UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Creación de una guía para la aplicación del nivel básico, medio y alto del Reglamento de Protección de Datos para microempresas

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: **Jesús Llopis Ferriol**

Tutor: **Juan Vicente Oltra Gutiérrez**

Curso 2015-2016

Resumen

El presente trabajo de fin de grado sirve de guía para aplicar la Ley Orgánica de Protección de Datos paso a paso en empresas pequeñas. Esta desarrollado forma que sea inteligible por personal no especializado y pueda ser aplicado con facilidad, celeridad y sin un coste económico elevado.

Durante el trascurso del proyecto abarcaremos las diferentes etapas necesarias para la adaptación a la legislación vigente en materia de protección de datos. El proyecto comienza con una explicación sobre qué es la protección de datos y porque resulta fundamental. Seguidamente se explican los niveles de seguridad existentes y se proporciona un breve resumen de los pasos que van a seguirse para llevar a cabo la adaptación. Para un mayor entendimiento se propone un ejemplo ficticio de una microempresa para ayudar al usuario a tener una mejor comprensión de las medidas necesarias. Sobre este ejemplo se aplicarán los pasos descritos en cada apartado del presente trabajo.

Veremos las diferentes fases para llevar a cabo la adaptación, desde un primer análisis de la empresa que nos ayude a diferenciar la información necesaria, pasando por las medidas de seguridad que se deben adoptar o como tratar los datos personales y terminando con el desarrollo de un documento que recoja todas las medidas desarrolladas.

El proyecto está apoyado por una aplicación móvil, desarrollada para dispositivos con sistema operativo Android, que sirve para tener un mayor control sobre las fases completadas.

Palabras clave: Ley Orgánica de Protección de Datos, legislación, microempresa, niveles de seguridad, manual de uso de TIC por personal sin formación específica

Abstract

This thesis provides guidance for applying the Organic Law on Data Protection step by step in small businesses. The thesis is developed in a way that can be understandable by non-specialists and can be applied easily, quickly and without a high cost.

During the course of the project we will cover the different necessary stages to adapt to the current legislation on data protection. The project starts with an explanation of what is data protection and because it is fundamental. Then, the security levels are explained and a brief summary of the steps that will be followed to perform the adaptation provided. For a better understanding a fictional example of a small business is given to help the user to have a better understanding of the necessary measures proposed. The steps in each section of this thesis will apply on this example.

We'll see the different phases to carry out adaptation, from a first analysis of the company to help us differentiate the necessary information. through security measures to be taken or process personal data and ending with the development of a document containing all developed measures.

The project is supported by a mobile application, developed for devices with Android operating system, to have more control over the completed phases.

Key words: Organic Law on Data Protection, legislation, small business, security levels, ICT manual for people without specific training

Índice general

1. Introducción

1.1 Objetivo del proyecto

El objetivo principal del Trabajo de Fin de Grado es la elaboración de un manual de apoyo para la aplicación de la **Ley Orgánica 17/1999 de Protección de datos** en pequeñas empresas, así como una aplicación de apoyo que ayude a facilitar la implantación de las medidas necesarias para el cumplimiento de dicha ley.

El objetivo nace del desconocimiento de la LOPD en las microempresas ya sea por falta de formación, personal especializado o debido al coste de implementación, que pese a no ser muy alto, puede representar un gasto económico importante si se contrata a terceros para que lleven a cabo las medidas pertinentes para adaptarse a la ley.

Utilizando el presente documento cualquier usuario no especializado debe ser capaz de implantar una serie de medidas que hagan cumplir la normativa vigente en materia de protección de datos en su empresa. La guía ayudará usuario a reconocer que archivos de su empresa pueden llegar a ser susceptibles de incumplir la ley, de adaptarlos para el cumplimiento de la misma y tomar las medidas de seguridad necesarias para su protección. También se proporciona la documentación necesaria para ayudar a hacer más fácil el proceso de implementación, evitando al usuario una redacción de documentos extra.

La aplicación de apoyo servirá al usuario para comprobar que está realizando todos los pasos requeridos y tomando las medidas necesarias para que su empresa entre dentro de la legalidad.

1.2 ¿Qué es la LOPD?

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) es una ley orgánica española cuyo objetivo es proteger y garantizar, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas, así como de su honor, intimidad y privacidad personal y familiar.

La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Es decir, si nuestra empresa o la actividad que desarrolla recogen nombres, apellidos, fotografías, números de la seguridad social, DNIs, etc., significará que se están tomando datos personales, ya que con ellos podemos llegar a identificar a una persona.

Pero no solo debemos tener en cuenta la ley promulgada en el 1999, posteriormente aparece el **Real Decreto 1720/2007 de medidas de seguridad de los ficheros automatizados que contengan datos personales** suponiendo una enorme revisión del anterior reglamento pasando de 29 artículos a 158. Cabe destacar que el nuevo reglamento regula las medidas de seguridad de los tratamientos no automatizados (papeles).

Aunque el presente proyecto esté sustentado por estas leyes cabría destacar la reciente aprobación del **Reglamento General de Protección de Datos de la Unión Europea** aprobado el 27 de abril de 2016. Al ser aprobado tan recientemente y debido al desconocimiento de cómo va a afectar en general al tratamiento de datos, ya que no entrará en funcionamiento hasta 2018, se ha decidido no modificar en proyecto íntegramente e incluir un Anexo, el 6.13, que explica los principales cambios que se proponen en este nuevo reglamento.

1.3 ¿Está mi empresa obligada a cumplir con la LOPD?

Según el artículo 1 y siguientes de la LOPD 15/1999 la misma es aplicable para todas aquellas personas físicas o jurídicas que sean propietarias de datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento.

Es decir, en el caso de ser el usuario el administrador de la empresa o estar ejerciendo la actividad económica como autónomo, estará obligado a cumplir la ley en cualquier situación donde se recojan datos de carácter personal, veamos algunos ejemplos:

-Se almacenan documentos con los datos de los clientes y/o proveedores donde aparecen datos que los pueden identificar, como su nombre y apellidos, en formato físico (documentación escrita en papeles) o en formato digital (Cualquier tipo de programa informático: Hojas de cálculo, documentación, programas de facturación, etc.)

-Se almacenan currículos de la gente que pide trabajo a la empresa, bien en formato físico o digital.

-Se tiene trabajadores en nómina y por tanto sus datos están almacenados (contrato, nómina, seguridad social, etc.) en papel o ordenador.

-Se recogen datos a través de un formulario de contacto en la web o por correo electrónico.

-Se graban imágenes con una cámara de seguridad.

Parece evidente que se debe aplicar la LOPD en cualquier caso en que se recoja información sobre personas físicas, pero existen algunas excepciones que pueden causar confusión cuando el objeto de recogida de datos sea alguna entidad ambigua. Veamos algunos ejemplos:

Caso 1: Mi empresa solo recoge datos de empresas como entidad, no utiliza datos de personas físicas.

En el momento en que se almacena el correo electrónico con el que se contacta con la empresa, su número de teléfono o cualquier dato semejante que utilicemos para contactar con dicha entidad estamos tratando con un dato de carácter personal, puesto que puede ayudar a identificar a la persona con la que nos comunicamos.

Caso 2: Los datos de mis trabajadores, las facturas y todos los datos personales de mi empresa son llevados por una asesoría.

En este caso la responsabilidad del tratamiento de los datos, aunque sean llevados por la asesoría, recaen sobre la misma empresa. Por tanto, en el caso de que esos datos no cumpliesen con la LOPD la responsabilidad sería de la empresa. En el caso poco probable de que los datos no estuviesen en mi empresa y fuesen íntegramente tratados por nuestra asesoría sería nuestra responsabilidad asegurarnos de que la asesoría cumple con las medidas pertinentes que aseguren el cumplimiento de la ley.

Caso 3: Mi empresa solo vende al cliente directo, no utilizo facturas, únicamente un sistema de tickets.

En el caso de que no almacenásemos ningún tipo de datos personales podríamos funcionar sin aplicar ningún tipo de medida, pero en un negocio estándar va a ser imposible funcionar de esta manera. En el momento en que un cliente realice un pedido, haga una reserva o mande un e-mail ya estaríamos tratando con datos de carácter personal, por lo que ya estaríamos incumpliendo la ley si no tratamos estos datos de forma adecuada.

En resumen, en una empresa actual va a ser casi imposible trabajar sin utilizar ningún tipo de dato de carácter personal.

¿Pero qué podría pasar si decido no adaptar mi negocio a la ley por el motivo que sea?

El incumplimiento de la ley 15/1999 de Protección de Datos de Carácter Personal en cualquiera de sus aspectos puede tener consecuencias nefastas:

-Vulneración de los derechos de los empleados, clientes, proveedores con sus consecuencias legales consiguientes.

-Degradación de la imagen de nuestra marca/compañía.

-Multas, que dependiendo del nivel de gravedad, oscilan entre los 900 y los 600.000 euros.

A continuación exponemos cuales serían los diferentes niveles de gravedad y la posible sanción económica arreglo a los artículos 44 y 45 de la LOPD.

Leves: multas entre 900 y 40.000 euros.

Las acciones que podrían acarrear este tipo de sanción serían:

> a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

Graves: multas entre 40.000 y 300.000 euros

Las acciones que podrían acarrear este tipo de sanción serían:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.

c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

j) La obstrucción al ejercicio de la función inspectora.

k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones

reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

Muy graves: multas entre 300.000 y 600.000 euros

Las acciones que podrían acarrear este tipo de sanción serían:

a) La recogida de datos en forma engañosa o fraudulenta.

b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

c) No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Todas estas sanciones vienen descritas en el artículo 45 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.4 Definiciones Básicas

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Fichero no automatizado: Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzo a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica. (Todos aquellos datos que estén en papel y almacenados en carpetas, archivadores, etc.)

Ficheros de titularidad pública: Los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, las entidades u organismos dependientes de las mismas con personalidad jurídico pública y sometidas al derecho administrativo y las Corporaciones de derecho público, exclusivamente en cuanto dichos ficheros se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica.

Ficheros de titularidad privada: Los ficheros de los que sean responsables las entidades sometidas al derecho privado, no vinculados en ningún caso con el ejercicio de potestades de derecho público, incluyendo aquellos de los que sean responsables las fundaciones no sanitarias del sector público, las sociedades del sector público empresarial del Estado, Comunidades Autónomas, Provincias o Municipios, con independencia de su estructura accionarial, y las Corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica. (Todos aquellos ficheros que tienen las empresas privadas o los autónomos)

Fuentes accesibles al público: A los efectos de la LOPD se consideran fuentes accesibles al público aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Existen tres sistemas de tratamiento:

- **Automatizados:** Se aplica a los ficheros almacenados en los ordenadores.
- **No automatizados**: Se aplica a los datos en papel.
- **Mixtos:** Se aplica a aquellos que tienen tanto datos en el ordenador y como en papel.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. (En el caso de ser autónomo el responsable será el mismo y en caso de ser una microempresa será la sociedad mercantil la responsable.)

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 el caso de ser autónomo el responsable será el mismo y en caso de ser una microempresa será el administrador o una persona designada para ello.)

Documento de Seguridad: Documento que debe contener toda la información relativa a cómo van a ser tratados los datos de carácter personal de la empresa, especificando las medidas para garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, los procedimientos a realizar, las medidas de seguridad pertinentes y todo aquello que involucre la seguridad de los datos.

Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

En el caso de las microempresas o autónomos suelen ser: El informático de la empresa o la empresa de informática que lleve el mantenimiento, la asesoría que trabaje para nosotros o cualquier otra empresa que tenga acceso a los datos personales de nuestra empresa.

Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

Identificación: Procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: Procedimiento de comprobación de la identidad de un usuario.

Copia de respaldo: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Derechos Arco: Los denominados derechos ARCO son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales. Estos derechos se regulan en el Título III de la Ley Orgánica de Protección de Datos (LOPD) y en el Título III de su Reglamento de Desarrollo, y son cuatro: Acceso, Rectificación, Cancelación y Oposición.

Se trata de derechos cuyo ejercicio sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado, de forma que el responsable del fichero puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

El ejercicio de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a plazo, por lo que resulta necesario establecer procedimientos para su satisfacción. Si la persona reclamante cree que sus derechos no han sido atendidos en forma y plazo según la LOPD y su reglamento, puede acudir a la tutela de la Agencia Española de Protección de Datos (AEPD).

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 que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

- Justificación: No es necesaria, salvo si se ha ejercitado el derecho en los últimos doce meses.
- Plazos: 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. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.
- Denegación: debe motivarse e indicar que cabe invocar la tutela de la AEPD. Son motivos de denegación que el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud (salvo que se acredite un interés legítimo al efecto) y que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de sus datos.

Derecho de Rectificación: Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

- Justificación: debe indicarse a qué datos se refiere y la corrección que haya de realizarse aportando documentación.
- Plazo: 10 días hábiles.
- Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD.

Derecho de Cancelación: Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos.

- Justificación: debe indicarse el dato a cancelar y la causa que lo justifica, aportando documentación
- Plazo: 10 días hábiles.
- Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Derecho de Oposición: 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 supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de prospección comerciales o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

- Justificación: concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.
- Plazo: 10 días hábiles.
- Denegación: debe motivarse e indicar que cabe invocar la tutela de la AEPD.

2. Primeros Pasos

2.1 Conocer los diferentes niveles de seguridad

Antes de empezar a explicar las medidas pertinentes que debemos adoptar para el total cumplimiento de La Ley 15/1999 de Protección de Datos debemos conocer los diferentes niveles que existen en las medidas de seguridad previstas en el Real Decreto 1720/2007. El nivel dependerá de la sensibilidad de los datos que vamos a manejar y de lo comprometido que sea el tratamiento de los mismos.

A continuación se indican los ficheros y tratamientos a los que corresponde aplicar las medidas de seguridad relativas a cada uno de los niveles de seguridad definidos en el artículo 80 de la Ley Orgánica de Protección de Datos.

NIVEL ALTO. Ficheros o tratamientos con datos:

- 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;
- recabados con fines policiales sin consentimiento de las personas afectadas;
- y derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- 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;
- y de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

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

- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero;
- y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Las medidas de seguridad se aplican acumulativamente, lo que significa que a los ficheros que requieran un nivel de seguridad medio se les aplicarán también las medidas previstas para el nivel básico y a los fichero con un nivel de seguridad alto también se les aplicarán las medidas de seguridad previstas para los niveles básico y medio.

2.2 Pasos a seguir para la implementación de la LOPD

Antes de empezar con la explicación paso a paso de cómo implementar correctamente la LOPD en nuestra negocio es conveniente conocer por encima los diferentes pasos que vamos a llevar a cabo de forma resumida. Esto nos ayudará a esquematizar mejor los procedimientos que vamos a llevar a cabo sin entrar todavía en materia.

En el apartado 3 procederemos a desarrollar los pasos que se exponen a continuación:

1. Definir quienes van a ser los encargados del tratamiento de datos y el responsable de seguridad.
2. Detectar los ficheros de nuestra empresa que contengan datos personales, normalmente suelen ser ficheros que almacenan datos sobre clientes, proveedores y personal de la empresa. Esto no quiere decir que no puedan existir más ficheros que contengan datos de carácter personal.
3. Inscribir dichos ficheros en la Agencia Española de Protección de datos (AEPD).
4. Elaborar el Documento de Seguridad dónde figurarán las medidas a adoptar para cumplir con los diferentes niveles de seguridad.
5. Implantar las medidas recogidas en el Documento de Seguridad.
6. Firmar contratos de confidencialidad y protección de datos con los encargados del tratamiento.
7. Notificar a toda la gente a la que implique la implantación de la LOPD (trabajadores, clientes, proveedores, usuario de la web) mediante la documentación adecuada el estado de la empresa respecto a la legalidad vigente.
8. Preparar las respuestas para la gente que exija el reconocimiento de los derechos ARCO.

3. Aplicación de la LOPD

3.1 Ejemplo microempresa

Para ayudar al usuario a comprender mejor el proceso de adaptación vamos a utilizar un ejemplo ficticio pero bastante habitual i que pueda servir para la demostración de cómo aplicar medidas a distintos niveles.

DESCRIPCIÓN BÁSICA

El negocio consiste en una pequeña clínica particular dónde tendremos al médico y dueño de la clínica como administrador del negocio y a dos enfermeros que le respaldan.

La mayoría de los clientes, sino el 100%, van a ser particulares que necesiten urgentemente ayuda médica o que simplemente no quieran recurrir a la sanidad pública. En muchos de los casos el propio seguro se encargará de pagar la factura pertinente ya que el negocio está asociado con diferentes compañías de seguros, pero vamos a dejar este tema un poco de lado ya que no nos interesa su funcionamiento interno sino el cómo vamos a aplicar la LOPD.

ENCARGADOS DEL TRATAMIENTO EXTERNOS

El negocio va a tener contratada una empresa de asesoría que se encargará de llevar la contabilidad y otra empresa de informática que se encargará del mantenimiento de los equipos, del software de gestión de datos de los pacientes y de la página web dónde los clientes puedan consultar acerca de los servicios que se ofrecen y un sistema de cita previa on-line.

VIDEOVIGILANCIA

Tendremos un par de cámaras de seguridad dentro de la clínica para prever cualquier imprevisto que pueda aparecer, las cámaras cubren el interior del local y los datos se almacenan en un disco duro interno.

INFORMÁTICA

La empresa dispone de 2 ordenadores, el de recepción y el que utiliza el médico en su consulta. Ambos ordenadores almacenarán en una base de datos los historiales médicos de los clientes de la clínica mediante un software de gestión. Están protegidos por contraseñas personales para cada usuario: una del médico y otras de personal, la primera dispondrá de privilegios extra.

Los informáticos no siempre realizarán el mantenimiento personándose en la clínica, a veces accederán a los equipos de forma remota interactuando con programas que contienen datos personales.

3.2 Fase 1: Análisis y toma de datos

Para iniciar la adaptación tal como indicamos en el apartado 2.2 el primer paso será definir quienes van a ser los encargados del tratamiento de datos, así como el responsable de seguridad.

Normalmente en los negocios autónomos o microempresas el **responsable de seguridad** suele ser el mismo administrador de la empresa puesto que como dueño del negocio es el más interesado en que se cumplan la ley. Aunque esto no significa que no pueda delegar dicha responsabilidad en alguno de sus empleados.

En el caso de nuestro ejemplo el responsable sería el médico y dueño del negocio.

Los **encargados del tratamiento de datos** van a ser todos aquellos que entren en contacto con los datos de carácter personal que tenga la empresa. Esto implicaría todos aquellos que trabajan con datos de forma directa o bien con datos cedidos.

Toda **empresa externa** que con objeto de prestar un servicio acceda a datos personales de los cuáles seamos responsables es considerada encargada de tratamiento y por tanto debemos firmar un **contrato de acceso a datos** (Podemos encontrar un modelo en el Anexo 11). Dicho contrato deberá estipular la clase de tratamiento que van a recibir los datos así como las medidas de seguridad a cumplir por el encargado del tratamiento.

En nuestro ejemplo los encargados del tratamiento de datos serán:

- Los enfermeros que tratan usualmente con datos de los pacientes rellenando sus fichas médicas, tomando los datos de los clientes que soliciten cita previa, etc.
- La asesoría que lleva la contabilidad de la empresa, realiza el pago de impuestos, gestiona la seguridad social, elabora las nóminas, etc.
- La empresa de informática que se encarga del mantenimiento de los equipos informáticos y de la página web.

Pasamos a ejemplificar los datos de nuestra microempresa.

***NOTA:** Los datos que se van a proporcionar en el ejemplo son totalmente ficticios y cualquier coincidencia con datos de personas y empresas reales son pura coincidencia.

DATOS EMPRESA

NOMBRE: MedicHelp

DIRECCIÓN: C/Viver, 15 **C.P:** 03850

POBLACIÓN: Valencia **PROVINCIA:** Valencia

CIF: B12568596 **TELEFONO:** 963 556 689 **FAX:** 963 556 985

EMAIL: rrhh@medichelp.es **WEB:** www.medichelp.es

ACTIVIDAD PRINCIPAL: Asistencia Sanitaria

RESPONSABLE DE SEGURIDAD: José Tojeiro Gómez.

RESPONSABLE DE CUSTODIA DE LOS FICHEROS: José Tojeiro Gómez.

Nº DE EMPLEADOS: 3

REPRESENTANTE LEGAL

NOMBRE: José Tojeiro Gómez.

DNI: 21692689D

EMAIL: jose.tojeiro@medichelp.es

DATOS DE LOS ENCARGADOS EXTERNOS DEL TRATAMIENTO

- ASESORÍA LEGALITE S.L
  - CIF: B85636954
  - DIRECCIÓN: C/ Lepanto nº 17 pta. 5
  - REPRESENTANTE LEGAL: María Torres López

- INFOTECH S.L
  - CIF: B45855689
  - DIRECCIÓN: C/Rue del Percebe nº 18 pta.7
  - REPRESENTANTE LEGAL: Juan Martínez Oltra

Acto seguido se deberá realizar un análisis de los datos que la empresa trata y/o almacena, tiendo en cuenta que los ficheros se deben agrupar en cuanto a la finalidad de los mismos, siendo independiente para estos los distintos soportes y formatos en los que está almacenado.

Por ejemplo, el fichero de clientes de una empresa habitualmente está compuesto por los presupuestos, los pedidos, albaranes y facturas de los clientes, así como los correos electrónicos que les mandamos. Este fichero puede estar en formato manual y automatizado.

