Guía de adaptación de la Ley Orgánica de Protección de Datos en las Entidades Locales

INDICE

1 Introducción

La Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, en adelante, LOPD, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, por parte de los Organismos Públicos y las Entidades Privadas.

La LOPD establece una serie de obligaciones en pos de la protección de los datos personales contenidos en ficheros que poseen empresas y Administraciones Públicas, y que son tratadas por éstas con diferentes finalidades: gestión de personal, proveedores, clientes, campañas de marketing, etc.

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general es la Agencia Española de Protección de Datos (AGPD).

La LOPD obliga a todas las Administraciones Públicas, incluidos los Ayuntamientos y Diputaciones Provinciales, debido a que estas entidades tratan datos de carácter personal mediante el padrón municipal, gestión tributaria, etc. Estos datos requieren la implantación de las medidas de seguridad exigidas por la Ley.

Este documento explicará el proceso de aplicación y adaptación de una Entidad Local a la Ley de forma que se garanticen los derechos de las personas respecto a los datos de carácter personal que manejan dichas entidades.

Con esta guía de adaptación a la LOPD, una Entidad Local conocerá cuáles son los pasos a seguir para su adecuación y las actuaciones obligatorias para su aplicación, entendiendo que la adecuación a la LOPD no debe considerarse como una adaptación puntual sino como un proceso de **actualización continua**.

2 Legislación aplicable

La normativa vigente en materia de protección de datos es la siguiente:

- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de Diciembre, de Desarrollo de la Ley Orgánica de Protección de Datos.

A finales del año 2007, se aprobó el nuevo **Reglamento de Desarrollo de la LOPD que entra en vigor el 19 de abril de 2008,** que desarrolla tanto los principios de la Ley, como las medidas de seguridad a aplicar en los sistemas de información. Se aplica tanto a ficheros en soporte automatizado, como en cualquier otro tipo de soportes.

Este nuevo Reglamento aúna y completa en un solo documento todas las disposiciones vigentes y aplicables de desarrollo de la Ley Orgánica de Protección de Datos y deroga el Real Decreto 994/1999, de 11 de junio, de Medidas de Seguridad de Ficheros Automatizados.

Esta normativa obliga a todas las Entidades Locales a implementar una serie de medidas y procedimientos que garanticen la protección de los datos personales.

De acuerdo con la Ley, son **datos de carácter personal** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, es decir, toda información que aporte datos sobre una persona física concreta o bien que a través de dicha información se pueda llegar a identificar.

Quedan excluidos cualquier tipo de datos relativos a personas jurídicas siempre y cuando la finalidad del uso de los datos esté destinado a la empresa.

La Ley y su Reglamento de desarrollo mencionan también el concepto de fichero, como cualquier conjunto de datos de carácter personal, en cualquier formato, electrónico, papel, etc.

Los datos de carácter personal se dividen en grupos, nivel básico, medio y alto, que permitirán posteriormente la aplicación de diferentes medidas de seguridad y protección para cada grupo:

Nivel Básico: ficheros que contengan datos de carácter personal:

Nivel Básico: ficheros que contengan datos de carácter personal:

- Identificativos (nombre, apellidos, direcciones de contacto (tanto físicas como electrónicas), teléfono (tanto fijo como móvil).
- Características personales.
- Circunstancias sociales.
- Académicos y profesionales.
- Empleo y carrera administrativa.
- Información comercial.
- Económico-Financieros.
- Transacciones.

Nivel Medio:

- Relativos a la comisión de infracciones administrativas o penales.
- Que se rijan por el artículo 29 de la LOPD: prestación de servicios de solvencia patrimonial y crédito.
- De Administraciones Tributarias, y que se relacionen con el ejercicio de sus potestades tributarias.

- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.
- De Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias.
- De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.
- De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

Nivel Alto:

- De Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
- Datos recabados con fines policiales sin consentimiento del afectado.
- Derivados de actos de violencia de género.

Excepciones:

Según el punto 5, del Artículo 81 del desarrollo de la Ley, en el caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan datos sin guardar relación con su finalidad.

Según el punto 6 del mismo artículo, también se consideran como excepciones y podrán implantarse medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

3 Metodología para la aplicación de la LOPD en las Entidades Locales

La LOPD obliga a todas las empresas y organismos, tanto privados como públicos que dispongan de datos de carácter personal a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que se posea.

Todos los ficheros y tratamientos de datos personales realizados por la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local y todas las Entidades de derecho público, con personalidad jurídica propia, vinculadas a cualquier Administración, son ficheros o tratamientos de titularidad pública.

En el caso concreto de las Administraciones Públicas, éstas poseen ficheros con datos personales. En particular, los Ayuntamientos y Diputaciones Provinciales poseen ficheros con datos relativos al padrón municipal, gestión tributaria, catastro, etc.

La posesión de estos ficheros conlleva una serie de obligaciones que deben cumplir e implantar una serie de medidas de seguridad en el tratamiento y protección de datos de carácter personal.

Para un adecuado cumplimiento de la Ley, los Ayuntamientos y Diputaciones Provinciales deberán seguir la siguiente metodología:

1. Identificación de los ficheros de carácter personal.
2. Identificación de los responsables de la organización en materia de protección de datos de carácter personal.
3. Creación, modificación o supresión de ficheros en el Boletín Oficial.
4. Inscripción de ficheros en el registro de la Agencia Española de Protección de Datos (AGPD).
5. Redacción del documento de seguridad.

6. Aplicación de las medidas técnicas necesarias para asegurar el nivel de protección de los ficheros que contengan datos de carácter personal.
7. Auditoria de todas las medidas establecidas en el documento de seguridad.

3.1 Identificación de los ficheros de carácter personal

El punto de partida del proceso de adaptación y cumplimiento de la LOPD consiste en identificar el origen de la información que maneja la Entidad Local, determinando los datos de carácter personal presentes en esa información.

Por lo tanto será necesaria una identificación de los ficheros que contengan datos de carácter personal que están dentro del alcance de aplicación de la LOPD, distinguiendo:

- Ficheros automatizados.
- Ficheros no automatizados o manuales.

Según el Artículo 3 de la LOPD, se entiende por Fichero "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Una vez han sido localizados los ficheros en la Entidad, es necesario sistematizar de una manera lógica y coherente toda la información recabada.

Dentro de una Entidad es probable encontrar multitud de ficheros físicos, es decir, todos aquellos que son creados mediante la organización de datos personales con independencia de la aplicación que los crea o los trata.

Como fichero lógico entendemos un fichero o conjunto de ficheros físicos, que contienen el mismo tipo de datos, y que son tratados para una misma finalidad o finalidades compatibles.

Una vez que se haya realizado el inventario de ficheros físicos, se procederá a la agrupación de los mismos en ficheros lógicos, esto permitirá la sistematización de los ficheros a inscribir en la Agencia Española de Protección de Datos.

De igual forma se procederá a la hora de incluir ficheros no automatizados (en soporte papel), agrupándolos teniendo en cuenta la finalidad genérica del tratamiento, no siendo necesario declarar dos veces este fichero a la AGPD.

Posteriormente se deberá determinar el nivel de seguridad de los ficheros identificados.

Para llevar a cabo dicha tipificación, se clasificarán los ficheros en función de la naturaleza de los datos, visto anteriormente (nivel básico, medio o alto). El Reglamento de desarrollo de la LOPD establece los tres niveles de seguridad para los ficheros y establece una serie de medidas que la Entidad deberá implementar para cada nivel.

3.2 Identificación de los responsables de la organización en materia de protección de datos

En la Ley se definen tres roles de responsabilidad sobre los ficheros o tratamiento de datos de carácter personal, con diferentes funciones:

- **Responsable del fichero o del tratamiento de datos de carácter personal**: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

  Para el caso de las Entidades Locales, será cada Entidad quien adopte la figura de responsable de fichero, respecto de aquellos ficheros que se han creado y se vayan creando en un futuro.

  Funciones:

  Las funciones que debe asumir el responsable del fichero o tratamiento de la información son las siguientes:

  - Notificar para su implantación en el registro de la Agencia Española de Protección de Datos la creación, modificación y cancelación de ficheros que contengan datos de carácter personal.
  - Atender las solicitudes de acceso, rectificación, cancelación y oposición ejercidas por el afectado. Además el responsable del fichero deberá conceder al interesado un medio sencillo y gratuito para el ejercicio de estos derechos.
  - Implantar las medidas de seguridad oportunas según los niveles que requieran los ficheros con datos de carácter personal.
  - Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones.

- Definir y documentar las funciones y obligaciones de cada uno de los usuarios con acceso a datos de carácter personal y a los sistemas de información.
- Adoptar las medidas necesarias para limitar el acceso del personal a datos personales y a los soportes que los contengan para la realización de trabajos que no impliquen el tratamiento de datos personales, estableciendo mecanismos para evitar que un usuario pueda acceder a recursos distintos a los autorizados.
- Encargarse de que exista una relación actualizada de usuarios y perfiles de usuarios. Además de establecer mecanismos de forma que los usuarios sólo tendrán acceso a los recursos que precisen en el desarrollo de sus funciones.
- Adoptar medidas para la correcta identificación y autentificación de los usuarios. En el caso de que el sistema de autentificación se base en contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
- Encargarse de verificar cada seis meses el correcto funcionamiento del procedimiento de realizar copias de respaldo y recuperación de datos.

- **Encargado del tratamiento:** persona física o jurídica, pública o privada, u órgano administrativo que solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

  En la mayoría de las organizaciones, el propio responsable del fichero realizará el tratamiento de los ficheros, por tanto también recaerá sobre él la figura del encargado del tratamiento.

Funciones:

- Realizar el tratamiento de los datos por cuenta del responsable del fichero.
- Implantar las medidas de seguridad oportunas según los niveles que requieran los ficheros con datos de carácter personal, por encargo del responsable del fichero.
- El responsable del fichero debe asegurarse que el encargado del tratamiento cumple con la LOPD, para lo que puede pedir por ejemplo, una auditoria interna.

- **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.

  En cada Entidad se podrán asignar uno o varios responsables de seguridad, nombrados por el responsable del fichero.

  El cargo de responsable de seguridad no supone delegación de responsabilidad por parte del Responsable del fichero.

  Funciones:

  Las funciones en el caso de niveles básico y medio de seguridad de ficheros son:

  - Coordinar y controlar las medidas recogidas en el documento de seguridad. Esta designación puede ser única del responsable para todos los ficheros o diferenciando según el sistema de tratamiento.

  En el caso de nivel alto en medidas de seguridad:

  - Comprobar, al menos una vez al mes, la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados.

- Controlar los mecanismos que permiten el registro de accesos a datos de nivel alto, revisar al menos una vez al mes la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados.

En lo referente al resto de personal de la Entidad, será necesaria una formación del personal que trabaje con los datos de carácter personal. Para ello es conveniente realizar reuniones informativas y formativas que sensibilicen al personal sobre la necesidad de proteger los datos de carácter personal, consiguiendo una reducción de las incidencias y mejorando la seguridad de la Entidad.

3.3 Creación, modificación o supresión de ficheros en el Boletín Oficial

Según aparece en el Capítulo I de la LOPD, referido a ficheros de titularidad pública, en su Artículo 20 de creación, modificación o supresión, "*la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente*".

En el caso de Entidades Locales será el Boletín Oficial de la Provincia el Diario oficial en el que publicarán la creación, modificación o supresión de los ficheros que posean.

En todo caso la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero y deberá revestir la forma que establezca su legislación específica.

Esta disposición o acuerdo deberá contener, según el Artículo 54 del Real Decreto 1720/2007:

- Identificación del fichero o tratamiento con su denominación y descripción de su finalidad y usos previstos.
- Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados suministrarlos, el procedimiento de recogida y su procedencia.
- Estructura básica del fichero mediante la descripción 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 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 pudiese ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- El nivel básico, medio o alto de seguridad que resulte exigible.

En el caso de **modificación de ficheros**, la disposición o acuerdo a publicar debe indicar los cambios producidos en los puntos anteriores.

En las disposiciones que se dicten para la **supresión de ficheros**, se debe establecer el destino de los mismos, o en su caso, las previsiones que se adoptan para su destrucción.

