GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía para entidades locales: cómo adaptarse a la normativa sobre protección de datos

En colaboración con:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

El Observatorio de la Seguridad de la Información es un referente nacional e internacional al servicio de los ciudadanos, empresas y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Datos de contacto:
Instituto Nacional de Tecnologías de la Comunicación (INTECO)
Observatorio de la Seguridad de la Información
Avda. José Aguado, 41. Edificio INTECO. 24005 León
Teléfono: +(34) 987 877 189 / Email: observatorio@inteco.es
www.inteco.es

Depósito Legal: LE - 316 - 2009
Imprime: gráficas CELARAYN, s.a.

Índice

1. Contexto y destinatarios de la guía

Esta guía tiene como propósito ofrecer información práctica y recomendaciones para la adaptación de las Entidades Locales a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante, LOPD) y, en especial, a su Reglamento de Desarrollo (en adelante RDLOPD), en vigor desde abril de 2008.

El objetivo último es acercar a las Entidades Locales (en adelante, EELL) el contenido de la normativa en materia de protección de datos de carácter personal, para determinar los procesos de adaptación a la LOPD y RDLOPD.

1.1. BENEFICIOS QUE APORTA EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

1.1.1. COMPROMISO DE LAS EELL CON LOS DERECHOS FUNDAMENTALES

En el compromiso de las EELL con el cumplimiento de la Constitución Española se encuentra el derecho fundamental de la protección de datos personales, que se concreta en el cumplimiento de la LOPD y del RDLOPD.

La LOPD garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente su honor, intimidad y privacidad personal y familiar.

El Reglamento de Desarrollo de la LOPD, aprobado mediante el Real Decreto 1720/2007, actualiza esta norma de alto rango, adecuando su ámbito a las prácticas y riesgos actuales a los que se encuentran expuestos los datos de los ciudadanos. Una de las principales novedades que aporta el Reglamento, que sustituye al anterior de 1999, es que su alcance comprende tanto los ficheros en soporte informático como los archivos documentales.

1.1.2. CALIDAD EN LA GESTIÓN ADMINISTRATIVA DE PROCESOS BASADOS EN LAS TIC Y SUELO INDISPENSABLE PARA EL DESARROLLO FUTURO DE LA LEY 11/2007

Entre los beneficios para las EELL de la implantación de las medidas exigidas, además de dar cumplimiento a la Ley, estarían los siguientes:

- Implica una **protección adecuada de los datos personales** que evita su mal uso, deterioro, acceso no autorizado o pérdida.

- **Mejora la calidad** en la gestión administrativa de procesos basados en las TIC.

- Genera un **fondo imprescindible para el desarrollo de la adaptación a la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos**. Esta Ley tiene entre sus objetivos la creación de las condiciones de confianza en el uso de las tecnologías. Al mismo tiempo, establece las medidas necesarias para la preservación de la integridad de los derechos fundamentales y, en especial, los relacionados con la intimidad por medio de la garantía de seguridad de los sistemas, datos y comunicaciones.

Las Administraciones Públicas Locales, en consecuencia, deberán garantizar, a partir de 2010, el principio de igualdad y accesibilidad a los servicios prestados de manera electrónica, pero también la seguridad y la privacidad de los datos y de las comunicaciones con los ciudadanos y empresas.

De esta forma, el respeto a la normativa vigente de protección de datos se convierte en un asunto crítico para la aplicación efectiva de la Ley 11/2007 por los Gobiernos Locales.

1.1.3. EL PAPEL DE LAS EELL COMO EJEMPLO PARA EL ENTORNO

El cumplimiento de la LOPD por parte de las Entidades Locales debe servir como **referencia para su entorno de influencia**, siendo ejemplo de cumplimiento y origen de difusión y concienciación de la protección de los datos personales.

1.2. DESTINATARIOS DE LA GUÍA

La guía esta dirigida a los Ayuntamientos, Entidades Supramunicipales, Diputaciones, Consells y Cabildos Insulares. En consecuencia, los destinatarios de esta guía son:

- Los Alcaldes, Concejales, Presidentes y Diputados.
- Los Secretarios, Tesoreros e Interventores.
- Los coordinadores de protección de datos de Ayuntamientos y mancomunidades, consultores tecnológicos, responsables de informática y asesores jurídicos de la Administración Local.

En la elaboración de los contenidos de esta guía se ha pensando en especial en aquellas Entidades de pequeño y mediano tamaño.

Su Ayuntamiento o Entidad Local, ¿cuenta con una política de tratamiento de datos eficaz y conforme a ley?

El establecimiento de una política de protección de datos personales no sólo atañe a los responsables de seguridad, que suelen ser profesionales de perfil informático, sino que requiere la implicación y el compromiso de los técnicos responsables de las Áreas.

Es clave la decisión y voluntad de los responsables políticos de la Entidad.

Los responsables de una Entidad Local deberán evidenciar su compromiso con la LOPD, mediante el establecimiento e implantación de un **plan para la adaptación a la normativa sobre protección de datos**. Este plan deberá tener en cuenta los siguientes aspectos:

- Establecer una **planificación realista** de adaptación al RDLOPD.
- Elaborar el **Documento de Seguridad** (o actualizarlo, en caso de que ya exista), describiendo claramente los objetivos, alcance y nivel de los ficheros afectados, la organización de la protección de datos en la Entidad y las medidas de seguridad a implementar.
- Identificar explícitamente los **roles y responsabilidades** de los usuarios y los técnicos en materia de protección de datos, ya se trate de personal interno o de colaboradores externos.
- Facilitar los **recursos materiales, técnicos y humanos** necesarios para la debida implantación de las medidas de seguridad requeridas por el RDLOPD.
- Comunicar y **dar formación** a todos los usuarios y técnicos que acceden a los datos de carácter personal de la Entidad.

El cumplimiento de la LOPD es responsabilidad de todos

El respeto a los principios de protección del honor, la intimidad y la privacidad personal y familiar de los ciudadanos por las Entidades Locales es de suma importancia.

Las consecuencias de su incumplimiento implican responsabilidades para la Entidad y para el personal (interno o colaboradores externos) que accede a los datos de carácter personal.

2. Marco legal

El marco legal en materia de protección de datos responde a la necesidad de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor, intimidad y privacidad personal y familiar. Se trata de evitar que los datos sean utilizados de forma inadecuada o fraudulenta, o sean tratados o cedidos a terceros sin consentimiento inequívoco del titular.

A nivel europeo, **la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995** constituye un texto de referencia en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los datos.

A nivel estatal, la Sentencia 292/2000, de 30 de Noviembre de 2000 del Tribunal Constitucional señala que el derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE (con quien comparte el objetivo de ofrecer una protección constitucional de la vida privada personal y familiar) atribuye a su titular el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley. Esta Ley, conforme al art. 18.4 CE, debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad del derecho fundamental a la protección de datos respecto del de la intimidad radica en su distinta función, lo que implica que también su objeto y contenido difieran:

- La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8).

- En cambio, **el derecho fundamental a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado**.

En 1992 nace la **Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD),** que regula de forma específica la materia de protección de datos. Su ámbito de aplicación se circunscribe a los ficheros de carácter automatizado, estableciendo el derecho de información y acceso a los datos, el derecho de rectificación y cancelación, los principios relativos a la calidad de los datos, a la información sobre su recogida, el consentimiento, la seguridad y la cesión de los mismos. Esta norma sienta una serie de garantías y derechos dentro de un marco normativo nacional.

En 1999 se aprueba la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), norma que deroga la LORTAD y que tiene como finalidad principal transponer a la normativa nacional la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Como principal novedad, la LOPD introduce en su ámbito de aplicación los ficheros no automatizados o ficheros manuales[1], centrando toda su protección en el tratamiento de datos de carácter personal sea cual sea el soporte o medio de su tratamiento, con el fin de proteger los derechos fundamentales y libertades públicas de los ciudadanos.

1 Ficheros manuales o ficheros en papel.

Operativamente, la Ley se apoya en el **Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal**, aprobado por Real Decreto 994/1999 de 11 de junio y publicado en el BOE de 25 de junio de 1999. El Reglamento constituye un instrumento para facilitar los mecanismos prácticos de cumplimiento de las prescripciones establecidas en la LOPD, cuyo nuevo **Reglamento de Desarrollo ha sido aprobado por Real Decreto 1720/2007 de 21 de diciembre**. Este Reglamento, en vigor desde el 19 de abril de 2008, deroga al anterior, y articula, entro otras, las siguientes novedades:

- Se aplica también a los ficheros y tratamientos no automatizados (manuales) y se fijan criterios específicos sobre las medidas de seguridad de los mismos.

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

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

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

3. Principios básicos de la protección de datos de carácter personal

Calidad, secreto y seguridad de los datos, información en la recogida y consentimiento del afectado son principios básicos dispuestos en los artículos 4, 5 y 6 de la LOPD

3.1. CALIDAD DE LOS DATOS

Se debe perseguir la calidad de los datos, de forma que se garantice el uso adecuado de los mismos, sin que puedan ser utilizados para finalidades incompatibles con aquellas para las que hubieran sido recabados. Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Este principio de calidad garantiza además que los datos sean exactos y estén actualizados y que no se mantendrán indefinidamente sin justificación. **Los datos deberán ser tratados de forma leal y lícita.**

En el caso de que alguna obligación legal establezca la necesidad de conservar los datos una vez concluida la finalidad que motivó su recogida, el responsable del fichero sólo podrá conservarlos previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el RDLOPD[2].

2 El bloqueo de los datos consiste en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos. (art. 5.1 b) RDLOPD)

3.2. INFORMACIÓN EN LA RECOGIDA DE DATOS

El afectado será informado, en el momento en el que se recaben sus datos, del alcance del tratamiento que se va a realizar. El art.5 LOPD establece lo siguiente:

> *Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
>
> a. *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
>
> b. *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
>
> c. *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
>
> d. *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
>
> e. *De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

Este principio de información se debe incorporar de manera legible en formularios, cupones, cuestionarios o impresos, tanto automatizados como manuales, en los que se proceda a la recogida de datos. Además se incorporará en los contratos que se suscriban, con la finalidad de informar sobre el tratamiento que se va a realizar de los datos de clientes, proveedores o personal laboral. Se incluirán de igual forma en los procesos de convocatorias de oposiciones y licitaciones. Hay que tener en cuenta que el consentimiento se considera nulo en el caso de que en el contrato se incorporen consentimientos no relacionados con la finalidad principal que no sean destacados de forma adecuada.

Este principio de información constituye un elemento estratégico y debe existir siempre, aun cuando no quepa consentimiento. Prueba de su importancia está en la acreditación del mismo recogida en el art. 18 del RDLOPD, que establece lo siguiente:

> *El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.*

3.3. CONSENTIMIENTO DEL AFECTADO

El consentimiento del afectado implica la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales.