El fichero manual lo componen los documentos que almacenamos en papel, como presupuestos, pedidos, albaranes y facturas.

El fichero automatizado está compuesto por distintos ficheros individuales, hojas de Excel, bases de datos, copias de respaldo, etc.

Aunque el fichero está contenido en varios soportes (unos automatizados y otros manuales) y formatos, a efectos de notificación este es un único fichero, ya que la finalidad es única: realizar la gestión fiscal, contable y administrativa de los servicios solicitados.

Es preciso analizar también qué datos personales recabamos, almacenamos y/o tratamos, ya que en función de estos se aplicará al fichero un nivel de seguridad mayor o menor. En la inscripción a la AEPD se deben notificar los tipos de datos que recabamos y/o tratamos.

Pasamos a nuestro ejemplo ¿Qué ficheros deberíamos tener en cuenta a la hora de inscribirlos en el registro de la Agencia Española de Protección de Datos?

La respuesta básica sería: Todos aquellos que contengan datos de carácter personal, en el ejemplo serían los siguientes:

- **CLIENTES:** Existe una base de datos con los historiales médicos de los clientes que recaban todo tipo de datos personales.
- **PROVEEDORES:** Tendremos también almacenados en documentos físicos una lista de proveedores de material médico.
- **VIDEOVIGILANCIA:** Las grabaciones que realiza la cámara de seguridad contienen imágenes personales de los clientes.
- **RECURSOS HUMANOS:** Los datos de nuestros trabajadores también estarán almacenados en soportes físicos y en los ordenadores.

3. 3 Fase 2: Medidas a cumplir

Antes de proceder con la inscripción de nuestros ficheros de datos personales en La Agencia Española de Protección de Datos, debemos identificar el nivel de las medidas de seguridad que se deben aplicar en cada fichero. ¿Pero como sé qué nivel exige cada tipo de fichero?

Para ello deberemos volver al apartado 2.1 dónde se define el tipo de datos que recoge cada nivel y contrastar con los datos que contiene cada uno de nuestros ficheros.

En resumen los datos de **nivel básico** recogen: nombre, apellidos, DNI, imagen, domicilio, correo electrónico, los datos de **nivel medio**: infracciones administrativas o penales, datos que definan la personalidad tales como hobbies, actividades o currículos y por último los datos de **nivel alto** engloban datos más sensibles como: raza, ideología, pensamiento político, vida sexual o salud entre otros.

En el caso de los ficheros que hemos detectado en nuestra empresa se clasificarían de la siguiente manera:

- **Fichero Clientes** [NIVEL ALTO]: Aquí aparte de los datos de nivel básico de cada cliente también tenemos datos de nivel alto relativos a la salud de los pacientes que ayudarán al médico a realizar mejor su diagnostico.
- **Fichero Proveedores** [NIVEL BAJO]: De los proveedores tan solo conoceremos datos a un nivel básico, nombres, teléfonos y correos electrónicos que nos permitan contactar con ellos para realizar los pedidos.
- **VideoVigilancia**: El fichero de videovigilancia difiere del resto de ficheros puesto que recogen datos de carácter identificativo y en su inscripción en la AEPD no será necesario seleccionar su nivel.
- **Fichero Recursos Humanos** [NIVEL BAJO]: De nuestros trabajadores solo almacenaremos datos de nivel bajo.

Una vez tengamos claro que el nivel de seguridad de cada uno de nuestros ficheros deberemos adoptar una serie de medidas para cada nivel. En las figuras 1,2 y 3 encontraremos un cuadro resumen de las medidas agrupadas por nivel y tipo de fichero.

Todas estas medidas están regidas por una serie de artículos que encontramos en **el Real Decreto 1720/2007, de 21 de diciembre** y que podremos consultar en El Boletín Oficial del Estado (BOE).

En el Anexo 1 encontraremos un cuadro resumen de todas las medidas para agilizar la aplicación cuando seamos conocedores de dichas medidas.

3.3.1. Medidas nivel básico

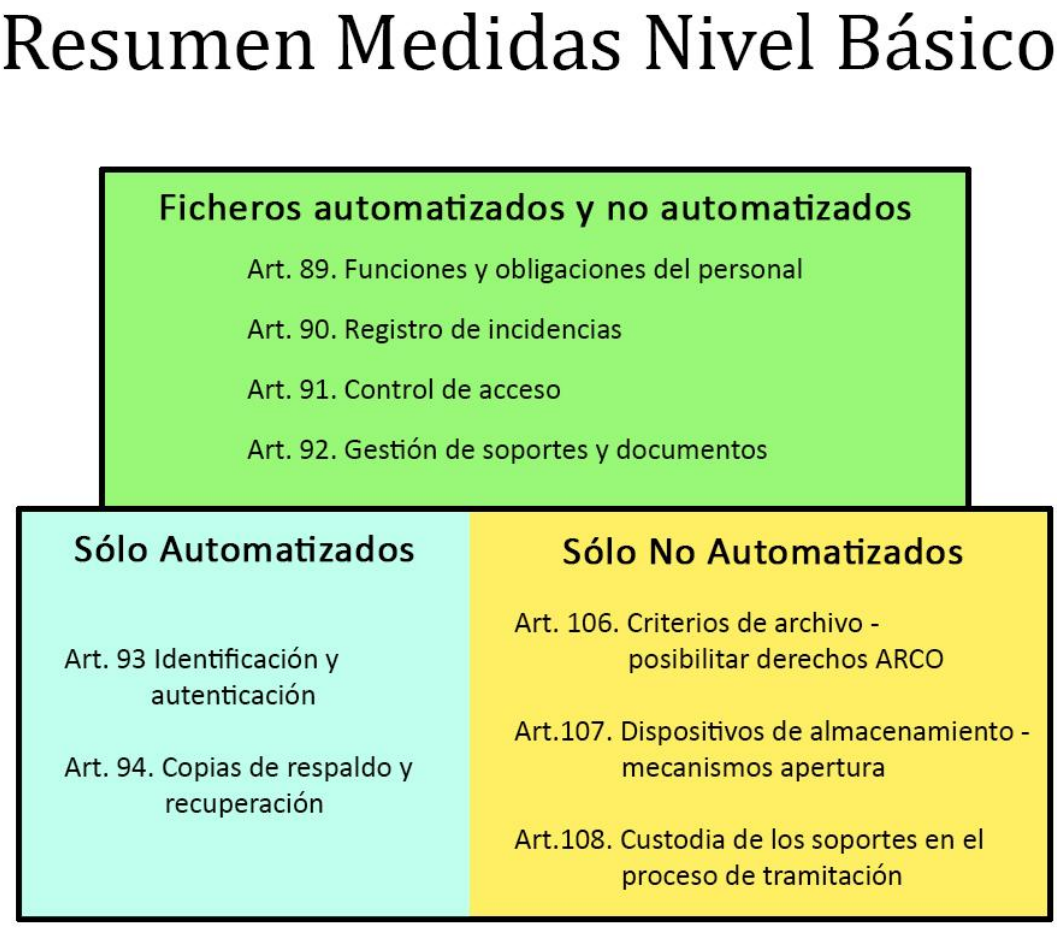


Figura 1: Tabla resumen de las medidas de nivel básico, *Fuente:* Real Decreto 1720/2007.

A continuación encontraremos los artículos tal y como aparecen en el Real Decreto 1720/2007 publicado en el Boletín Oficial del Estado. Seguidamente las medidas a adoptar que nos propone la guía aplicadas sobre nuestro ejemplo de microempresa.

Ficheros automatizados y no automatizados

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. (Podemos encontrar un modelo de registro de incidencias en el Anexo 7)

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Ficheros sólo automatizados

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Ficheros sólo no automatizados

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Medidas correctoras

Pasemos a ver como afectarían los distintos artículos a nuestra empresa ficticia y que medidas tomaríamos para asegurar su cumplimiento.

Art. 89. Funciones y obligaciones del personal: El médico deberá definir en el documento de seguridad que roles utilizan sus empleados y a que ficheros tienen acceso dichos roles. Es decir, los enfermeros, los informáticos y los trabajadores de la asesoría aparecerán en el documento de seguridad junto a los permisos que se les apliquen. Todos estos deben ser informados de su responsabilidad para con los datos a los que tengan acceso y de las consecuencias que puede acarrear el incumplimiento de las normas de seguridad. En el Anexo

2 encontramos un documento tipo, para facilitar dichas notificaciones, que deberá adjuntarse al documento de seguridad firmado por los afectados.

Es también recomendable hacer firmar a todo el personal con acceso a datos personales un compromiso de confidencialidad, para asegurarnos una mayor protección. Podremos encontrar el documento tipo en el Anexo 5.

Art. 90. Registro de incidencias: Debemos contar con un documento, bien digital o en papel, para registrar cualquier tipo de incidencia que pueda ocurrir, contamos con un modelo en el Anexo 7.

Art. 91. Control de acceso: El médico deberá tener controlado quien puede acceder a qué, lo más fácil sería un sistema de control utilizando permisos. Por ejemplo: tendríamos un usuario Enfermero que pueda acceder solo a los ficheros a los que está autorizado.

Art. 92. Gestión de soportes y documentos: Los archivadores, carpetas, CD's, etc. que contengan datos personales deberán ir identificados. Como muchos de dichos ficheros van a ser tratados por el personal informático, por ejemplo a la hora de realizar copias de seguridad, el responsable de la empresa de informática tiene que figurar en el documento de seguridad como encargado del tratamiento con los permisos pertinentes.

Si algún fichero fuese enviado a algún sitio el envío debe ser autorizado por el responsable de seguridad y quedar reflejado en el documento de seguridad. Disponemos de un modelo de Autorización de salida de documentos y soportes en el Anexo 6.

Art. 93. Identificación y autenticación: Deberemos tener un usuario y contraseña para todos los usuarios que utilicen ordenador en la empresa. La periodicidad con que se debe cambiar la contraseña aparecerá en el documento de seguridad y no debe rebasar un año.

Art. 94. Copias de respaldo y recuperación: La empresa de informática puede ayudarnos a establecer un sistema de copias de seguridad semanales, siempre cuándo les hayamos otorgado el permiso para hacerlo y quede reflejado en el documento de seguridad. Se debe notificar al informático responsable que cada 6 meses deberá comprobar las copias.

Las copias podría hacerlas el propio médico, pero no es recomendable puesto que los datos pueden correr peligro por el desconocimiento informático.

Las copias deberán guardarse en algún sitio seguro dónde solo los responsables de las mismas puedan acceder, por ejemplo un cajón con cerradura.

Art. 106. Criterios de archivo: La empresa está obligada a permitir el ejercicio de los derechos ARCO de cualquier usuario del cual se almacenen datos personales, por tanto deberemos tener bien localizada la información y preparar la documentación necesaria para facilitar a los usuarios el ejercicio de sus derechos. Podemos encontrar plantillas de cómo responder a los usuarios que soliciten ejercer cualquier derecho ARCO sobre nuestra documentación en el Anexo 3.

Art. 107. Dispositivos de almacenamiento: Deberemos tener toda aquella documentación escrita que contenga datos de carácter personal en un sitio que limite el acceso al personal no

autorizado. El lugar de almacenamiento puede ser por ejemplo un armario o un cajón con llave, del que solo tienen copias el médico y los responsables de los datos que contengan.

Art. 108. Custodia de los soportes en el proceso de tramitación: Si por ejemplo pasamos algunos datos a la empresa gestora para realizar un trámite, la persona responsable, por defecto el médico; o si ha sido autorizado, algún empleado de la gestoría, deberá asegurarse de que nadie más tenga acceso a esos datos.

3.3.2. Medidas nivel medio

A continuación expondremos una serie de medidas que van dirigidas a ficheros de nivel medio. Esto quiere decir que todos aquellos ficheros considerados de nivel básico quedarán exentos de estas medidas, no obstante los ficheros de nivel alto deberán cumplir con ellas también, así como con las de nivel básico y nivel alto. En el caso de nuestra empresa ficticia solo aquellos documentos o ficheros con datos sobre los clientes que recaban información sobre su salud (Datos de Nivel Alto) deberán cumplir con las medidas siguientes.

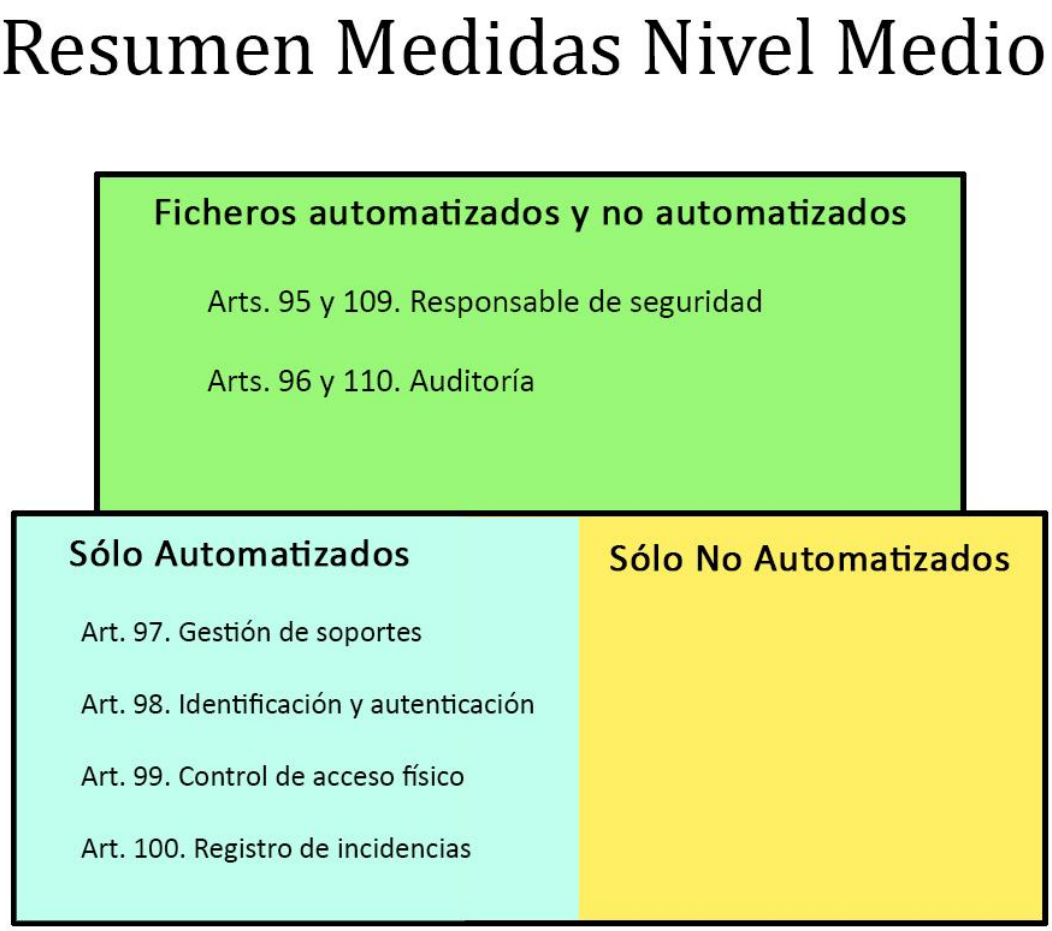


Figura 2: Tabla resumen medidas nivel medio. *Fuente:* Real Decreto 1720/2007.

Ficheros automatizados y no automatizados

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.

b) Niveles de seguridad.

c) Encargado del tratamiento.

d) Prestaciones de servicios sin acceso a datos personales.

e) Delegación de autorizaciones.

f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

g) Copias de trabajo de documentos.

h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.

b) Registro de incidencias.

c) Control de acceso.

d) Gestión de soportes.

Ficheros sólo automatizados

Artículo 96. Auditoría.

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

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

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

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

Medidas Correctoras

Igual que hemos hecho en el apartado anterior, procedemos a explicar cómo afectaría cada uno de los artículos propuestos a nuestra empresa ficticia.

Arts. 95 y 109. Responsable de Seguridad: En el documento de seguridad de la empresa deberá aparecer quien o quienes son los responsables de seguridad, aquellos encargados de llevar a cabo las medidas que el propio documento propone.

El más interesado en el cumplimiento de estas medidas y el usuario con más permisos es el dueño de la clínica, por tanto resulta lógico asignarle a él este rol. En caso de que el trabajo a realizar excediese las posibilidades del mismo, se podría designar otro responsable para tratar con el documento de seguridad. En el Anexo 4 encontramos un modelo de Carta de nombramiento del responsable de seguridad.

Arts. 96 y 110. Auditoría: Cada dos años el Servicio de Auditoría de Protección de Datos comprobará que nuestra empresa cumpla con lo siguiente:

- Análisis de la situación actual de la empresa.
- Comprobar que los ficheros inscritos ante el Registro General de Protección de Datos se corresponden con la situación real y actual de la organización.
- Comprobar que la organización recaba, trata y almacena los datos personales cumpliendo con los principios de calidad, deber de información al interesado y obtención del consentimiento, establecidos legalmente.
- Analizar si existen cesiones de datos en la actualidad y comprobar que su realización es conforme a derecho.
- Analizar si existen transferencias internacionales de datos en la actualidad y comprobar que su realización es conforme a derecho.
- Determinar si se firman los debidos contratos con aquellas personas o entidades que tienen acceso a los datos para la prestación de un servicio al responsable del fichero (encargados del tratamiento) y si los mismos contienen las estipulaciones contempladas en la legislación.
- Análisis del Informe de Auditoría previo, si lo hay, con el fin de conocer cuáles son las deficiencias en el momento de su redacción, las medidas correctoras propuestas, si éstas han sido implementadas y las deficiencias corregidas.
- Revisión de procedimientos, normativas, reglas y estándares de seguridad elaborados e implantados en la organización.
- Análisis y verificación del cumplimiento de las obligaciones que le corresponden al responsable de seguridad.
- Revisión y comprobación del cumplimiento de las políticas internas de la organización, incidiendo en las relacionadas con las funciones y obligaciones del personal (deber de secreto, confidencialidad, etc.).
- Comprobar que las medidas de seguridad implantadas en la organización tanto a nivel físico como informático para la defensa de la integridad, seguridad y confidencialidad de los datos personales son las adecuadas y se ajustan a lo

señalado en el RLOPD 1720/2007 (España M. d., Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 2008).

- Analizar el Documento de Seguridad y comprobar que cumple con todos los requisitos de contenido mínimo que marca la Ley, atendiendo a nuevas interpretaciones y recomendaciones de la AEPD.
- Redacción del Informe de Auditoría de la organización relacionando todas las incidencias encontradas y proponiendo las medidas correctoras o complementarias pertinentes.

Con el seguimiento de la presente guía el usuario debería ser capaz de cumplir con todos estos requisitos sin necesidad de contratar una empresa externa que se encargue de realizar la auditoría.

En el apartado 3.6 detallaremos el procedimiento para llevar a cabo una Auditoría interna.

Art. 97. Gestión de soportes: Deberemos establecer un documento o aplicación para tener controlados los documentos con datos de carácter personal que puedan entrar o salir de la empresa. Al ser un negocio bastante pequeño nos podría servir un documento Word o Excel donde apuntar el tipo de documento o soporte, la fecha y hora, el emisor o receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable del envío o recepción que deberá estar debidamente autorizada.

Art.98. Identificación y autenticación: A no ser que nuestro médico tenga idea de informática deberá pedir al encargado de llevar el control de las contraseñas de los ordenadores, de la base de datos de pacientes o de todo soporte digital que requiera de autenticación, que limite el número de intentos de acceso.

Art. 99. Control de acceso físico: Estando el ordenador en el despacho principal donde trabaja el médico y teniendo almacenados ahí los únicos datos que requieren de un nivel medio de seguridad, se debe de limitar el acceso a toda persona no autorizada previamente en el documento de seguridad. Una forma sencilla sería cerrando el despacho con llave cuándo el médico no se encuentra en el local.

Art. 100. Registro de incidencias: En el registro de incidencias, del que hablamos en las medidas de nivel básico, se debe incluir también la información de cuando se realiza un proceso de recuperación de datos de nivel medio. Es decir, en el momento que tengamos que recuperar cualquier información de las copias de seguridad de algún documento que involucre a los clientes deberá constar en el registro de incidencias. Podemos encontrar un modelo de Registro de incidencias en el Anexo 7.

Todo proceso de recuperación de datos debe ir autorizado por el responsable del fichero. Podemos encontrar un modelo de Autorización para la recuperación de datos en el Anexo 8.