En las siguientes páginas podemos ver una plantilla modelo para la creación y supresión de ficheros a través del Boletín Oficial de la Provincia:

BOLETÍN OFICIAL DE LA PROVINCIA DE XXX

Ayuntamiento de XXX

El Pleno del Ayuntamiento, en sesión extraordinaria celebrada el xx de xx de xx, adoptó el acuerdo:

CREACIÓN Y SUPRESIÓN DE FICHEROS DE CARÁCTER PERSONAL

El apartado 1 art. 20 de la Ley Orgánica 15/1.999 de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) establece que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente y en su apartado 2 establece que ésta deberá indicar: La finalidad del fichero y los usos previstos para el mismo; las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos; el procedimiento de recogida de los datos de carácter personal; la estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo; Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros; los órganos de las Administraciones responsables del fichero; los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición y las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Por otra parte, se indica que en las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Por otra parte, el art. 39.2 de la misma disposición legal establece que serán objeto de inscripción en el Registro General de Protección de Datos los ficheros de que sean titulares las Administraciones Públicas.

En cumplimiento de las obligaciones que la citada normativa impone a las Administraciones Públicas, por medio del presente, el Pleno, por unanimidad,

ACUERDA:

Primero: Creación de ficheros.
Se crean en este Ayuntamiento los ficheros de datos de carácter personal señalados en el Anexo I.

Segundo: Supresión de ficheros
Quedan suprimidos los siguientes ficheros: fichero de nóminas, contabilidad creados por Acuerdo de fecha xx/xx/xxxx. Los ficheros a suprimir serán migrados a los nuevos ficheros respectivos, conforme a lo dispuesto en el art. 20.3 de la LOPD.

Tercero: Medidas de seguridad
Los ficheros automatizados que por el presente acuerdo se crean, cumplen las medidas de seguridad establecidas en el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Cuarto: Publicación y entrada en vigor
La presente resolución será publicada en el Boletín Oficial de la Provincia y entrará en vigor al día siguiente de su publicación.

ANEXO I

FICHERO: PADRÓN MUNICIPAL DE HABITANTES Y CENSO MUNICIPAL

1.- Finalidad del Fichero y los usos previstos para el mismo:

La finalidad del fichero es el registro administrativo donde constan los vecinos del municipio. El uso de este fichero es la gestión de altas, bajas y modificaciones de los habitantes del Municipio y censo municipal.

2.-Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos:

Vecinos del municipio.

3.-Procedimiento de recogida de los datos de carácter personal:

El propio interesado, la gestión propia en colaboración con el INE y resto de Ayuntamientos.

4.-Estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo:

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección postal. Datos de características personales: fecha y lugar de nacimiento, sexo, nacionalidad y lugar de procedencia. Datos académicos: nivel de estudios.

5.-Cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

No se prevén.

6.-Órganos de la Administración responsables del fichero.

Ayuntamiento de xxxx

7.-Servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

Ayuntamiento de xxx

(Dirección postal)

8.-Medidas de seguridad.

Nivel Básico.

Figura 1: Creación y supresión de ficheros en el Boletín Oficial de la Provincia

3.4 Alta de ficheros en la Agencia de Protección de Datos

Están obligados a notificar la creación de ficheros para su inscripción en el Registro General de Protección de Datos, de acuerdo con lo dispuesto en la LOPD, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal.

Según el Real Decreto 1720/2007, en su Artículo 55 de notificación de ficheros de titularidad pública:

"*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***".

Como veíamos en un punto anterior de "*Identificación de ficheros de carácter personal*", debemos tener localizados e inventariados todos los ficheros físicos y agrupados en ficheros lógicos, esto nos permitirá la sistematización de los ficheros a inscribir en la Agencia Española de Protección de Datos.

En cuanto a la determinación del nivel de seguridad del fichero lógico que será inscrito en la Agencia Española de Protección de Datos, habrá que tener en cuenta los distintos niveles de seguridad que corresponden a los diferentes ficheros físicos que se agrupan en el fichero lógico, y aplicar el más alto de ellos.

Una vez han sido localizados y determinados los ficheros de datos de carácter personal se procederá a su notificación de los mismos a la Agencia Española de Protección de Datos para su inscripción.

La notificación se deberá realizar cumplimentando los modelos o formularios electrónicos publicados en la AGPD.

Para realizar las notificaciones de ficheros, la AGPD (www.agpd.es) pone a disposición de los responsables de ficheros con datos de carácter personal, el sistema

de **Notificaciones Telemáticas a la AGPD (NOTA),** (https://www.agpd.es/index.php?idSeccion=581) se trata de una herramienta informática que asesora acerca de los requerimientos de la notificación, y permite presentar las notificaciones a través de Internet con y sin firma electrónica, y en otros soportes como el papel.

Además permite conocer el estado de tramitación de las notificaciones remitidas a través de Internet, mediante certificado de firma electrónica o mediante el código de envío generado por el formulario electrónico.

Presentación de las solicitudes:

En el caso de notificación de ficheros de titularidad pública, la presentación de las solicitudes de inscripción podrá realizarse indistintamente en soporte papel, informático o telemático, aunque en cualquiera de los casos, su cumplimentación debe realizarse a través del formulario electrónico de Notificaciones Telemáticas a la AGPD (NOTA):

- Vía telemática por Internet con firma electrónica: a través de un certificado de firma electrónica reconocido, presentando las solicitudes en el Registro Telemático de la AGPD.
- Vía telemática por Internet sin firma electrónica: firmando la hoja de solicitud y presentándola en la AGPD o en cualquier registro de las Administraciones Públicas.
- En formato papel: este formato incluye un código óptico de lectura para agilizar su inscripción.

Pasos para la notificación de un fichero mediante el formulario electrónico NOTA:

1º.- Responder a las preguntas iniciales del asistente:

A través del formulario se deberán indicar las siguientes cuestiones:

- El tipo de solicitud de inscripción:
  - Notificación de una nueva inscripción (Alta).
  - Modificación de un fichero ya registrado.
  - Supresión de un fichero ya inscrito.

En el caso de modificación y supresión de ficheros se deben indicar el código de inscripción y CIF del responsable con el que el fichero figura inscrito en el RGPD.

- El Modelo de declaración, con la posibilidad de utilizar:
  - Una notificación precumplimentada.
  - El formulario electrónico vacío.
- La forma de presentación elegida:
  - Internet con firma electrónica.
  - Internet con presentación convencional de la hoja de solicitud.
  - Formulario en formato papel con código de barras.

Figura 2: Formulario de alta de ficheros de titularidad pública

Formulario NOTA de titularidad pública, caso de **Modificación de ficheros**:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad pública
CONTENIDO DE LA NOTIFICACIÓN

NOTIFICACIONES TELEMATICAS A LA AEPD

Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

☐ Alta ☒ Modificación ☐ Supresión

Modificación

Denominación del Ministerio / Consejería / Ayuntamiento o Entidad Local / Ente público.

CIF/NIF con el que figure inscrito el fichero

Código de Inscripción

☐ Responsable del fichero o tratamiento
☐ Derechos de oposición, acceso,rectificación y cancelación
☐ Disposición general de creación, modificación o supresión
☐ Encargado del tratamiento
☐ Identificación y finalidad del fichero
☐ Origen y procedencia de los datos
☐ Tipos de datos, estructura y organización del fichero
☐ Medidas de seguridad
☐ Cesión o comunicación de datos
☐ Transferencias Internacionales

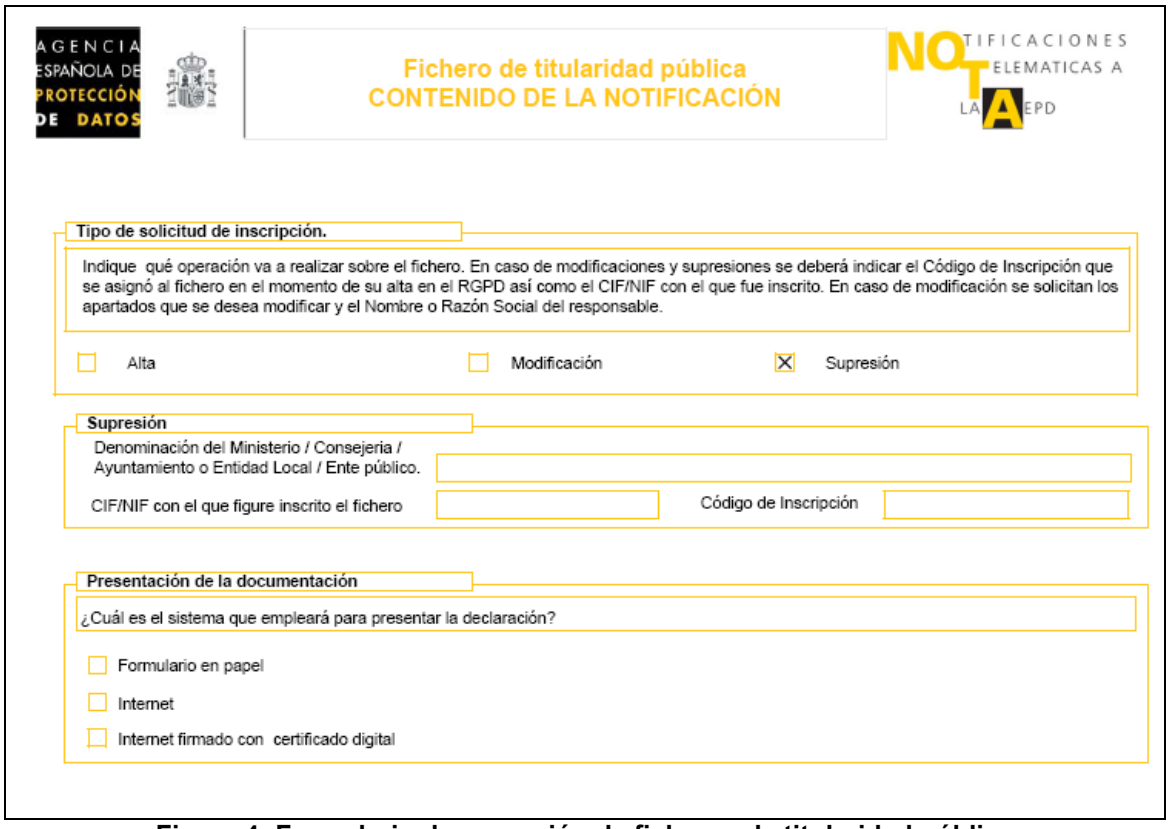
Presentación de la documentación

¿Cuál es el sistema que empleará para presentar la declaración?

☐ Formulario en papel
☐ Internet
☐ Internet firmado con certificado digital

Figura 3: Formulario de modificación de ficheros de titularidad pública

Formulario NOTA de titularidad pública, caso de **supresión de ficheros**:



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad pública
CONTENIDO DE LA NOTIFICACIÓN

NOTIFICACIONES TELEMATICAS A LA AEPD

Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

☐ Alta ☐ Modificación ☒ Supresión

Supresión

Denominación del Ministerio / Consejeria / Ayuntamiento o Entidad Local / Ente público.

CIF/NIF con el que figure inscrito el fichero

Código de Inscripción

Presentación de la documentación

¿Cuál es el sistema que empleará para presentar la declaración?

☐ Formulario en papel
☐ Internet
☐ Internet firmado con certificado digital

Figura 4: Formulario de supresión de ficheros de titularidad pública

2º. Cumplimentar los apartados de la notificación

Se compone de dos páginas de detalle y la hoja de solicitud, en las que hay que rellenar obligatoriamente los siguientes campos:

- Responsable del fichero.
- Disposición general de creación, modificación o supresión.
- Identificación y finalidad del fichero.
- Origen y procedencia de los datos.
- Tipos de datos, estructura y organización del fichero.
- Medidas de seguridad: nivel básico, medio o alto.

Es en este punto donde se han de establecer los sistemas de tratamiento de los datos, hay que indicar que los datos son tratados automatizadamente en los diferentes sistemas informáticos y, además, en formato papel.