Tal y como señala la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el consentimiento no será preciso en los siguientes casos:

- Cuando los datos de carácter personal se recojan para el **ejercicio de las funciones propias de las Administraciones Públicas** en el ámbito de sus competencias.
- Cuando se refieran a las **partes de un contrato o precontrato** de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de los datos tenga por finalidad proteger un **interés vital del interesado** en los términos del artículo 7 apartado 6 de la Ley.
- Cuando los datos figuren en **fuentes accesibles al público** y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen

los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

3.4. DATOS ESPECIALMENTE PROTEGIDOS

Este principio hace referencia a datos de carácter personal que revelan la ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y comisión de infracciones penales o administrativas.

3.5. SEGURIDAD DE LOS DATOS

Todas las empresas, organizaciones, asociaciones e instituciones, públicas y privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal, deben aplicar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

3.6. DEBER DE SECRETO

Este principio recoge las obligaciones de secreto, confidencialidad y custodia que incumben a todo el personal y, de manera particular, a aquellos que en el desarrollo de sus funciones accedan a ficheros que contienen datos personales.

3.7. COMUNICACIÓN DE DATOS

Se entiende por comunicación de datos toda revelación de datos realizada a una persona distinta del afectado o interesado. Los datos de carácter perso-

nal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

3.8. ACCESO POR CUENTA DE TERCEROS

Supone la prestación de un servicio al responsable del fichero por parte de una tercera empresa denominada Encargado del Tratamiento, que accede a los datos del fichero para el cumplimiento de la prestación contratada, actuando en nombre, por cuenta y de acuerdo a las instrucciones establecidas por el Responsable del Fichero.

4. Agentes y organismos implicados

4.1. PRINCIPALES AGENTES[3]

- **Afectado / interesado**: es la persona física titular de los datos que serán objeto del tratamiento. En el caso que nos ocupa, los afectados serían los ciudadanos cuyos datos están siendo tratados por la Entidad Local.

- **Responsable de fichero o tratamiento**: la Entidad local que decide sobre la finalidad, contenido y uso del tratamiento se considera responsable del fichero.

- **Encargado de tratamiento**: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero (que en este caso será la Entidad Local).

- **Cesionario de datos**: persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

- **Responsable de seguridad**: persona/s a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- **Usuario**: persona autorizada para acceder a datos o recursos.

4.2. ORGANISMOS IMPLICADOS

A nivel nacional, la Agencia Española de Protección de datos es el ente encargado de velar por el cumplimiento de la normativa sobre la protección de datos. Además, las comunidades autónomas de Madrid, Cataluña y el País Vasco disponen a su vez de Agencias de ámbito autonómica. Las competencias de las agencias autonómicas versan sobre los ficheros

3 El Anexo II incluye un Glosario que profundiza en las definiciones de los agentes implicados y conceptos referentes a la protección de datos.

de titularidad pública creados o gestionados por la Comunidad Autónoma, 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.

4.2.1. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, que son las siguientes:

- 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.
- Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
- Atender las peticiones y reclamaciones formuladas por las personas afectadas.
- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
- Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

- Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
- Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
- Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
- Redactar una memoria anual y remitirla al Ministerio de Justicia.
- Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
- Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46 de la Ley respecto de las infracciones de las Administraciones Públicas.
- Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Agencia Española de Protección de Datos
www.agpd.es

4.2.2. AGENCIA CATALANA DE PROTECCIÓN DE DATOS

Tiene, respecto de su ámbito de actuación, las competencias de registro, control, inspección, sanción y resolución, y también la adopción de propuestas e instrucciones. Estas competencias se concretan en las funciones siguientes:

- Velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal y controlar su aplicación, especialmente aquello que hace referencia a los derechos de información, acceso, rectificación, cancelación y oposición.

- Velar por el cumplimiento de las disposiciones que la Ley de Estadística de Cataluña dispone con respecto a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, salvo aquello que hace referencia a las transferencias internacionales de datos. A estos efectos, la Agencia, dentro de su ámbito de competencias, puede adoptar instrucciones y resoluciones dirigidas en los órganos administrativos y solicitar la colaboración del Instituto de Estadística de Cataluña.

- Dictar, sin perjuicio de competencias de otros órganos, las instrucciones necesarias para adecuar los tratamientos personales a los principios de la legislación en materia de protección de datos de carácter personal.

- Requerir a los responsables y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal y, si ocurre, ordenar el cese de los tratamientos y la cancelación de los ficheros, excepto lo que hace referencia a las transferencias internacionales de datos.

- Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

Agencia Catalana de Protección de Datos
www.apdcat.net

4.2.3. 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.

Las funciones de la Agencia se detallan a continuación:

- Velar por el cumplimiento de la legislación en materia de protección de datos y controlar su aplicación.

- Ejercer labores informativas, encaminadas a facilitar a las personas el conocimiento de sus derechos en materia de protección de datos.

- Dar trámite a las peticiones y reclamaciones formuladas por los ciudadanos en el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en relación con los ficheros sobre los que la Agencia Autonómica de la Comunidad de Madrid tiene atribuidas competencias.

- Dictar, en su caso, las instrucciones que sean necesarias para adaptar los tratamientos de datos de carácter personal a los principios de la normativa aplicable en materia de protección de datos.

- Adoptar las medidas que resulten de aplicación, para que los responsables de los ficheros adapten los tratamientos de datos de carácter personal a la normativa vigente en materia de protección de datos.

- Ordenar la inmovilización de los ficheros que no se ajusten a las disposiciones legales en materia de protección de datos.

Agencia de Protección de Datos de la Comunidad de Madrid
www.madrid.org/apdcm

4.2.4. AGENCIA VASCA DE PROTECCIÓN DE DATOS

Tiene la consideración de autoridad de control, y la ley le garantiza la plena independencia y objetividad en el ejercicio de sus funciones.
Las funciones principales de la Agencia se detallan a continuación:

- 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.

- Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la legislación vigente en materia de protección de datos.

- Atender las peticiones y reclamaciones formuladas por los afectados.

- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

- Requerir a los responsables y a los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a dicha legislación, salvo en la que se refiera a transferencias internacionales de datos.

- Ejercer la potestad sancionadora y, en su caso, proponer la iniciación de procedimientos disciplinarios contra quienes estime responsables de las infracciones tipificadas en el artículo 22 de la ley, así como adoptar las medidas cautelares que procedan, salvo en lo que se refiera a las transferencias internacionales de datos. Todo ello en los términos previstos en la ley.

- Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará anualmente una relación de dichos ficheros con la información adicional que el director de la Agencia Vasca de Protección de Datos determine.

- Velar por el cumplimiento de las disposiciones que la legislación sobre la función estadística pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 24.

- Colaborar con la Agencia de Protección de Datos del Estado y entidades similares de otras comunidades autónomas en cuantas actividades sean necesarias para una mejor protección de la seguridad de los ficheros de datos de carácter personal y de los derechos de los ciudadanos en relación con los mismos.

- Atender a las consultas que en materia de protección de datos de carácter personal le formulen las Administraciones Públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de la ley.

Agencia Vasca de Protección de Datos
www.avpd.euskadi.net

5. Ficheros incluidos en el ámbito de aplicación de la LOPD

Los ficheros de datos de carácter personal en soporte informático no presentan grandes dudas, puesto que para su creación se exige, con carácter previo, la grabación, depuración y estructuración del conjunto de datos que forman parte del fichero.

En cuanto a los ficheros manuales, para poder determinar que los datos registrados son susceptibles de tratamiento, y en consecuencia, se encuentren incluidos en el ámbito de aplicación de la LOPD, hay que atender a los siguientes requisitos:

- Que el tratamiento se refiera a datos de carácter personal comprendidos en un fichero en soporte no automatizado.

- Que dichos datos se encuentren estructurados u ordenados conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

¿Qué ficheros se regirán por sus disposiciones específicas y por la LOPD?

- Los ficheros regulados por la legislación de régimen electoral.
- Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
- Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las fuerzas armadas.
- Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.
- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

¿Qué ficheros quedan exentos de la aplicación de la LOPD?

- Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- Los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

6. Fases de implantación de la LOPD

Las obligaciones que establece la LOPD son de aplicación a todas las EELL, independientemente de su tamaño, siempre que almacenen y traten datos de carácter personal en sus sistemas de información.

Esas obligaciones se concretan en unos principios de cumplimiento básico que integran las fases de implantación, que son:

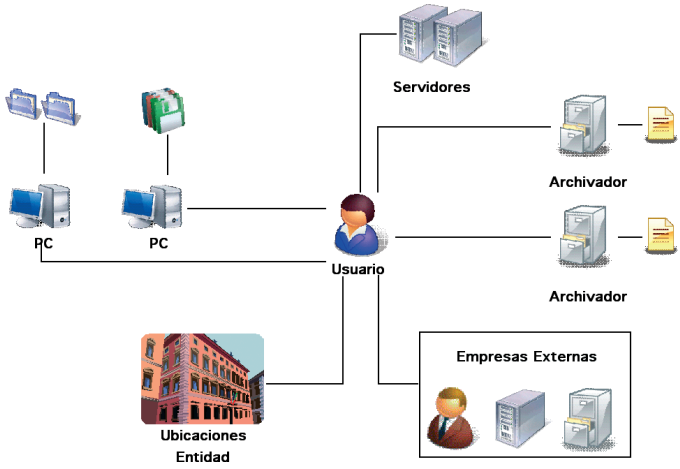
- Adaptación de los ficheros.
- Legitimación de datos de carácter personal.
- Protección: políticas de seguridad de los datos.

Fases de implantación de la LOPD en EELL

7. Fase I: Adaptación de los ficheros

En el ejercicio de sus competencias, las EELL realizan una serie de funciones o actividades que generan la recogida y el tratamiento de datos personales, en ficheros automatizados y no automatizados, relativos a diferentes colectivos: ciudadanos, empleados, etc.

Almacenamiento de datos personales en EELL



Una Entidad Local está obligada a notificar la creación de los ficheros para su inscripción ante el Registro General de Protección de Datos[4] (Art. 55 RDLOPD: Notificación de ficheros) siempre que se encuentren dentro del alcance de aplicación del RDLOPD, independientemente de la estructura de las bases de datos utilizadas.

4 Órgano de la AEPD al que corresponde velar por la publicidad de los ficheros y tratamientos de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos.

El plazo de inscripción de los ficheros es de 30 días desde la publicación en el Boletín Oficial del Estado o Diario Oficial del acuerdo de creación, modificación, o supresión del fichero por el organismo público correspondiente.