3.3.3. Medidas nivel alto

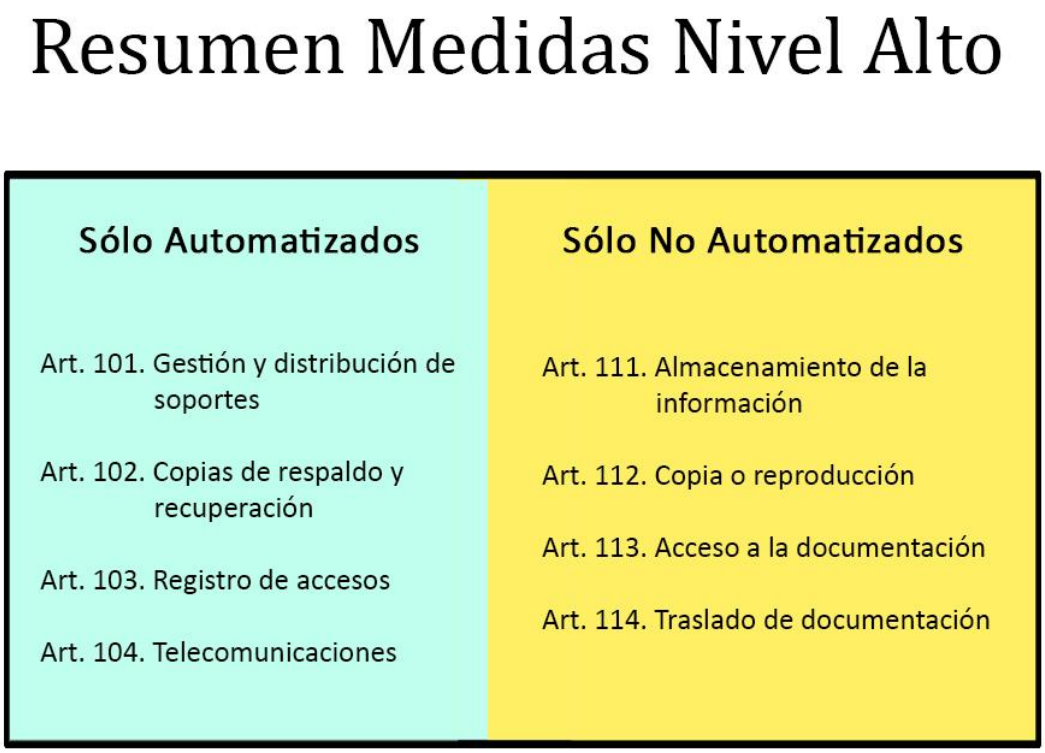


Figura 3: Tabla resumen medidas nivel alto, Fuente: Real Decreto 1720/2007.

Sólo Automatizados

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Ficheros sólo no automatizados

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Medidas correctoras

Como hemos hecho en las medidas de nivel básico y medio, pasamos a describir como afectarían las medidas de nivel alto a nuestro ejemplo de negocio.

Art. 101. Gestión y distribución de soportes: Para la aplicación de esta medida conviene tener contratada una empresa informática o bien un informático que tenga conocimientos sobre el cifrado de datos. Nuestra base de datos de clientes no podrá salir de la empresa a no ser que vaya encriptada de manera que resulte imposible acceder a dichos datos sin descifrarlos.

Deberemos tener en cuenta también los ordenadores que utilizamos a la hora de tratar dichos datos, el ordenador deberá soportar un sistema de cifrado para garantizar su seguridad. En el caso de que esto no fuese posible deberá constar en el documento de seguridad y se adoptarán las medidas necesarias para tener en cuenta los riesgos.

Es importante que la empresa que lleve nuestra información sea de confianza y personal especializado en temas de cifrado de datos.

Art. 102. Copias de respaldo y recuperación: Es conveniente tener más de una copia de seguridad de los datos y tener al menos una separada de las demás. Imaginemos que hay un incendio en el edificio y la oficina queda íntegramente destruida, perderíamos todos los datos a no ser que almacenemos una copia de seguridad en un lugar diferente.

Igual que las demás, la copia separada deberá cumplir las medidas de seguridad exigidas anteriormente.

Art. 103. Registro de accesos: En el caso de que el único que pudiese acceder a la base de datos de clientes fuese el responsable del fichero, en este caso el médico, no tendríamos porque establecer un registro de accesos, pero es muy probable que la aplicación que manejamos o el propio ordenador que la contiene fallen alguna vez y precisen de la revisión de un informático. En este caso deberíamos, aparte de autorizarlo en el fichero de seguridad como ya hemos explicado en apartados anteriores, pedirle que nos genere un Registro automático de los accesos a la aplicación. Un registro que contenga los datos del usuario que accede, la fecha y hora, si ha sido autorizado o denegado, etc. Con este registro el responsable de seguridad debe cerciorarse de que nadie accede sin permiso y redactar un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Art. 104. Telecomunicaciones: Toda comunicación de datos personal de nivel alto que realicemos por redes públicas o redes inalámbricas, es decir toda comunicación vía e-mail, teléfono, carpetas en red; debe ir cifrada. Una vez más deberemos contar con el apoyo de un informático dotado de los conocimientos necesarios.

Art. 111. Almacenamiento de la información: En el caso de la clínica los datos de nivel alto están guardados en el ordenador y por lo tanto no tendríamos que aplicar ninguna medida. A aún así, como ya hemos explicado anteriormente, es necesario que la habitación donde estén ubicados los datos tenga la seguridad necesaria para evitar el acceso no autorizado.

En el caso de poseer datos de nivel alto en un formato no automatizado tendríamos que guardarlos bajo llave u otro dispositivo que impida su acceso.

Art. 112. Copia o reproducción: Todas la copias que realicemos deben estar supervisadas por el personal autorizado en el documento de seguridad y posteriormente ser desechadas de forma que queden irrecuperables.

Art. 113. Acceso a la documentación: Igual que cuando accedíamos a datos en el ordenador de nivel alto establecíamos un registro de acceso, debe ser igual para cuando se acceden datos en formato no automatizado, sobra decir que el acceso a dichos datos debe ir previamente autorizado.

Art. 114. Traslado de documentación: Si alguna vez tenemos que trasladar documentación tendremos que ir con cuidado de que nadie puede acceder a ella, si por ejemplo vamos a mover un archivador de la oficina a casa este debe ir protegido con un maletín con cierre.

3.4 Fase 3: Inscripción de ficheros en la AEPD

3.4.1. ¿Qué es la AEPD?

Hemos hablado anteriormente de la Agencia Española de Protección de Datos o AEPD ¿Pero que es realmente este organismo? ¿Qué funciones lleva a cabo?

La Agencia Española de Protección de Datos (AEPD), creada en 1993, es el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Tiene su sede en Madrid y su ámbito de actuación se extiende al conjunto de España.

Es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la Administración pública en el ejercicio de sus funciones. Su principal misión es velar por el cumplimiento de la legislación de protección de datos por parte de los responsables de los ficheros (entidades públicas, empresas privadas, asociaciones, etc.) y controlar su aplicación a fin de garantizar el derecho fundamental a la protección de datos personales de los ciudadanos. La AEPD lleva a cabo sus potestades de investigación fundamentalmente a instancias de los ciudadanos, aunque también está facultada para actuar de oficio. La Agencia es estatutaria y jerárquicamente independiente y se relaciona con el Gobierno a través del Ministerio de Justicia.

En España, además, existen agencias de protección de datos de carácter autonómico en Cataluña y en el País Vasco, con un ámbito de actuación limitado a los ficheros de titularidad pública declarados por las Administraciones autonómicas y locales de sus respectivas comunidades autónomas.

3.4.2. Nombramiento de responsables

Ahora que conocemos un poco mejor la AEPD estamos en disposición de comenzar con la inscripción de ficheros.

En primer lugar debemos tener identificados los diferentes ficheros que vamos a inscribir y el nivel de protección que tiene cada uno de ellos (cosa que aprendimos en el apartado 3.3), así como también designar quien serán los encargados del tratamiento de cada fichero y el responsable de seguridad.

En el caso de MedicHelp (nuestra microempresa ejemplo):

El **encargado de Seguridad** seria el médico de cabecera y dueño de la clínica, José Tojeiro Gómez.

Para cada uno de los ficheros tendremos diferentes **encargados del tratamiento de datos**:

- **Fichero Clientes** [NIVEL ALTO] – InfoTech S.L., la empresa informática que tenemos contratada para que nos lleve el mantenimiento informático, la web y la aplicación que gestiona la base de datos de los clientes.
- **Fichero Proveedores** [NIVEL BAJO] – Enfermeros, los enfermeros que tengamos contratados (Los nombres pueden variar ya que la plaza no suele ser fija) serán los que se encarguen del inventario de la clínica, por tanto los responsable de pedir material médico cuando este escasee.
- **Fichero Recursos Humanos** [NIVEL BAJO] – Asesoría Legalité, se encargarán de la redacción de las nóminas, la gestión del presupuesto, inscripción de trabajadores en la Seguridad Social, etc.
- **VideoVigilancia** [NIVEL BAJO] **–** InfoTech S.L., la empresa de informática gestionará el almacenamiento de las cintas de seguridad.

3.4.3. Inscripción

Ahora que tenemos los ficheros correctamente identificados, procedemos a su inscripción en la AEPD.

Si buscamos AEPD en Google nos aparecen dos resultados a tener en cuenta. El primer enlace, marcado con un recuadro rojo en la figura 4, es la página oficial de la Agencia Española de Protección de Datos. Podemos encontrarla en la siguiente dirección web: www.agpd.es.

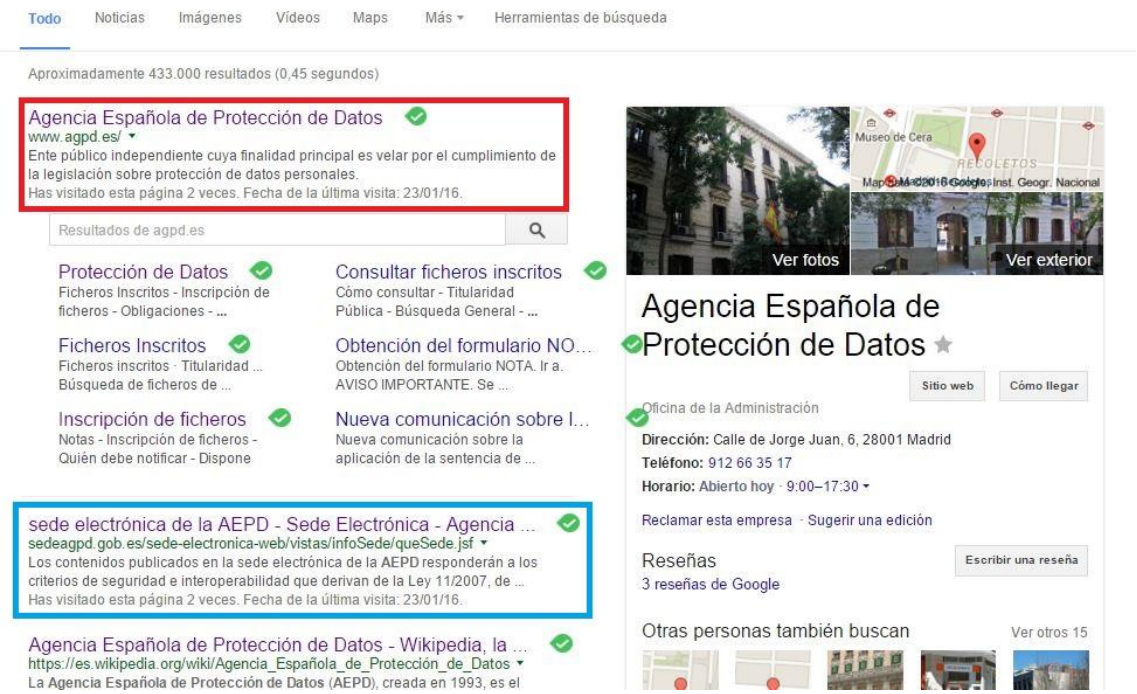


Figura 4: Búsqueda en Google de la AEPD. *Fuente:* Google

En esta página encontramos las últimas noticias sobre materia en protección de datos, así como toda clase de información pertinente a la legislación. También nos permite consultar los ficheros que tenemos inscritos, accediendo en el menú al apartado “Ficheros Inscritos” y seleccionando la opción del menú desplegable “Titularidad Privada” (Marcado en rojo en la Figura 5). Para buscar los ficheros debemos ingresar el nombre del responsable del fichero inscrito, así como el CIF en el caso de que sea una empresa o el NIF en caso de ser autónomo.

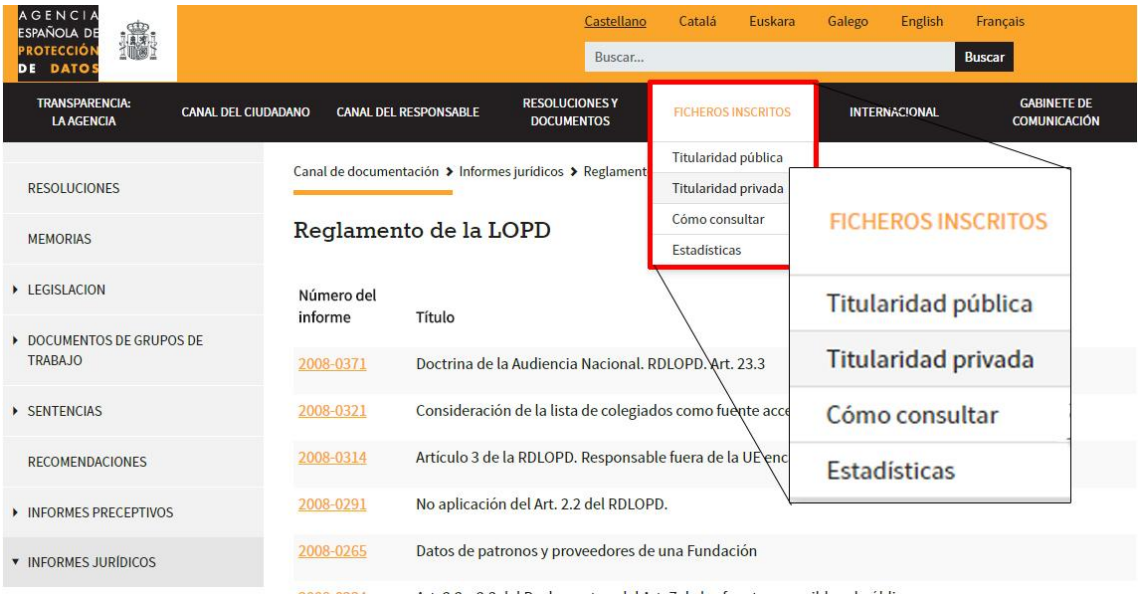


Figura 5: Consulta de Ficheros Inscritos de Titularidad privada. *Fuente:* https://www.agpd.es

Esta página puede resultarnos útil para ampliar nuestros conocimientos en materia de protección de datos, pero a la hora de llevar a cabo la inscripción de nuestros ficheros, el enlace que nos interesa es el que nos lleva a la **Sede Electrónica de la AEPD**, aparece marcado con un cuadro de color azul en la Figura 4. Podemos acceder a la página desde el siguiente enlace: http://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/queSede.jsf

Figura 6: Sede electrónica de la AEPD. *Fuente:* https://sedeagpd.gob.es

Para empezar con la inscripción de ficheros, iremos a la tercera opción del menú de la izquierda "Procedimientos electrónicos", marcado en color rojo en la figura 6. Una vez se nos habrá la nueva ventana, debemos seleccionar la sexta opción de la lista "Inscripción de ficheros", marcado en rojo en la figura 7.

Figura 7: Procedimientos electrónicos, Inscripción de Ficheros. *Fuente:* https://sedeagpd.gob.es

A continuación nos aparecerá un texto donde se explica brevemente que es la inscripción de ficheros, cómo se lleva a cabo y que derechos se tienen sobre estos ficheros, lo leeremos detenidamente y al final del texto pulsaremos en la opción de “Continuar”.

Importante: Debemos que tener en cuenta que para cada fichero de nuestra empresa que vayamos a inscribir se debe realizar el procedimiento completo. Es decir, como tenemos tres ficheros diferenciados: Clientes, Proveedores y Recursos Humanos, deberemos realizar tres inscripciones diferentes.

Figura 8: Opciones para la inscripción de ficheros*. Fuente:* https://sedeagpd.gob.es

Accederemos a una nueva ventana dónde se nos proponen dos acciones (Figura 8):” Iniciar una nueva Notificación” y “Reanudar una Notificación”. Como aún no tenemos inscrito ningún fichero pulsaríamos en la primera opción, “Iniciar una nueva Notificación”.

La otra opción nos permite acceder a la edición de una notificación todavía incompleta y que fue interrumpida por el usuario. Mientras se está editando la notificación, hay apartados donde se permite la interrupción de la notificación mediante el uso del botón Interrumpir. Se generará en ese momento un código de reanudación que permitirá posteriormente continuar con la edición.

Figura 9: Elección de titularidad y modo de presentación. *Fuente:* https://sedeagpd.gob.es

En la siguiente ventana (Figura 9) se nos pregunta qué tipo de titularidad tiene el fichero que vamos a inscribir y de qué modo vamos a presentar la solicitud.

La titularidad del fichero será "Titularidad Privada" puesto que estamos en el caso de una empresa particular, en el caso de tratarse de un organismo público seleccionaríamos la segunda opción.

Respecto al modo de presentar la solicitud, la notificación podrá presentarse con o sin certificado electrónico. La presentación **sin certificado electrónico** generará un documento de solicitud que deberá imprimirse, firmarse y remitirse a la Agencia Española de Protección de Datos. La dirección para enviar la solicitud es la siguiente:

Calle Jorge Juan, 6, 28001 Madrid

La presentación **con certificado electrónico** generará un documento que servirá como justificante de la presentación de la notificación y que no será necesario remitir. Además, la presentación con certificado electrónico permitirá anexar documentación a la notificación.

Para presentar notificaciones con firma electrónica se debe tener en cuenta dos cosas:

- Poseer un certificado electrónico emitido por una Autoridad de Certificación. En el enlace siguiente podemos encontrar información sobre los principales proveedores de servicios de certificación: http://firmaelectronica.gob.es/Home/Ciudadanos/Principales-Autoridades-Certificacion.html

- Tener instalado Java en el ordenador y configurar la ejecución de la app para la firma. En www.java.com podemos encontrar la última versión de Java, así como las instrucciones para instalar y utilizar el software.

Como estamos basando nuestra guía sobre un ejemplo ficticio podríamos llevar a cabo la demostración sobre cualquiera de las dos vías, con certificado y sin. Como intentamos reflejar con la mayor fidelidad posible la realidad de las microempresas, vamos a suponer que no tenemos Certificado Digital debido al desconocimiento de la existencia y de la aplicación del mismo.

Marcaríamos entonces la casilla de "Titularidad Privada" y seleccionaríamos el modo "Sin Certificado".

La siguiente ventana (Figura 10) nos propone que pasos hemos de seguir para llevar a cabo la inscripción, los leeremos atentamente y continuaremos pulsado en la opción de "Acceso al trámite".

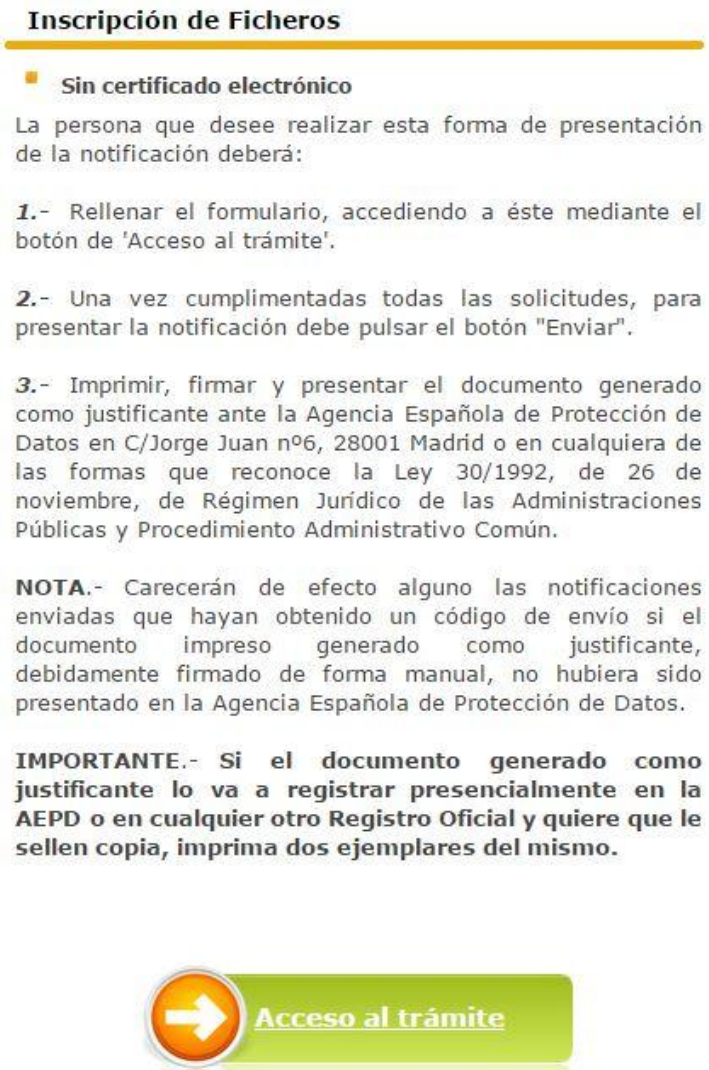


Figura 10: Instrucciones para la inscripción de ficheros sin certificado electrónico.
Fuente: https://sedeagpd.gob.es

En la nueva ventana tendremos que cumplimentar un formulario con los datos de la persona física que actúa en representación del responsable, la dirección a efectos de notificación, la selección del medio en que se quiere ser notificado, el anexo de documentación (sólo en el caso de presentación con certificado electrónico) y la verificación del conocimiento de los deberes del declarante.