Son opcionales los campos de:

- Derechos de oposición, acceso, rectificación y cancelación.
- Encargado del tratamiento.
- Cesión o comunicación de datos.
- Transferencias internacionales.

Posteriormente se guarda la notificación antes de pasar a la siguiente fase de cumplimentación, ya que una vez que se haya optado por cumplimentar la hoja de solicitud no se podrán realizar nuevos cambios en la notificación.

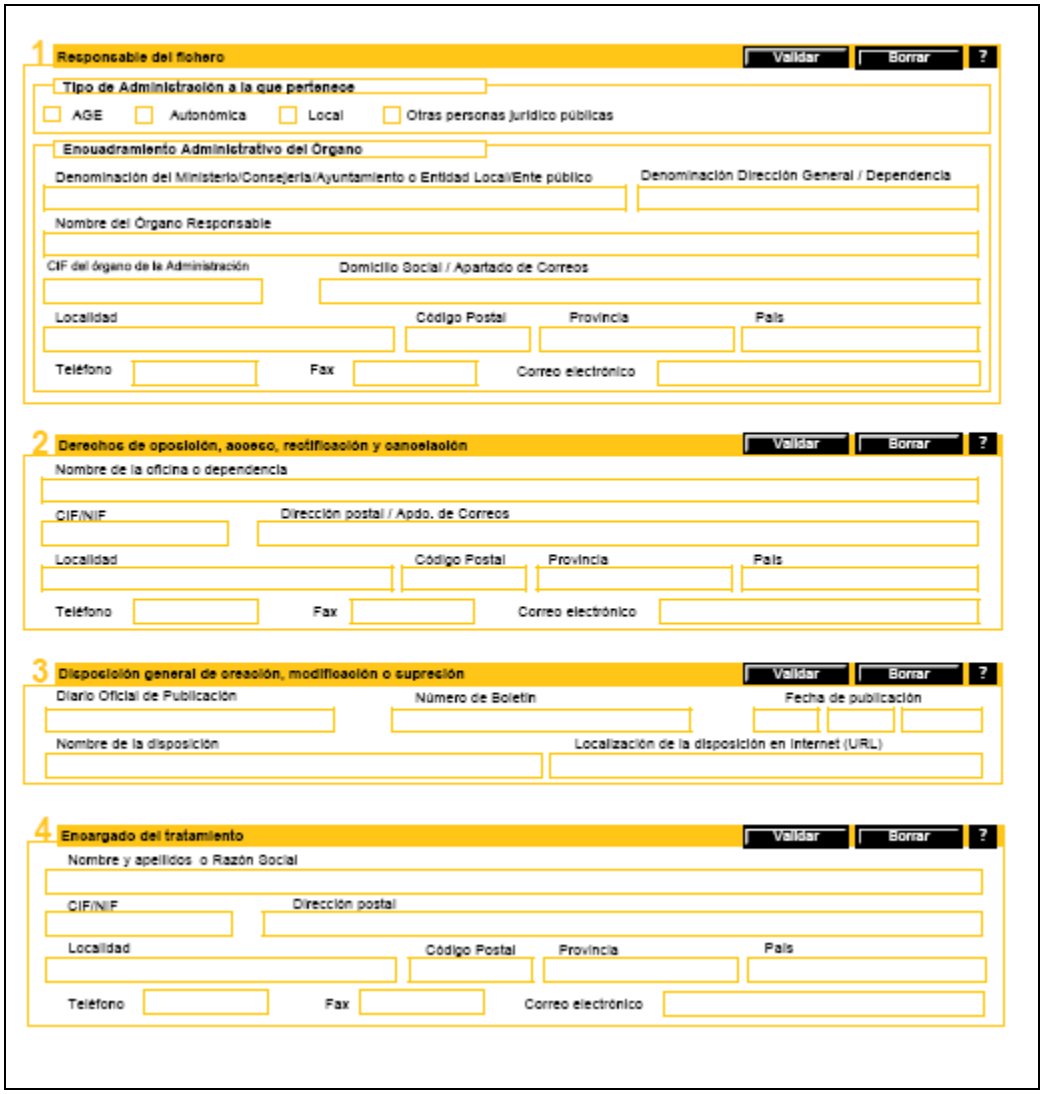


Figura 5: Formulario de notificación

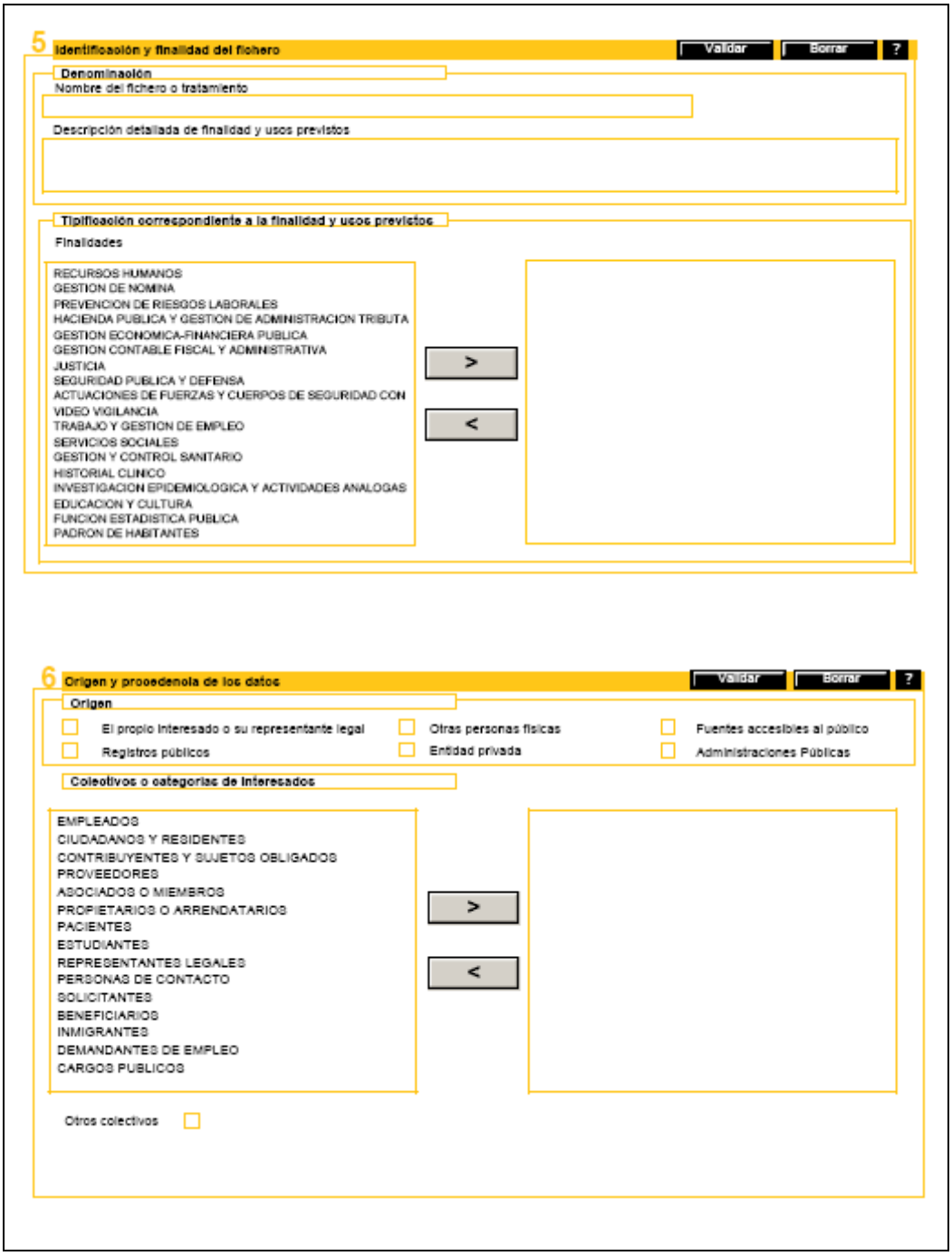


Figura 6: Formulario de notificación

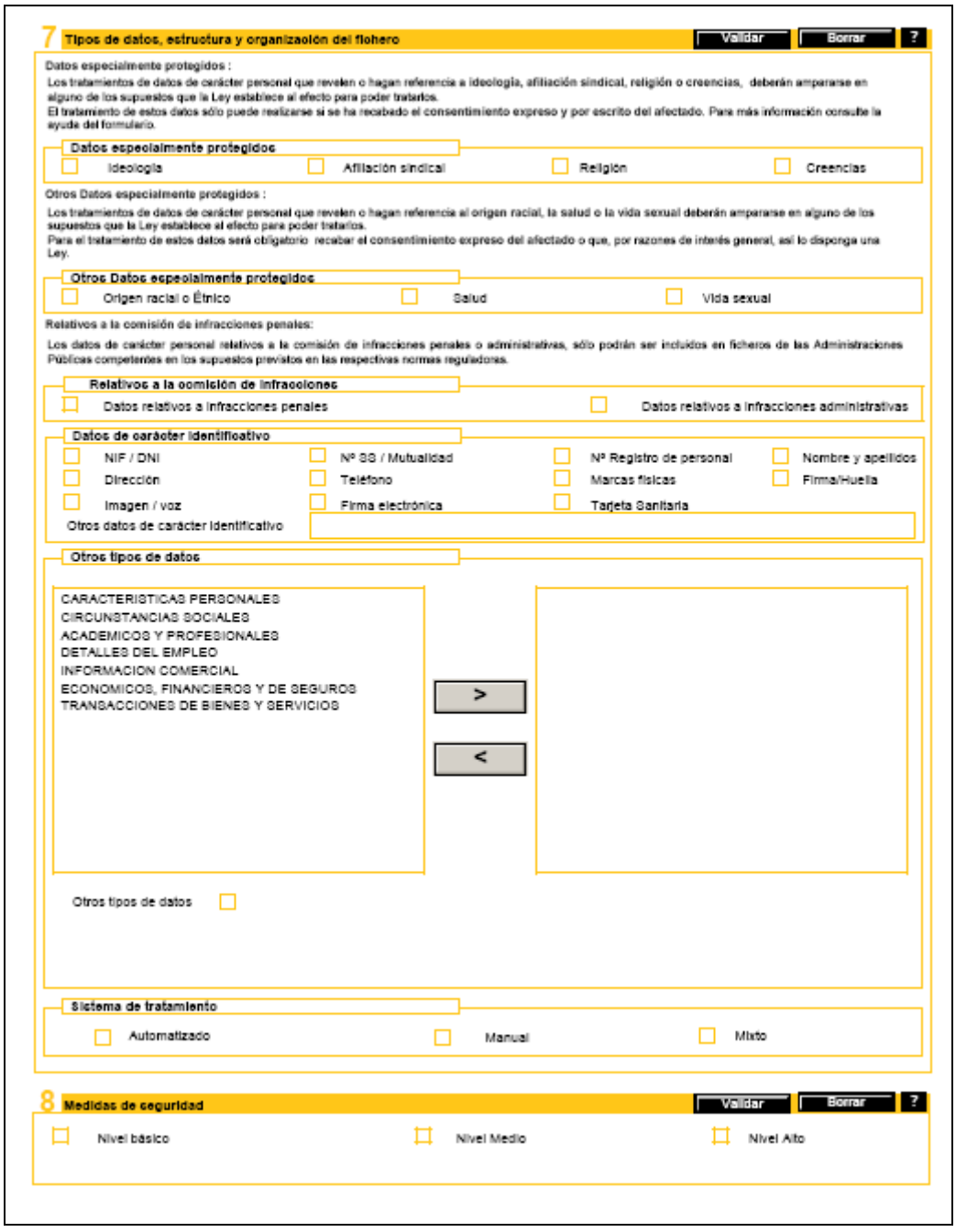


Figura 7: Formulario de notificación

Figura 8: Formulario de notificación

3º. Cumplimentar y firmar la Hoja de solicitud

En este paso se indican los datos identificativos de la persona que firma la solicitud y el cargo o la condición del firmante en relación con el responsable del fichero.

Hoja de solicitud

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad publica
SOLICITUD DE INSCRIPCIÓN

NOTIFICACIONES TELEMÁTICAS A LA AEPD

Tipo de solicitud

Actuación sobre el fichero

Datos de registro de entrada (A consignar en la Agencia Española de Protección de Datos).