Las Agencias Autonómicas serán de referencia para todas aquellas EELL de la autonomía correspondiente; es decir, cada Entidad deberá declarar los ficheros con datos de carácter personal a su correspondiente Agencia autonómica, en su caso. Una vez realizada la declaración, la Agencia autonómica inscribirá de oficio los ficheros ante la AEPD, con el fin de velar por la publicidad y calidad del Registro General de Protección de Datos.

El proceso de inscripción ante la AEPD incluye las fases siguientes, que se analizarán en detalle en los siguientes epígrafes:

- Identificar e inventariar los ficheros.
- Formalizar el trámite de disposiciones públicas.
- Cumplimentar el formulario para la declaración de ficheros.

7.1. IDENTIFICACIÓN E INVENTARIO DE FICHEROS

La primera tarea que deben llevar a cabo las EELL es la identificación de los colectivos cuyos datos están siendo tratados por la Entidad. A título de ejemplo, estos colectivos pueden ser:

- Ciudadanos.
- Empleados.
- Personas afectadas por actividades de gestión de manera indirecta, multas o trámites específicos de carácter puntual.

De estos colectivos, se obtiene información de diferente naturaleza: datos identificativos (nombre, dirección...), datos fiscales (bancarios, AEAT,…), datos comerciales o aquellos datos relativos a afiliación sindical.

Identificados los colectivos sobre los que la EELL recabará información, se debe localizar dónde se encuentran los datos, teniendo en cuenta que la información puede ser almacenada en ficheros automatizados, no automatizados o manuales, y mixtos.

Hecho esto, se definirá cada fichero de manera clara y ordenada, recogiendo todos aquellos datos que se obtienen de cada colectivo, (identificativos, fiscales, etc.), para continuar con el proceso de declaración.

7.2. FORMALIZACIÓN DEL TRÁMITE DE DISPOSICIONES PÚBLICAS

La Ley obliga a todas las EELL, independientemente de su tamaño y personalidad jurídica, a la inscripción de los ficheros de carácter personal ante el Registro General de Protección de Datos.

En el caso de aquellos organismos de titularidad pública, la Ley puntualiza que la notificación de los ficheros ante el Registro General de Protección de Datos sólo podrá hacerse previa disposición general, publicada en el Boletín Oficial o Diario Oficial, ya sea del Estado o de la Comunidad Autónoma correspondiente.

Una buena práctica, cuando sea viable, es elaborar un **proyecto de ordenanza** que refleje la creación, modificación o supresión de ficheros de carácter personal.

El proyecto constará de dos partes:

- El desarrollo de la ordenanza propiamente dicha, donde se explique de manera clara la finalidad de la publicación y las medidas de seguridad a adoptar respecto a los ficheros de datos personales.
- Anexos por cada fichero de carácter personal que deba crear el organismo, detallando la siguiente información obligatoria:
    - La **identificación del fichero o tratamiento**, indicando su denominación, la descripción de su finalidad y los usos previstos.
    - El **origen de los datos**, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
    - La **estructura básica del fichero** mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
    - Las **comunicaciones de datos previstas**, indicando, en su caso, los destinatarios o categorías de destinatarios.
    - Las **transferencias internacionales de datos previstas** a terceros países, con indicación, en su caso, de los países de destino de los datos.
    - Los **órganos responsables** del fichero.
    - Los servicios o unidades ante los que pudiesen ejercitarse los derechos de **acceso, rectificación, cancelación y oposición**.
    - El **nivel básico, medio o alto** de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del RDLOPD.

Se publicará en el Boletín Oficial del Estado o Diario Oficial, para formalizar el trámite de disposiciones públicas exigido por la Agencia de Protección de Datos.

La inscripción de ficheros deberá encontrarse actualizada en todo momento. Así, cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55 del RDLOPD.

Tratándose de ficheros de titularidad pública, cuando se pretenda la supresión del fichero o la modificación que afecte a alguno de los requisitos previstos en el artículo 55, deberá haberse adoptado, con carácter previo a la notificación, la correspondiente norma o acuerdo en los términos previstos en los artículos 52 a 54 del capítulo I del Título V del RDLOPD.

De otro lado, una de las novedades del RDLOPD es el sistema de tratamiento de datos. En este sentido, se establece en el Reglamento de Desarrollo de la LOPD que la notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte/s empleados para el tratamiento de los datos. Así, cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación.

Ejemplo de Disposición Pública a elaborar por las EELL

Ordenanza aprobada por el Pleno de la Corporación Municipal, sesión celebrada el día …. de …. de ….
Por la parte que se aprueba la creación (modificación o supresión) de los ficheros de datos de carácter personal del Ayuntamiento de…
Primero: Creación de ficheros (Modificación o Supresión).

Se crean en este Ayuntamientos los ficheros de datos de carácter personal señalados en el Anexo I.
Segundo: Medidas de seguridad.
Los ficheros, independientemente del soporte en que se encuentren, que por la presente Ordenanza se crean, cumplen las medidas de seguridad establecidas en el RD 1720/2007 de 21 de Diciembre, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros que contengan datos de carácter personal. (En caso de supresión de ficheros: motivo de la supresión, destino de los mismos y, en su caso, destrucción)
Tercero: Publicación.
De conformidad con… se ordena que la presente Ordenanza sea publicada en el Boletín Oficial de…
Cuarto: Entrada en vigor.
La presente ordenanza entrará en vigor al día siguiente de su publicación en el Boletín Oficial de…

ANEXO I

Fichero: (Nombre Fichero)
1. Identificación del fichero o tratamiento, indicando su denominación, finalidad y usos previstos.
2. Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
3. Estructura básica del fichero, con descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
4. Comunicaciones de datos previstas, indicando, en su caso, los destinatarios o categorías de destinatarios.
5. Transferencias internacionales de datos previstas, con indicación, en su caso, de los países de destino de los datos.
6. Órganos responsables del fichero.
7. Servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
8. El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del RDLOPD.

ANEXO n (un anexo para cada fichero)

7.3. FORMULARIO PARA LA DECLARACIÓN DE FICHEROS

La Entidad, mediante disposición pública, habrá notificado en el Boletín Oficial correspondiente o Diario Oficial la creación, modificación, y cancelación de ficheros de carácter personal, trámite exigido por Ley a todos aquellos organismos de titularidad pública[5] con carácter previo a la declaración del fichero mediante el formulario NOTA

En este sentido, el RDLOPD establece en su artículo 54.1.c lo siguiente, refiriéndose a la declaración de un fichero público:

> *La disposición o acuerdo de creación del fichero deberá contener entre otros extremos: la estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.*

En este sentido se entiende por sistema de tratamiento el modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

El formulario NOTA es el sistema de Notificaciones Telemáticas a la Agencia Española de Protección de Datos que permite a los responsables de ficheros con datos de carácter personal cumplir con la obligación de notificar sus ficheros ante la Agencia Española de Protección de Datos.

---

*5 Como señala el art. 55.1 del RDLOPD: **"Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente**".*

Es una herramienta fácil e intuitiva que ayuda a los responsables de ficheros en el proceso de notificación[6].

Obtención del formulario NOTA a través de www.agpd.es

El formulario electrónico NOTA consta de dos partes:

- **Formulario de notificación de ficheros**, en el que se facilitan datos del tipo: responsable del fichero, origen y finalidad de los datos tratados, nivel de seguridad aplicable al fichero, Boletín Oficial o Diario de la Provincia en el que se realizó el trámite de disposición pública, etc.

---

*6 El artículo 130.3 del RDLOPD establece que: **"La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita. Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia"***

- **Formulario hoja de solicitud**, que recoge únicamente los datos del responsable, o persona con capacidad legal que efectúa la notificación de los ficheros ante el Registro General de Protección de Datos.

Ambas partes ofrecen el mismo aspecto visual de un formulario en soporte papel pero en formato electrónico PDF y pueden ser cumplimentados desde el sitio web de la AEPD o archivar el documento en el equipo y cumplimentarlo mediante un programa de lectura del formato PDF.

Como primer paso se ha de **rellenar el formulario de Notificación**, que permite optar por dos modelos de declaración:

- **Declaración tipo:** mediante esta opción del formulario electrónico, se pueden declarar ficheros de titularidad pública de forma rápida y simplificada, ya que la notificación está precumplimentada parcialmente para ficheros relacionados con la gestión de los de recursos humanos, gestión del padrón, gestión económica o control de acceso. Si el responsable considera que la declaración tipo no se ajusta parcialmente a los requerimientos propios de la Entidad en cuestión, puede realizar algunos cambios añadiendo datos específicos.

- **Declaración normal:** en el caso de que la declaración tipo no se adapte al fichero que el responsable pretende notificar, deberá optar por este formato de declaración, donde se presenta un formulario vacío.

Realizados los apartados de la notificación, se recomienda guardar los cambios efectuados antes de pasar a la siguiente fase: cumplimentar la Hoja de Solicitud que nos facilita el sistema.

El sistema de NOTA se puede presentar ante el registro a través de los siguientes medios: Internet, con y sin firma electrónica, y formulario impreso en papel. A continuación se describen estos medios por la diferente casuística que encierra cada uno de ellos:

- **Internet con certificado:** la Agencia Española de Protección de Datos pone a disposición de los responsables la notificación de los ficheros a través de Internet con una firma electrónica[7].

  Cumplimentada la Notificación y la Hoja de Solicitud por parte del responsable, o persona con representación suficiente para el tratamiento del fichero, será necesario proceder a la firma electrónica del formulario NOTA para su envío.

  Una vez firmado, se enviará automáticamente al Registro Telemático de la Agencia Española de Protección de Datos, creado mediante Resolución de la Agencia de 12 de julio de 2006, para la remisión de solicitudes, escritos, y comunicaciones por medios telemáticos con certificado de firma electrónica reconocido.

  Recibido el formulario NOTA en el Registro Telemático, se emitirá por el mismo medio un mensaje de confirmación de la solicitud, en el que constarán los datos proporcionados por el interesado, junto con la acreditación de la fecha y hora en que se produjo la recepción y una clave de identificación de la transmisión.

  La no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica la no recepción efectiva del mismo. En este caso, deberá realizarse la presentación en otro momento o a través de otros medios.

- **Internet sin certificado:** la notificación de los ficheros podrá realizarse a través de Internet, aunque el responsable del fichero no disponga de un certificado de firma electrónica.

---

7 La firma electrónica asocia la identidad de una persona o de un equipo informático al mensaje o documento que se envía, basándose en un método criptográfico para cifrar y descifrar información utilizando técnicas que hacen posible el intercambio de mensajes de manera segura y que las comunicaciones sólo puedan ser leídos por las personas a quienes van dirigidas.