Como seguimos utilizando nuestra empresa ficticia (MedicHelp) para rellenar la solicitud (Figura 11), los datos del declarante no van a ser otros que los del propietario del negocio que es el encargado de llevar a cabo todo el proceso de inscripción. Esto no quiere decir que en cualquier otro caso no pueda ser algún empleado el que lleve a cabo la inscripción de los ficheros, en ese caso se deberá estar autorizado y se debe notificar en el documento de seguridad.

Figura 11: Formulario del Declarante. *Fuente:* https://sedeagpd.gob.es

Tenemos que seleccionar el medio de notificación (Figura 12), que no es más que la forma en que se nos va a notificar la inscripción de nuestros ficheros.

Figura 12: Selección del medio de notificación. *Fuente:* https://sedeagpd.gob.es

Las opciones disponible en el desplegable (Figura 12) van a variar según si realizamos la inscripción utilizando Certificado Digital o no.

Para más información sobre el tipo de notificaciones existentes y de que opciones se dispone según si tenemos certificado o no, podemos acceder a la guía sobre inscripción de ficheros que nos brida la AEPD mediante el siguiente enlace: https://sedeagpd.gob.es/sede-electronica-web/resources/pdf/Guia_rapida_NOTA.pdf

A continuación debemos leer el texto que nos aparece a continuación y marcar la casilla "Conocimiento de los deberes del declarante" indicando que somos conocedores del uso que se va a dar a los datos que introduzcamos y de las responsabilidades legales que esto conlleva.

Pulsaremos en el botón "siguiente" que aparece debajo a la derecha.

Figura 13: Formulario del Responsable de Ficheros. *Fuente:* https://sedeagpd.gob.es

En este apartado (Figura 13) se cumplimentará con los datos del responsable del fichero, la persona física o jurídica que decide sobra la finalidad, contenido y uso del fichero. En función de la titularidad del fichero, público o privado, aparecerán campos específicos para su cumplimentación. Con certificado electrónico podrá anexarse documentación relacionada con el responsable, p.ej., si se solicita una modificación de la inscripción con cambio del responsable, se puede adjuntar la documentación que justifique dicho cambio.

Al pulsar el botón “Siguiente” nos aparecerá un cuadro preguntando por el tipo de operación que vamos a realizar (Figura 14).

Figura 14: Selección de la operación a realizar sobre el fichero. *Fuente:* https://sedeagpd.gob.es

Como todavía no hemos realizado la inscripción de ningún fichero seleccionamos la primera opción “Alta de fichero”.

La opción de Alta nos ofrece dos posibilidades (Figura 15), la primera es rellenar el formulario de manera manual, los datos de inscripción aparecerán vacios, y la segunda seleccionando un modelo predeterminado que ya tendrá algunos apartados llenos con los valores apropiados. En el caso de que el fichero que vayamos a inscribir coincida con alguno de los modelos TIPO podríamos utilizarlo para ahorrar tiempo.

Figura 15: Modelos tipo de operación. *Fuente:* https://sedeagpd.gob.es

Según el tipo de titularidad, pública o privada, nos aparecerán unos modelos determinados. Como es la primera vez que inscribimos un fichero vamos a rellenar los campos de forma manual sin seleccionar ningún modelo.

La gráfica de la Figura 16 nos indica que apartados debemos cumplimentar obligatoriamente y cuáles no y para qué tipo de titularidad.

Apartado	Titularidad	Requerido
2.Derechos de oposición, acceso, rectificación	Ambas	Opcional
3. Disposición Gral. De creación, modificación o supresión	Pública	Obligatorio
4.Encargado del Tratamiento	Ambas	Opcional
5.Identificación y Finalidad	Ambas	Obligatorio
6.Origen y procedencia de los datos	Ambas	Obligatorio
7.Tipos de datos y Sistema de Tratamiento	Ambas	Obligatorio
8.Medidas de Seguridad	Ambas	Obligatorio
9.Cesión	Ambas	Opcional
10.Transferencias Internacionales	Ambas	Opcional

Figura 16: Apartados a cumplimentar. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

El primer apartado que abordaremos es el de “Derechos de oposición, acceso, rectificación”. Apartado que, al ser opcional, aparece oculto y sólo se despliega en el caso que se desee cumplimentar (Figura 17).

Figura 17: Formulario de derechos ARCO. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Se debe completar con la dirección dónde los clientes pueden ir a ejercer sus derechos ARCO sobre sus datos personales. En este caso la dirección será la ubicación de la clínica.

El tercer apartado, "Disposición General de Creación, Modificación o Supresión" (Figura 18), permite indicar la disposición general publicada, en el diario oficial correspondiente, relativa a la creación, modificación o supresión de ficheros de las Administraciones Públicas

Solo aparece en caso de que el fichero a inscribir sea de titularidad pública. Por tanto, continuando con nuestro ejemplo, no tendremos que rellenarlo.

Figura 18: Formulario de Disposición general de creación, modificación o supresión. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

El cuarto aparado trata sobre el Encargado del Tratamiento (Figura 19). Este apartado aparece como opcional ya que únicamente se tiene que cumplimentar cuando un tercero realice el tratamiento por cuenta del responsable.

En el caso que nos ocupa deberemos nombrar, en cada fichero que vamos a inscribir, a su correcto encargado de tratamiento. Para ello, en el sub-apartado de “Nombramiento de responsables” podemos ver quienes se van a encargar de tratar cada fichero.

Figura 19: Formulario de Encargado del tratamiento. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Para el fichero “Clientes” nombraríamos como encargado del tratamiento a la empresa informática que nos gestiona, InfoTech S.L, para el fichero de “Proveedores” al enfermero responsable y para el fichero “Recursos Humanos” a nuestra gestoría encargada, Legalité.

El siguiente apartado, llamado “Identificación y Finalidad del fichero” (Figura 20), tenemos que ponerle un nombre al fichero que estamos inscribiendo e indicar la finalidad y usos previstos del mismo.

Figura 20: Formulario de Identificación y finalidad del fichero, *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Rellenaremos los datos del fichero que estamos inscribiendo en este momento (Clientes, Proveedores o Recursos Humanos) utilizando las descripciones que ya hemos dado con anterioridad en el Apartado 3.1.

Recordamos que cada fichero se inscribe de forma individual por tanto el orden en que realicemos las inscripciones no es relevante.

El próximo apartado se titula “Origen y Procedencia de los datos” (Figura 21), aquí deberemos marcar al menos una de las casillas correspondientes al origen de los datos de carácter personal del fichero. Asimismo, permite seleccionar la categoría de los colectivos de donde proceden los datos hasta un máximo de seis.

Figura 21: Formulario de Origen y procedencia de los datos. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Dependiendo del fichero que se trate tendrá diferente procedencia, por ejemplo el fichero que hemos llamado Clientes el origen que marcaríamos sería “Otras personas físicas”, ya que tomamos los datos de nuestros clientes y “el propio interesado o su representante legal”, ya que es el médico que apunta los datos referentes a la salud del cliente. Siguiendo con el mismo fichero, en el siguiente apartado seleccionaríamos el colectivo “Pacientes”.

Seguidamente tenemos un nuevo apartado titulado “Tipos de datos, estructura y organización del fichero” (Figura 22), este nos permite indicar los tipos de datos que se incorporan al fichero o tratamiento, así como indicar otros tipos de datos de carácter identificativo y seleccionar una o varias, hasta un máximo de seis, categorías de tipos de datos o definirlos explícitamente . Asimismo, permite indicar el sistema de tratamiento.

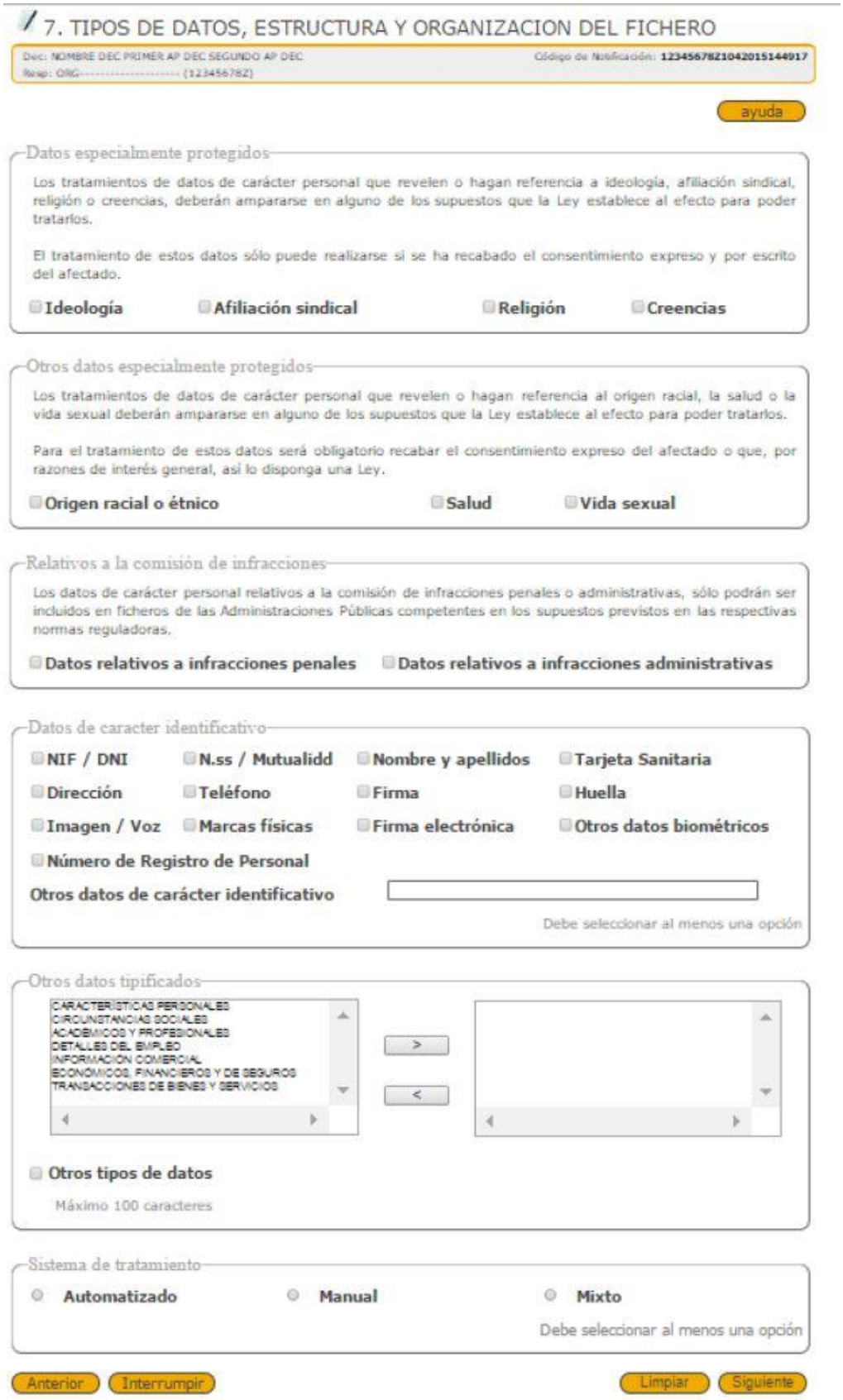


Figura 22: Formulario de Tipo de datos, estructura y organización del fichero. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Siguiendo con el ejemplo del apartado anterior, para el fichero Clientes marcaríamos las casilla de “Salud” de el segundo cuadro “Otros datos especialmente protegidos”, así como también las casilla “NIF/DNI”, “N.ss /Mutualidad”, “Nombre y apellidos”, “Tarjeta Sanitaria” y “Otros datos biométricos” en el cuadro de “Datos de carácter identificativo”. Por último indicaremos que el archivo tiene un sistema de tratamiento de carácter Automatizado, puesto que la base de datos de nuestros clientes está en nuestro ordenador principal.

Para rellenar el siguiente apartado, “Medidas de seguridad” (Figura 23), tendremos que tener claro el nivel de seguridad de los datos del fichero que estamos inscribiendo. Si todavía no está claro del todo el nivel de seguridad que exige el fichero conviene regresar al apartado 2.1 “Conocer los diferentes niveles de seguridad” y asegurarse.

Figura 23: Formulario sobre Medidas de seguridad. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Para el nuestra empresa ya definimos el nivel de seguridad de cada fichero al principio de este apartado.

El siguiente apartado, “Cesión o comunicación de datos” (Figura 24), únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. Permite seleccionar uno o varios, hasta un máximo de seis, destinatarios de las cesiones e indicar aquellos destinatarios que no se encuentran definidos en el cuadro de selección.
Apartado que aparece oculto y sólo se despliega en el caso que se desee cumplimentar.

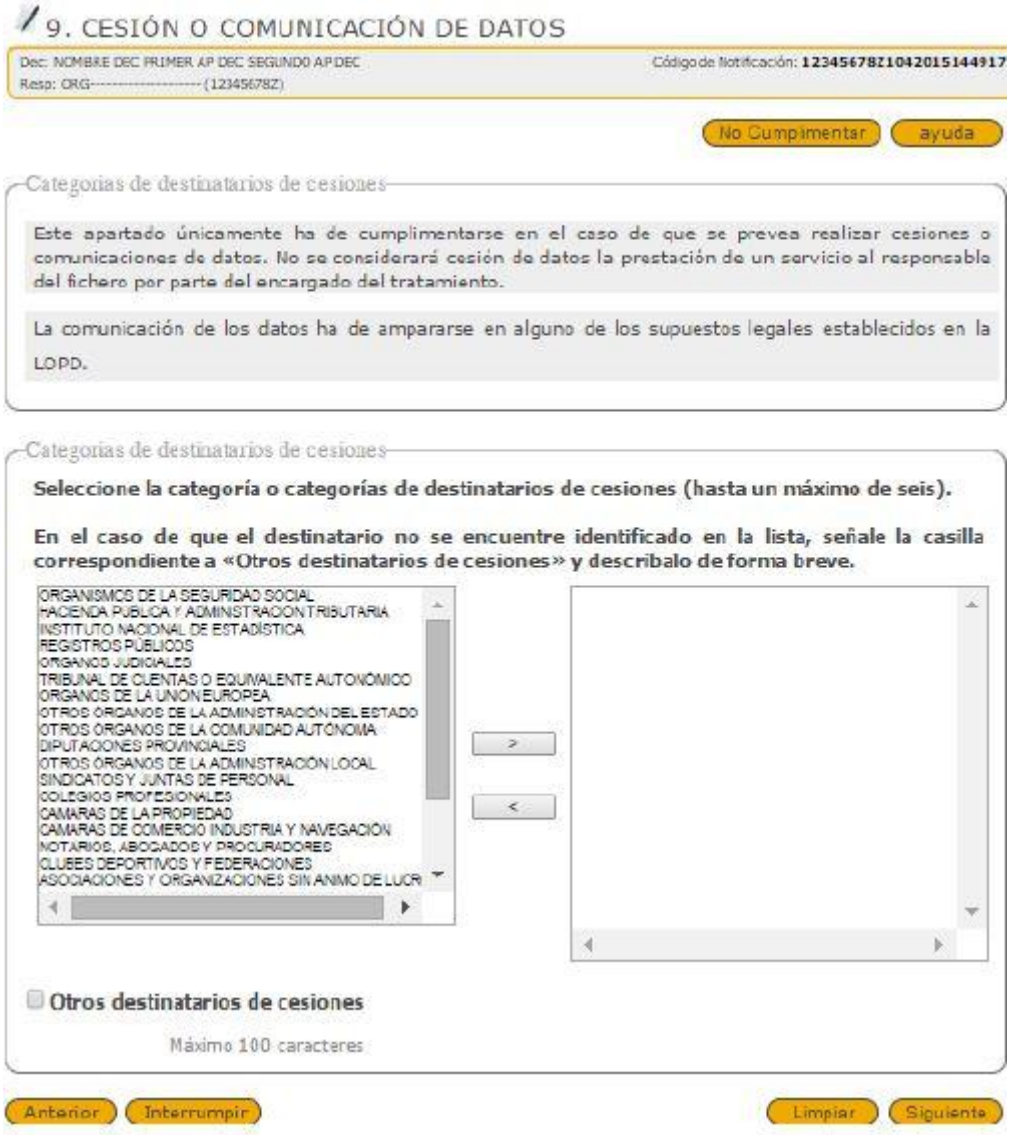


Figura 24: Formulario de cesión o comunicación de datos. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Hay que tener en cuenta que no se considerará cesión de datos la prestación de un servicio al responsable del fichero por parte de cualquier encargado del tratamiento.

En el caso de que en un principio no nos interese conceder la cesión de los datos de nadie podemos dejarlo sin cumplimentar y en el caso de querer realizar alguna cesión posterior modificarlo.

Al igual que el apartado anterior, el siguiente también es opcional. Solo deberemos cumplimentar el formulario de "Transferencias Internacionales" (Figura 25) en el caso de que vayamos a realizar un tratamiento de datos fuera del Espacio Económico Europeo.

El apartado igual que el resto de opcionales aparece oculto y solo se despliega en el caso de que se desee cumplimentar.

Figura 25: Formulario de Transferencias Internacionales. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Tanto este apartado como el anterior de momento no nos interesa cumplimentarlos para ninguno de los ficheros a inscribir de MedicHelp.

Para terminar pulsaremos en “Finalizar Edición”, acto seguido nos aparece un cuadro con el resumen de las operaciones o solicitudes de inscripción (Figura 26), hasta un máximo de diez, que formaran parte de la notificación que se va a mandar.

Figura 26: Resumen de la notificación. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Añadiremos los ficheros que falten pulsando en "Añadir otra solicitud". Una vez tengamos todos los ficheros que nos interesa inscribir en este cuadro procederemos a enviar la notificación.

Según la forma de presentación elegida la manera de proceder cambiará:

Sin certificado digital

Al pulsar el botón accedemos a la pantalla de Confirmación del Envío (Figura 27), aquí se nos muestran las instrucciones para presentar la solicitud.

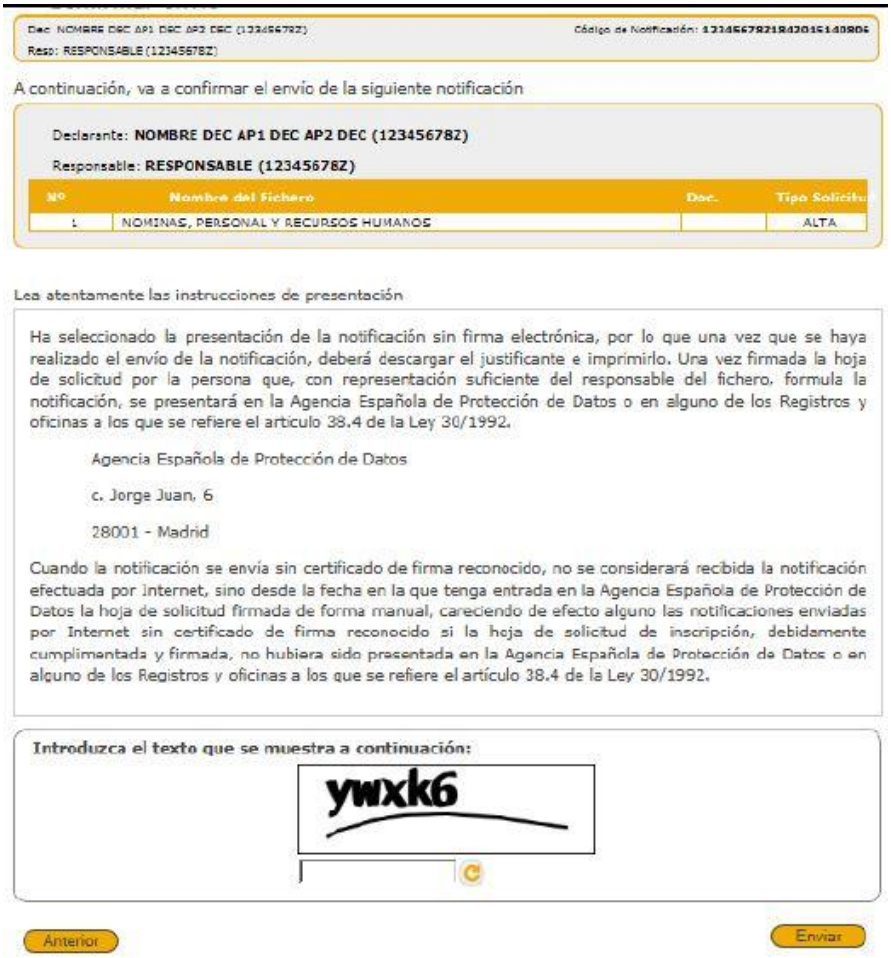


Figura 27: Instrucciones de presentación del fichero. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

En una notificación sin certificado digital primero debemos descargar el justificante, imprimirlo, firmarlo y presentarlo en la Agencia Española de Protección de Datos o en alguno de los Registros y Oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992.

Una vez llegue el justificante a la AEPD se comenzará a tramitar la notificación.

En el caso de producirse algún error aparecerá una nueva pantalla mostrando un Código de Reanudación para que podamos repetir el envío sin perder la información ya cumplimentada.

Con certificado digital

Al pulsar en el botón “Enviar notificación” se accede a la pantalla de Confirmación del Envío. Al acceder comenzará a cargarse la applet de firma electrónica, para que este funcione debemos tener instalado Java en nuestro equipo.

Si tenemos Java configurado correctamente nos debe aparecer una advertencia de seguridad (Figura 28) a la que debemos contestar **Permitir**.