Soporte de la solicitud y modo de presentación

Número del envío

Persona física que actúa en representación del responsable del fichero ante la AEPD

Datos del responsable del fichero (del Apartado 1)

CIF / NIF

Declarante

Nombre

Primer Apellido

Segundo Apellido

NIF

Cargo o condición del firmante en relación con el responsable del fichero

Dirección a efectos de notificación

Apellidos y Nombre o razón Social

Dirección postal

Localidad

Código Postal

Provincia

País

Teléfono

Fax

Correo electrónico

Medio de notificación

Dirección electrónica servicio Notificaciones

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, solicito la inscripción en el Registro General de Protección de Datos del fichero de datos de carácter personal al que hace referencia el presente formulario de notificación. Asimismo, bajo mi responsabilidad manifiesto que dispongo de representación suficiente para solicitar la inscripción de este fichero en nombre del responsable del fichero y que éste está informado del resto de obligaciones que se derivan de la LOPD. Igualmente, declaro que todos los datos consignados son ciertos y que el responsable del fichero ha sido informado de los supuestos legales que habilitan el tratamiento de datos especialmente protegidos, así como la cesión y la transferencia internacional de datos. La Agencia Española de Protección de Datos podrá requerir que se acredite la representación de la persona que formula la presente notificación.

En a de de

Firma de la persona que efectúa la notificación

Conocimiento de los deberes del declarante

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 Española de Protección de Datos (AEPD) de fecha 28 de abril de 2005, (B.O.E. nº 117) por la que se crean y modifican los ficheros de datos de carácter personal existentes en la AEPD. 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 presenta la notificación de ficheros y solicita su inscripción en el Registro General de Protección de Datos se utilizarán en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud y posteriores comunicaciones con la AEPD. Tendrán derecho a acceder a sus datos personales, rectificarlos o, en su caso, cancelarlos en la AEPD, 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.

Figura 9: Hoja de solicitud

4º. Generar o enviar la notificación

Este paso variará según el tipo de presentación elegido:

1.- A través de Internet con certificado de firma electrónica reconocido:

Las notificaciones realizadas a través de Internet con certificado de firma electrónica se remiten al Registro Telemático de la AGPD.

Una vez cumplimentada la notificación y la hoja de solicitud de forma correcta, es necesario indicar al formulario que no se van a realizar más cambios mediante el botón «Finalizar formulario» antes de proceder a la firma de la notificación. En este momento aparece un icono en el lugar previsto para la firma de la persona que efectúa la notificación.

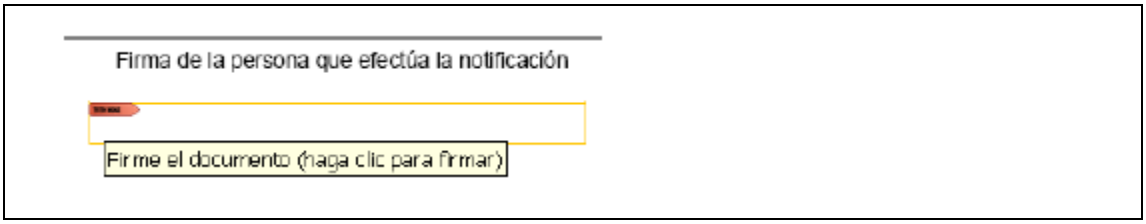


Figura 10: Firma del formulario

Pulsando el icono que aparece, se firmará la notificación con el certificado de firma reconocido, correspondiente a la persona que formula la notificación. Una vez firmada, se enviará la notificación mediante el formulario electrónico al Registro Telemático de la AGPD mediante el botón *«Generar/Enviar».*

Una vez recibida la notificación en el Registro Telemático de la AGPD, se emite por el mismo medio un mensaje de confirmación de la solicitud, en el que constan los datos proporcionados por el interesado, junto con la acreditación de la fecha y hora en que produjo la recepción y una clave de identificación de la transmisión.

El código AGPD, es el número de inscripción que el Registro General de la Agencia Española de Protección de Datos le asigna al fichero. Una vez realizado el envío de la notificación, el Registro comunica el código que se asigna.

Fichero de titularidad pública
SOLICITUD DE INSCRIPCIÓN
Confirmación de la recepción de la notificación en la AEPD

Figura 11: Confirmación de recepción de solicitud

2.- A través de Internet sin certificado de firma electrónica reconocido.

En el caso de las notificaciones realizadas a través de Internet sin firma electrónica, una vez cumplimentada la notificación y la hoja de solicitud de forma correcta, se envían mediante el formulario electrónico pulsando el botón *«Generar/Enviar»* que se encuentra en la hoja de solicitud.

El formulario le indica que se está conectando con el servidor de la AGPD y seguidamente el sistema envía la hoja de solicitud (en formato PDF) que confirma que la notificación ha sido enviada correctamente. Dicha hoja de solicitud, firmada de forma manual por la persona que efectúa la notificación, es la que se debe remitir a la AGPD o a alguno de los Registros y oficinas a los que se refiere el Artículo 38.4 de la Ley 30/1992.

La dirección de la AGPD es:

Agencia Española de Protección de Datos

Calle Jorge Juan, 6

28001 Madrid

La hoja de solicitud también puede enviarse por fax a los números 91 445 25 29 ó 91 448 36 80.

3.- En formato papel con código de barras bidimensional PDF 417

Una vez cumplimentadas la hoja de solicitud, para obtener el modelo que se presenta en la AGPD, se pulsa el botón «Finalizar formulario» que se encuentra al final de la hoja de solicitud generándose el código de barras bidimensional PDF 417 (nube de puntos), así como el correspondiente código de envío que establece la correspondencia entre el contenido que figura en cada una de las páginas que componen el modelo de notificación y la nube de puntos generada.

La hoja de solicitud una vez firmada se envía a la dirección de la AGPD, con el código bidimensional impreso, así como las dos páginas con el contenido de la notificación en las que debe figurar el código de envío generado por el formulario electrónico.

En el caso de ficheros de titularidad pública, debe acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero. Si el diario oficial en el que se encuentra publicada la norma o acuerdo es accesible desde Internet, basta con indicar en la notificación la dirección electrónica de su localización.

En la siguiente imagen vemos un ejemplo de un alta de fichero en la Agencia de Protección de Datos:

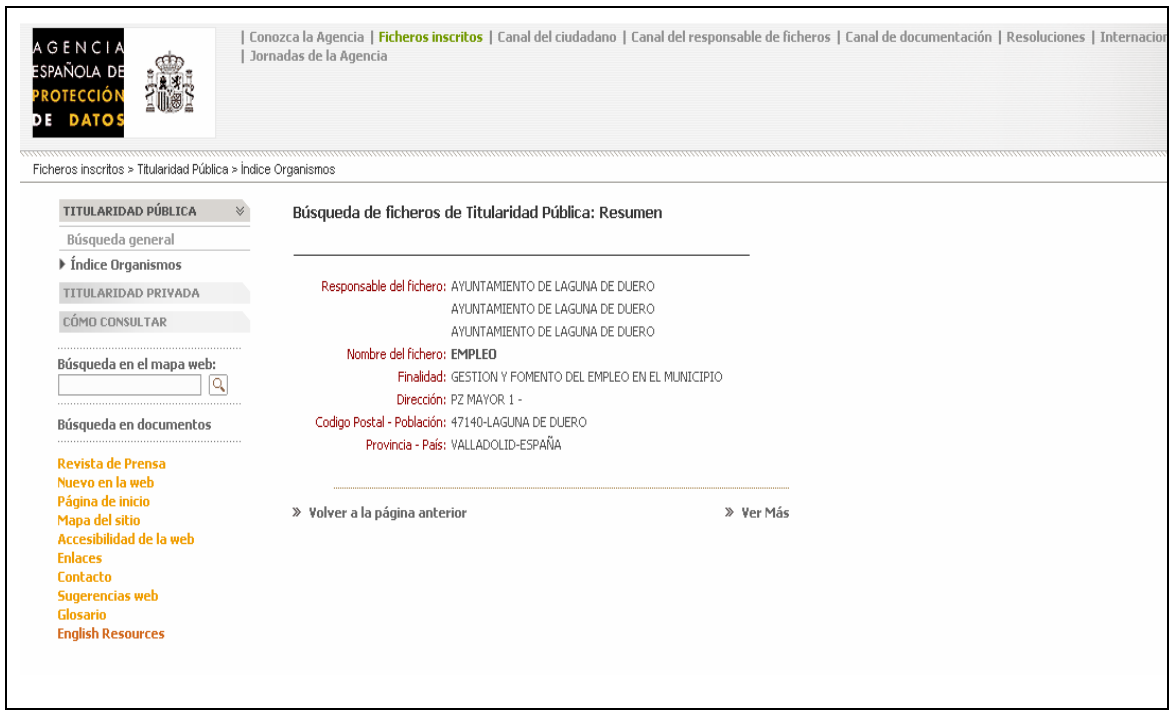


Figura 12: Alta de Ficheros en la AGPD

3.5 Redacción del Documento de Seguridad

El Artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, establece en su punto 1 que "*el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural*".

En el Real Decreto 1720/2007, de 21 de diciembre, se establecen las medidas de índoles técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente y que será de obligado cumplimiento para el personal de acceso a los sistemas de información.

Por tanto en este documento deben centrarse todas las políticas, reglas y procedimientos de seguridad establecidos por el responsable del fichero o tratamiento.

Puede existir un único documento de seguridad que comprenda a todos los ficheros o tratamientos, puede haber un documento de seguridad individual para cada fichero o tratamiento, o podrán elaborarse distintos documentos agrupando ficheros o tratamientos según el sistema utilizado en la Entidad. La Agencia Española de Protección de Datos recomienda la primera de las opciones, elaborando un único documento de seguridad para todos los ficheros.

El documento de seguridad debe contener como mínimo los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de seguridad y de recuperación de los datos en los ficheros o tratamientos automatizados.
- Las medidas a adoptar en caso de transporte de documentos y soportes, así como para la destrucción de los documentos y soportes, o la reutilización de los mismos.

Además en el caso de que fueran de aplicación medidas de seguridad de nivel medio o alto, el documento de seguridad deberá contener:

- La identidad del responsable o responsables de seguridad.
- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

Todo el personal de la Entidad que, en el desarrollo de sus funciones tenga acceso a los datos almacenados en los ficheros, deben conocer y cumplir las medidas de seguridad contenidas en el documento de seguridad.

El documento se debe mantener actualizado en todo momento y debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el

sistema de tratamiento empleado, en su organización, en el contenido de la información incluidos en los ficheros o tratamientos, o como consecuencia de los controles periódicos realizados.

3.5.1 Modelo de documento de seguridad

Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del Reglamento de Seguridad, la Agencia Española de Protección de Datos, dispone de un "Modelo de Documento de Seguridad, (https://www.agpd.es/upload/Informa%20AEPD/guia_seguridad.pdf) que pretende servir de guía y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos.

Como hemos visto antes, el reglamento da varias opciones a la hora de disponer de uno o varios documentos de seguridad. En este caso el modelo planteado expone un modelo único, organizado en dos partes: en la primera se recogen las medidas que afectan a todos los ficheros y tratamientos de forma común, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma específica.

El contenido principal de este documento queda estructurado como sigue:

I. **Ámbito de aplicación del documento**

   En este apartado se explicará que el documento de seguridad se aplica a los ficheros que contienen datos de carácter personal, a los sistemas de información, soportes y equipos empleados para el tratamiento de los datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

   Además se incluirá una relación de los ficheros o tratamientos de que se dispone y el nivel de seguridad que les corresponde.

II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

- Identificación y autenticación

  En este punto se deben especificar las medidas y normativas de identificación y autenticación del personal autorizado para acceder a los datos personales. En el caso de que la autentificación se realiza mediante contraseña se indicará el procedimiento de asignación, distribución y almacenamiento de las mismas, e indicar la periodicidad con la que se deberán cambiar. También habrá que incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña.