Para ello, una vez cumplimentada la Notificación y la Hoja de solicitud de forma correcta, se deberá enviar únicamente la Notificación electrónicamente pulsando el botón “Generar/Enviar” que se encuentra en la Hoja de solicitud.

El formulario indicará que se está conectando con el servidor de la Agencia Española de Protección de Datos y, acto seguido, enviará una nueva Hoja de Solicitud (en formato PDF) que confirma que la Notificación ha sido enviada correctamente.

Dicha Hoja de solicitud, cumplimentada y firmada por la persona que efectúa la notificación, es la que deberá remitirse a la AEPD: Agencia Española de Protección de Datos, C/ Jorge Juan Nº6, 28001- Madrid.

No se considerará recibida la Notificación efectuada por Internet hasta que tenga entrada en la Agencia Española de Protección de Datos la Hoja de Solicitud debidamente cumplimentada y firmada de forma manual por el responsable del fichero.

- **Formulario en papel:** Los responsables que no dispongan de los medios necesarios para la notificación de ficheros a través de Internet podrán presentar el formulario electrónico cumplimentado en soporte papel. Para ello, se ha de cumplimentar tanto el formulario Notificación de ficheros como la Hoja de Solicitud de forma correcta.

  Cubierto el formulario, el responsable deberá imprimir la Notificación y la Hoja de Solicitud en un formato de seguridad, facilitado por la Agencia, donde se genera y figurará un código de barras bidimensional (nube de puntos).

  Firmada la Hoja de Solicitud por la persona que, con representación suficiente, formula la notificación de los ficheros de datos personales, éste presentará conjuntamente el formulario de Notificación de ficheros y la Hoja de Solicitud ante la Agencia Española de Protección de Datos mediante correo ordinario o presencialmente.

Código de barras bidimensional (www.agpd.es)

8. Fase II: Legitimación de datos de carácter personal

En el tratamiento de datos personales necesarios para el ejercicio de las competencias de las EELL, estas deben atender una serie de obligaciones, a las que se aludía en la exposición de los principios básicos de la protección de datos:

- Informar al afectado con carácter previo al tratamiento de los datos de carácter personal.
- Recoger los datos imprescindibles para el ejercicio de las competencias de la Entidad Local.
- Facilitar a los ciudadanos el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición.Se analiza a continuación las implicaciones para la Entidad de cada una de estas obligaciones.

8.1. DEBER DE INFORMACIÓN PREVIO AL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL

El deber de información previo al tratamiento de datos personales forma parte de los principios básicos de protección de datos, y se constituye como un deber prestacional previo del responsable de fichero. Del cumplimiento de este deber depende, de modo esencial, la eficacia del derecho fundamental a la protección de datos.

Es obligación de los Organismos Públicos que van a registrar y tratar datos de carácter personal **informar al interesado de forma previa, expresa, precisa e inequívoca**, a través del medio que se utilice para la recogida de los mismos. La información debe incluir los siguientes puntos:

- La **existencia de un fichero** o tratamiento de datos de carácter personal, la finalidad de la recogida de éstos y los destinatarios de la información.
- El **carácter obligatorio o facultativo** de su respuesta a las preguntas que les sean planteadas.

- Las **consecuencias** de la obtención de los datos o de la negativa a suministrarlos.
- La posibilidad de **ejercitar los derechos** de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del **responsable del tratamiento** o, en su caso, de su representante[8].

Propuesta de modelo para la recogida de información

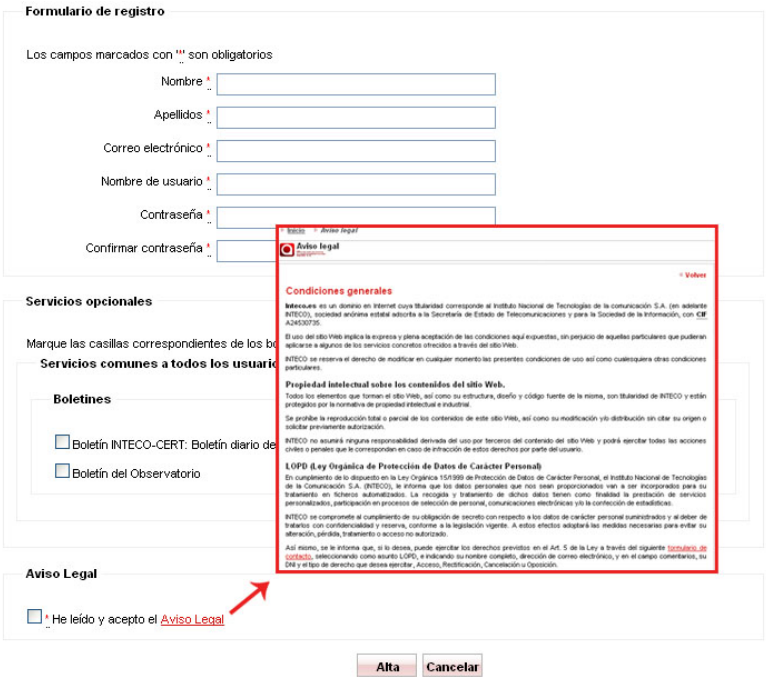
> *Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describir), inscrito en el Registro General de Protección de Datos, y podrán ser cedidos a (indicar). El órgano responsable del fichero es (indicar), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, junto con la documentación acreditativa de la identidad, es (indicar), todo lo cual se informa en cumplimiento del Articulo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Se debe incorporar la cláusula en todos los formularios de recogida de datos personales, independientemente del formato del mismo (en papel o a través de páginas web).

Debe utilizarse algún medio que asegure, sin lugar a dudas, que el interesado ha leído el texto y otorga su consentimiento. En el caso de recoger los datos mediante una página web, se suele obligar a marcar una casilla situada al lado del texto.

8 Cuando los datos de carácter personal no hayan sido recabados directamente por la EELL que realiza su tratamiento, el interesado deberá ser informado, en un plazo de tres meses, de forma expresa, precisa e inequívoca de la procedencia de los datos recogidos, así como de la finalidad de la recogida, de la identidad y dirección del responsable y de la posibilidad de ejercicio de los derechos A.R.C.O

Ejemplo de formulario en página web



En el caso de ser un formulario en papel, basta la indicación del consentimiento en la firma del documento.

Ejemplo de formulario impreso (www.agpd.es)

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el abajo firmante, con representación suficiente del responsable del fichero, formula la siguiente notificación, y manifiesta que todos los datos consignados son ciertos.

En _____ a _____ de _____ de _____

Fdo.:

En cumplimiento del artículo 5 de la Ley 15/1999, por el que se regula el derecho de información en la recogida de los datos, se advierte de los siguientes extremos: Los datos de carácter personal, que pudieran constar en esta notificación, se incluirán en el fichero de nombre "Registro General Protección de Datos", creado por Resolución del Director de la Agencia de fecha 27 de julio de 2001, (B.O.E. nº 197, 17-8-2001) por la que se crean y modifican los ficheros de datos de carácter personal existentes en la Agencia Española de Protección de datos. La finalidad del fichero es velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de los datos. Los datos relativos a la persona física que actúa como declarante de la notificación, únicamente se utilizarán en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud. Tendrán derecho a acceder a sus datos personales, rectificarlos o, en su caso, cancelarlos en la Agencia Española de Protección de Datos, órgano responsable del fichero.
En caso de que en la notificación deban incluirse datos de carácter personal, referentes a personas físicas distintas de la que efectúa la solicitud o del responsable del fichero, deberá, con carácter previo a su inclusión, informarles de los extremos contenidos en el párrafo anterior.

8.2. OTROS ASPECTOS RELEVANTES PARA LA LEGITIMACIÓN DE LOS DATOS

Los impresos de solicitud de información deben contener exclusivamente los campos necesarios para llevar a cabo la finalidad específica. **Los datos personales deben estar permanentemente actualizados y se deberán cancelar cuando se queden obsoletos.**

En el formulario de recogida de datos debe especificarse qué datos son obligatorios para llevar a cabo la finalidad correspondiente, y cuáles son de carácter voluntario, y por tanto no imprescindibles para el objetivo específico. No se requerirá el **consentimiento del interesado** respecto de los datos que recabe la EELL para el ejercicio de sus competencias, esto es, para el desempeño de sus actividades como Administración municipal. Así, la utilización de los datos del Padrón por los distintos servicios municipales será posible siempre que se utilicen para actos dictados en ejercicio de las com-

petencias municipales y que su utilización sea exclusivamente de los datos identificativos de la persona y los datos del domicilio, siempre y cuando este último sea relevante para el ejercicio de la competencia.

Por un lado, **se podrán ceder los datos** del padrón a otras Administraciones Públicas o miembros de la corporación política que lo soliciten, sin consentimiento previo del afectado, solamente cuando sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes (por ejemplo, para enviar una carta personalizada por necesidades de información: información cultural de la Entidad Local, actividades sociales, aparcamientos de residentes, etc.).

Por el contrario sí será necesario el consentimiento del afectado para tratar datos personales en el ámbito de otras actividades complementarias que no forman parte de las competencias en sentido estricto (por ejemplo, el tratamiento de datos personales necesario para la gestión de actividades voluntarias o extraprestacionales como felicitar a los ciudadanos por su onomástica o en Navidad).

Para el supuesto en el que los responsables de ficheros necesiten realizar un tratamiento de **datos considerados especialmente protegidos** (afiliación sindical, religión o creencias), se requerirá autorización expresa y por escrito por parte del interesado.

Otros datos especialmente protegidos, como los datos de salud, vida sexual u origen racial o etnia, necesitarán el consentimiento del interesado cuando no exista una ley que posibilite su recogida. En el caso de los datos de salud hay que considerar como datos personales los referentes a salud pasada, presente y futura, física o mental de un individuo. Se consideran datos de salud los referidos a porcentaje de discapacidad o su información genética. En este sentido hay una excepción: estos datos podrán ser tratados sin consentimiento cuando resulten necesarios para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o la gestión de servicios

sanitarios, siempre que este tratamiento lo realice un profesional sujeto a secreto profesional.

Cabe destacar que todos aquellos datos que vayan a ser cedidos a otros Organismos Públicos, salvo que la Ley disponga lo contrario (ej. contrato negocial, datos públicos por interés legitimo, etc.), han de tener la autorización pertinente, tal y como determina el artículo 6.1 de la LOPD. No será preciso dicho consentimiento para recoger datos personales si así viene establecido en una ley, o cuando se recojan en el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, por ejemplo los casos de la Agencia Estatal de Administración Tributaria y los datos solicitados por Jueces, Ministerio Fiscal, Tribunales, etc.