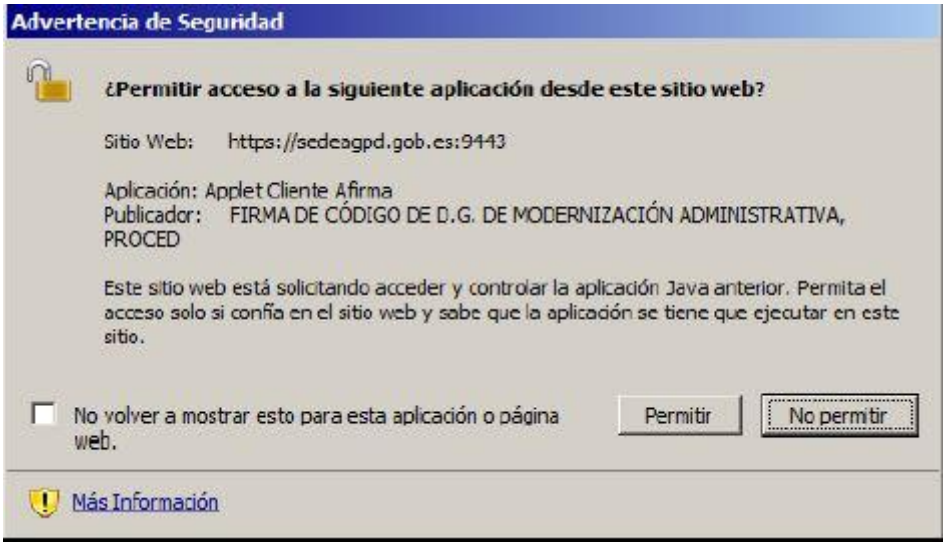


Figura 28: Advertencia de Seguridad sobre la applet. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

Seguidamente nos aparecerá otra pantalla, esta vez de Java(Figura 29), preguntando si deseamos ejecutar la Applet Cliente Firma, pulsaremos en **Ejecutar**.

Figura 29: Notificación Java sobre la applet. *Fuente:* Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA (AEPD).

A continuación aparecen las operaciones que forman parte de la notificación y las instrucciones de presentación. Leeremos las instrucciones detenidamente y pulsaremos en "Firmar y enviar".

Aparecerá una ventana de confirmación de mano del applet de firma electrónica que muestra los certificados digitales para poder realizar la firma, pulsaremos en "Aceptar".

Si al enviar la notificación está todo correcto aparecerá una pantalla donde podremos descargar el justificante y regresar a la página principal. Es importante conservar el justificante por si posteriormente hay algún problema.

En el caso de que hubiese algún error en la notificación, igual que al realizar la operación sin certificado digital, aparecerá una pantalla de Error que presentará el código de reanudación para no perder la información ya cumplimentada.

Para terminar con el procedimiento solo hace falta decir que todos los pasos que hemos descrito tan solo son un resumen de la guía oficial que proporciona la AEPD para la notificación de fichero mediante el Servicio Electrónico NOTA que podemos encontrar en la siguiente dirección:

https://sedeagpd.gob.es/sede-electronicaweb/resources/pdf/Guia_rapida_NOTA.pdf.

Si aparece alguna duda podemos consultar la guía donde se explica más detenidamente el procedimiento.

3.5 Fase 4: Elaboración del documento de seguridad

El documento de seguridad es fundamental a la hora de aplicar la LOPD. Se trata de un documento que recoge las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas serán de obligado cumplimiento para el personal que tenga acceso a dichos datos.

El documento de seguridad que propone la AEPD debe contener los siguientes apartados como mínimo:

- Ámbito de aplicación del documento.
- Medidas, normas, procedimiento, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- Información y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas antes las incidencias.
- Procedimientos de revisión.

Procedemos a ejemplificarlo con los datos de nuestra empresa ficticia MedicHelp. El formato que vamos a utilizar es el propuesto en el modelo de Documento de Seguridad que

encontraremos en la página oficial de la AEPD. Podemos encontrarlo en el siguiente enlace: https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php

NOTA: El texto original publicado en la guía aparecerá en cursiva, mientras que el texto que introduzcamos estará en formato normal.

Descripción de los ficheros

A continuación exponemos los ficheros que han sido inscritos en la Agencia Española de Protección de datos:

FICHERO	CÓDIGO ENVIO	CÓDIGO INSCRIPCIÓN
CLIENTES	Aquí pondremos el código que se nos dio cuando hicimos la inscripción de los ficheros	Aquí el código que nos mandarán una vez esté completa la inscripción del fichero
PROVEEDORES		
RECURSOS HUMANOS		
VIDEOVIGILANCIA		

De acuerdo con la LOPD y el RDLOPD procedemos a la descripción de cada uno de los ficheros inscritos:

FICHERO	CLIENTES
Descripción	Fichero que recoge toda la información pertinente a los pacientes de MedicHelp.
Nivel de seguridad	Alto
Responsable de seguridad	José Tojeiro Gómez
Encargado del tratamiento	InfoTech S.L.
Estructura del fichero:	• Nombre y apellidos • NIF/NIE • Teléfono • Correo electrónico • Fotografía • Nº SS/Mutualidad • Firma • Edad, nacionalidad, lugar de nacimiento, sexo • Dirección • Historial médico • Datos bancarios
Finalidad del fichero:	Confeccionar una base de datos con los clientes de la clínica para facilitar un mejor diagnóstico y control por parte del personal sanitario de MedicHelp.
Procedencia de los datos:	Clientes de MedicHelp.
Procedimiento de recogida:	Los datos se introducirán manualmente de mano de José Tojeiro, dueño del negocio.
Cesiones previstas:	Ninguna
Transferencias internacionales:	Ninguna
Sistema de tratamiento:	Automatizado
Ejercicio de los derechos ARCO:	Todos. Para poder ejercerlos el interesado debe acudir

	a la misma clínica. **DIRECCIÓN:** C/Viver, 15 **C.P:** 03850 **POBLACIÓN:** Valencia **PROVINCIA:** Valencia
Descripción copias de respaldo y procedimientos de recuperación:	Copia semanal de los datos
Conexión con otros sistemas:	Ninguno
Funciones del personal:	Creación de una Base de Datos
Usuario Autorizados:	José Tojeiro Gómez Usuario: administrador

FICHERO	**PROVEEDORES**
Descripción	Ficheros que recoge toda la información pertinente a los proveedores de material médico de MedicHelp.
Nivel de seguridad	Básico
Responsable de seguridad	José Tojeiro Gómez
Encargado del tratamiento	Enfermeros
Estructura del fichero:	• Nombre y apellidos • NIF/NIE • Teléfono • Firma • Dirección • Datos bancarios • Correo electrónico • Facturas • Albaranes
Finalidad del fichero:	Recoger todos los proveedores de materiales que necesitamos para tener abastecida la clínica.
Procedencia de los datos:	Empresas externas
Procedimiento de recogida:	Los datos se recogen mediante llamadas, consultas a webs o correos electrónicos.
Cesiones previstas:	Ninguna
Transferencias internacionales:	Ninguna
Sistema de tratamiento:	Manual
Ejercicio de los derechos ARCO:	Todos. Para poder ejercerlos el interesado debe acudir a la misma clínica. **DIRECCIÓN:** C/Viver, 15 **C.P:** 03850 **POBLACIÓN:** Valencia **PROVINCIA:** Valencia
Descripción copias de respaldo y procedimientos de recuperación:	Ninguno
Conexión con otros sistemas:	Ninguno
Funciones del personal:	Abastecer a MedicHelp con el material que necesite
Usuario Autorizados:	José Tojeiro Gómez Usuario: administrador Enfermeros Usuario: Enfermero_1, Enfermero_2

FICHERO	RECURSOS HUMANOS
Descripción	Fichero que recoge la información pertinente a los trabajadores de nuestra empresa.
Nivel de seguridad	Básico
Responsable de seguridad	José Tojeiro Gómez
Encargado del tratamiento	Asesoría Legalite S.L
Estructura del fichero:	• Nombre y apellidos • Edad, Fecha y lugar de nacimiento, nacionalidad • Sexo, estado civil • NIF/NIE • Nº Seguridad Social /Mutualidad • Nómina • Datos académicos y profesionales • Fotografía • Teléfono • Firma • Dirección • Datos bancarios • Correo electrónico
Finalidad del fichero:	Confección de las nóminas, contratos, seguros y almacenamiento de información sobre el personal.
Procedencia de los datos:	Empleados contratados
Procedimiento de recogida:	Los datos son proporcionados por los trabajadores a la hora de contratarles.
Cesiones previstas:	Ninguna
Transferencias internacionales:	Ninguna
Sistema de tratamiento:	Mixto
Ejercicio de los derechos ARCO:	Todos. Para poder ejercerlos el interesado debe acudir a la misma clínica. **DIRECCIÓN:** C/Viver, 15 **C.P:** 03850 **POBLACIÓN:** Valencia **PROVINCIA:** Valencia
Descripción copias de respaldo y procedimientos de recuperación:	Ninguno
Conexión con otros sistemas:	Ninguno
Funciones del personal:	
Usuario Autorizados:	José Tojeiro Gómez Usuario: administrador Asesoría Legalite S.L Usuario: asesoria

FICHERO	VIDEOVIGILANCIA
Descripción	Fichero que recoge imágenes del interior de la clínica.
Nivel de seguridad	Básico
Responsable de seguridad	José Tojeiro Gómez
Encargado del tratamiento	InfoTech S.L
Estructura del fichero:	• Audio • Vídeo
Finalidad del fichero:	Vigilancia para evitar robos
Procedencia de los datos:	Cámaras de seguridad
Procedimiento de recogida:	Las cámaras graban en franjas de 30 minutos
Cesiones previstas:	Cuerpos de seguridad del estado
Transferencias internacionales:	Ninguna
Sistema de tratamiento:	Automatizado
Ejercicio de los derechos ARCO:	Todos. Para poder ejercerlos el interesado debe acudir a la misma clínica. **DIRECCIÓN:** C/Viver, 15 **C.P:** 03850 **POBLACIÓN:** Valencia **PROVINCIA:** Valencia
Descripción copias de respaldo y procedimientos de recuperación:	Ninguno
Conexión con otros sistemas:	Ninguno
Funciones del personal:	
Usuario Autorizados:	José Tojeiro Gómez Usuario: administrador InfoTech S.L. Usuario: informatico

Ámbito de aplicación del documento

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de **José Tojeiro Gómez**, *incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.*
En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

Nombre del Fichero	Tipo de fichero	Identificador en el Registro General de Protección	Nivel de seguridad a adoptar
Clientes	Automatizado	Este apartado se debe completar con el nombre y el identificador del fichero inscrito en el Registro General de Protección de Datos de la AEPD, podemos acceder a estos datos desde la página web de la AEPD.	Alto
Proveedores	Manual		Básico
Recursos Humanos	Mixto		Básico
Videovigilancia	Automatizado		Básico

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

IDENTIFICACIÓN Y AUTENTICACIÓN

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

Disponemos de dos cuentas de usuario para acceder a los ordenadores de la empresa. Una dispondrá de todos los permisos disponibles y acceso completo a toda la información, la otra cuenta será la utilizada por los empleados y tendrá acceso limitado a algunas funciones. Ambas irán protegidas por una contraseña de más de 6 caracteres. Dicha contraseña se cambiará cada 6 meses.

A la hora de acceder se dispondrá tan solo de 3 intentos, quedando el sistema bloqueado si no se consigue una autenticación exitosa.

Cada vez que un usuario intente acceder al sistema o lo consiga se quedará guardada la información de inicio de sesión así como la fecha y hora a la que se realizó. Estos datos se deberán almacenar durante un período de 2 años como mínimo.

Las contraseñas serán designadas por el dueño del negocio. Puede darse el caso de que se delegue esta responsabilidad en la empresa de informática contratada. En caso de ser así deberá figurar un documento adjunto que muestre la delegación de dicha responsabilidad.

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

El ordenador principal, utilizado por el administrador y dónde se almacenan datos de nivel alto, se hallará bajo lleva en un despacho cerrador con llave. La única persona que dispondrá de dicha llave será José Tojeiro Gómez.

Los documentos de nivel básico se hallarán protegidos bien en un cajón o en un armario con llave, disponible para todo el personal de la empresa o bien en el ordenador de recepción, protegido con usuario y contraseña.

Exclusivamente el propietario de MedicHelp, José Tojeiro Gómez *está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero.*

Para solicitar el acceso a determinados datos el procedimiento será el siguiente: El empleado o entidad que desee acceder a los datos hablará con el propietario de la empresa, José Tojeiro,

para que dé su autorización. Dependiendo de a que fichero se desee acceder se procederá de forma diferente.

Si se trata de un fichero no automatizado se deberá anotar a que fichero se va a acceder, así como la hora, fecha y el motivo. El dueño de la clínica será el encargado de abrir el armario o cajón dónde se encuentre dicho fichero y sacarlo. El fichero no deberá ser copiado ni editado sin autorización del encargado de seguridad. Una vez el empleado haya terminado de utilizar el fichero se volverá a guardar en su lugar correspondiente y se anotará la hora a la que ha sido devuelto.

Si se tratase de un fichero automatizado el procedimiento será similar, se tendrá que anotar que tipo de datos y en que formato van a estar, dichos datos deben ir cifrados si se trata de datos de nivel alto.

*En la descripción de ficheros, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizad c*ada vez que se renueve el personal de la clínica o por defecto cada 6 meses.
De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

REGISTRO DE ACCESOS

AUTOMATIZADOS

En los accesos a los datos de los ficheros de nivel alto, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Los datos del registro de accesos se conservaran durante dos años.
El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de "Comprobaciones para la realización de la auditoría de seguridad" de este documento.

No será necesario el registro de accesos cuando:

- *el responsable del fichero es una persona física,*
- *el responsable del fichero garantice que sólo él tiene acceso y trata los datos personales,*
- *y se haga constar en el documento de seguridad.*

El acceso a la documentación se limita exclusivamente al personal autorizado.
Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados: Cada vez que se realice un acceso a información que contenga datos de nivel alto se debe anotar en un registro de control los datos pertinentes a quién ha realizado el acceso, cuando lo ha realizado y porqué. Este registro será simplemente una hoja de Excel protegida con contraseña para que solo pueda modificarla el responsable de seguridad.

GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en cualquiera de los armarios o cajones protegidos con llave de la empresa, *lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:*

FICHERO	PERSONAL AUTORIZADO	LUGAR ALMACENAMIENTO
Clientes	José Tojeiro Gómez, InfoTech S.L	Cajón con llave ubicado en el despacho, ordenador del despacho
Proveedores	Enfermeros	Armario Principal protegido con llave común
Recursos Humanos	José Tojeiro Gómez, Asesoría Legalite S.L.	Ordenador del despacho

Los siguientes soportes <relacionar aquellos a que se refiere> *se exceptúan de las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.*

Los siguientes soportes en formato físico y que contenga datos de carácter personal *se identificarán utilizando los sistemas de etiquetado siguientes:* Nombre, Fichero al que pertenece, fecha de la copia, responsable del fichero, finalidad.
Los soportes se almacenarán de acuerdo a las siguientes normas:

- Irán en todo momento identificados con la etiqueta o nombre correspondiente que revele las características anunciadas anteriormente.
- La salida de soportes y documentos que contengan datos de carácter personal debe ser autorizada por el responsable de seguridad mediante el documento adjunto correspondiente.
- Debe establecerse un sistema que registre las entradas y salidas de soportes.
- En caso de tratarse de datos de nivel alto los datos deben utilizar un sistema de cifrado.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento:

En primer lugar para realizar el envío de cualquier soporte o documento se debe consultar con el dueño y responsable de seguridad, José Tojeiro. Si este da su consentimiento se debe reflejar mediante una autorización que aparecerá adjunta al final de este documento. (Podemos encontrarla en el Anexo 6).

A continuación procederemos a anotar en el documento de control de salida de ficheros el nombre del fichero a sustraer, el tipo de documento, la fecha y hora de salida, el número de documentos o soportes incluidos en el envío, el tipo de información que contiene, la forma de envío y la persona responsable de recibirlo.

Una vez vayamos a enviarlo debemos asegurarnos de que nadie pueda acceder a la información. En el caso de los ficheros automatizados protegiéndolos mediante una contraseña y en el caso de los ficheros de nivel alto mediante cifrado, los ficheros no automatizados mediante un maletín con llave u otro tipo de contenedor que evite el acceso a personas no autorizadas.

Una vez el documento llegue a su destino la persona encargada de tratar con él deberá ser autorizada con anterioridad por José Tojeiro, constando esto en la autorización pertinente de envío, de modo que se tendrán que proporcionar las claves necesarias para la apertura del documento en su destino, siempre que esté preparada la autorización.

Una vez el documento esté en su sitio de recepción se deberá anotar en el documento de control de salida de ficheros.

Los soportes que vayan a ser desechados, deberán ser previamente analizados para asegurarse de que no contengan información necesaria. Una vez se tenga claro que van a ser eliminados y dependiendo del tipo de soporte que los contenga se procederá de la siguiente manera:

Documentación escrita: Se utilizará una trituradora de papel que imposibilite que el documento sea leído o recompuesto.

CDs, Discos duros, pendrives: En el caso de que se desee conservar el formato físico se puede llevar a cabo un formateo completo del hardware. Si no fuese posible, como en el caso de los CDs se deberán desechar de forma que sea imposible su utilización.

ACLARACIONES: Al final de este documento debe constar un adjunto con el registro de los ficheros que salen y entran en la empresa siguiendo la normativa anteriormente expuesta, este anexo se deberá actualizar periódicamente para asegurar el buen cumplimiento de la LOPD.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

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.

COPIAS DE RESPALDO Y RECUPERACIÓN

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad: semanal.

Los procedimientos establecidos para las copias de respaldo y para su recuperación son los siguientes:

La empresa al cargo del mantenimiento informático, InfoTech, se encargará de la realización de las copias de seguridad de los discos duros de todos los ordenadores de la empresa de manera semanal.

A parte, los datos de la base de datos de clientes que contienen datos de carácter personal se almacenarán en un lugar que no esté ubicado dentro de la empresa, por ejemplo en la nube o el algún dispositivo externo, esto queda a decisión de la empresa a cargo de la informática.

Cada 6 meses el responsable de seguridad debe verificar que el sistema de copias de seguridad está funcionando correctamente.

En el caso de realizarse algún cambio de software o alguna intervención técnica en los sistemas de información de la empresa se realizará una copia de seguridad completa del sistema.

En el Anexo 8 podremos encontrar el modelo de Autorización para la recuperación de los datos en caso de que no sea el responsable directo quien realice dicha recuperación.

Información y obligaciones del personal

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

A todos los miembros del personal en el momento de su incorporación se les entregará un documento de explicativo sobre sus funciones y obligaciones para con la empresa, podemos encontrar el modelo en el Anexo 9. El trabajador deberá leer el documento con detenimiento y si está de acuerdo con lo dispuesto lo firmará y se lo entregará al responsable de seguridad. El documento firmado y sellado por la empresa y el trabajador se adjuntará al presente documento de seguridad.

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

Constituye una obligación del personal notificar al José Tojeiro Gómez *las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias."*

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

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

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

Se delegan las siguientes autorizaciones en los usuarios relacionados:

Nombre Usuarios Relacionados	José Tojeiro Gómez	Nombre enfermero 1	Nombre enfermero 2	Nombre empleado responsable de Info Tech	Nombre empleado responsable de Legalité
DNI	21692689D				
Acceso a Ficheros	Todos	Proveedores	Proveedores	Clientes	Recursos Humanos
Acceso a Soportes	Si	No	No	No	No
Salida autorizada de soportes	Si	No	No	No	No
Perfil	Responsable de seguridad	Usuario Autorizado	Usuario Autorizado	Encargado del tratamiento	Encargado del tratamiento
Puesto de trabajo	Responsable del negocio	Trabajador	Trabajador	Empleado externo	Empleado externo

NOTA: Los nombre de los empleados deberán figurar, como estamos en un ejemplo ficticio y para ahorrar confusiones aparecen sin definir. Por ejemplo donde pone enfermero 1 deberá aparecer el nombre real del empleado.

CONSECUENCIAS DEL INCUMPLIMIENTO DE ESTE DOCUMENTO DE SEGURIDAD

Tanto por denuncia de los titulares de los datos, como de oficio, puedo ser inspeccionado por la Agencia Española de Protección de Datos, que, si comprueba el incumplimiento de las obligaciones impuestas por la normativa, o la vulneración de derechos de los titulares de los datos, puede iniciar un expediente sancionador, e imponer multas cuyo importe puede ascender a seiscientos mil euros (600.000 €).

Se establecen una serie de sanciones a los responsables de los ficheros y a los encargados del tratamiento de los ficheros que contengan datos de carácter personal. Estas se clasifican en leves, graves y muy graves, atendiendo a la infracción cometida.

- SANCIONES
- LEVES Multa de 601,01 € a 60.101,21 €
- GRAVES Multa de 60.101,21 € a 300.506,05 €
- MUY GRAVES Multa de 300.506,05 € a 601.012,10 €

La cuantía de las sanciones que impone la LOPD se gradúa atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a cualquier otra circunstancia que sea relevante para determinar el grado de culpabilidad.

Son infracciones leves: Sanciones entre 601,01€ y 60.101,21€

- No solicitar la inscripción del fichero en la Agencia Española de Protección de Datos.
- Recopilar datos personales sin informar previamente
- No atender a las solicitudes de rectificación o cancelación
- No atender las consultas por parte de la AGPD.

