMACIÓN	COMENTARIOS
Revista General de información y documentación	**www.eubd.ucm.es**	La Revista General de Información y Documentación que realiza la Escuela Universitaria de Biblioteconomía y Documentación y publica el Servicio de Publicaciones de la UCM, tiene periodicidad semestral, y fue fundada en el año 1992. Sus secciones son Estudios, Informes, Notas, Varía y Reseñas. Acepta trabajos en las lenguas oficiales de España e inglés, francés e italiano.
AR: Revista de Derecho Informático	**www.alfa-redi.org**	AR es la publicación digital editada en Hispanoamérica, de mayor continuidad y relevancia en temas de Políticas y Marco Regulatorio de la Sociedad de la Información. AR es un instrumento para el desarrollo de doctrina, legislación y jurisprudencia en la región.
Datospersonales.org	**www.datospersonales.org**	La revista de la Agencia de Protección de Datos de la Comunidad de Madrid.
Saberes	**www.uax.es/publicaciones/saberes**	La Unidad de Publicaciones Electrónicas colabora con el Rectorado de la Universidad Alfonso X el Sabio y con su Comisión de Investigación facilitando un vehículo para difundir la producción científica de profesores y alumnos, así como la de otros colaboradores, a través de la organización de las diferentes secciones que comprenden sus revistas electrónicas especializadas.

DATOS PERSONALES EN LA RED

ANEXO V: REFERENCIAS BIBLIOGRAFICAS





ANEXO V: REFERENCIAS BIBLIOGRAFICAS

- Álvarez Marañón, Gonzalo. "Mecanismos de Seguridad." CSIC.
- Auditoria Sistemas. "Listas de exclusión y otras novedades en el desarrollo del reglamento de la LOPD de 2007". 2008. einnova. <http://www.auditoriasistemas.com>.
- Battaner, Santiago. "Intimidad, privacidad y protección de datos de carácter personal." Baquia Magazine: Baquia Knowledge Center, 2006.
- Blanco Losada, Luisa Ana. "Elaboración e implantación del Plan de Protección de Datos del Ayuntamiento de Madrid." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2007.
- Bru Cuadrada, Elisenda. "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad." IDP: Revista de Internet, Derecho y Política 2007.
- Bufete Alberto Picón. "Beneficios del cumplimiento de la normativa de protección de datos personales." Navactiva, 2005.
- "Las agencias autonómicas de protección de datos personales." Navactiva, 2005.
- Cámara de Navarra de Comercio e Industria. "¿Hasta que punto le afecta a una pyme la normativa de protección de datos?": Novactiva, 2004.
- Consejo Regional de Cámaras de Castilla y León. "Manual Práctico de Firma Electrónica." Ed. Consejo Regional de Cámaras de Castilla y León: Junta de Castilla y León.
- Costa Carballo, Carlos Manuel da. "Algunas cuestiones jurídicas relativas a la documentación automatizada: cofidencialidad y protección de los datos." Revista general de información y documentación 1992: 17-50.
- Elizburu Garayoa, Idoia. "LOPD, la primera herramienta para la seguridad en la empresa." Navactiva, 2007.
- Fernández Gómez, Fernando. "Ingenieria Social." Boletín del Criptonomicón.72 (2000).
- Fleischer, Peter. "Data Protection on the Internet." Ed. Justice and Home Affairs European Parliament Committee on Civil Liberties, 2008.
- Fronteras Electrónicas. "Privacidad en Internet." Biblioweb de SinDominio, 1998.

✓ Fundetec. "Antonio Silván Rodríguez." Boletín Fundetec Enero-Marzo,2008 2008.

✓ "Fundetec reúne a los responsables autonómicos de promocionar la Sociedad de la Información entre las pymes." Boletín Fundetec Enero-Marzo,2008 2008.

✓ Informe de Seguridad de la PYME europea y española 2007: Fundetec, 2007.

✓ Hernández i Moreno, Josep Xavier et al. "Reflexiones en torno a la protección de los datos de carácter personal." Nuevas Politicas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas 2005: 21-45.

✓ Herrera Bravo, Rodolfo. "La protección de datos personales como garantía básica de los derechos fundamentales." Derechos Humanos. Órgano Informativo de la Comisión de Derechos Humanos del Estado de México Enero-Febrero,2005 2005.

✓ "Privacidad e Internet: El problema del tratamiento invisible y automatizado de datos personales." Derechos Humanos. Órgano Informativo de la Comisión de Derechos Humanos del Estado de México Enero-Febrero, 2005 2005.

✓ INE. Encuesta sobre el uso de TIC y Comercio Electrónico en las empresas 2006/2007: Instituto Nacional de Estadística, 2007.

✓ Informationsfreiheit, Der Bundesbeauftragte für den Datenschutz und. "Resolución sobre la necesidad urgente de normas internacionales para proteger los datos de pasajeros que usarán los gobiernos a los efectos de la aplicación de la ley y la seguridad en las fronteras." 29ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Montreal, Canadá: Office of the Privacy Commissioner of Canada, 2007.

✓ Lanzos Sanz, Antonio. "España: La Protección Jurídica de los Datos de Carácter Personal del Internauta." AR: Revista de Derecho Informático 2003.

✓ López Carmona, Francisco José. "La protección de datos personales y el Registro de Ficheros en la Agencia de Protección de Datos Personales de la Comunidad de Madrid." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2006.

✓ Lorza González, José Ramón de. "Protección de datos de carácter personal." El Graduado: Boletín Informativo del Ilustre Colegio Oficial de Graduados Sociales de Madrid 2005: 18-25.

✓ Martínez Candano, Beatriz. "El papel de las Agencias de Protección de Datos Autonómicas." Monografías.com, 2006.

✓ Observatorio de la Seguridad de la Información. "Protección de Datos de Carácter Personal." Guías Legales: INTECO.

✓ Peso Navarro, Emilio del. "El Proyecto de Reglamento Único de la Ley de Protección de Datos." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2005.

✓ Piñar Mañas, José Luis. "Los retos de la Administración Electrónica: especial referencia a la protección de datos de carácter personal." Libro marrón, Círculo de Empresarios 2007: 281-300.

✓ Poullet, Yves, and Jean-Marc Dinant. "Hacia nuevos principios de protección de datos en un nuevo entorno TIC." IDP: Revista de Internet, Derecho y Política 2007.

✓ Pérez i Velasco, Maria del Mar. "Intercambio de datos entre administraciones públicas." IDP: Revista de Internet, Derecho y Política 2006.

✓ "Quíen espía nuestro pasos en Internet." iWorld 2000.

✓ Rodrigo i Díaz, Alfred. "La independencia de las Agencias de Protección de Datos." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2006.

✓ Rodríguez Carballo, Alvaro M. "La protección de datos en la Administración Pública de Galicia." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2005.

✓ Rodríguez, Joaquín A. "Delitos y seguridad informática. Aplicación de la Ley Orgánica de Protección de Datos Personales (LOPD)." Mapping 2002: 42-49.

✓ Rojas Pozo, José Luis. "La Constitución Europea y la protección de datos personales." Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid 2005.

DATOS PERSONALES EN LA RED

Junta de Castilla y León

ORSI.ES

Estrategia Regional para la Sociedad Digital del Conocimiento de Castilla y León (ERSDI)