  En los ficheros con un nivel medio de seguridad, se indicará la limitación de intentar reiteradamente el acceso no autorizado al sistema de información.

- Control de acceso

  Será necesario indicar que el personal solo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

  Además se detallarán los mecanismos establecidos por el responsable del fichero, pare evitar que un usuario pueda acceder a recursos con derechos distintos a los autorizados.

  También será necesario identificar a la persona autorizada para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero.

  Se especificará cual son los procedimientos para solicitar el alta, modificación y baja de las autorizaciones.

- Control de acceso físico

  En el caso de ficheros automatizados y con un nivel de seguridad medio, se indicará el personal que tiene acceso a los locales donde se encuentran ubicados los sistemas de información.

- Registro de accesos

  Para los ficheros automatizados, en los accesos a los datos de los ficheros de nivel alto, se registrará por cada acceso la identificación del usuario, fecha y hora, el fichero, el tipo de acceso y si ha sido denegado o autorizado.

  Se debe indicar el periodo de tiempo durante el cual se conservarán los datos del registro de acceso, que en todo caso será inferior a dos años.

  Para el caso de de ficheros no automatizados, el acceso a la documentación se limitará al personal autorizado, especificando el mecanismo para identificar los accesos.

- Gestión de soportes y documentos

  En este punto se debe indicar el lugar de acceso restringido, el personal autorizado y el procedimiento para habilitar o retirar los permisos de acceso de aquellos soportes que contengan datos de carácter personal.

  Además se indicará el procedimiento a seguir para dar las oportunas autorizaciones a la salida de soportes y documentos con datos de carácter personal fuera de los locales bajo el control del responsable del tratamiento.

  Se indicará como llevar a cabo la destrucción o borrado de soportes, así como las medidas previstas para evitar la sustracción, pérdida o acceso indebido a la información.

- Registro de entrada y salida de soportes

  En el caso concreto de ficheros automatizados y con nivel medio y alto en medidas de seguridad, se indicará el procedimiento a seguir para su registro de entrada y salida, así como la gestión de dicho registro.

- Gestión y distribución de soportes

  Para los soportes automatizados y con un nivel alto se mostrará en este punto los criterios de etiquetado.

  En el caso de distribución y salida de soportes que contengan datos de carácter personal se deberá indicar el procedimiento para cifrar los datos garantizando que la información no sea inteligible ni manipulada durante su transporte.

  Para los dispositivos portátiles que vayan a estar fuera de las instalaciones, y no permitan el cifrado de la información se explicará las medidas alternativas a tomar.

- Criterios de archivo para ficheros no automatizados

  Establecer los criterios para el archivo de este tipo de ficheros que garanticen su conservación, localización y la consulta de información, así como posibilitar los derechos de los ciudadanos de acceso, rectificación y cancelación.

- Almacenamiento de la información

  Establecimiento de medidas que impidan el acceso a la información que contengan los ficheros no automatizados.

  En el caso de ficheros con un nivel alto de seguridad se indicará los elementos de almacenamiento, así como los lugares físicos y de protección con que cuentan.

- Custodia de soportes

  Los ficheros no automatizados cuyos datos estén en proceso de tramitación, deberán ser custodiados por las personas que estén a su cargo, impidiendo el acceso a personal no autorizado.

- Acceso a datos a través de redes de comunicaciones

  En este punto se relacionarán los accesos previstos y los ficheros a los que se prevea acceder a través de redes de comunicaciones, garantizando un nivel de seguridad equivalente al correspondiente en los accesos en modo local.

  En el caso concreto de datos de ficheros automatizados con un nivel alto de seguridad que se transmitan por redes públicas o inalámbricas de comunicaciones electrónicas, éstos deberán ir cifrados previamente, indicando los mecanismos de cifrado que se utilicen.

- Régimen de trabajo fuera de los locales de la ubicación del fichero

  Se indicará los ficheros sobre los que se pueda realizar tratamiento fuera de los locales del responsable del fichero, indicando el periodo de tiempo de validez y los usuarios concretos.

- Traslado de documentación

  Relacionar las medidas implantadas para el traslado de documentación no automatizada impidiendo su manipulación.

- Ficheros temporales

  Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el reglamento de medidas de seguridad, y serán

borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

- Copia o reproducción

  Se indicará el personal autorizado para realizar el control en la realización de copias o reproducción de los documentos con datos personales de ficheros no automatizados.

- Copias de seguridad

  Indicar la periodicidad para la realización de copias de respaldo en el caso de ficheros automatizados.

  En el caso de ficheros con nivel alto, se especificará los lugares donde se guardarán las copias de respaldo.

- Responsable de seguridad

  En este punto se indicará la persona o personas responsables de seguridad y el periodo de tiempo de desempeño de su cargo.

III. Procedimiento general de información al personal

En este capítulo se explicará cual es el procedimiento elegido para informar a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo.

IV. Funciones y obligaciones del personal

Este apartado hace referencia a la obligación que tiene todo el personal que acceda a datos de carácter personal, de conocer las normas y reglas que le afectan.

Por tanto se indicará que el personal notificará al responsable del fichero o de seguridad las incidencias encontradas.

También se deben incluir las obligaciones detalladas de los responsables de los ficheros, responsables de seguridad, etc. indicando la persona o el cargo que corresponde a cada perfil.

V. Procedimiento de notificación, gestión y respuestas ante las incidencias

Una incidencia de seguridad es un incumplimiento de la normativa desarrollada en el documento de seguridad o cualquier anomalía que afecte a la seguridad de los datos de carácter personal.

En el caso de ocurrir alguna incidencia es necesario tener descrito en este punto como se procederá para la notificación y gestión de incidencias, indicando quien tiene que notificar la incidencia, a quien y de que modo, así como quien gestionará la incidencia. Además se explicará como se guardan las incidencias y la forma y datos que se registran.

En el caso concreto de ficheros automatizados con un nivel medio y alto de seguridad se indicará el procedimiento para registrar la recuperación de datos.

VI. Procedimientos de revisión

- Revisión del documento de seguridad

  En este punto se especificará el procedimiento para llevar a cabo la modificación del documento de seguridad, indicando las personas que lo harán, lo aprobarán y la comunicación de las modificaciones al personal que pueda verse afectado.

  Siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, se debe revisar y actualizar el documento de seguridad.

- Auditoría

  Para el caso concreto de medidas de seguridad de nivel medio se indicará el procedimiento para la realización de las auditorias internas y externas.

  En el caso de ficheros automatizados, se realizará una auditoría con carácter extraordinario cuando se lleven a cabo 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.

- Informe mensual sobre el Registro de accesos

  Se indicará en este punto los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto.

VII. Consecuencias del incumplimiento del Documento de Seguridad

En este apartado se indicarán las sanciones en caso de incumplimiento de las obligaciones y medidas de seguridad establecidas en el propio documento de seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros

Deberemos añadir un anexo por cada fichero con datos de carácter personal que posea la Entidad, indicando en este apartado entre otros los siguientes datos:

- Nombre del fichero o tratamiento.
- Unidades con acceso al fichero o tratamiento.
- Identificador y nombre del fichero en el RGPD.
- Nivel de medidas de seguridad a adoptar

En el caso de ficheros con un nivel medio de medidas de seguridad, se indicará la persona designada por el responsable del fichero para coordinar y controlar dichas medidas. En este caso se incluirá además la siguiente información:

- Administrador.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento.
- Código Tipo Aplicable.
- Estructura del fichero principal.
- Información sobre el fichero o tratamiento.
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación.
- Información sobre conexión con otros sistemas.
- Funciones del personal con acceso a los datos personales.
- Descripción de los procedimientos de control de acceso e identificación.
- Relación actualizada de usuarios con acceso autorizado.
- Terceros que acceden a los datos para la prestación de un servicio.
- Relación de actualizaciones de este Anexo.

Anexo II. Nombramientos

Se adjuntarán originales o copias de los nombramientos de los diferentes perfiles incluidos en el documento, como el responsable de seguridad, etc.

Anexo III. Autorizaciones firmadas para la salida o recuperación de datos

En este apartado se adjuntarán todas las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos.

Anexo IV. Inventario de soportes

Si el inventario de soportes se gestiona de forma no automatizada, es decir en papel, se deberá recoger la información asociada al mismo.

Anexo V. Registro de Incidencias

Si el registro de incidencias se gestiona en papel, no automatizada, se recogerá en este anexo la información al efecto.

Anexo VI. Encargados de tratamiento

Cuando el acceso de un tercero a los datos del responsable del fichero es necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos.

Se incluirá en este punto el contrato realizado que indique que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizara con fin distinto al que figure en dicho contrato, ni los comunicarán ni siquiera para su conservación a otras personas.

Anexo VII: Registro de entrada y salida de soportes

Si el registro de entrada y salida de soportes, obligatorio a partir del nivel medio, se gestiona de forma no automatizada, se recogerá en este punto dicha información.

3.6 Aplicación de las medidas técnicas necesarias para cada nivel de seguridad

El Real Decreto 1720/2007 que aprueba el Reglamento de Desarrollo de la LOPD, establece una serie de medidas que el responsable del fichero deberá implementar para cada nivel de seguridad, agrupados en tres niveles, básico, medio y alto, la clasificación es disjunta pero las medidas de protección a llevar a cabo son progresivas por lo que un determinado nivel presupone o engloba el anterior:

MEDIDAS DE SEGURIDAD	NIVELES DE SEGURIDAD		
	BASICO	MEDIO	ALTO
Documento de Seguridad	√	√	√
Funciones y obligaciones del personal	√	√	√
Responsable de seguridad		√	√
Registro de incidencias	√	√	√
Identificación y autentificación	√	√	√
Control y Registro de acceso	√	√	√
Gestión de soportes y documentos	√	√	√
Copias de respaldo y recuperación	√	√	√
Auditoria		√	√
Telecomunicaciones			√
Criterios de archivo	√	√	√
Almacenamiento	√	√	√
Custodia soportes	√	√	√
Copia o reproducción			√
Traslado documentación			√

Con el nuevo Reglamento se establecen cambios en las medidas de seguridad de ficheros con datos de carácter personal. Las Entidades deberán adecuar sus sistemas de seguridad de protección de datos al nuevo reglamento, para ello la AGPD ha establecido una serie de periodos de adaptación desde el 19 de abril de 2008:

	Medidas de seguridad de nivel básico	Medidas de seguridad de nivel medio	Medidas de seguridad de nivel alto
FICHEROS AUTOMATIZADOS	12 Meses	12 Meses	18 Meses
FICHEROS NO AUTOMATIZADOS	12 Meses	18 Meses	24 Meses

Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del nuevo Reglamento, deben tener implantadas desde el momento de su creación la totalidad de las medidas de seguridad reguladas.

Según el Titulo VIII del Real Decreto 1720/2007, el Documento de Seguridad debe contemplar no solo las medidas de seguridad para ficheros automatizados, sino también deberá cumplir las medidas de seguridad de los ficheros no automatizados.

A continuación mostramos las medidas de seguridad para cada nivel, indicando en color negro las medidas que se mantienen respecto al Reglamento de Medidas de Seguridad, Real Decreto 994/1999, de 11 de Junio, en azul las medidas nuevas que aparecen en el Reglamento de desarrollo de la Ley, Real Decreto1720/2007, y en gris las que desaparecen con respecto al anterior:

➢ Documento de Seguridad

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
• 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 ficheros y sistemas de información • Procedimientos de notificación, gestión y respuesta ante incidencias • Procedimientos realización de copias de respaldo y recuperación de datos • Medidas a adoptar para el transporte, así como en caso de reutilización o desecho de soportes (utilizando medidas para evitar el acceso o recuperación de información) • Tratamiento de datos por cuenta de terceros en case a una relación contractual (Prestación de servicios). Podrá delegarse en el proveedor de servicios la llevanza del documento de seguridad	• Identificación del responsable de seguridad • Control periódico del cumplimiento del documento • Medidas a adoptar en caso de reutilización o eliminación de soportes	

➢ Funciones y obligaciones para el personal

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
• Funciones y obligaciones claramente definidas y documentadas • Funciones de control o autorizaciones delegadas claramente definidas y documentadas • Difusión, entre el personal, de las normas que les afecten y de las consecuencias por el incumplimiento		

➢ Responsable de seguridad

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
	• Uno o varios, nombrados por el Responsable del fichero • Encargado de coordinar y controlar las medidas recogidas en el documento de seguridad • Designación única del responsable para todos los ficheros o diferenciando según sistema de tratamiento • No supone delegación de responsabilidad, por parte del Responsable del fichero	

➢ Registro de Incidencias

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
• Registro de incidencias: tipo, momento de su detección, persona que la notifica, persona a la que se comunica, los efectos derivados y las medidas correctoras aplicadas. • Procedimiento de notificación y gestión de las incidencias:	**SOLO FICHEROS AUTOMATIZADOS** • Registrar la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y aquellos que hayan tenido que ser grabados manualmente • Autorización por escrito del Responsable del fichero para la ejecución de los procedimientos de recuperación.	