Por otro lado, también es una obligación el **secreto profesional**, en virtud del cual los datos personales no han de ser revelados. Por ello, el profesional del tratamiento de los datos deberá difundir a todos aquellos que no sean funcionarios y que participan en el tratamiento, parcial o total, las consecuencias del incumplimiento de sus obligaciones.

El apartado tercero del artículo 123 del RDLOPD, señala que la obligación de secreto se extiende a las informaciones que los funcionarios conozcan en el ejercicio de las funciones de inspección, incluso después de haber cesado en las mismas.

8.3. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (ARCO)

Todo ciudadano tiene una serie de derechos en relación a los datos personales que se almacenan o tratan por parte de las distintas EELL, que, a su vez, tienen la obligación legal de facilitar su ejercicio.

Estos derechos conocidos como ARCO (Acceso, Rectificación, Cancelación y Oposición) sólo pueden ser ejercidos por el interesado ante el responsable del fichero, excepto en los casos en que el interesado es menor de edad o

posee algún tipo de incapacidad, en cuyo caso puede actuar mediante representante legal.

Cada responsable de fichero debe facilitar una forma de contacto gratuita y concreta, como puede ser la dirección postal. Adicionalmente, los Organismos públicos tienen la obligación de poner a disposición de los ciudadanos aquellos medios telemáticos necesarios para facilitar la vida de los mismos por los siguientes canales de comunicación:

- Registro electrónico, para recibir a través de correo electrónico todo tipo de solicitudes, escritos y comunicaciones dirigidos a la Administración.

- Atención telefónica que posibilite, dentro de unos criterios de seguridad, recibir las solicitudes o comunicados de una manera directa y personal.

Realizado el contacto con el interesado, se le debe informar del proceso a seguir para la tramitación de su solicitud.

El ejercicio de los derechos deberá llevarse a cabo mediante una solicitud dirigida al responsable del fichero, que contendrá:

- Nombre y apellidos.

- Fotocopia del DNI del interesado. En los casos excepcionales descritos anteriormente, además, serán necesarios los datos del representante legal y el documento acreditativo de la representación. La fotocopia del DNI puede ser sustituida siempre que se acredite la identidad por cualquier otro medio válido legalmente (pasaporte, permiso de conducir, etc.).

- Domicilio a efectos de notificaciones.

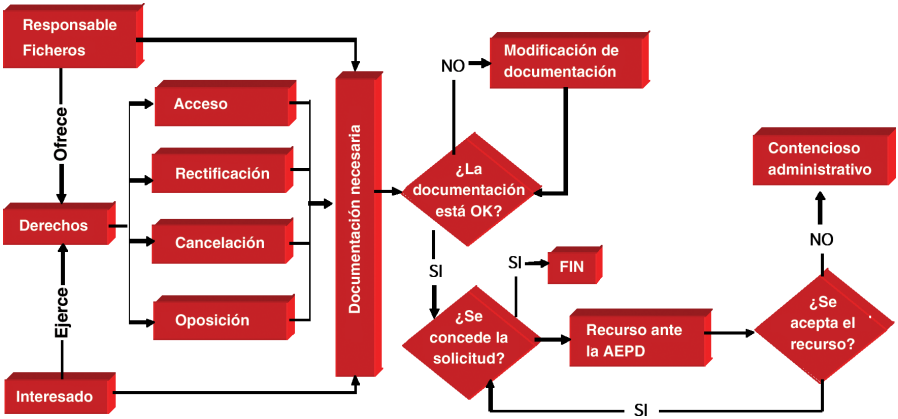
- Fecha y firma del solicitante.

- Documentación adicional para la justificación de la petición que se formula.

El interesado podrá utilizar cualquier medio que permita acreditar el envío de la solicitud.

El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tengan acceso a datos de carácter personal puedan informar del procedimiento a seguir por el interesado para el ejercicio de sus derechos.

Derechos de los interesados



El interesado puede ejercer su derecho de reclamación ante la AEPD en los siguientes casos:

- Que no sea atendida su solicitud en el plazo estipulado por Ley.
- Que le sea denegado el ejercicio de sus derechos respecto a los datos personales.

El artículo 117 y siguientes del RDLOPD describen el procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición que puede iniciar el/los afectado/s, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

Si el procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición no prospera, el interesado dispone de la opción de trámite por vía contencioso-administrativa.

A continuación se desarrolla el contenido de cada uno de los derechos:

Derecho de acceso[9] (art. 15 LOPD)

La Entidad tiene la obligación de informar gratuitamente de todos aquellos datos que posee sobre un ciudadano.

La información, cualquiera que sea el soporte en el que se facilite, se ofrecerá en un formato que se pueda leer y entender, facilitando los datos siguientes:

- Datos de la persona interesada.
- Origen de los datos, que puede ser el propio interesado u otra Entidad que los ha cedido. En el caso de que los datos provengan de fuentes externas, deberán especificarse las mismas, identificando la información que proviene de cada una de ellas.
- Organizaciones a las que se les ha cedido los datos.
- Especificación de las finalidades para las que se recabaron los datos.

9 Disponibles Modelos de ejercicio del derecho de acceso en: https://www.agpd.es/portalweb/canalciudadano/denunciasciudadano/derecho_acceso_den/index-ides-idphp.php

El responsable del fichero deberá contestar toda solicitud que se le dirija, con independencia de que figuren o no datos personales del interesado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción, es decir, se debe responder igualmente cuando no se tienen datos de carácter personal del interesado que ejercita su derecho de acceso.

La Entidad deberá resolver la petición por parte del ciudadano en un plazo máximo de un mes desde la recepción de la solicitud.

La solicitud de este derecho sólo podrá ser realizada en plazos superiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá ejercitarlo con anterioridad.

En los supuestos de denegación de acceso del artículo 30 RDLOPD, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Derecho de rectificación[10] (art. 16 LOPD)

Cualquier individuo tiene derecho a la corrección de todos aquellos datos que considere inexactos o incompletos, inadecuados o excesivos sobre su persona, por lo que podrá solicitar del responsable del fichero la rectificación de los mismos.

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse, y deberá ir acompañada de la documentación que evidencie la rectificación solicitada. El responsable del tratamiento tendrá la obligación de hacer efectiva la solicitud de rectificación del interesado en el plazo de diez días.

10 Disponibles Modelos de ejercicio del derecho de rectificación: https://www.agpd.es/portalweb/canal-ciudadano/denunciasciudadano/derecho_rectificacion_den/index-ides-idphp.php

Derecho de cancelación[11] (art. 16 LOPD)

Cuando los datos del interesado sean inexactos o incompletos, inadecuados o excesivos sobre su persona, éste podrá solicitar del responsable del fichero la cancelación de los mismos.

La cancelación dará lugar al bloqueo de los datos, entendiéndose como la identificación y reserva de datos con el fin de impedir su tratamiento, manteniéndolos exclusivamente a disposición de las Administraciones públicas, Jueces y Tribunales.

Prescritas las posibles responsabilidades derivadas del tratamiento de datos personales se deberá proceder a la supresión o borrado de dichos datos.

Las condiciones que suponen el bloqueo de datos deberán indicarse en el documento de seguridad, donde figurarán las características de acceso a los datos únicamente por los sujetos establecidos en la normativa y bajo las condiciones especificadas. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de cancelación del interesado en el plazo de diez días.

El RDLOPD distingue entre cancelación y revocación del consentimiento al señalar, en su artículo 17, que el afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

---

11 Disponibles Modelos de ejercicio del derecho de cancelación: https://www.agpd.es/portalweb/canal-ciudadano/denunciasciudadano/derecho_cancelacion_den/index-ides-idphp.php

Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, para que éstos cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

El artículo 33 apartados 1 y 2 del RDLOPD recoge los supuestos de denegación de los derechos de rectificación y cancelación. Concretamente señala que:

> *1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.*
>
> *2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.*

Al igual que en los supuestos de denegación de acceso del artículo 30 RDLOPD, en todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Derecho de oposición[12] (art. 34 RDLOPD)

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

- Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 del Reglamento, cualquiera que sea la empresa responsable de su creación.

- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 del Reglamento.

12 Disponibles Modelos de ejercicio del derecho de oposición: Disponibles Modelos de ejercicio del derecho de oposición: https://www.agpd.es/portalweb/canalciudadano/denunciasciudadano/derecho_oposicion_den/index-ides-idphp.php

9. Fase III: Políticas de seguridad de los datos

Toda Entidad, con independencia de su tamaño y finalidad de negocio, deberá implantar un conjunto de políticas de seguridad respecto a los datos que manejan en el ejercicio de sus competencias.

Estas políticas tienden a garantizar la continuidad de sus actividades en el caso de que se produzcan incidencias, fallos, infracciones por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos o en otro tipo de soportes, como el papel.

Por ello, la LOPD, a través del Reglamento de 21 de diciembre del 2007, obliga a todas las empresas, organizaciones, asociaciones e instituciones, tanto públicas como privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal, a aplicar una serie de medidas de seguridad de carácter técnico y organizativo que garanticen la confidencialidad, integridad y disponibilidad de la información.

Las medidas deberán ser adoptadas e implantadas por el responsable del fichero, y en su caso por el Encargado del Tratamiento donde se traten datos de carácter personal. Las medidas se pueden clasificar de la siguiente forma:

- **Medidas organizativas**, destinadas a establecer procedimientos, normas, reglas y estándares de aplicación, que garanticen la seguridad y cuyos destinatarios son los usuarios que tratan los datos de los ficheros.

- **Medidas técnicas**, destinadas principalmente a conservar la integridad física de la información, para evitar robos, pérdidas o alteraciones no justificadas.

Estas medidas serán de aplicación a todos aquellos ficheros que contengan datos de carácter personal, independientemente de su soporte (electrónico o papel), así como a los locales donde se almacenan dichos datos y los continentes que los soportan (armarios, archivadores, ordenadores, servidores, etc.).

A los ficheros de datos de carácter personal se les aplica las medidas de seguridad según el grado de información sensible que contienen, en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

Los niveles de seguridad aplicables se clasifican en básico, medio y alto atendiendo al tipo de dato de carácter personal a proteger:

NIVEL BÁSICO

Nombre, apellidos, DNI, teléfono, domicilio, nº cta bancaria • Los referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, cuando los datos se utilicen únicamente con la finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean miembros • Los ficheros no automatizados que de forma incidental contengan datos especialmente protegidos • Los ficheros cuyo tratamiento tenga como finalidad el cumplimiento de deberes públicos, en el caso de datos como el grado de minusvalía o la declaración de la condición de invalidez.