Son infracciones graves: Sanciones entre 60.101,21€ y 300.506,25€

- No inscribir los ficheros en la AGPD.
- Utilizar los ficheros con distinta finalidad con la se crearon.
- No tener el consentimiento del interesado para recabar sus datos personales
- No permitir el acceso a los ficheros.
- Mantener datos inexactos o no efectuar las modificaciones solicitadas
- No seguir los principios y garantías de la LOPD
- Tratar datos especialmente protegidos sin la autorización del afectado

- No remitir a la AGPD las notificaciones previstas en la LOPD.
- Mantener los ficheros sin las debidas condiciones de seguridad.

Son infracciones muy graves: Sanciones entre 300.506,25€ y 601.012,1€

- Crear ficheros para almacenar datos que revelen datos especialmente protegidos.
- Recogida de datos de manera engañosa o fraudulenta.
- Recabar datos especialmente protegidos sin la autorización del afectado.
- No atender u obstaculizar de forma sistemática las solicitudes de cancelación o rectificación.
- Vulnerar el secreto sobre datos especialmente protegidos.
- La comunicación o cesión de datos cuando ésta no esté permitida.
- No cesar en el uso ilegítimo a petición de la AGPD.
- Tratar los datos de forma ilegítima o con menosprecio de principios y garantías que le sean de aplicación.
- No atender de forma sistemática los requerimientos de la AGPD.
- La transferencia temporal o definitiva de datos de carácter personal con destino a países sin nivel de protección equiparable o sin autorización

En el documento informativo sobre las funciones y obligaciones del personal aparecerá una cláusula relativa a si el usuario es conocer o no de dichas sanciones, cláusula que únicamente se debe firmar en el caso de que el usuario esté al tanto de las mismas.

Procedimientos de notificación, gestión y respuesta ante las incidencias

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de José Tojeiro Gómez

El procedimiento a seguir para la notificación de incidencias será:

Todas las personas que formen parte de la empresa deben notificar cualquier anomalía que detecten que pueda afectar al tratamiento de datos de carácter personal. Las incidencias que se detecten deben ser registradas y notificadas al responsable del tratamiento para que se resuelvan.

El registro tendrá los siguientes campos:

- Tipo de incidencia
- Fecha y hora en que se produjo
- Efectos derivados

- Medidas correctoras aplicadas
- Persona que realiza la notificación
- Responsable de su resolución

El registro de incidencias se gestionará mediante:

Un Excel compartido para los usuarios de la empresa que contemple los datos expuestos anteriormente. El registro de incidencias se deberá imprimir de forma mensual y adjuntarlo al documento de seguridad. Encontraremos un modelo de registro de incidencias en el Anexo 7.

La restauración de los datos de cualquier clase de copia de seguridad deberá notificarse en el registro de incidencias. Dicha restauración debe estar autorizada por el responsable e ir adjunta al registro de incidencias.

Procedimientos de revisión

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El documento de seguridad solo se podrá modificar bajo la autorización expresa del responsable del mismo y bajo su supervisión. Cualquier cambio propuesto se deberá analizar para ver que cumpla con la normativa vigente y una vez añadido es conveniente que se registre la modificación para tener supervisada una posible modificación o anulación posterior.

Por otra parte cualquier cambio en el documento que pueda afectar al personal de la empresa o a cualquier entidad relacionada con los datos almacenados se debe notificar a los afectados antes de llevar a cabo su realización.

AUDITORÍA

Los cambios propuestos como resultado de la auditoría llevada a cabo por: (aquí tendríamos que indicar quien ha realizado la auditoría, normalmente se suele contratar a alguna empresa externa para que la realice) llevada a cabo el día: (Aquí pondríamos la fecha de cuando se realizó la auditoría) son los siguientes: (A continuación detallaríamos las modificaciones propuestas)

NOTA: En el apartado Auditoría encontraremos más información de cómo llevarla a cabo

Documentación Complementaria

A continuación deberán aparecer todos los documentos complementarios necesarios que hemos ido describiendo a lo largo del documento.

NOMBRAMIENTOS

(Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad.)

AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

(Adjuntar las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, incluyendo aquellas que se refieran a salidas que tengan un carácter periódico o planificado. Incluir asimismo, las autorizaciones relativas a la ejecución de los procedimientos de recuperación de datos.)

DELEGACIÓN DE AUTORIZACIONES

En su caso, personas en las que el responsable del fichero ha delegado (Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel,…)

INVENTARIO DE SOPORTES

(Si el inventario de soportes no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de “Gestión de soportes y Documentos” de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento.)

REGISTRO DE INCIDENCIAS

(Si el registro de incidencias no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento.

Si el registro de incidencias está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo que lo contiene.)

ENCARGADOS DE TRATAMIENTO

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

Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, y que no los comunicarán, ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar)

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

(Si el registro de entrada y salida de soportes al que se refiere el apartado de "Gestión de soportes y documentos", y que es obligatorio a partir del nivel medio, no está informatizado, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD>.

Si el registro de entrada y salida está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene.)

MEDIDAS ALTERNATIVAS

(En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado.)

3.6 Auditoría de Seguridad

Una vez terminemos con la redacción del documento de seguridad deberemos asegurarnos de que se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal realizando una Auditoría de Seguridad.

Podemos encontrar todo el procedimiento descrito en la "Guía de Seguridad de Datos" proporcionada por la Agencia Española de Protección de Datos que encontraremos en la siguiente dirección:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

La realización de esta auditoría es obligatorio para ficheros con datos de nivel medio/alto y puede realizarse de manera interna o externa, es decir, podemos hacerla nosotros mismos o contratar a otra empresa especializada para que la lleve a cabo. En ambos casos se debe realizar al menos cada dos años, a no ser que se realice alguna modificación sustancial en el sistema de información, en este caso se realizaría otra auditoría para comprobar la adaptación y se iniciaría el período de los dos años desde aquí.

ALCANCE, PLANIFICACIÓN Y RECOLECCIÓN DE DATOS

En primer lugar debemos tener claro cuáles van a ser los ficheros que contienen datos de carácter personal objeto de la auditoría, el tratamiento que se les aplica, los procedimiento llevados a cabo, etc.

Debemos tener a nuestra disposición los recursos que nos permitan llevar a cabo la auditoría, es decir: todo aquello relacionado con los ficheros como fuentes de información, ubicación en las instalaciones, etc.

Los datos que vamos a necesitar serán los siguientes:

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, Identificación y autorización, borrado de soportes, cifrado, etc.).
- Documento de Seguridad y auditorías anteriores (si las hubiese).
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables, etc.
- Inspección visual. etc.

Una vez tengamos toda la información recogida pasaremos a la evaluación de las pruebas.

COMPROBACIONES A REALIZAR

Procedemos a exponer las preguntas que debemos asegurarnos de haber respondido una vez terminemos con la auditoría:

ASPECTOS GENERALES		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?
		¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?

ENCARGADO DE TRATAMIENTO		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Se realiza el tratamiento por persona distinta al responsable del fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?
		Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al

		cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?
		Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?
		Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) ¿ha elaborado el encargado el documento de seguridad?, ¿identifica el fichero o tratamiento y el responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?

PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	Si el tratamiento no afecta a datos personales ¿se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos?
		Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?

DELEGACIÓN DE AUTORIZACIONES		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, ¿se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	El almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero?, ¿consta dicha autorización en el Documento de Seguridad?
		¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado?

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Cumplen el nivel de seguridad correspondiente?
		¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?

DOCUMENTO DE SEGURIDAD		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Ha elaborado el responsable del fichero el Documento de Seguridad?
		¿Contiene los aspectos mínimos exigidos por el Reglamento?
		¿Está el documento actualizado?, ¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?
		¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?
		¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?
		¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?
		¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?
		Si el tratamiento se realiza por cuenta de terceros ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia?
		¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?
		¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?
	MEDIO	¿Establece la identidad del responsable o responsables de seguridad?, ¿se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?
		¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?
		¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?
		¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?

FUNCIONES Y OBLIGACIONES DEL PERSONAL		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?
		¿Están documentadas y reflejadas en el documento de seguridad?
		¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?
		¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?
		¿Conoce las consecuencias de su incumplimiento?

REGISTRO DE INCIDENCIAS		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?
		¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?
		¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?
AUTO-MATIZADO		¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?
	MEDIO	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?
		¿Existe la autorización por escrito del responsable del fichero?

CONTROL DE ACCESO		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?
		¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?
		¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?
		¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?
		¿Ha establecido el responsable del fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?
		El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?

AUTO-MATIZADO	MEDIO	¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?
NO AUTO-MATIZADO	ALTO	¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente?, ¿están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?
		Si los locales del responsable no permiten disponer de un área de acceso restringido ¿ha adoptado el responsable medidas alternativas?, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, se ha motivado adecuadamente?

COPIAS DE RESPALDO Y RECUPERACIÓN		
Sistema de Tratamiento	**Nivel**	**Comprobación**
AUTO-MATIZADO	BÁSICO	¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?
		¿Están reflejados estos procedimientos en el Documento de Seguridad?
		¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?
		¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?
		Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?
		¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese periodo?
		¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?
	ALTO	¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?
		¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?

REGISTRO DE ACCESOS		
Sistema de Tratamiento	**Nivel**	**Comprobación**
AUTO-MATIZADO	ALTO	¿Existe el registro de accesos? En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito?, ¿se ha hecho constar en el Documento de Seguridad?
		¿Se está recogiendo en este registro la información mínima exigida en el Reglamento?
		¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad?
		¿Existe la posibilidad de desactivar estos mecanismos?
		¿Se conservan los datos registrados por un período mínimo de dos años?
		¿Revisa el responsable de seguridad periódicamente la información registrada?
		¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados?
NO AUTO-MATIZADO		¿El acceso a la documentación se realiza exclusivamente por personal autorizado?
		¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios?
		¿Se ha establecido un procedimiento para registrar el acceso de personas no incluidas en el caso anterior?, ¿es adecuado?

GESTIÓN DE SOPORTES Y DOCUMENTOS		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Está identificado el tipo de información contenido en el soporte o documento?
		¿Existe y se mantiene un inventario de soportes?
		¿Se almacenan los soportes o documentos en lugares de acceso restringido?
		¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?
		¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?
		¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el responsable del fichero o está debidamente autorizada en el Documento de Seguridad?
		¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte?
		Cuando se desecha un soporte o documento conteniendo datos de carácter personal ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se

		procede a su destrucción o borrado?, ¿son adecuadas estas medidas?
		¿Se dan de baja en el inventario estos soportes o documentos desechados?
		Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?
	MEDIO	¿Existe un registro de entrada de soportes o documentos?, ¿y un registro de salida?
		¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?
		¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas?, ¿Consta en el Documento de Seguridad dicha autorización?
		¿Se han anotado todas las entradas y salidas de soportes?
AUTO-MATIZADO	ALTO	¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? ¿son adecuados y cumplen su finalidad?
		¿La distribución de soportes se realiza de forma cifrada, o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte?
		¿Se cifran los datos en los dispositivos portátiles cuando éstos salen de las instalaciones del responsable del fichero?
		Si fuera imprescindible el tratamiento de datos en dispositivos portátiles que no permitan el cifrado de datos ¿se ha hecho constar motivadamente en el Documento de Seguridad?, ¿se han adoptado medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos?, ¿son adecuadas?
NO AUTO-MATIZADO		¿Se adoptan medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero?, ¿son apropiadas estas medidas?
		La generación de copias o reproducción de documentos ¿se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?
		¿Se destruyen las copias o reproducciones desechadas de forma que no se pueda acceder a la información contenida en las mismas?

IDENTIFICACIÓN Y AUTENTICACIÓN		
Sistema de Tratamiento	**Nivel**	**Comprobación**
AUTO-MATIZADO	BÁSICO	¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?
		¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?
		El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?
		¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e

		integridad?
		¿Se cambian las contraseñas con la periodicidad establecida en el documento de seguridad?
		¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?
	MEDIO	¿Se limita el intento reiterado de acceso no autorizado al sistema?, ¿se anotan estos intentos en el registro de incidencias?

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES		
Sistema de Tratamiento	**Nivel**	**Comprobación**
AUTO-MATIZADO	BÁSICO	¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?
	ALTO	¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de cifrado es eficaz?

AUDITORÍA		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	MEDIO	¿Se realiza la actual auditoría en el plazo establecido desde la anterior?
		Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?
		¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?
		¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?

CRITERIOS DE ARCHIVO		
Sistema de Tratamiento	**Nivel**	**Comprobación**
TODOS	BÁSICO	¿Existe legislación específica con criterios para el archivo de soportes o documentos?, ¿garantizan estos criterios la conservación de documentos, la localización y consulta de la información?, ¿posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación?
		En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos?, ¿es adecuado este procedimiento?

ALMACENAMIENTO DE LA INFORMACIÓN		
Sistema de Tratamiento	**Nivel**	**Comprobación**
NO AUTO-MATIZADO	BÁSICO	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?

CUSTODIA DE SOPORTES		
Sistema de Tratamiento	**Nivel**	**Comprobación**
NO AUTO-MATIZADO	BÁSICO	¿Se custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación?, ¿se impide en todo momento que sea accedida por persona no autorizada?

INFORME SOBRE LA AUDITORÍA

Una vez hayamos contestado a las preguntas expuestas anteriormente estaremos preparados para redactar un informe identificando las deficiencias encontradas y las medidas correctoras pertinentes. El informe debe incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados, así como las recomendaciones propuestas.

Una vez redactado, el informe será analizado por el responsable de seguridad que se encargará de llevar a cabo las medidas necesarias para adaptar la empresa a la legislación vigente.

4. Aplicación de Apoyo

En el siguiente apartado presentamos la aplicación de apoyo realizada para la aplicación de la LOPD en microempresas. Ha sido desarrollada para Android 4.0.3, Nivel de API 15, en el entorno de desarrollo Android Studio. Su principal objetivo es un mejor seguimiento de los pasos realizados al ir siguiendo la presente guía.

INSTALACIÓN

Para llevar a cabo la instalación solo debemos de localizar el archivo de instalación de la App y ejecutarlo, podemos ver el instalador en la Figura 30 llamado "app-release". Como podemos observar se trata de un archivo .apk, siglas que significan Android Application Package.

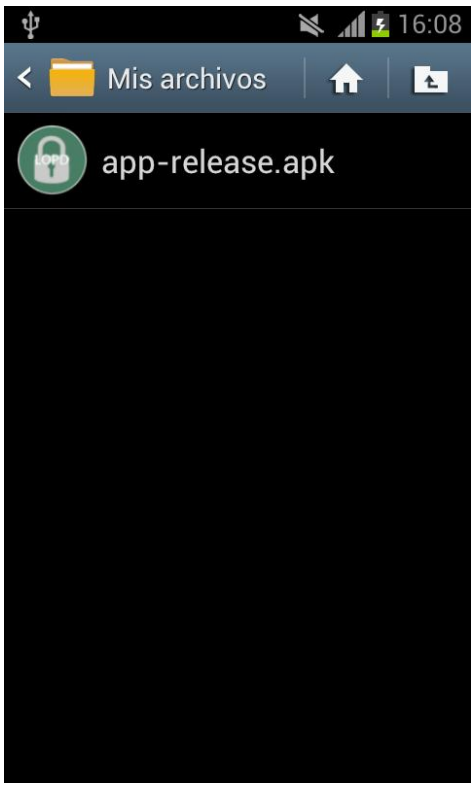


Figura 30: apk de la APP de apoyo

FUNCIONALIDAD

Una vez tengamos la aplicación instalada nos aparecerá en el menú de nuestro dispositivo Android con el nombre de ImplaLOPD, tal como vemos en la figura 31.

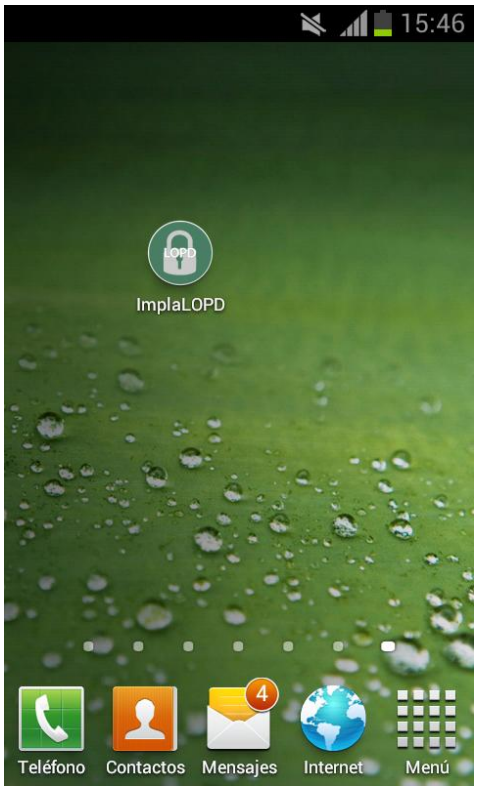


Figura 31: Icono app ImplaLOPD

Una vez abierta, encontraremos el menú principal donde deben aparecer todos los ficheros que hayamos creado, como todavía no hemos creado ninguno aparece la etiqueta de "*No hay ficheros*".

Estos Ficheros son aquellos que contengan datos personales y hayamos decidido inscribir en la AEPD. Siguiendo con el ejemplo de la guía, estos ficheros serían Clientes, Proveedores y Recursos Humanos.

Para crear un nuevo fichero solo debemos pulsar sobre el botón con el símbolo + , marcado con un cuadrado rojo en la Figura 32.

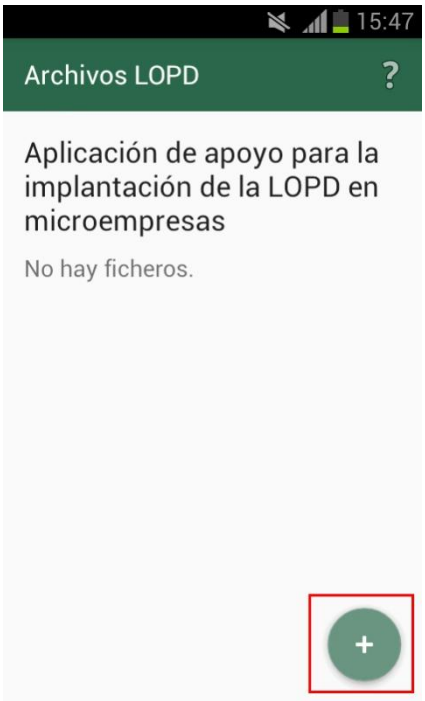


Figura 32: Pantalla Menú principal

Una vez pulsado el botón de *Nuevo Fichero* nos aparecerá una nueva pantalla, Figura 33, dónde se pedirán los datos del fichero a crear. Tendremos que indicar el nombre del fichero, el encargado del tratamiento, el responsable de seguridad, el nivel de seguridad, el tipo del fichero y su Finalidad. Una vez tengamos todos estos campos llenos podremos crear el fichero pulsando en el botón *Guardar*.

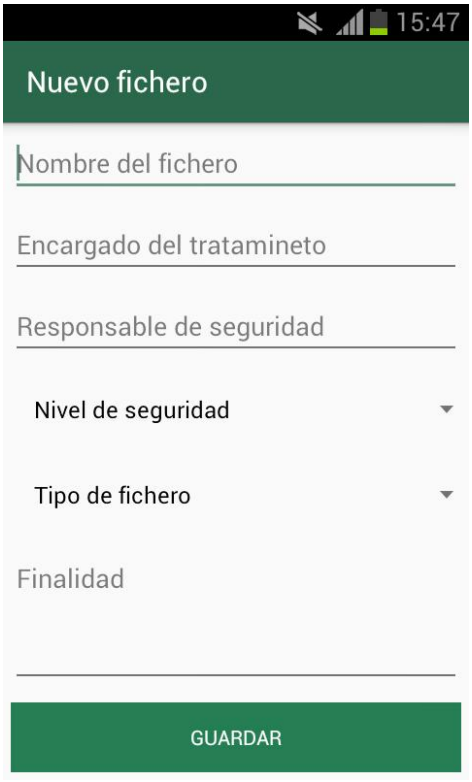


Figura 33: Pantalla Nuevo Fichero

Una vez se cree el fichero volveremos a la pantalla principal dónde podremos ver que el nuevo fichero, en este caso ejemplo con el nombre "*Fichero ejemplo*", ha sido creado correctamente (Figura 34). Podemos observar que al lado del nombre aparecer una barra de progreso y que está al 0%. Esta barra indica hasta qué punto hemos llevado a cabo los pasos de la guía. Si llevamos a cabo todos los pasos al final tendremos el 100%.

Figura 34: Fichero ejemplo

Al pulsar sobre el "*Fichero ejemplo*" nos aparecerá una nueva pantalla con todos los datos del propio fichero y un Checklist con todos los pasos a realizar para la inscripción del mismo, Figura 35.