➢ Identificación y Autentificación

Medidas de Seguridad de nivel Básico		
Medidas de seguridad de nivel Medio		
Medidas de seguridad de nivel Alto		
SOLO FICHEROS AUTOMATIZADOS • Relación actualizada de usuarios y accesos autorizados (control de acceso) • Procedimientos de identificación y autentificación personalizada. • Procedimientos de asignación, distribución de contraseñas • Almacenamiento ininteligible de contraseñas activas • Periodicidad con que se cambian las contraseñas (caducidad), en ningún caso superior a un año.	**SOLO FICHEROS AUTOMATIZADOS** • Se establecerá el mecanismo que permita la identificación, de forma inequívoca y personalizada, de todo usuario y la verificación de que está autorizado • Limite de intentos reiterados de acceso no autorizado	

➢ Control y Registro de acceso

<table>
<tr><th colspan="3">Medidas de Seguridad de nivel Básico</th></tr>
<tr><th colspan="3">Medidas de seguridad de nivel Medio</th></tr>
<tr><th colspan="3">Medidas de seguridad de nivel Alto</th></tr>
<tr>
<td>

Control de accesos permitidos a cada usuario según las funciones asignadas.
Relación actualizada de usuarios, perfiles de usuario, y accesos autorizados
Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados
Concesión de permisos de acceso, sólo por personal autorizado
Medidas extensivas al personal ajeno con acceso a los recursos de información

</td>
<td>
<u>SOLO FICHEROS AUTOMATIZADOS</u>

Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información

</td>
<td>
<u>SOLO FICHEROS AUTOMATIZADOS</u>

Registrar usuario, hora, fichero accedido, si ha sido denegado o autorizado, tipo de acceso y registro accedido.
Control por parte del Responsable de Seguridad (informe mensual)
Conservación por 2 años de los registros
No será necesario:

Que el responsable del fichero o del tratamiento sea un persona física
Que el responsable del fichero o tratamiento garantice que únicamente él tiene acceso y los trata.

<u>SOLO FICHEROS NO AUTOMATIZADOS</u>

Control de accesos autorizados
Identificación accesos para documentos accesibles por múltiples usuarios

</td>
</tr>
</table>

➢ Gestión de soportes y documentos

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
• Inventario de soportes • Identificación del tipo de información que contienen, o sistema de etiquetado • Acceso restringido al lugar de almacenamiento • Autorización de las salidas de soportes (incluidas a través de e-mail) • Medidas para el transporte y el desecho de soportes	**SOLO FICHEROS AUTOMATIZADOS** • Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega • Medidas para impedir la recuperación posterior de datos de un soporte que vaya a ser desechado o reutilizado • Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento	**SOLO FICHEROS AUTOMATIZADOS** • Etiquetado de soportes comprensible para los usuarios autorizados y complejo de descifrar para el resto de usuarios. • Cifrado de datos en la distribución de soportes • Cifrado de datos de dispositivos portátiles cuando estén fuera de los locales del responsable del fichero • No utilización (tratamiento) de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. (En caso contrario, motivación justificada en el Documento de Seguridad y adopción de contramedidas oportunas)

➢ Copias de respaldo y recuperación

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
SOLO FICHEROS AUTOMATIZADOS • Verificar la definición, funcionamiento y aplicación de los procedimientos de copia y recuperación, al menos cada seis meses. • Copia de respaldo semanal. • Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. Solo en el caso de existencia de documentación y que la copia semanal no permitiera alcanzar este objetivo se procederá a grabar manualmente los datos que corresponda • Las pruebas no se realizarán con datos reales, salvo que se registren y se asegure un nivel de seguridad adecuado. En caso de realizar una prueba con datos reales se deberá de efectuar copia de seguridad.		**SOLO FICHEROS AUTOMATIZADOS** • Copia de respaldo y procedimientos de recuperación en lugar diferente a aquél en el que se encuentren los equipos o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación

➢ Auditorias

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
	• Al menos, bienal, interna o externa. Con carácter extraordinario, siempre que se realicen modificaciones en el SI que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas. (Iniciará un nuevo cómputo de dos años) • Verificación y control de la adecuación de las medidas • Informe de detección de deficiencias y propuestas correctoras • Análisis del responsable de seguridad y conclusiones al responsable del fichero o tratamiento • Adopción de las medidas correctoras adecuadas	

➢ Telecomunicaciones

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
		SOLO FICHEROS AUTOMATIZADOS • La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos.

➢ Criterios de archivo

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
SOLO FICHEROS NO AUTOMATIZADOS • El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición		

➢ Almacenamiento

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
SOLO FICHEROS NO AUTOMATIZADOS • Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura		**SOLO FICHEROS NO AUTOMATIZADOS** • Armarios, archivadores, etc. de documentos en áreas con acceso protegido con puertas con llave.

➢ Custodia soportes

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
SOLO FICHEROS NO AUTOMATIZADOS • Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		

➢ Copia o reproducción

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
		SOLO FICHEROS NO AUTOMATIZADOS • Sólo puede realizarse por los usuarios autorizados. • Destrucción de copias desechadas.

➢ Traslado documentación

Medidas de Seguridad de nivel Básico	Medidas de seguridad de nivel Medio	Medidas de seguridad de nivel Alto
		SOLO FICHEROS NO AUTOMATIZADOS • Medidas que impidan el acceso o manipulación.

3.7 Auditorías

A partir de un nivel medio en las medidas de seguridad de los ficheros de carácter personal, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de las medidas de seguridad.

Además siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad, se realizará una auditoria extraordinaria.

Pasos en la realización de las auditorias:

- En primer lugar será necesario identificar los ficheros que contienen datos de carácter personal objeto de la auditoría, tratamiento sobre los mismos, sistema de tratamiento, procedimientos, etc.
- Posteriormente se procede a identificar el nivel de medidas de seguridad que debe ser adoptado en base a la naturaleza de la información que contengan los diferentes ficheros que son tratados por parte de la Entidad o responsable del fichero. En función del nivel de seguridad, se reflejarían las medidas a adoptar para cada uno de los ficheros y se comprobaría si estas medidas se han establecido en la Entidad. En el caso de que la auditoria la realice una empresa externa, ésta no necesita en ningún caso visualizar los datos personales de los ficheros, sino que le basta con conocer los campos que contienen.

  En el punto IV, del Modelo de Documento de Seguridad que ofrece la Agencia Española de Protección de Datos existe una relación de algunas de las comprobaciones que se pueden realizar para la realización de la auditoría de seguridad y poder verificar el cumplimiento de las disposiciones del Reglamento.

- Como resultado de la auditoria se generarán dos tipos de informes:
    - Unos informes preliminares por fichero, que incluya:
        - Adecuación de las medidas y controles establecidas a lo dispuesto en el Título VIII del Reglamento.
        - Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
        - Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
        - Será analizado por el responsable de seguridad, y elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
    - Un informe final de Auditoria por fichero, una vez subsanadas las irregularidades, que recoja los cumplimientos, incumplimientos y recomendaciones.
- Como último paso, los informes de auditoría son revisados por el responsable de seguridad, que notifica las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la AGPD.

4 Consideraciones especiales

En el manejo de datos de carácter personal, las Entidades Públicas deberán tener en cuenta una serie de consideraciones:

- Advertencia y consentimiento en la recogida de datos de carácter personal.
- Comunicación de datos entre Administraciones Públicas.
- Regulación de movimientos con terceros.
- Transferencia internacional de datos.
- Derechos de acceso, rectificación, cancelación y oposición de los ciudadanos.

4.1 Advertencia y consentimiento en la recogida de datos de carácter personal

Los Artículos 5 y 6 de la LOPD nos hablan tanto del derecho de información en la recogida de datos como del consentimiento del afectado en el tratamiento de los mismos, como conceptos que hay que diferenciar.

Información en la recogida de Datos:

La LOPD indica que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- 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.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del fichero o su representante.

Por lo tanto, en el momento en que una Entidad vaya a realizar una recogida de datos de carácter personal, y se utilicen cuestionarios u otros impresos, se podrá añadir como cláusula las advertencias anteriores. En caso de no existir dicho cuestionario, se realizará un impreso independiente con la cláusula y que la persona firme, de manera que quede constancia de que ha sido informado y de que da su consentimiento a la recogida de datos y a su tratamiento.

Cuando los datos de carácter personal no hayan sido recabados del interesado, éste debe ser informado de forma expresa, precisa e inequívoca por el responsable del

fichero o su representante dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad.

Este derecho de información no será necesario en los siguientes casos:

- Cuando lo prevea expresamente una Ley.
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos.
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterios de la Agencia Española de Protección de Datos.
- Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad, prospección comercial, en cuyo caso en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento.

Consentimiento del afectado:

El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal, salvo en aquellos supuestos en que no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

Este consentimiento no será necesario 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 comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de datos tenga por finalidad proteger un interés vital del interesado.
- Cuando los datos se encuentren en fuentes accesibles al público y haya un interés legítimo del responsable del fichero o del destinatario de los datos.

Los datos de carácter personal solo se podrán recoger para su tratamiento y no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Los datos de carácter personal recogidos deberán ser tratados de forma leal y lícita y siempre atendiendo a los siguientes principios de calidad de los datos:

- Deberán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.
- Solo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenidos.
- Los datos deben ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
- Los datos serán cancelados cuando ya no sean necesarios para la finalidad para la que se recogieron.
- Los datos de carácter personal serán tratados de forma que permitan el ejercicio de acceso, en tanto no proceda su cancelación.

El responsable del fichero o tratamiento y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional

respecto de los mismos y al deber de guardarlos, estas obligaciones subsistirán incluso después de finalizar su relación con el titular del fichero o con el responsable del mismo.

La **cláusula de recogida de datos** es el documento que se debe utilizar como nota legal para figurar en todos los contratos, folletos o formularios en los cuales se lleve a cabo una recogida de datos de carácter personal.

En la página siguiente podemos ver dos ejemplos de cláusulas de recogida de datos de carácter personal, un modelo sin cesión de datos y otro con la cesión de datos.

MODELO DE CLAÚSULA DE RECOGIDA DE DATOS DE CARÁCTER PERSONAL

TEXTO SIN CESIÓN DE DATOS

Los datos recabados, conforme a lo previsto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, en el presente contrato serán incluidos en un fichero denominado **(Nombre del fichero ante la AEPD)**, inscrito en el Registro General de la Agencia Española de Protección de Datos y cuya titularidad pertenece a **(nombre de la Entidad dirección)**, en adelante Responsable del Fichero.

La finalidad de esta recogida de datos de carácter personal es **(indicar finalidades)**. En caso de negarse a comunicar los datos, podría ser imposible mantener cualquier tipo de relación **(administrativa, comercial o laboral)** con usted.

Vd. da, como titular de los datos, su consentimiento y autorización al Responsable del Fichero para la inclusión de los mismos en el fichero ut supra detallado. En cualquier caso, podrá ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición (siempre de acuerdo con los supuestos contemplados por la legislación vigente) dirigiéndose a **(nombre de la entidad)**, con dirección **(dirección)**, o bien y con carácter previo a tal actuación, solicitar con las mismas señas que le sean remitidos los impresos que el Responsable del Fichero dispone a tal efecto.

Por todo ello, para que conste a los efectos oportunos, Vd. Muestra su conformidad con lo que en esta cláusula detallado, de acuerdo con la firma estampada en el documento al que esta cláusula figura anexionado.