NIVEL MEDIO

Comisiones de infracciones administrativas o penales • Aquello de lo que sean responsables las Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias • Ficheros de entidades gestoras, servicios comunes de la Seguridad Social, mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social • Hacienda pública (datos relativos a tributos u otras obligaciones fiscales que trata la administración, no los relativos a los impuestos que declaran las empresas) • Datos que permitan deducir el comportamiento de los ciudadanos.

NIVEL ALTO

Ideología o afiliación sindical • Religión o creencias • Origen radical o étnico • Salud (servicios sociales, necesidades de atención médica especial) • Vida sexual • Recogidos para fines policiales sin consentimiento del interesado • Violencia de género.

El RDLOPD establece los niveles de seguridad de forma acumulativa, teniendo la consideración de mínimos legales exigibles. Así, en caso de tratamiento de ficheros de nivel medio, deberán implantarse todas y cada una de las medidas de seguridad descritas para el nivel básico y las del nivel medio. Igualmente sucederá con los ficheros de nivel alto, que deberán implantar las medidas descritas para el nivel básico, el medio y el alto.

Cada organización podrá incrementar las medidas de seguridad de los datos de acuerdo a otros criterios, ofreciendo de esta forma mayores garantías, siempre y cuando se ajusten a los mínimos exigidos respecto a los datos tratados.

Antes de analizar las medidas de seguridad que el Reglamento prevé para ficheros automatizados y no automatizados, se muestran una serie de particularidades:

- **Acceso a través de redes de comunicaciones desde una ubicación externa a los sistemas de información que tratan los datos personales.**

  Deberán adoptarse medidas de seguridad que garanticen la seguridad de la información.

- **Tratamiento de los datos fuera de la ubicación de los sistemas de información que los almacenan.**

  Esta medida de seguridad hace referencia al supuesto en el que se realice algún tipo de tratamiento de datos personales fuera de las instalaciones de la Entidad Local. Tendría cabida en este supuesto el ejemplo en el que un empleado utilice un portátil desde su hogar, o traslade expedientes mediante su almacenamiento en un disco duro externo o en una memoria USB.

  Con esta medida de seguridad se garantiza el control de los datos tratados fuera de la Entidad en dispositivos especialmente sensibles, ya que conllevan un mayor nivel de riesgo de pérdida de confidencialidad e integridad.

- **Generación de ficheros temporales necesarios para desarrollar las actividades de la Entidad Local.**

Los ficheros temporales, independientemente del plazo de vigencia que tengan y su finalidad, deberán tener implantadas las medidas de seguridad que son requeridas para los datos que contenga (es decir, si sólo contiene datos de identificación, bastará con cumplir las medidas de nivel básico, si contiene datos financieros o suficientes para tener un perfil del usuario, se deberán implantar las medidas de nivel medio, y si contiene datos de salud, ideología o afiliación sindical dispondrá además de las medidas de nivel alto[13].

A continuación se desarrollan las medidas de seguridad específicas para los ficheros automatizados y para ficheros no automatizados[14].

9.1. MEDIDAS DE SEGURIDAD PARA FICHEROS AUTOMATIZADOS[15]

Se estructuran según los niveles de seguridad (básico, medio y alto) definidos en el RDLOPD para los ficheros automatizados.

9.1.1. MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Documento de seguridad

Es un documento interno a elaborar por la Entidad Local, de obligado cumplimiento para todo el personal que accede a los ficheros de datos de carácter personal y a los sistemas de información, o que haya conocido o haga uso de esa información por otros medios.

---

13 El RDLOPD obliga a fijar políticas de seguridad para aquel personal que no está autorizado al acceso a los datos de carácter personal pero pueden hacer peligrar la seguridad como por ejemplo personal de limpieza que abandona documentación en el exterior, personal de mantenimiento que desconecta el fluido eléctrico sin avisar, etc.

14 Las medidas comunes a los dos tipos de tratamiento se han ubicado en esta primera parte, en la de ficheros automatizados. Quedará indicado de forma explícita las medidas de seguridad que afectan sólo a cada tipo de ficheros tanto automatizados como no automatizados.

15 Se recomienda la lectura de la Guía de Seguridad de la AEPD disponible en www.agpd.es

En él deben quedar recogidos todas las **políticas, reglas, medidas y procedimientos de seguridad** establecidos por el responsable del fichero.
Se debe mantener **siempre actualizado** ante cualquier modificación de los ficheros, del personal y de los sistemas de información de que dispone la Entidad.

El documento de seguridad debe contener:

- Ámbito de aplicación: especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal.
- Estructura y descripción de los ficheros y sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante incidencias.
- Procedimiento de copias de respaldo y recuperación de datos.
- Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o alto, el documento de seguridad deberá contener, además de los campos descritos anteriormente, los siguientes:

- Identificación del responsable de seguridad.
- Control periódico del cumplimiento del documento.

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia así como los ficheros objeto de este tratamiento.

Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

Funciones y obligaciones del personal

Todo el personal que acceda a los datos de carácter personal está obligado a **conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.**

Constituye una obligación del personal notificar al responsable del fichero (o de seguridad, en su caso) las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en la Guía de Seguridad de la AEPD.

> Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Se deben incluir las obligaciones detalladas de los perfiles que afectan a todos los ficheros (por ejemplo, administrador/es de los sistemas, responsable/s de informática, responsable/s de seguridad, responsable/s de seguridad física, etc). Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del Documento se asignan a perfiles concretos.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

El responsable de ficheros establecerá la delegación de autorizaciones en los usuarios que se relacionen, identificando a los usuarios respecto de sus perfiles y autorizaciones necesarias para el desarrollo de su ejercicio.

Procedimiento de notificación, gestión y registro de incidencias

Se entiende por incidencia cualquier **anomalía que afecte o pudiera afectar a la seguridad, a la integridad, confidencialidad o disponibilidad de los datos**. Así se pueden considerar los accesos no autorizados, la pérdida o extravío de datos, una incorrecta gestión de los soportes, las averías de equipos, etc.

Cualquier persona que sea conocedora de una incidencia respecto a la seguridad de los datos de carácter personal o de las medidas de seguridad correspondientes tiene la obligación de comunicarlo al responsable de seguridad, que emprenderá las medidas necesarias para su corrección, o el traslado de la misma al área de la Entidad Pública que se encargue de su resolución, realizando en este caso un seguimiento para verificar las acciones llevadas a cabo.

El responsable del fichero o, por delegación, el responsable de seguridad, será el responsable de **mantener un registro de las incidencias** en el que, además de los datos especificados en la notificación, se incluirán las medidas adoptadas en cada caso para la solución de dicha incidencia.

Resuelta la incidencia, el responsable de seguridad debe verificar su resolución. En el caso de que el propio responsable haya sido la persona que ha resuelto la incidencia deberá ser una persona diferente la que verifique. De

esta forma se consigue que no recaiga en la misma persona la resolución y verificación del incidente.

En el nivel básico de seguridad se deben cubrir los siguientes campos en el registro: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Del mismo modo se debe realizar el procedimiento de notificación y la gestión de las mismas.

Identificación y autenticación

El RDLOPD establece que el responsable del fichero se encargará de la elaboración de **un listado actualizado de usuarios con acceso autorizado a los sistemas de información y por consiguiente, a los datos de carácter personal que tratan**. Sobre estos usuarios se han de establecer procedimientos de identificación y autenticación para dicho acceso.

Se establece como necesaria la identificación y autenticación de forma inequívoca y personalizada de todos los usuarios autorizados en el sistema.

Ello supone que cada usuario tendrá un nombre de usuario individual y una contraseña asociada al mismo, de uso personal e intransferible, que se valida cada vez que accede al sistema.

En resumen, para esta medida de seguridad y sólo para ficheros automatizados, dentro del nivel básico se deben contemplar: la identificación y autenticación personalizada, el procedimiento de asignación y distribución de contraseñas, el almacenamiento ininteligible de las contraseñas y la periodicidad del cambio de contraseñas (< 1 año).

Control de acceso

El responsable del fichero se encargará de fijar qué usuarios están autorizados a acceder a ciertos recursos, como por ejemplo, equipos informáticos, programas, aplicaciones, bases de datos, redes, etc., de acuerdo con su perfil funcional y sus competencias laborales.

Para ello, una vez identificados los usuarios, se han de establecer mecanismos para evitar que puedan acceder a datos o recursos con derechos distintos de los autorizados, asegurando la confidencialidad y disponibilidad de la información.

En el caso de existir personal ajeno a la Entidad (colaboradores externos, subcontratas de servicios, etc.), que traten datos personales para desarrollar sus actividades y necesiten acceso a los mismos, serán debidamente informados y formados acerca de todas las obligaciones en materia de protección de datos de carácter personal establecidas en el documento de seguridad.

Respecto del control de acceso, se deben atender para el nivel básico: la relación actualizada de usuarios y accesos autorizados, el control de accesos permitidos a cada usuario según las funciones asignadas, los mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados, la concesión de permisos de acceso sólo por personal autorizado así como las mismas condiciones para personal ajeno con acceso a los recursos de datos.

Gestión de soportes

El RDLOPD establece que los soportes informáticos que contengan datos de carácter personal deberán estar claramente identificados, siempre y cuando, las características físicas del soporte lo permitan. Esta identificación deberá reflejar el contenido del soporte de manera clara para aquellas personas autorizadas a su tratamiento.

En cuanto al traslado de soportes o documentos que contengan datos de carácter personal fuera de los locales en los que está ubicado el fichero, deberán aplicarse todas aquellas medidas que imposibiliten su pérdida o deterioro.

Cuando un soporte informático (copias de seguridad, disquetes, cintas, etc.) vaya a ser reutilizado, se adoptarán las medidas necesarias para su formateo, con objeto de impedir cualquier recuperación posterior de la información que contenía almacenada el dispositivo. Si el soporte no puede ser reutilizado o se quiere eliminar, se procederá a su destrucción física de forma que resulte totalmente irrecuperable la información que contiene.

Para el nivel básico, en lo que respecta a la medida de gestión de soportes se debe realizar un inventario de soportes, la identificación del tipo de información que contienen, o el sistema de etiquetado, el acceso restringido al lugar de almacenamiento, la autorización de las salidas de soportes (incluidas a través de e-mail) y las medidas para el transporte y el desecho de soportes.

Copias de respaldo y recuperación

La recuperación de los datos de las copias de seguridad se realizará por el responsable de seguridad o aquellos administradores de sistema designados por él, previa autorización. Tanto el proceso de copia de seguridad, como el de recuperación de datos, deberán someterse a una verificación por parte del responsable del fichero al menos cada seis meses.

La medida de copias de respaldo en el nivel básico, y sólo para ficheros automatizados, comprenderá: la copia de respaldo semanal, los procedimientos de generación de copias de respaldo y recuperación de datos, la verificación semestral de los procedimientos, la reconstrucción de los datos a partir de la última copia o la grabación manual en su caso, si existe documentación que

lo permita, así como las pruebas con datos reales y la copia de seguridad y aplicación del nivel de seguridad correspondiente.