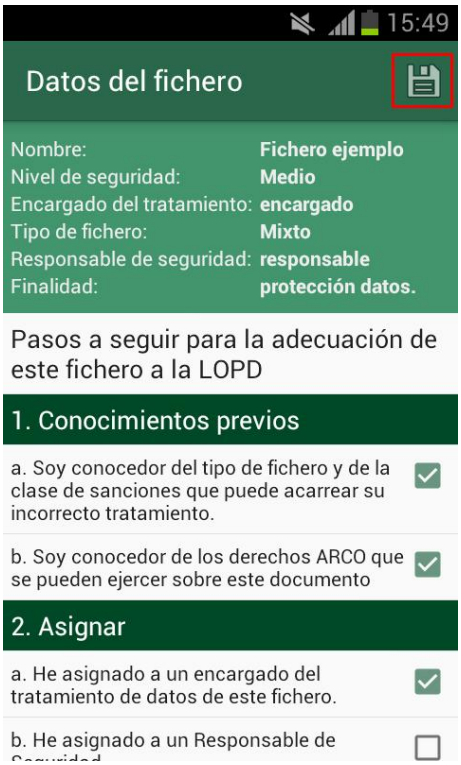


Figura 35: Datos del fichero

Conforme vayamos avanzando en la guía y por tanto en la aplicación de la LOPD sobre el fichero, deberemos ir marcando aquellos pasos realizados. Una vez hayamos seleccionado en el checklist aquellos que hemos completado solo tendremos que *guardar* pulsado el icono marcado con un cuadro rojo en la Figura 35.

Una vez más regresamos a la pantalla principal dónde esta vez la barra de progreso aparecerá ya completada dependiendo del número de pasos que hayamos marcado, Figura 36.

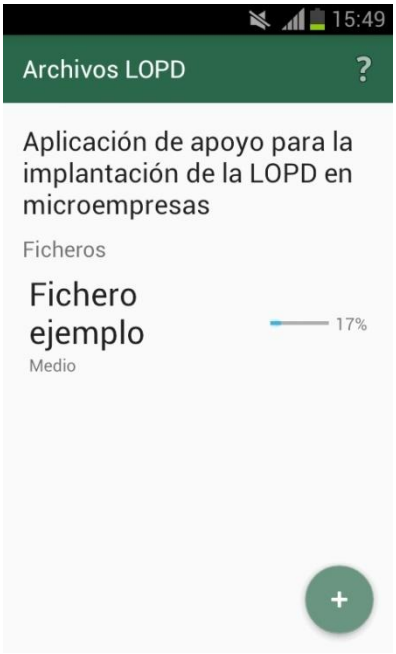


Figura 36: Fichero en progreso.

5. Bibliografía

[1] Agencia Española de Protección de Datos. *Guía de Videovigilancia.* NILO Industria Gráfica, S.A. Consultado en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf. 2010.

[2] Agencia Estatal de Seguridad Aérea. *Procedimiento para el ejercicio y respuesta de los derechos ARCO*. AESA. Consultado en: http://www.seguridadaerea.gob.es/media/4048989/proc_ejerc_y_resp_derch_arco.pdf.

[3] Cuida tus datos. *El consentimiento del afectado*. Cuidatusdatos.com. Consultado en: http://www.cuidatusdatos.com/obligacioneslopd/principioslopd/consentimiento/. 2008.

[4] Agencia Español de Protección de Datos. *Guía de Seguridad de Datos*. NILO Industria Gráfica, S.A. Consultado en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf. 2010.

[5] Agencia Español de Protección de Datos. *Guía rápida de notificación de ficheros mediante el Servicio Electrónico NOTA.* sedeagpd.gob.es/. Consultado en: https://sedeagpd.gob.es/sede-electronica-web/resources/pdf/Guia_rapida_NOTA.pdf. Noviembre, 2015.

[6] Agencia Estatal, Boletín Oficial del Estado. *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.* BOE nº17 Referencia BOE-A-2008-979. Consultado en: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979. Enero, 2008.

[7] Legaltis Blog. *Los tres niveles en la protección de datos.* Legaltis.wordpress.com. Consultado en: https://legaltis.wordpress.com/2013/07/02/los-tres-niveles-en-la-proteccion-de-datos/. Julio, 2013.

[8] Cuida tus datos. *Los niveles de seguridad*. Cuidatusdatos.com. Consultado en: http://cuidatusdatos.com/obligacioneslopd/medidasseguridad/nivelesdeseguridad/index.html. 2008.

[9] Agencia Español de Protección de Datos. *Guía responsable de ficheros.* sedeagpd.gob.es/. Consultado en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf. 2008.

[9] Agencia Español de Protección de Datos. *Guía de seguridad de datos.* sedeagpd.gob.es/. Consultado en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.doc. 2010.

[10] Agencia Estatal, Boletín Oficial del Estado. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* BOE nº298 Referencia BOE-A-1999-23750. Consultado en: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. Diciembre, 1999.

[11] Wikipedia, la enciclopedia libre. *Agencia Española de Protección de datos.* Es.wikipedia.org. Consultado en: https://es.wikipedia.org/wiki/Agencia_Espa%C3%B1ola_de_Protecci%C3%B3n_de_Datos. 2016.

[12] Ayuda Ley Protección de Datos. *Glosario de términos sobre Protección de Datos.* Ayudaleyprotecciondatos.es. Consultado en: http://ayudaleyprotecciondatos.es/glosario/.

[13] Julio César Miguel Pérez. *5 pasos imprescindibles para implantar la LOPD*. CFI, Soluciones para profesionales. Grupocfi.es.

[14] Consejo Europeo. *Reglamento general de protección de datos.* consilium.europa.eu. Consultado en: http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation/. Abril, 2016.

[15]Noticias Jurídicas. *Aprobado el Reglamento europeo de Protección de Datos: nuevas reglas adaptadas a la era digital.* Noticias.juridicas.com. Consultado en: http://noticias.juridicas.com/actualidad/noticias/11018-aprobado-el-reglamento-europeo-de-proteccion-de-datos:-nuevas-reglas-adaptadas-a-la-era-digital/. Abril, 2016.

6. Anexos

Anexo 1: Cuadro Resumen de las medidas de Seguridad

	Nivel Básico	Nivel Medio	Nivel Alto
RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

	Nivel Básico	Nivel Medio	Nivel Alto
IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS Identificación y autenticación personalizada. Procedimiento de asignación y distribución de contraseñas. Almacenamiento ininteligible de las contraseñas. Periodicidad del cambio de contraseñas (<1 año).	SOLO FICHEROS AUTOMATIZADOS Límite de intentos reiterados de acceso no autorizado.	
GESTIÓN DE SOPORTES	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 autorizado para recepción/entrega.	SOLO FICHEROS AUTOMATIZADOS Sistema de etiquetado confidencial. Cifrado de datos en la distribución de soportes. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		SOLO FICHEROS AUTOMATIZADOS Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	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 (ARCO)		

	Nivel Básico	Nivel Medio	Nivel Alto
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	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			SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.

Anexo 2: Información para el personal

INFORMACIÓN PARA LOS TRABAJADORES/USUARIOS SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Nombre Trabajador:

NIF:

Por el presente documento se informa a los trabajadores de sus deberes y obligaciones en materia de protección de datos. El trabajador reconoce expresamente conocer y aceptar las medidas de seguridad incluidas en el DOCUMENTO DE SEGURIDAD Y asume las mismas expresamente en cumplimiento de la normativa vigente en materia de protección de datos.

NORMAS, MEDIDAS Y PROCEDIMIENTOS DE SEGURIDAD

Con el objetivo de dar cumplimiento a lo establecido en el artículo 89.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, la entidad establecerá las siguientes medidas de seguridad, desarrolladas en el correspondiente DOCUMENTO DE SEGURIDAD que deberán ser conocidas y aceptadas por todo el personal:

1.**Funciones y obligaciones del personal y acceso:** que incluye la relación de usuarios y funciones de los mismos.

2.**Identificación y autenticación**: Los usuarios tendrán acceso autorizado únicamente a los datos y recursos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3.**Acceso**: el personal solo puede acceder a datos que tiene autorizados, impidiendo el acceso a otros datos.

4.**Gestión de soportes:** dichos soportes están inventariados conforme a lo establecido en el Documento de Seguridad. Al mismo tiempo, el trabajador reconoce conocer y tratar los registros de entrada y salida de datos de carácter personal, registro de incidencias y registro de recuperación de datos.

5.**Copias de respaldo**: las copias de respaldo se realizan conforme a lo determinado en el documento de seguridad.

6.**Soportes no automatizados**: el trabajador conoce expresamente las medidas de seguridad relativas al tratamiento de soportes no automatizados recogidas en el Documento de Seguridad.

7.**Deber de secreto:** Las personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligadas al secreto profesional respecto de los mismos y al

deber de guardarlos. Esta obligación seguirá vigente incluso después de finalizar las relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

FUNCIONES Y OBUGACIONES DEL PERSONAL Usuarios:

- Cumplimiento de la normativa de seguridad recogida en el documento de seguridad.
- Mantener el secreto de la información sobre datos personales.
- Hacer uso de los datos únicamente para los fines para los cuales han sido recabados.
- No divulgar las contraseñas de que dispongan para acceder tanto a los sistemas informáticos como a los ficheros que contengan datos de carácter personal
- Solicitar las autorizaciones necesarias para el tratamiento de dichos datos siempre que se refieran a salidas o entradas de soportes informáticos
- No utilizar con fines privados los sistemas informáticos de la entidad, sin autorización del empresario.
- Informar al responsable de seguridad sobre cualquier incidencia que se produzca.

DERECHOS DE LOS CIUDADANOS

El ejercicio de los derechos de acceso, cancelación, rectificación y oposición es personalísimo, es decir, que estos derechos deben ser ejercidos directamente por los interesados ante cada uno de los responsables de los ficheros. Además, no se exigirá contraprestación alguna por el ejercicio de estos derechos.

Para ejercitar los derechos de acceso, cancelación, rectificación y oposición el titular de los datos deberá dirigirse por escrito al responsable del fichero de la entidad de que se trate, acompañando dicho escrito con una copia del **DNI** del solicitante. Es necesario utilizar cualquier medio que permita acreditar el envío y la recogida de su solicitud. Algunos de los derechos relacionados con la protección de datos son:

- Derecho a ser informado y a que le sea recabado su consentimiento
- Derecho de acceso
- Derecho de cancelación
- Derecho de rectificación
- Derecho de oposición
- Derecho a indemnización
- Derecho de consulta al Registro General de Protección de datos
- Derecho de impugnación de valores

- Derecho de exclusión de las guías telefónicas
- Derecho a no recibir publicidad no deseada

CONSECUENCIA DEL INCUMPLIMIENTO DE LAS OBLIGACIONES POR PARTE DE LOS TRABAJADORES

Las consecuencias por el incumplimiento de las obligaciones de seguridad por parte de los trabajadores pueden ser de tipo administrativo, laboral, civil y penal.

Y para que conste a los efectos oportunos, firma el presente documento.

En _____ a _____ de _____ de 20___.

Firmado y sellado Entidad: **Firmado Trabajador/Usuario:**

Anexo 3: Plantillas de respuesta a los derechos ARCO

RESPUESTA PARA EL DERECHO DE ACCESO

Estimado señor o señora: _____ con DNI: _____

Recibida su solicitud de acceso a los datos personales el día ___/____/___, que sobre su persona obran en ficheros de los que somos responsables, le informamos de lo siguiente:

Sus datos (indicar los datos existentes en el fichero):

Origen de los datos (indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero):

Comunicaciones realizadas autorizadas por usted (indicar, en su caso, a que terceros se les han comunicado los datos):

Comunicaciones que se prevé realizar (sólo en el caso de que esté prevista alguna comunicación de datos no citada en el apartado anterior):

Atentamente, _____ a día _____ de _____ de 20___

Firma:

RESPUESTA PARA EL DERECHO DE RECTIFICACIÓN

Estimado señor o señora: _____ con DNI: _____

Recibida su solicitud respecto a los datos personales el día ___/____/___, que sobre su persona obran en ficheros de los que somos responsables, le informamos de que se ha procedido a dar respuesta a su solicitud. Los datos rectificados son los siguientes:

Tipo de Dato	Datos Antiguos	Datos Rectificados

Atentamente, _____ a día _____ de _____ de 20___

Firma:

RESPUESTA AL DERECHO DE CANCELACIÓN

Estimado señor o señora: _____ con DNI: _____

Recibida su solicitud respecto a los datos personales el día ___/____/___, que sobre su persona obran en ficheros de los que somos responsables, le informamos de que se ha procedido a dar respuesta a su solicitud. Los datos personales recabados sobre su persona han sido eliminados de cualquier fichero o sistema de información de nuestra organización.

Atentamente, _____ a día _____ de _____ de 20___

Firma:

RESPUESTA PARA EL DERECHO DE OPOSICIÓN

Estimado señor o señora: _____ con DNI: _____

Recibida su solicitud respecto a los datos personales el día ___/____/___, que sobre su persona obran en ficheros de los que somos responsables, le informamos de que se ha procedido a dar respuesta a su solicitud. La organización ha bloqueado sus datos personales para evitar el uso de los mismos.

Atentamente, _____ a día _____ de _____ de 20___

Firma:

Anexo 4: Carta de nombramiento del responsable de seguridad

CARTA DE NOMBRAMIENTO DE RESPONSABLE DE SEGURIDAD

Por la presente _____, con DNI _____ trabajador de la entidad _____ con el CIF_____, es nombrado responsable de seguridad desde la fecha estipulada al final del presente documento, conforme a lo estipulado en el artículo 95 del RLOPD. El trabajador acepta expresamente dicho cargo.

La función básica del responsable de seguridad está vinculada a la coordinación y control de las medidas de seguridad definidas en el Documento de Seguridad. El trabajador conoce expresamente dicho documento, así como las medidas de seguridad legales incluidas en el mismo, entre las que destacan:

1.Cumplimiento de la normativa de seguridad recogida en el documento de seguridad.

2.Mantener el secreto de la información sobre datos personales.

3.Hacer uso de los datos únicamente para los fines para los cuales han sido recabados.

4.No divulgar las contraseñas de que dispongan para acceder tanto a los sistemas informáticos como a los ficheros que contengan datos de carácter personal.

5. Solicitar las autorizaciones necesarias para el tratamiento de dichos datos siempre que se refieran a salidas o entradas de soportes informáticos

6. No utilizar con fines privados los sistemas informáticos de la entidad, sin autorización del empresario.

7. Informar al responsable de seguridad sobre cualquier incidencia que se produzca.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Y para que conste a los efectos oportunos, firma el presente documento, en _____

a _____ de _____ de 20___.

Firmado Responsable de Seguridad: **Firmado Representante legal de la empresa:**

Anexo 5: Compromiso de confidencialidad

COMPROMISO DE CONFIDENCIALIDAD

El abajo firmante, _____ con DNI _____ (en adelante EL TRABAJADOR) en el marco de la relación laboral que le une con la entidad _____ con CIF _____ cuyo representante legal es _____ con DNI (en adelante LA ENTIDAD) _____ acuerdan lo siguiente:

1. Datos e información confidencial:

Se considera información confidencial:

- Todo tipo de datos de carácter personal de clientes, trabajadores, etc.
- Datos económicos vinculados de alguna manera a la actividad de la entidad.
- Estrategias empresariales asumidas por la entidad
- Métodos de negocio
- Documentos contractuales
- Propiedad intelectual/Patentes
- Desarrollo de nuevos productos

2. Protección de datos:

LA ENTIDAD cumple con todas las exigencias de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos y el Reglamento de Medidas de Seguridad (Real Decreto 1720/2007, de 20 de diciembre). EL TRABAJADOR ha sido informado de sus obligaciones y derechos en relación con las leyes anteriormente citadas y se compromete a cumplir, en el desarrollo de sus funciones en LA ENTIDAD, con la normativa vigente, nacional y comunitaria, relativa a la protección de datos de carácter personal y, en particular, con la Ley Orgánica 15/1999, de 13 de diciembre y disposiciones complementarias o cualquier otra norma que las sustituya en el futuro.

3. Confidencialidad:

EL TRABAJADOR se obliga de forma irrevocable ante LA ENTIDAD a no revelar, divulgar o facilitar a ninguna persona física o jurídica, pública o privada, ajena a LA ENTIDAD cualquier información confidencial, ya no utilizarla para su propio beneficio o para beneficio de cualquier otra persona. EL TRABAJADOR se compromete a utilizar la información confidencial únicamente en la forma que exija el desempeño de sus funciones en LA ENTIDAD, Y no disponer de ella de ninguna otra forma o con otra finalidad.

4. límite de la obligación de confidencialidad:

EL TRABAJADOR se compromete a cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con LA ENTIDAD.

EL TRABAJADOR tiene la obligación de devolver la información confidencial a la que haya tenido acceso en el momento en que termine la relación contractual.

5. Consecuencia derivadas del incumplimiento:

EL TRABAJADOR se hace responsable frente a LA ENTIDAD Y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a LA ENTIDAD de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

En _____ a _____ de _____ de 20___.

Firmado y sellado Entidad: **Firmado Trabajador/Usuario:**

Anexo 6: Autorización de salida de documentos o soportes

AUTORIZACIÓN DE SALIDA DE SOPORTES

_____, en calidad de responsable de seguridad de la entidad: _____, con DNI: _____ autoriza a _____, con DNI: _____ para retirar los siguientes documentos y/o soportes:

Nombre Documento /Soporte	Tipo	Destino	Fecha salida

En _____ a _____ de _____ de 20___.

Firma Responsable: Firma Autorizado:

Anexo 7: Registro de incidencias

REGISTRO DE INCIDENCIAS	
Nº Incidencia:	
Fecha / Hora:	
Persona que Notifica: **Departamento:**	
Tipo de incidencia:	
Descripción:	
Efectos derivados:	
Medidas Correctoras:	
Acciones para datos de nivel medio	
Procedimiento de recuperación de datos:	
Persona que ejecutó el proceso:	
Datos que se han grabado :	

Anexo 8: Autorización para la recuperación de datos

AUTORIZACIÓN PARA LA RECUPERACIÓN DE LOS DATOS

Don/Doña _____con NIF_____

en calidad de Responsable del Fichero_____ autoriza a

_____ para llevar a cabo la recuperación de los

datos de dicho fichero.

Firmado:

Fecha:

Anexo 9: Información para el cliente

Razón social:

CIF/NIF:

Domicilio:

Conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (a partir de ahora LOPD) le informamos de lo siguiente:

- Esta entidad ha recogido los datos de carácter personal que le conciernen con el consentimiento expreso del cliente, exclusivamente para la finalidad expresada en el párrafo siguiente, y los ha incorporado a un fichero de titularidad privada que cumple con la normativa vigente en materia de protección de datos.
- Los datos han sido recabados del propio interesado o su representante legal.
- Los datos se utilizarán con el siguiente fin: _____
- Sus datos de carácter personal serán cancelados cuando dejen de ser necesarios.
- Usted puede ejercitar los derechos de acceso, rectificación, cancelación, oposición sobre sus datos personales.
- El responsable del fichero, y, en su caso, el encargado del tratamiento, han adoptados las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, según las condiciones establecidas en la legislación vigente.

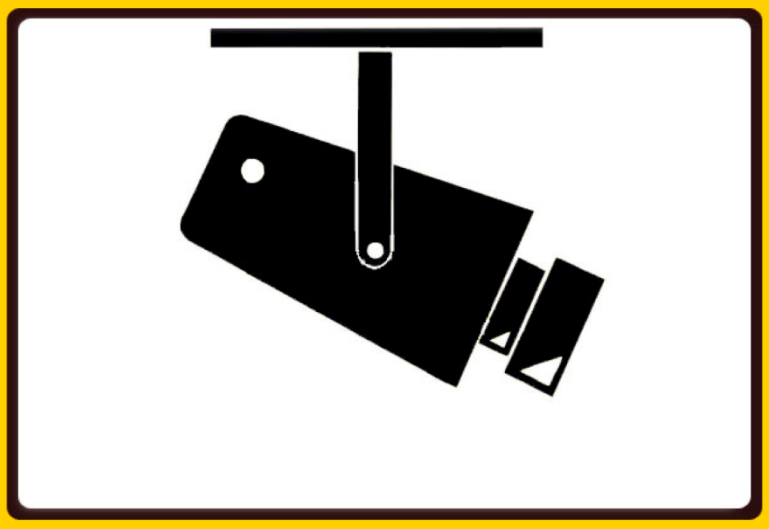
Y para que así conste a los efectos oportunos, firmo el presente documento,

En _____ a _____ de _____ de 20___.

Firma Interesado: Firma y sello empresa:

Anexo 10: Cláusula informativa sobre Videovigilancia

ZONA VIDEOVIGILADA



LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

CLAUSULA INFORMATIVA SOBRE VIDEOVIGILANCIA: Art. 3, apartado B. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

FICHERO PRIVADO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

Le informamos que los datos que obtenemos a través de la videovigilancia no serán cedidos bajo ningún concepto, exceptuando los cuerpos de seguridad pertinentes. Y serán tratados dentro de la normativa vigente en materia de protección de datos, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal. (LOPD) Estos datos serán incluidos en un fichero informático denominado videovigilancia, La función de recabar estos datos es proteger los nuestros bienes.

El responsable de dicho fichero es:

con C.I.F.:

con domicilio a efectos de notificaciones en C/

Código Postal:

Población:

de la provincia de

Usted tiene derecho a recibir respuesta de cualquier pregunta, consulta o aclaración que le surja derivada de esta acción. Usted tiene derecho al acceso, oposición, rectificación, cancelación, de sus datos de carácter personal, mediante escrito y adjuntando DNI, a la dirección antes indicada o por correo electrónico a

Todos sus datos serán dados de baja definitivamente de nuestra base de datos por los siguientes motivos: 1º- cada 30 días como máximo, 2º- cuando hayan dejado de ser necesarios para los fines que motivaron su recogida.