Figura 13: Cláusula de recogida de datos de carácter personal

MODELO DE CLAÚSULA DE RECOGIDA DE DATOS DE CARÁCTER PERSONAL

TEXTO CON CESIÓN DE DATOS

Los datos recabados, conforme a lo previsto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, en el presente contrato serán incluidos en un fichero denominado **(Nombre del fichero ante la AEPD)**, inscrito en el Registro General de la Agencia Española de Protección de Datos y cuya titularidad pertenece a **(nombre de la Entidad dirección)**, en adelante Responsable del Fichero.

Asimismo, el titular de los datos autoriza expresamente a ceder los mismos a las siguientes organizaciones: **(listado de empresas u organizaciones)**, con la finalidad de que estas compañías puedan remitir, por cualquier medio, información sobre sus respectivos servicios, productos, ofertas o promociones especiales **(incluir más u otras finalidades si fuere oportuno)**. Para ello el Responsable del Fichero cederá, con la finalidad indicada, los siguientes datos de carácter personal: **(listado de datos cedidos),** pudiendo Vd. en todo caso ejercitar los derechos que le asisten y que, a renglón seguido, se especifican.

La finalidad de esta recogida de datos de carácter personal es: **(indicar la finalidad de la recogida)**. En caso de negarse a comunicar los datos, podría ser imposible mantener cualquier tipo de relación (administrativa, comercial o laboral) con usted.

Vd. da, como titular de los datos, su consentimiento y autorización al Responsable del Fichero para la inclusión de los mismos en el fichero ut supra detallado. Así mismo, declara estar informado de las condiciones y cesiones detalladas en la presente cláusula y, en cualquier caso, podrá ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición (siempre de acuerdo con los supuestos contemplados por la legislación vigente) dirigiéndose a **(nombre de la entidad)**, con dirección **(dirección)**, o bien y con carácter previo a tal actuación, solicitar con las mismas señas que le sean remitidos los impresos que el Responsable del Fichero dispone a tal efecto.

En caso de que se oponga a la cesión de sus datos en los términos previstos marque una cruz en esta casilla. En caso contrario, se entenderá que presta su consentimiento tácito a tal efecto.

Figura 14: Cláusula de recogida de datos de carácter personal con cesión de datos

El responsable del fichero o tratamiento deberá conservar el soporte en el que consten estas cláusulas. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Consentimiento para el tratamiento de datos de menores de edad:

Según el artículo 13 del Reglamento de desarrollo de la LOPD, podrá procederse al tratamiento de los datos de mayores de catorce años con su consentimiento salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

No podrán obtenerse datos del menor que permita obtener información sobre los demás miembros del grupo familiar, como datos relativos a la actividad profesional de sus progenitores, información económica, etc. No obstante si podrá recabarse información de la identificación y dirección de los padres o tutores con la finalidad de recabar la autorización necesaria.

La información dirigida a menores de edad deberá expresarse en un lenguaje que sea fácilmente comprensible por ellos.

La figura del responsable del fichero o tratamiento es el responsable de garantizar que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento recabado a sus padres o tutores.

4.2 Comunicación de datos entre Administraciones Públicas

En el caso de datos de carácter personal elaborados o recogidos por las Administraciones Públicas para el desarrollo de sus funciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiera sido prevista por las disposiciones de creación del fichero o por disposición de rango superior que regule su uso o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Se permite la comunicación de datos entre Administraciones Públicas cuando una de ellas obtenga o elabore los datos con destino a otra.

En estos casos no será necesario el consentimiento previo del interesado.

No obstante la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sólo con el consentimiento del interesado.

4.3 Regulación del movimiento con terceros

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con la funciones legitimas del cedente y del cesionario con el previo consentimiento del interesado. Esta relación cedente/cesionario debe plasmarse a través de un contrato de cesión de datos de carácter personal.

De cara a la cesión de datos no será preciso el consentimiento ni un soporte contractual cuando:

- Cuando la cesión está autorizada en una Ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que tiene atribuidas.
- Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticas o científicos, o cuando los datos de carácter personal hayan sido recogidos o elaborados por una Administración Pública con destino a otra.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera que requiera acceder a un fichero o para realizar los estudios epidemiológicos.

No se considera comunicación de datos el acceso de un tercero cuando dicho acceso sea necesario para la prestación de un servicio al Responsable del tratamiento.

El tratamiento de datos de carácter personal por cuenta de terceros deberá estar regulado en un contrato de prestación de servicios que deberá contar por escrito o en alguna forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en el contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Se deberá establecer:

- Las instrucciones del responsable del fichero.
- Fin de la utilización de los datos.
- Prohibición de comunicación a otras personas.
- Las medidas de seguridad a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, de igual forma ocurrirá con los soportes o documentos en que consten datos de carácter personal objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a fines distintos que los estipulados en el contrato, responderá a las infracciones incurridas.

En la página siguiente podemos ver un ejemplo de **acuerdo de confidencialidad** entre organizaciones cuando sea necesario proporcionar información confidencial a la empresa contratada, este modelo se utilizará como referencia en aquellos casos en los que la Entidad Local lleve a cabo relaciones contractuales con un tercero y se prevea la posibilidad de proporcionarle información confidencial.

ACUERDO DE CONFIDENCIALIDAD

Por el presente documento, D/Dª _____ con NIF nº _____ actuando en nombre y representación de la empresa_____en adelante denominada **la Empresa**, con CIF_____, con domicilio comercial en _____participante en el proyecto _____, en adelante **PROYECTO**,

MANIFIESTA

- Que la **EMPRESA** se dedica a _____
- Que la **EMPRESA** dispone de información tecnológica referente al **PROYECTO**
- Que la **EMPRESA** está interesada en tener acceso a la información necesaria para llevar a cabo el **PROYECTO**

Por lo expuesto la **EMPRESA**,

SE COMPROMETE A:

PRIMERO.- A que toda la información de carácter confidencial suministrada y obtenida, NO sea facilitada a ninguna otra persona que no esté implicada en el proceso.

SEGUNDO.- A que la información de carácter confidencial obtenida en el proceso NO llegue a conocimiento de terceros por causas de negligencia, entendiéndose a tales efectos que el riesgo de pérdida casual, robo, etc. de dicha información, será responsabilidad de la **EMPRESA**.

TERCERO.- A que la información de carácter confidencial obtenida NO se utilice con fines distintos al del proyecto.

CUARTO.- A responder por el incumplimiento de las obligaciones asumidas en los compromisos anteriores, sin perjuicio, en su caso, de la responsabilidad penal de acuerdo con la legislación vigente.

En cualquier caso la **EMPRESA**, está obligada al cumplimiento de lo dispuesto en:

- La Ley Orgánica de Protección de Datos 15/1999 de 13 de Diciembre, sus disposiciones de desarrollo, y demás normativa vigente.

QUINTO.- En todo caso, la **EMPRESA** garantiza que el acceso a la información se limitará estrictamente a aquellos empleados de la misma que necesiten información para cumplir con los fines precisos en el **PROYECTO** y que éstos estarán obligados a guardar el secreto, a que obliga la Ley, de la información obtenida, extendiéndose el presente acuerdo a aquellas empresas subcontratadas y sus empleados, para la realización del PROYECTO.

SEXTO.- La duración de los compromisos asumidos en el presente documento comprenderá la completa duración del **PROYECTO**, y se prorrogará por un periodo de……..año/s a partir de la fecha de finalización del contrato, salvo que la Junta de Castilla y León autorice su difusión.

Y para que así conste a los efectos oportunos se extiende por duplicado en el lugar y fecha indicados

En ……,a…….de ……. de 20…..

Entidad

_____

Firma representante_____

DNI representante_____

Figura 15: Modelo de Acuerdo de Confidencialidad

En el caso de intercambio de información confidencial entre diferentes organizaciones, se realizará un contrato de confidencialidad, que se utilizará como referencia en aquellos casos en los que la organización lleve a cabo relaciones contractuales con un tercero y se prevea la posibilidad de intercambiar información confidencial entre ambas. En la página siguiente podemos ver un modelo de dicho contrato de confidencialidad.

CONTRATO DE CONFIDENCIALIDAD

Al objeto de garantizar la confidencialidad del presente [**Proyecto, colaboración entre las partes implicadas**], se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el (**tipo: contrato, acuerdo,...]** por ambas partes.

El contenido del acuerdo es el que figura a continuación. Contenido

DE UNA PARTE: **[nombre de la organización]**y en su nombre y representación (con poder suficiente para ello) D/Dña. **[nombre completo],** en calidad de **[cargo, administrador, apoderado,...]**

DE OTRA PARTE: **[nombre de la organización].** y en su nombre y representación **(con poder suficiente para ello)** D/Dña. [nombre completo], en calidad de **[cargo, administrador, apoderado,...]**

Reunidos en **[lugar de la firma del contrato]**, a **[día]** de **[Mes]** de **[Año]**

EXPONEN

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

PRIMERA - Definiciones

A los efectos del presente Acuerdo, los siguientes términos serán interpretados de acuerdo con las definiciones anexas a los mismos. Entendiéndose por:

- «Información propia»: tendrá tal consideración y a título meramente enunciativo y no limitativo, lo siguiente: descubrimientos, conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos de cualquier tipo, aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o no incluida en la solicitud de oferta
presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

- «Fuente»: tendrá la consideración de tal, cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ella la que suministre la Información Propia y/o cualquiera de los implicados (accionistas, directores, empleados, …) de la empresa o la organización.

- «Destinatarios»: tendrán la consideración de tales cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ellos quienes reciban la Información Propia de la otra parte.

SEGUNDA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» los efectos del presente acuerdo.

TERCERA.- Exclusión del Presente Acuerdo.

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que:
I – Sea de conocimiento público en el momento de su notificación al «Destinatario» o después de producida la notificación alcance tal condición de pública, sin que para ello el «Destinatario» violentara lo establecido en el presente acuerdo, es decir, no fuera el «Destinatario» la causa o «Fuente» última de la divulgación de dicha información.
II – Pueda ser probado por el «Destinatario», de acuerdo con sus archivos, debidamente comprobados por la «Fuente», que estaba en posesión de la misma por medios legítimos sin que estuviese vigente en ese momento algún y anterior acuerdo de confidencialidad al suministro de dicha información por su legítimo creador.
III – Fuese divulgada masivamente sin limitación alguna por su legítimo creador.
IV – Fuese creada completa e independientemente por el «Destinatario», pudiendo este demostrar este extremo, de acuerdo con sus archivos, debidamente comprobados por la «Fuente».

CUARTA.- Custodia y no divulgación.

Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme.

Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

QUINTA.- Soporte de la «Información propia».

Toda o parte de la «Información propia», papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de «Información propia», con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida.

SEXTA.- Responsabilidad en la Custodia de la «Información propia».

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuentas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como da existencia del presente Acuerdo.

Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente». El «Destinatario» deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas, de lo dispuesto en este Acuerdo.

Sin perjuicio de lo anterior, la «Fuente» podrá pedir y recabar del «Destinatario», como condición previa al suministro de la «Información propia», una lista de los directivos y empleados que tendrán acceso a dicha información, lista que podrá ser restringida o reducida por la «Fuente».

Esta lista será firmada por cada uno de los directivos y empleados que figuren en ella, manifestando expresamente que conocen la existencia del presente Acuerdo y que actuarán de conformidad con lo previsto en él. Cualquier modificación de la lista de directivos y/o empleados a la que se hizo referencia anteriormente será comunicada de forma inmediata a la «Fuente», por escrito conteniendo los extremos indicados con anterioridad en este párrafo.

Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta dos sus directivos y/o empleados como de las consecuencias que de ella se pudieran derivarse de conformidad con lo previsto en el presente Acuerdo.

SÉPTIMA.- Responsabilidad en la custodia de la «Información propia».

El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explicita de la «Fuente».
Al objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto. (En aquellos casos en los que no fuera necesaria la devolución de la «Información propia» deberá eliminarse este párrafo)

OCTAVA.- Incumplimiento.

El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

NOVENA.- Duración del Acuerdo de Confidencialidad.