9.1.2. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Responsable de seguridad

Para facilitar el trabajo en materia de seguridad de la información, el responsable del fichero designará por escrito uno o varios responsables encargados de coordinar y controlar el cumplimiento de las medidas de seguridad descritas en el documento de seguridad.

Esta figura es designada como responsable de seguridad, encargado de velar por el cumplimiento de las medidas, reglas y normas de seguridad establecidas por el responsable del fichero, no siendo responsable jurídico ante estamentos reguladores y sancionadores.

En todo caso, la designación no debe ser entendida como una delegación de responsabilidad. El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.

Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán a un proceso de auditoría interna o externa, al menos cada dos años, por una persona que examine de forma objetiva e independiente el cumplimiento del RDLOPD.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

Se elaborará un Informe de Auditoría con el resultado de la revisión realizada que incluya todos los datos, hechos, no conformidades y observaciones surgidas en la evaluación, así como las medidas correctoras correspondientes a las desviaciones halladas.

Los Informes de Auditoría serán analizados por el responsable de seguridad, quien elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas, quedando dichos informes a disposición de la AEPD.

Identificación y autenticación

Esta medida descrita para el nivel básico se ve reforzada en este apartado, debido a la obligación de adoptar medidas que impidan el intento reiterado de acceso no autorizado al sistema.

Se debe implantar el bloqueo automático de acceso, por ejemplo, cuando se registren tres intentos de acceso fallido de forma consecutiva, permitiendo de esta manera, al responsable de seguridad evitar amenazas de usuarios no autorizados que intenten realizar ataques para averiguar contraseñas de acceso.

Control de acceso físico

Esta medida de seguridad se ve aumentada en el nivel medio para los ficheros automatizados, ya que se deben establecer las restricciones de acceso físico a los locales donde se encuentren ubicados los sistemas de información o servidores con datos de carácter personal.

El responsable de seguridad deberá reflejar en el documento de seguridad un listado con todas aquellas personas que tengan derecho de acceso a las salas que albergan físicamente los servidores, además de establecer qué

tipo de medidas de seguridad serán implantadas para restringir el acceso de personal no autorizado a las instalaciones.

Gestión de soportes

La medida de seguridad de gestión de soportes en el nivel medio, y sólo para ficheros automatizados, comprenderá: un sistema de registro de entrada y salida de soportes informáticos que permita, directa e indirectamente, conocer: el tipo de soporte, fecha y hora, origen, tipo de información, procedimiento de recepción/envío y la persona responsable que deberá estar autorizada para la recepción/entrega.

Registro de incidencias

Esta medida de seguridad se ve aumentada en el nivel medio para los ficheros automatizados ya que afecta a la recuperación de los datos de las copias de seguridad, requiriendo un registro del personal que ejecuta la recuperación, los datos que han sido recuperados, y en su caso, los datos grabados manualmente.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

9.1.3. MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Gestión y distribución de soportes

La finalidad última de esta medida consiste en evitar que, ante cualquier incidencia que pueda producirse en la distribución de los datos o en el soporte que los contiene, terceras personas no autorizadas puedan acceder a la información y modificarla. Por ello, se recomienda la utilización de mecanismos de seguridad mediante claves de acceso a los ficheros o la encriptación de los datos con programas especializados para evitarlo.

Así, la medida de gestión de soportes en el nivel alto y sólo para ficheros automatizados comprende el sistema de **etiquetado confidencial, el cifrado de datos en la distribución de soportes así como el cifrado de información en dispositivos portátiles fuera de las instalaciones**, evitando el uso de dispositivos que no permitan el cifrado o que se adopten medidas alternativas.

Registro de accesos

Esta medida implica que todas las aplicaciones o programas internos que traten con datos de carácter personal, han de configurarse para que registren y almacenen los datos de todos aquellos usuarios que acceden o intentan acceder a la aplicación.

Esta medida de seguridad se ve aumentada en el nivel alto para los ficheros automatizados respecto del registro de accesos (usuario, hora, fichero, tipo de acceso, autorizado o denegado), la revisión mensual del registro por el responsable de seguridad y la conservación durante dos años. No será necesario este registro si el responsable del fichero es una persona física y es el único usuario.

Copias de respaldo y recuperación

Las copias de seguridad y los procedimientos de restauración de datos deben ser conservados fuera de la ubicación principal de los sistemas de información, a fin de garantizar la continuidad de la actividad y la disponibilidad de la información ante cualquier incidencia grave o muy grave, sea física o lógica, que afecte a los equipos o servidores centrales (incendios, inundaciones, etc.).

Telecomunicaciones

Habitualmente se utilizan redes de telecomunicaciones abiertas[16] para transmitir ficheros y archivos. Para evitar que durante la transmisión de datos puedan producirse intercepciones o manipulaciones no deseadas de datos

16 Tipo de redes en las cuales los datos no son cifrados mientras se transmiten entre dos puntos, permitiendo que puedan ser interceptados.

de carácter personal, deben utilizarse mecanismos de cifrado de los datos utilizando programas especializados, o transmitir datos a través de redes privadas, que garanticen que la comunicación entre dos puntos es segura y no pueda ser interceptada por terceras personas.

9.2. MEDIDAS DE SEGURIDAD PARA FICHEROS NO AUTOMATIZADOS

Las siguientes medidas de seguridad -desarrolladas en el apartado anterior- son de obligado cumplimiento tanto en ficheros automatizados como no automatizados, por lo que tienen que implementarse de igual forma en estos últimos: documento de seguridad, funciones y obligaciones del personal, registro de incidencias, control de acceso, gestión de soportes, responsable de seguridad y auditoría. Por tanto, se remite al lector al punto anterior para conocer las implicaciones.

Se analizan a continuación las medidas de seguridad de nivel básico, medio y alto específicas para ficheros no automatizados.

9.2.1. MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Criterios de archivo

Todos los organismos e instituciones públicas, necesitan gestionar la creación, distribución y recuperación de los documentos que utilizan en el desarrollo de sus actividades.

La gestión documental es una metodología para regular la producción, circulación, uso y control de los documentos que tiene como objetivo el mantenimiento y disposición de los documentos de una organización, a lo largo de su ciclo vital, de forma eficiente.

El RDLOPD establece que, en caso de no existir legislación aplicable a este tipo de soportes, será el responsable del fichero quien establezca sus propios criterios de archivo documental.

Dispositivos de almacenamiento

El Reglamento establece que todos aquellos ficheros en soporte papel que contengan datos de carácter personal deben estar debidamente almacenados, imposibilitando su acceso a todas aquellas personas que no tengan autorizado su tratamiento. Para ello, los mecanismos de seguridad más utilizados son los armarios o archivadores, que deberán disponer de mecanismos adecuados de cierre como llaves de seguridad, candados (con llave o código de dígitos) o tarjetas magnéticas.

Lo importante es garantizar que el acceso a la documentación no se realiza por personas no autorizadas. Por ejemplo, si los expedientes están en el despacho del único funcionario que los trata, y éste siempre lo cierra con llave cuando no está, no será necesario añadir una nueva medida de seguridad adicional.

Custodia de los soportes

Cuando la documentación que contenga datos de carácter personal no se encuentre almacenada según las medidas anteriormente mencionadas (armarios con llave, tarjetas magnéticas, etc.) por encontrarse en proceso de revisión o tramitación, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.

Si el responsable del tratamiento de los documentos se ausenta de su puesto de trabajo, deberá aplicar las medidas de seguridad oportunas a fin de evitar que personal no autorizado acceda a los documentos como guardar la documentación en cajoneras, armarios o estanterías a ser posible bajo llave.

9.2.2. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Las medidas de seguridad de nivel medio que establece el RDLOPD para ficheros no automatizados son el nombramiento de un responsable de seguridad y la realización de auditorias periódicas.

Estas medidas son de común desarrollo e implantación al de los ficheros automatizados (Véase Medidas de seguridad para ficheros automatizados, nivel medio).

9.2.3. MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Almacenamiento de la información

Esta medida exige a la Entidad Local la custodia de aquellos armarios o archivadores provistos de medidas de seguridad propias (llaves, tarjetas magnéticas), en áreas que imposibiliten el acceso de personal no autorizado a los datos.

Las medidas que deben adoptar estas dependencias pueden consistir en la restricción de acceso mediante llaves de seguridad, lectores de tarjeta magnéticos, dispositivos de acceso mediante claves, dispositivos biométricos, etc.

Cuando resultase desproporcionada o inviable la adopción de este tipo de medidas, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas a la documentación (por ejemplo, cerrar con llave las dependencias donde se realiza el tratamiento de los datos personales cuando el personal autorizado no esté presente en la misma).

Copia o reproducción

En el ejercicio de las actividades de un organismo público, se hace puntualmente necesaria la realización de copias de documentos originales para evitar su deterioro, pérdida, etc.

En el caso de las copias realizadas a documentos que contengan datos de carácter personal de nivel alto, sólo podrán ser realizadas y supervisadas por las personas que se autoricen en el documento de seguridad.

Se obliga a la destrucción de la copia cuando ha dejado de tener el uso para el que fue creada, garantizando la imposibilidad de recuperación de la información.

Acceso a la documentación

El RDLOPD establece que **el acceso a la documentación se limitará exclusivamente al personal autorizado.**

De un lado, se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

De otro, y por lo que respecta al acceso de personas no incluidas en el párrafo anterior, el acceso deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Con el fin de evitar accesos no autorizados, se deben implantar mecanismos de prevención y de detección, como llaves de seguridad o tarjetas magnéticas, para garantizar un adecuado control de acceso a los recursos en los locales correspondientes de la Entidad.

En la detección de accesos indebidos se recomienda la utilización de medios técnicos, en la medida que sea posible, como cámaras de vigilancia de circuito cerrado o alarmas, que permitan detectar qué personas han accedido a las dependencias sin autorización.

Traslado de la documentación

Cuando la documentación, independientemente de los datos personales que contenga, haya de ser trasladada fuera de su ubicación original, se han de aplicar medidas de seguridad que impidan el acceso o manipulación de los datos por parte de terceras personas.

El traslado se podrá hacer por valija separada cuando se trate de un servicio de correo interno, custodiado por un funcionario público o por personal laboral propio. En caso de que se requieran medidas de seguridad más rigurosas, se recomienda realizar el desplazamiento mediante armarios dotados de las pertinentes medidas de seguridad como la utilización de llaves o lectores magnéticos, y en la medida de lo posible, cuya posesión sólo corresponderá al responsable de seguridad.