Anexo 11: Contrato de acceso a los datos por cuenta de terceros

De una parte ,
_____, entidad de nacionalidad Española con domicilio en la calle _____, de _____ y provista de Número de Identificación Fiscal _____, representada en este acto por D/Dña. _____, mayor de edad, con DNI _____ (en adelante, "Responsable del Fichero").

Y de otra parte,
_____, entidad de nacionalidad Española con domicilio en la calle _____ de _____ y, provista de Número de Identificación Fiscal ……., representada en este acto por D/Dña……., mayor de edad, con DNI……. (en adelante, "Encargado de Tratamiento").

EXPONEN

I. Que el Responsable del Fichero es una entidad cuya actividad es la prestación de _____,

II. Que el Encargado de Tratamiento es una entidad cuya actividad se centra en prestar servicios de asesoramiento a empresas, habiendo sido contratado por el Responsable del Fichero para la prestación de servicios de asesoramiento empresarial.

III. Que para el desarrollo de los servicios para los que ha sido contratado, el Encargado de Tratamiento requerirá el acceso a datos de carácter personal contenidos en ficheros del Responsable del Fichero.

IV. Que siendo así, ambas partes han acordado formalizar el presente Contrato para regular, en lo relativo al tratamiento de los datos de carácter personal, la mencionada prestación de servicios, por parte del Encargado de Tratamiento

ESTIPULACIONES

Primera.- Objeto del contrato.

El objeto del presente Contrato es la regulación de la relación entre el Responsable del Fichero y el Encargado del Tratamiento, a los efectos de dar cumplimiento a lo establecido en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Segunda.- Tratamiento de datos de carácter personal.

El Responsable del Fichero manifiesta que es titular de ficheros que contienen datos de carácter personal recabados legalmente, debidamente inscritos en el Registro General de Protección de Datos (en adelante, "Ficheros") y que, en virtud de los servicios contratados al Encargado de Tratamiento, autoriza y delega su tratamiento, en la medida que sea necesario para la prestación de los mismos.

Tercera.- Finalidad del tratamiento.

El Encargado de Tratamiento, únicamente tratará los datos contenidos en los Ficheros para realizar por cuenta del Responsable del Fichero la prestación de los servicios contratados y, en ningún caso, los utilizará para finalidades distintas a las acordadas.

Cuarta.- Medidas de Seguridad.

El Encargado del Tratamiento deberá aplicar a los datos contenidos en los Ficheros, las medidas de seguridad establecidas reglamentariamente 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 13 de diciembre, de protección de datos de carácter personal.

Quinta.- Comunicación de datos a terceros.

Como norma general, el Encargado de Tratamiento no comunicará los datos de carácter personal accedidos en el marco del presente contrato a un tercero, ni siquiera para su conservación, salvo que en el contrato de prestación de servicios se detalle lo contrario.

En los casos en los que para la prestación de los servicios contratados, el Encargado de Tratamiento facilite datos personales, que previamente haya puesto a su disposición el Responsable del Fichero, a entidades cuya intervención sea necesaria para dar cumplimiento a esta relación contractual, dichas entidades se verán sometidas a las mismas reglas de protección de datos y confidencialidad que el Encargado de Tratamiento.

No obstante, con anterioridad a la facilitación de los datos por parte del Encargado del Tratamiento a estas entidades, éste deberá contar con la autorización expresa del Responsable del Fichero y regular esta relación de acuerdo con las exigencias del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Sexta.- Ejercicio de derechos.

En los casos en los que los titulares de los datos ejerciten sus derechos de acceso, rectificación, cancelación u oposición ante el Encargado de Tratamiento este deberá dar traslado de la mencionada solicitud, en el plazo máximo de 3 días, al Responsable del Fichero a fin de que por el mismo se resuelva, en los plazos establecidos por la normativa vigente.

Séptima.- Deber de información mutuo.

Ambas partes, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informan mutuamente de que los datos de la/ s persona/ s de contacto que figura en el encabezamiento del presente contrato serán incorporados a los ficheros titularidad de cada una de las partes con la finalidad de gestionar dicha relación.

Octava.- Deber de conservación.

El Encargado de Tratamiento conservará los datos de carácter personal a los que haya tenido acceso en razón del servicio prestado, así como cualquier soporte o documento en el que consten, durante el tiempo en que esté vigente dicho servicio o porque así venga dispuesto por Ley. Finalizado éste, procederá a devolver o, en su caso, destruir dichos datos o soportes.

Novena.- Responsabilidad.

El Encargado de Tratamiento se compromete a cumplir con las obligaciones establecidas en el presente Contrato y en la normativa vigente, en relación con el presente encargo de tratamiento. De conformidad con lo establecido en el artículo 12.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 20.3 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la misma, el Encargado de Tratamiento será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del presente Contrato, respondiendo de las infracciones en que hubiera incurrido personalmente.

Décima.- Designación de fuero.

Para todos los efectos derivados del presente Contrato, las partes se someten expresamente a los Juzgados y Tribunales de……., con renuncia a su propio fuero.

Y en prueba de conformidad, después de leer detenidamente el documento, las partes lo ratifican y firman por duplicado y a un solo efecto, en el lugar y fecha indicados.

En _____, a _____

D/Dña_____ D/Dña_____

Por (Responsable de Fichero) Por (Encargado de tratamiento)

Anexo 12: Información para usuario de internet

Aviso legal sobre el prestador del servicio:

De acuerdo con lo dispuesto en el artículo 10 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información le informamos de que la empresa _____ con C.I.F. _____ es la entidad responsable del sitio web: _____

Uso de cookies:

En este sitio web no se utilizan cookies ni se conservan datos como la dirección IP, o el nombre del dominio.

Protección de datos:

Asimismo, le informamos de que, los datos personales que nos ha facilitado en este sitio web serán incorporados a un fichero:_____ . Inscrito en la Agencia Española de Protección de Datos y que cumple con las medidas de seguridad exigidas por la ley, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Dichos datos se trataran con la finalidad de gestionar los servicios contratados de gestión y asesoramiento relacionados con la protección de datos y para mantenerle informado de las novedades y promociones comerciales de nuestra entidad.

Le recordamos que puede ejercitar los derechos de acceso, cancelación, rectificación u oposición enviando la solicitud a la dirección anteriormente indicada.

Anexo 13: Reglamento Europeo de Protección de Datos

El pasado 14 de abril de 2016 se aprobó en el Parlamento Europeo el nuevo Reglamento 2016/679 general de protección de datos que actualiza y moderniza los principios de la directiva establecida en 1995. Este nuevo reglamento persigue el objetivo de proporcionar a los ciudadanos un mayor control sobre su información privada y garantizar un estándar de protección más elevado en toda la Unión Europea.

La aplicación de este nuevo texto no se hará efectiva hasta el año 2018 pero tenemos que ir tomándolo en consideración puesto que va a representar un enorme cambio en la legislación con la que habíamos tratado hasta ahora.

Debido a las fecha de aprobación y al tiempo destinado a la redacción del presente proyecto no se puede incluir un análisis más extenso y detallado, pero se intentará reflejar con la mayor exactitud los principales cambios y novedades que va a traer este nuevo reglamento.

¿Qué incluyen las nuevas reglas de protección de datos?

En primer lugar tenemos un aumento considerable de los derechos de los interesados, personas que tienen datos en tratamiento. Estos nuevos derechos, como ya hemos comentado, incrementan el control de las personas sobre sus datos personales gracias a:

- La necesidad de un consentimiento claro y afirmativo sobre el tratamiento de los datos del interesado.
- Un acceso más sencillo del interesado a sus datos personales.
- El derecho al olvido, que es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet. Impide la difusión de información personal a través de internet cuando no se cumple la normativa o cuándo la información es obsoleta y ya no tiene relevancia, aunque la publicación original sea legítima.
- El derecho a la portabilidad de datos de un prestador de servicios a otro.
- Lenguaje claro y comprensible sobre las cláusulas de privacidad y multas a las empresas en caso de infracción.

El Reglamento trae también una serie de obligaciones de los responsables de los datos y de los encargados del tratamiento. Entre ellas la aplicación de medidas de seguridad adecuadas al riego de las operaciones de tratamiento, la notificación de las violaciones de datos (piratería) o el nombramiento de un delegado de protección de datos para poder realizar operaciones de riesgo.

Seguimiento, control e indemnización

El proyecto de Reglamento obligará a los miembros de la Unión Europea a crear una autoridad de control independiente a nivel nacional. Acorde a la directiva de unificación propuesta, se dispondrán nuevos mecanismos. En aquellos casos dónde haya varias naciones implicadas se adoptará el principio de ventanilla única, lo que significa que una empresa con filiales en

diversos Estados miembros solo tendrá que tratar con la autoridad de protección de datos en el estado en el que se encuentre su establecimiento principal.

El actual Comité de protección de datos se sustituirá por un nuevo Consejo Europeo de Protección de datos formado por los representantes de cada una de las 28 autoridades de control independientes.

Las nombradas autoridades de control servirán al interesado para exigir su derecho a presentar una reclamación, así como también su derecho al recurso judicial, la compensación y la responsabilidad. El interesado tendrá derecho a que un órgano jurisdiccional nacional revise las decisiones de su autoridad de protección de datos.

En lo relativo a las indemnizaciones, las sanciones a los responsables o encargados de tratar con datos de carácter personal podrán acarrear multas de hasta 20 millones de euros o del 4% de su volumen de negocios total anual, siempre en caso del incumplimiento de la normativa de protección de datos.

Nuevas normas sobre transmisión de datos

En el caso de la transferencia de datos personales a terceros países u organizaciones internacionales, una Comisión realizará la evaluación del nivel de protección del territorio destinatario. En caso de no adoptar una decisión sobre un territorio o sector, la transferencia podrá continuar mientras cumpla las garantías apropiadas o en casos especiales.

También se incluyen directivas sobre transmisión de datos para cuestiones judiciales y policiales, estableciendo unos estándares en el intercambio de datos dentro de las fronteras de la UE. La intención es lograr una cooperación más rápida y efectiva entre las autoridades policiales y judiciales de diferentes países y lograr un mayor nivel de seguridad.

Registro de datos de los pasajeros aéreos

Otra medida importante adoptada en el Parlamento Europeo ha sido la creación de un registro europeo de datos de los pasajeros que viajen con avión (PNR), en pos de combatir los ataques terroristas y promulgada a raíz del incremento de los mismos.

Esta medida obliga a las compañías aéreas a entregar a las autoridades nacionales los datos de los pasajeros con salida o llegada desde un estado miembro de la UE. Para proteger la privacidad de los pasajeros y asegurar la protección de sus datos, la información que se conserve deberá quedar “oculta” tras los primeros seis meses, pudiendo ser conservada hasta 5 años.

Anexo 14: Preguntas Frecuentes

A continuación expondremos algunas de las dudas más habituales a la hora de realizar la adaptación a la Ley Orgánica de Protección de Datos.

Dispongo de una página web que puede demandar un registro que guarde información de carácter personal de los usuarios ¿Cómo debo proceder?

Cualquier formulario en que se recaben datos de carácter personal debe ir acompañado de un a cláusula informativa, normalmente el usuario debe aceptarla, que informe a los usuarios de que sus datos van a ser almacenados. Podemos encontrar una cláusula modelo en el Anexo 12.

¿Cómo debo proceder si deseo instalar un sistema de cámaras de seguridad?

En primer lugar se debe realizar la inscripción de un fichero de videovigilancia en la página de la Agencia Española de Protección de Datos tal como hemos descrito en el apartado "Fase 3: Inscripcion de ficheros en la AEPD". Marcaremos como finalidad "Videovigilancia", en fuente de los datos pondremos "el propio interesado", en Dataos de carácter identificativo marcaremos "imagen/voz", señalaremos un tratamiento "Automatizado" y pondremos a "Las Fuerzas y cuerpos de seguridad del Estado" como destinatarios de posibles cesiones.

Una vez tengamos el fichero inscrito debemos colocar en las zonas videovigiladas un distintivo informativo ubicado en un lugar visible y disponer los impresos en que se detalle la información acerca de los derechos ejercibles y la identidad del responsable del fichero ante quien ejercerlos. Podremos encontrar la documentación en el Anexo 10.

¿Puedo utilizar los datos personales de mis clientes para enviarles publicidad?

Sí, siempre que el afectado haya dado su consentimiento explicito.

¿Cómo puedo conseguir eliminar mis datos de los ficheros de una empresa que me envía publicidad?

Para esto debes ejercer tus derechos ARCO, en concreto el derecho de cancelación. El afectado deberá dirigirse al responsable del fichero dónde se encuentran sus datos y este deberá proporcionarle la documentación necesaria para que el interesado pueda ejercer el derecho de cancelación. Recordamos que como empresa debemos disponer de la documentación necesaria para garantizar cualquiera de los derechos ARCO a quien lo solicite. Podemos encontrar la documentación necesaria en el Anexo 3.

¿Qué tipos de consentimiento son admitidos por la LOPD?

La LOPD define el consentimiento del afectado en el Artículo 3, apartado h, como: "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."

Por tanto, y según el artículo 6.1 que establece la condición de que el tratamiento de los datos de carácter personal requiere el consentimiento del afectado, podemos decir que el responsable del fichero solo podrá tratar con datos de carácter personal si se dispone del consentimiento del titular. ¿Cómo se puede obtener este consentimiento? Es aquí donde encontramos el conflicto. Existe la manera "expresa" y la manera "tácita" de obtener los datos.

El consentimiento expreso consiste en una afirmación del afectado aceptando el tratamiento de sus datos mediante un acto declarativo de la voluntad, bien de forma oral o escrita (esto puede ser mediante una llamada telefónica o bien marcado la casilla de algún documento, etc..)

El consentimiento tácito se produce cuando la persona afectada por el tratamiento, sabiendo que se van a recabar y tratar sus datos, no se manifiesta en contra de este tratamiento.

La LOPD solo exige un consentimiento expreso y escrito cuando se trata de dato especialmente protegidos (Artículo 7 de la LOPD), como la ideología, religión, creencias, afiliación sindical y en resumen cualquier dato de nivel alto que no sean datos relacionados con la salud, el origen racial y la vida sexual.

Teniendo en cuenta el artículo 12.3 del Real Decreto 1720/2007 que establece que "corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho" lo más recomendable resulta obtener siempre el consentimiento expreso por escrito independientemente del tipo de datos que vayamos a recoger.

¿Cómo me aseguro de que ninguno de mis empleados utilice los datos de mi empresa para su propio beneficio?

Todo persona perteneciente al negocio deberá firmar un compromiso de confidencialidad por el cual declara que acepta a cumplir con todas las exigencias de la LOPD 15/1999 y el Real Decreto 1720/2007, es conocedor de sus obligaciones y derechos para con las leyes anteriormente citadas y se compromete a acatar las posibles sanciones legales si no cumple con sus funciones para con la entidad. Podemos encontrar un modelo de este permiso en el Anexo 5.

¿Cómo puedo consultar el contenido de la inscripción en el Registro General de Protección de Datos?

La inscripción de un fichero se puede consultar en el Catálogo de ficheros inscritos en el Registro General de Protección de Datos en la sección de Ficheros inscritos de la página web de la AEPD: https://www.agpd.es/portalweb/ficheros_inscritos/index-ides-idphp.php.

También puede consultar la información relativa al código de inscripción, nivel de medidas de seguridad declarado, así como los datos consignados en el apartado de encargado de tratamiento en el Canal del Responsable / Consulta del contenido de la inscripción de la web de la AEPD https://www.agpd.es/portalweb/canalresponsable/consulta_contenido/index-ides-idphp.php. Para ello, la persona que haya presentado la última notificación relacionada con la

inscripción del fichero o la persona que haya sido debidamente autorizada por el responsable del fichero podrá identificarse mediante su certificado electrónico de firma.

¿Los datos relativos a personas jurídicas son también objeto de aplicación de la LOPD?

No. La LOPD sólo se aplica a los datos que se refieren a las personas físicas, con el objeto de garantizar proteger los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

¿Una vez tenga inscritos los ficheros con dato de carácter personal y redactado el documento de seguridad ya he terminado de aplicar la normativa de la LOPD en mi empresa?

No. Se deben implantar las medidas recogidas en el Documento de Seguridad e ir renovando toda la documentación y procedimiento que este exige de forma retroactiva.

El documento de seguridad, mientras la empresa siga activa, irá cambiando para adaptarse a la situación actual y para recoger nuevos datos tales como cesiones, contratos de confidencialidad, inventarios, etc.

Por tanto la adaptación a la LOPD es algo que no acaba en ningún momento, mientras la empresa cambie, deberemos adaptarnos.

¿Qué obligaciones en materia de medidas de seguridad tienen los encargados de tratamiento?

Tanto las prestaciones de servicios realizadas por los encargados de tratamiento en los locales del responsable del fichero, como las realizadas en los propios locales del encargado, se encuentran sujetas a la normativa de protección de datos.
Con carácter general, las obligaciones del encargado del tratamiento en materia de implantación de las medidas de seguridad se encuentran reguladas en los artículos 82 y 88 del Reglamento de desarrollo de la LOPD. Además el documento de seguridad de un encargado debe tener un contenido adicional específico que permita identificar sus encargos indicando:

- La identificación de los ficheros o tratamientos que se traten en concepto de encargado.
- Referencia expresa al contrato o documento que regule las condiciones del encargo.
- Identificación del responsable.
- Período de vigencia del encargo.

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a los restantes requisitos establecidos en el Reglamento de la LOPD.
Por último, el encargado de tratamiento debe implantar las medidas de seguridad adecuadas para sus propios ficheros. Entre ellas, debe mantener actualizado su documento de seguridad, fijar las obligaciones de su personal etc.

¿Puede el encargado hacerse cargo del documento de seguridad del responsable que le ha contratado?

No es infrecuente la existencia de tratamientos, como por ejemplo la confección de nóminas, en los que los datos se alojan y tratan casi por completo en los locales, recursos y soportes del encargado. Para estos casos, el reglamento se refiere en su artículo 88 a la "delegación de la llevanza del documento de seguridad". Para ello deben cumplirse ciertos requisitos:

- Que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado.
- Que esta circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable.
- Que la delegación se indique de modo expreso en el contrato celebrado al amparo del artículo 12 LOPD, con especificación de los ficheros o tratamientos afectados.

No podrá delegarse en el encargado la llevanza del documento de seguridad en lo relativo a aquellos datos contenidos en recursos propios del responsable.

¿Debe notificarse a la AEPD el documento de seguridad?

El documento de seguridad es un documento interno de la organización y no debe ser notificado a la Agencia Española de Protección de Datos.

7. Conclusiones y Futuras Mejoras

En este último capítulo incluimos una sección en la que describimos las conclusiones alcanzadas, realizando un resumen final, y analizando el conjunto de funcionalidades implementadas. Así como una breve descripción de cosas que se podrían mejorar en un futuro y que no han sido llevadas a cabo en el presente trabajo bien por falta de tiempo o de recursos.

Conclusiones

Durante el transcurso del proyecto, tras haber realizado un trabajo de investigación sobre la Ley Orgánica de Protección de Datos, así como de también de todos los reglamentos y recursos relacionados con ella, teniendo en cuenta las consideraciones necesarias para su aplicación, hemos logrado redactar una guía completa de cómo se debe proceder para adaptar una microempresa a la legalidad vigente en materia de protección de datos.

Pasando por las definiciones necesarias para la correcta compresión de todo el trabajo, la explicación de los diferentes artículos adaptados a un ejemplo de microempresa ficticio o la explicación paso por paso para inscribir un fichero o redactar un documento de seguridad me han proporcionado destreza y conocimiento en el campo de Protección de Datos en el suficiente nivel para llegar a redactar un manual.

La guía facilitará enormemente a las empresas la adaptación a la LOPD, evitando tener que llevar a cabo una lectura a fondo de los reglamentos, facilitándoles una información directa, esquematizada y redactada en un lenguaje sencillo y común evitando tecnicismos innecesarios y que se centra en la compresión del mayor número de usuarios posibles.

Así pues, podríamos considerar que el presente trabajo es un elemento que contribuye a difundir el conocimiento sobre las leyes que afectan a las empresas que traten con datos personales, enfatizando en su correcto cumplimiento y difundiendo una serie de prácticas que cada vez deberían ser más comunes.

Futuras Mejoras

Entre las mejoras, que cabría considerar y que no se han llevado a cabo por falta de recursos, tiempo o por temas de legalidad, podríamos incluir:

-**Adaptación de la LOPD sobre una microempresa real.** No se ha podido llevar a cabo una demostración real de cómo funciona la guía por la indisposición de una microempresa. Quizás en un futuro se podría plantear la utilización sobre alguna para corroborar su completo funcionamiento.

-**Adaptación al nuevo Reglamento Europeo de Protección de Datos**. Tal como se indica en el Anexo 13, el nuevo Reglamento ha sido aprobado el 14 de abril de 2016, permaneciendo sin aplicar hasta dentro de dos años, en 2018. Tanto por falta de tiempo, como por falta de ejemplos reales se ha decidido no incluir un desarrollo a fondo de cómo afectará este nuevo Reglemento a la actual LOPD. Aún no desarrollándolo completamente, se han comentado las posibles mejoras que este incluirá.

Creación de una guía para la aplicación del nivel básico, medio y alto del Reglamento de Protección de Datos para microempresas

-Jesús Llopis Ferriol-