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

DECIMA.- Legislación Aplicable

El presente Acuerdo de Confidencialidad se regirá por la Legislación Española, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales de (Valladolid), con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha ut supra.

Figura 16: Modelo de Contrato de Confidencialidad

4.4 Transferencia internacional de datos

Se considera **transferencia internacional de datos** toda transmisión de los mismos fuera del espacio económico europeo. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable de fichero.

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que haya sido objeto de tratamiento, o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD, salvo que se obtenga autorización previa del Director de la AGPD.

Excepciones:

- Cuando la transferencia internacional sea a través de los tratados o convenios firmados por España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico de médicos, prestación de asistencia sanitaria o tratamientos médicos.
- Cuando se refiera a transferencias dinerarias.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Para un contrato entre el afectado y el responsable del fichero, o entre éste y un tercero.
- Cuando sea necesaria para la salvaguardia de un interés público.
- Cuando sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- Cuando la transferencia se realice desde un registro público y sea acorde con la finalidad del mismo.

4.5 Derechos de acceso, rectificación, cancelación y oposición

La LOPD reconoce como derechos básicos de los afectados o titulares de los datos de carácter personal los derechos de acceso, rectificación, cancelación y oposición. Estos derechos son personalísimos y serán ejercidos por el afectado, acreditando su identidad.

La Entidad deberá conceder al interesado un medio sencillo y gratuito para el ejercicio de estos derechos.

El ejercicio de los derechos debe llevarse a cabo mediante comunicación dirigida al Responsable del fichero y contendrá:

- Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

Derecho de acceso:

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del

tratamiento, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicaciones electrónicas.
- Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud.

En la siguiente página podemos ver un modelo para el ejercicio del derecho de acceso, siempre que un ciudadano titular de datos de carácter personal desee acceder a conocer los datos que la Entidad tiene de él.

Posteriormente se muestra un posible modelo de contestación al derecho de acceso.

MODELO EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre: (Entidad local)
Dirección:

DATOS DEL SOLICITANTE

D./Dª (Nombre completo del solicitante), mayor de edad, con domicilio (nombre de la vía), nº (número), Localidad (Localidad, municipio), Provincia (provincia) C.P. (código postal), con D.N.I. (indicar el número), del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso a sus datos de carácter personal, de conformidad con los artículos 15 de la Ley Orgánica 15/1999 de Protección de Datos, y los artículos 27, 28, 29 y 30 del Real Decreto 1720/2007.

SOLICITA:

1. Que se le facilite gratuitamente el acceso a los ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, atendiendo que si transcurre este plazo sin que de forma expresa se conteste la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y el 29 del Real Decreto 1720/2007.

2. Que si la solicitud del derecho de acceso fuese estimada, se remita por (correo, correo electrónico, etc.) la información a la dirección (arriba indicada, indicar dirección de correo, etc.) en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3. Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona estén incluidos en sus ficheros, y los resultantes de cualquier colaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaros.

En (lugar), a (día) de (mes) de (año)

Firmado (nombre completo del solicitante)

Figura 17: Modelo de ejercicio de derecho de acceso

MODELO DE RESPUESTA AL DERECHO DE ACCESO

A la vista de la solicitud de D...., [tercero, funcionario, laboral, vecino, contribuyente, residente, etc. del Ayuntamiento de_____) sobre acceso a sus datos de de carácter personal incluidos en el fichero de [introducir fichero], habiendo considerado su solicitud adecuada a Derecho, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo, pasamos a informarle, dentro del plazo previsto [en el caso de que la solicitud no cumpla con los requisitos señalados en el artículo 8 se le comunicará al interesado dentro del plazo de diez días para que subsane los defectos], de lo siguiente:

1. El Ayuntamiento de _____ trata los siguientes datos de carácter personal relativos a su persona:

- Datos identificativos:
- Datos académicos:
- Datos de empleo y profesionales:
- Datos económico financieros:
- Datos de participación en servicio universitarios:
- Datos de salud:

2. La finalidad para la que se tratan sus datos es:

3. El origen de sus datos es:

4. Las empresas y organismos públicos cesionarios de sus datos son las siguientes: [introducir entidades cesionarias con la dirección. No será necesario introducir la dirección en el caso de organismos oficiales] para la finalidad de [___]

Quedamos a su disposición para cualquier cuestión.

Atentamente, El Sr Alcalde

Figura 18: Modelo de respuesta al derecho de acceso

Derechos de rectificación y cancelación

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo.

En la siguiente página podemos ver dos modelos para los ejercicios de derecho de rectificación y cancelación.

El modelo de derecho de rectificación se utilizará siempre que un ciudadano titular de datos de carácter personal desee rectificar los datos de carácter personal que la Entidad tiene de él.

El modelo de derecho de cancelación se utilizará siempre que un ciudadano titular de datos de carácter personal desee cancelar totalmente el uso de los datos de carácter personal que la Entidad tiene de él.

Además se muestran dos posibles modelos de contestación a dichos derechos de rectificación y cancelación.

MODELO EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre: (Entidad local)
Dirección:

DATOS DEL SOLICITANTE

D./Dª (Nombre completo del solicitante), mayor de edad, con domicilio (nombre de la vía), nº (número), Localidad (Localidad, municipio), Provincia (provincia) C.P. (código postal), con D.N.I. (indicar el número), del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación sobre sus datos de carácter personal, de conformidad con los artículos 16 de la Ley Orgánica 15/1999 de Protección de Datos, y los artículos 31, 32 y 33 del Real Decreto 1720/2007.

SOLICITA:

1. Que proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentran en sus ficheros.

2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4. Que, en caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En (lugar), a (día) de (mes) de (año)

Firmado (nombre completo del solicitante)

Figura 19: Modelo del ejercicio del derecho de rectificación

MODELO EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre: (Entidad local)
Dirección:

DATOS DEL SOLICITANTE

D./Dª (Nombre completo del solicitante), mayor de edad, con domicilio (nombre de la vía), nº (número), Localidad (Localidad, municipio), Provincia (provincia) C.P. (código postal), con D.N.I. (indicar el número), del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación sobre sus datos de carácter personal, de conformidad con los artículos 16 de la Ley Orgánica 15/1999 de Protección de Datos, y los artículos 31, 32 y 33 del Real Decreto 1720/2007.

SOLICITA:

1. Que en le plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.

2. Que, en el caso de que el responsable del fichero considere que la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En (lugar), a (día) de (mes) de (año)

Firmado (nombre completo del solicitante)

Figura 20: Modelo de ejercicio del derecho de cancelación

MODELO DE RESPUESTA AL DERECHO DE RECTIFICACÓN

A la vista de la solicitud de D...., [tercero, funcionario, laboral, vecino, contribuyente, residente, etc. del Ayuntamiento de_____) sobre la rectificación de sus datos de carácter personal incluidos en el fichero de [introducir fichero], habiendo considerado su solicitud adecuada a Derecho, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo, pasamos a informarle, dentro del plazo previsto, de lo siguiente:

1. Los datos de carácter personal relativos a ____ que constaban en nuestros ficheros han sido modificados de acuerdo a su solicitud efectuada en fecha ____, por lo que a partir de ahora consta en nuestros archivos.

Figura 21: Modelo de respuesta al derecho de rectificación

MODELO DE RESPUESTA AL DERECHO DE CANCELACIÓN

A la vista de la solicitud de D...., [tercero, funcionario, laboral, vecino, contribuyente, residente, etc. del Ayuntamiento de_____) sobre la cancelación de sus datos de carácter personal incluidos en el fichero de [introducir fichero], habiendo considerado su solicitud adecuada a Derecho, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo, pasamos a informarle, dentro del plazo previsto, de lo siguiente:

1. Los datos de carácter personal relativos a ____ que constaban en nuestros ficheros han sido cancelados por lo que no se realizará tratamiento alguno de los mismos en adelante.

Atentamente,

El Sr Alcalde

Figura 22: Modelo de respuesta al derecho de cancelación

Derechos de oposición

El derecho de oposición 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.
- 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.

El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud.

En la siguiente página podemos ver un modelo para ejercer el derecho de oposición.

En el caso de contestación, se podrá usar el modelo visto para el caso de cancelación de igual forma.

MODELO EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL RESPONSABLE DEL FICHERO:

Nombre: (Entidad local)
Dirección:

DATOS DEL SOLICITANTE

D./Dª (Nombre completo del solicitante), mayor de edad, con domicilio (nombre de la vía), nº (número), Localidad (Localidad, municipio), Provincia (provincia) C.P. (código postal), con D.N.I. (indicar el número), del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición al tratamiento de sus datos de carácter personal, de conformidad con los artículos 17 de la Ley Orgánica 15/1999 de Protección de Datos, y los artículos 34, 35 y 36 del Real Decreto 1720/2007.

SOLICITA:

1. Que en le plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualquier tratamiento de los datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en el Real Decreto 1720/2007 y me lo comuniquen de forma escrita a la dirección arriba indicada.

2. Que, en el caso de que el responsable del fichero considere que la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En (lugar), a (día) de (mes) de (año)

Firmado (nombre completo del solicitante)

Figura 23: Modelo de respuesta al derecho de oposición

4.6 Diferencias en el tratamiento de datos personales por las Administraciones Públicas

En cuanto a las diferencias entre el sector público y el privado con respecto a la LOPD, hay algunas cuestiones que diferencian la implantación de las medidas de seguridad, sometiéndose las Entidades Públicas a unos procedimientos de adaptación a la LOPD que presentan un grado de complejidad y dedicación superior a las entidades privadas:

- En el caso de la empresa privada, el responsable final del fichero es la persona jurídica, un autónomo o un empresario individual, y en la Administración, el responsable de fichero es la Entidad Pública, pero más en concreto, la Dirección General o dependencia que, en última instancia, decide sobre el destino y condiciones del tratamiento de datos.
- En la empresa privada, la declaración de ficheros se simplifica, pues las dinámicas de tratamientos de datos son semejantes de unas empresas a otras y todos los ficheros dependen del mismo responsable de ficheros. Por el contrario, en el caso de la Administración, la declaración de ficheros exige además la publicación en diario oficial de los ficheros que se pretende declarar y de sus contenidos.
- Las entidades públicas pueden disponer de ficheros de naturaleza privada y pública, por lo que hay que hacer un ejercicio de clasificación de los ficheros considerados según la tipología de su naturaleza.
- En el caso de la Administración Pública se excluye la obligación de pedir consentimiento para el tratamiento de los datos personales de los ciudadanos, es decir siempre que la Entidad trate datos personales necesarios para el ejercicio de sus funciones y en el ámbito de sus competencias, no necesita el consentimiento del ciudadano (Artículo 6.2 LOPD).

- Podrán realizarse cesiones de datos entre Administraciones Públicas sin consentimiento del interesado sólo en los casos en que coincidan las materias de los organismos (Artículo 21.1 LOPD).
- Se prevé la posibilidad de que una Administración elabore datos o los obtenga para comunicarlos a otras Administraciones Públicas, entendiéndose como una prestación de servicios entre Administraciones, realizados sin consentimiento (Artículo 21.2 LOPD).
- En el caso de cesión de datos de una Administración a ficheros de titularidad privada, se exige el consentimiento, incluso si se trata de datos que procedan de fuentes accesibles al público, salvo que una Ley prevea otra cosa (Artículo 21.3 LOPD).
- El régimen sancionador de la LOPD no es el mismo para ficheros de titularidad privada que para ficheros de titularidad pública. Mientras que los responsables de ficheros de titularidad privada pueden soportar sanciones de hasta 600.000€, los responsables de ficheros de titularidad pública no reciben sanciones económicas, y deberán adoptar únicamente las medidas que el Director de la Agencia Española de Protección de Datos proponga para que cesen o se corrijan los efectos de la infracción, es decir que sus motivaciones son orientadas al mantenimiento de una buena imagen y el peso del costo político.

Anexo I: Ley Orgánica 15/1999, de Protección de datos de carácter personal

Anexo II: Real Decreto 1720/2007 Reglamento de desarrollo de la Ley Orgánica de Protección de datos

Anexo III: Modelo de documento de seguridad de la Agencia Española de Protección de Datos