Anexo I Tratamiento de datos habituales por parte de las entidades locales

Para finalizar el análisis acerca de la adaptación de las Entidades Locales a la normativa sobre protección de datos, se ha considerado oportuno evaluar aquellos ficheros de datos personales susceptibles de un tratamiento más común, **por contener datos que requieren medidas de seguridad de nivel alto o tratarse de datos de gran relevancia para los interesados**.

Se han identificado los siguientes ficheros, cuya existencia es muy probable en el ámbito de una Entidad Local:

- Padrón de habitantes.
- Padrón de vehículos.
- Servicios sociales.
- Licencia de actividad de locales comerciales.
- Videovigilancia.

A continuación, se realiza un análisis de la utilización de estos ficheros en las Entidades Públicas Locales y se propone una serie de buenas prácticas para un adecuado tratamiento de los mismos.

PADRÓN DE HABITANTES

Todas las personas que viven en España tienen la obligación de inscribirse en el padrón municipal de habitantes del lugar donde tengan su residencia habitual, según la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (en adelante, LBRL).

Las EELL no tienen el deber de recabar el consentimiento del interesado para el tratamiento de los datos del padrón, ya que, como indica el artículo 6.2 de la LOPD, el padrón forma parte de las funciones administrativas que son competencia de los Ayuntamientos.

El artículo 16.3 de la LBRL dispone lo siguiente:

> *Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.*

Por lo tanto, **la Administración que solicite los datos al Ayuntamiento debe justificar que son para alguna de las competencias que le reconoce el ordenamiento jurídico**, además de argumentar la relevancia de la residencia o el domicilio para este tratamiento.

Por otro lado, respecto a los fines estadísticos, **los Ayuntamientos están obligados a facilitar la información de los datos del padrón al Instituto Nacional de Estadística**, siempre que se justifique su petición dentro de las competencias que le otorga la Ley de Función Estadística Pública.

Por lo que respecta a la cesión de estos datos a las Fuerzas y Cuerpos de Seguridad del Estado, cuando los datos sean solicitados dentro de una investigación policial, **el responsable del fichero del padrón únicamente debe comprobar que el solicitante acredita que pertenece como miembro a las Fuerzas y Cuerpos de Seguridad del Estado**. Esta situación viene regulada por el artículo 22.2 de la LOPD en el que se indica que la recogida y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad se puede realizar sin consentimiento del afectado cuando se trate de la prevención de un peligro real para la seguridad pública o para la represión de infracciones reales.

Respecto a las medidas de seguridad a aplicar a este tipo de ficheros, debe tenerse en cuenta que se trata de datos clasificados como nivel básico.

PADRÓN DE VEHÍCULOS

La finalidad del tratamiento de los datos de este fichero es la recaudación del impuesto municipal de circulación, además de mantener un registro de propietarios de vehículos (por ejemplo, para la gestión de transferencias).

Si en el momento en el que se establezca este tipo de fichero se incorporasen únicamente datos de salud de los propietarios de los vehículos –referentes exclusivamente al grado de discapacidad o a la simple declaración de la condición de discapacidad o invalidez del afectado– el fichero pasaría a ser clasificado de nivel básico, entrando, de esta forma, a ser considerado en la exclusión contemplada en el artículo 81.6 del RDLOPD sobre la aplicación de los niveles de seguridad.

En el caso de tener contratada la gestión de algún servicio relacionado con los vehículos, por el que se tenga que acceder a este fichero para poder realizar las funciones encomendadas, hay que prestar especial atención al artículo 12 de la LOPD, que hace referencia al acceso a los datos por cuenta de terceros.

La LOPD permite que el responsable del fichero habilite el acceso material a datos de carácter personal por parte de la entidad que va a prestarle un servicio (esto es, encargado del tratamiento) sin que pueda considerarse dicho acceso como una cesión de datos. Si bien se exige que en el contrato deben constar una serie de requisitos, tales como seguir las instrucciones del responsable del fichero, no utilizar los datos para un fin distinto, no comunicarlos a otras personas, estipular las medidas de seguridad del artículo 9 y, cumplida la prestación, destruir los datos o proceder a su devolución al responsable del fichero.

SERVICIOS SOCIALES

Los Servicios Sociales están disponibles y son accesibles para todos los ciudadanos sin discriminación por algún motivo personal. **Los ficheros de datos personales gestionados por los Servicios Sociales de las Entidades Públicas Locales se clasifican con nivel de seguridad alto**.

La LOPD, en su artículo 7, considera como datos especialmente protegidos los relativos a la ideología, afiliación sindical, religión y creencias, así como los datos personales que hagan referencia al origen racial, a la salud y a la vida sexual. Si bien, respecto a los primeros únicamente se puede llevar a cabo el tratamiento con el consentimiento expreso y por escrito del interesado. Respecto a los segundos, sólo podrán ser recabados cuando así lo disponga una Ley o cuando el afectado consienta expresamente.

Por lo tanto, cuando una entidad local recabe datos deberá manifestar una adecuada justificación de la finalidad de la propia prestación social.

En este sentido, a modo de ejemplo, cabe señalar la Resolución R/00431/2008 de la AEPD en la que figura como hecho probado la remisión de felicitaciones navideñas por parte de una Entidad Local, en cantidad aproximada de quinientas, utilizando para ello datos obtenidos de los participantes en actividades de las Escuelas de Padres, de la Escuela de Verano (en este caso los destinatarios eran menores), y de los servicios de Teleasistencia y Ayudas a domicilio (tratándose, en este caso, de beneficiarios de ayudas sociales). Dichos datos habían sido recopilados a partir de entrevistas personales realizadas por el Teniente de Cargo 3 y de los formularios de participación en las actividades citadas.

Ante estos hechos, entre los fundamentos de derecho empleados en la citada Resolución se encuentra el apartado 2 del artículo 4 LOPD -principio de calidad de datos- aplicable al supuesto de hecho que se analiza al disponer lo siguiente:

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

En definitiva, las EELL deben tener siempre presente el deber de informar al interesado cuando, en relación a los ficheros de datos personales gestionados por los Servicios Sociales de las Entidades Públicas Locales, se pretenda recabar el consentimiento, ya que los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

LICENCIA DE ACTIVIDAD DE LOCALES COMERCIALES

La solicitud de una licencia de actividad es un acto obligatorio y previo al inicio de cualquier actividad empresarial cuyo ejercicio requiera necesariamente un local. **El nivel de clasificación de los datos de estos ficheros es básico.**

Es habitual en las EELL que esta solicitud sea en formato papel, por lo que se debe incorporar a la misma un texto explicativo en el que se indiquen claramente los siguientes puntos:

- Existencia de un fichero, declarado en la Agencia de Protección de Datos, donde se van a incorporar los datos de la solicitud indicando quién es el responsable del fichero.
- Finalidad del tratamiento de los datos.
- Cesiones a terceros (en su caso).
- Forma de ejercer los derechos de acceso, rectificación, cancelación y oposición, ofreciendo un medio de contacto para su ejercicio.

VIDEOVIGILANCIA

La captación y grabación de imágenes de personas físicas identificadas o identificables por medio de sistemas de videocámaras es considerado por la LOPD, según su artículo 3a), como dato de carácter personal. Un número cada vez mayor de EELL instalan dispositivos de este tipo.

> Hay que tener en cuenta que se considera tratamiento de datos personales la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de imágenes.

La Agencia Española de Protección de Datos, en virtud de la competencia que la LOPD le otorga, dictó la Instrucción 1/ 2006, de 8 de noviembre de 2006, por la que se regula el tratamiento de imágenes, con el objeto de garantizar los derechos de las personas cuyas imágenes son tratadas por videocámaras con fines de vigilancia.

Se excluyen las imágenes grabadas para uso doméstico y el tratamiento de imágenes por parte de las Fuerzas y Cuerpos de Seguridad del Estado, que está regulado por la Ley Orgánica 4/97, de 4 de agosto.

Las principales exigencias a implantar son las siguientes:

- Para cumplir con el deber de información, se debe colocar en las zonas videovigiladas al menos un **distintivo informativo ubicado en lugar suficientemente visible**, tanto en espacios abiertos como cerrados.
- Este distintivo deberá de incluir una referencia a la “Ley Orgánica 15/1999, de Protección de Datos”, una indicación de la finalidad para la que se tratan los datos y una mención expresa a la identificación del responsable ante quién puedan ejercitarse los derechos en materia de Protección de Datos.

- **Sólo se considerará admisible la instalación de cámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que resulten menos intrusivos para la intimidad de las personas**.
- Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, que hayan justificado la instalación de las cámaras.
- La creación de un fichero de imágenes de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

Anexo II Glosario

- **Afectado o interesado**: persona física titular de los datos que sean objeto del tratamiento.
- **Responsable del fichero o tratamiento**: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- **Encargado del fichero o tratamiento**: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- **Responsable de Seguridad**: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- **Auditoría:** examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.
- **Datos de carácter personal**: cualquier elemento que permite determinar, de manera directa o indirecta, la identidad física, fisiológica, psíquica, económica, cultural o social de una persona física.
- **Fichero**: conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Es, por tanto, el soporte físico, sea automatizado o no, en el que se recoge y almacena, de manera organizada, el conjunto de datos que integra la información.
- **Fichero automatizado**: conjunto de datos almacenados en dispositivos informáticos (PC, lectores DVD, etc.) que requieren de herramientas capaces de descifrar la información que contienen para su tratamiento.
- **Fichero no automatizado**: conjunto de datos almacenados en soportes que no requieren de herramientas para su tratamiento, como el papel.
- **Sistema de tratamiento**: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Respecto a este término y según recoge el RDLOPD en su artículo 54.1.c, la disposición o acuerdo de creación del fichero deberá contener, entre otros extremos, la estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

- **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Cesión o comunicación de datos**: toda revelación de datos realizada a una persona distinta del interesado.
- **Autenticación:** procedimiento de comprobación de la identidad de un usuario.
- **Identificación:** procedimiento de reconocimiento de la identidad de un usuario.
- **Niveles de seguridad:** son los niveles en que se dividen las medidas de seguridad atendiendo a la naturaleza de la información tratada. En base a ello existen tres niveles de seguridad: básico, medio y alto.
- **Recurso:** cualquier parte que compone un sistema de información.
- **Sistema de información:** conjunto de ficheros automatizados, programas y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal (servidores, PC de sobremesa, etc.).
- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Soporte:** objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.
- **Accesos autorizados:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

- **Bloqueo de datos:** la identificación y reserva de los datos con el fin de impedir su tratamiento.
- **Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma que lo limite. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos sde nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines Oficiales y los medios de comunicación.

más información
http://www.inteco.es
http://observatorio.inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación