# ADstudio
# Diseño Gráfico y Publicidad

Universidad de Burgos

Autor del proyecto: D. Iván Ontañón Ramos
Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez
Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosio

MAGÍSTER EN ASESORÍA Y CONSULTORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
(MAC-TIC)

UNIVERSIDAD DE BURGOS
II Edición. Burgos, Julio 2010.

***Magíster financiado por la Fundación Centro de Supercomputación de Castilla y León***

A Christian,

sin él no hubiera sido posible

ADstudio

# Contenido

# ADstudio: diseño gráfico y publicidad

ADstudio es una empresa joven, pero ya consolidada en el mundo del diseño gráfico profesional y la publicidad, siempre buscando la creatividad para llegar al público y satisfacer todas las necesidades del cliente.

Conscientes de que la creatividad es lo que mueve el mundo empresarial, ADstudio convierte esa necesidad de crear ideas innovadoras con algo diferente en una realidad. Una buena comunicación es la base de cualquier actividad, articulando las posibilidades de futuro de una empresa y abarcando todo lo que una compañía quiere representar, sus productos, servicios y su manera de hacer negocios.

Diseñar una entidad no solamente consiste en crear una ágil campaña publicitaria, ni en crear un novedoso logotipo, ni dar una imagen de empresa moderna, sino que consiste en aquello que engloba todas esas partes.

ADstudio se dedica de una manera profesional al:

- Diseño de logotipos
- Diseño corporativo
- Diseño de packaging
- Diseño de tarjetas
- Diseño de revistas
- Diseño de folletos
- Diseño de flyers
- Diseño de stands
- Publicidad gráfica
- Publicidad exterior
- Book fotográficos
- Infografía
- Servicio de impresión

ADstudio como empresa vanguardista en el mundo de la comunicación y el marketing utiliza los más modernos medios que ofrece la Sociedad de la Información para poder desarrollar su trabajo, conscientes de las posibilidades de fracaso que implicaría no utilizar las últimas tecnologías de la información y comunicación en este tipo de actividades.

Por ello ADstudio necesita ajustarse a toda la normativa vigente sobre nuevas tecnologías, por lo que realizamos un asesoramiento completo y necesario para completar su adaptación, y seguir de esta manera, potenciando el mensaje de las empresas para las que trabaja.

El asesoramiento consiste en una revisión sobre Protección de Datos de carácter personal, comercio electrónico, pago electrónico, firma electrónica, propiedad intelectual, nombres de dominio, contratación informática, fiscalidad electrónica y administración electrónica.

# Sociedad de la Información

Nadie podía imaginar hace unos años la revolución que Internet y las demás tecnologías de la información iban a tener, pero es algo que nadie puede ignorar ahora. Es hora de sumarse a esta revolución, independientemente del tamaño de la organización, de los recursos que posea, del mercado al que este enfocado o lo técnica que sea. Es importante hoy en día que las empresas sean visionarias y emprendedoras, que estén dispuestas a evolucionar.

A través de estas tecnologías es como potenciamos todo el poder comunicacional hoy en día y que te permite aprovechar todas las oportunidades que se ofrecen constantemente. Disponemos más información actualmente que cualquier otra generación ha dispuesto nunca, por lo que es necesario establecer unas pautas y unos límites que debemos conocer. Todo el progreso que vivimos ha hecho posible la creación, el acceso y cruzamiento de todo tipo de informaciones en un entorno cultural nuevo. Con ello surge la necesidad de contar con una nueva rama del derecho que regule este nuevo campo de actuación.

El objetivo de este proyecto es la adecuación de una empresa publicitaria a los requisitos jurídicos necesarios en la sociedad en la que vivimos en torno a las tecnologías de la información y las comunicaciones, atendiendo a los aspectos más importantes que en ella se pueden plantear.

ADstudio

# Protección de Datos

## 3.1. INTRODUCCIÓN

El rápido desarrollo e introducción de las nuevas tecnologías de la información y las comunicaciones en la sociedad actual han provocado que el intercambio de datos sea más rápido y eficaz, teniendo como principal consecuencia el incremento de los tratamientos de datos de carácter personal. Rápidamente se pueden transformar datos almacenados en información muy útil con la que se pueden crear perfiles y realizar, de alguna forma, un cierto control social o ser utilizada como herramienta comercial, suponiendo una intromisión en su intimidad sin que la persona se percate del tratamiento de sus datos.

Existe una cierta tensión entre modernidad y protección del ciudadano. Por una parte, no es bueno poner freno a los avances estableciendo leyes que frenen el desarrollo de la sociedad y la potencialidad del progreso, pero también es necesario un adecuado uso de la tecnología para la protección de los ciudadanos y sus derechos. Por lo tanto se trata de un reto vivir con las exigencias que requiere el avance de la sociedad. De acuerdo a la Cumbre de la Sociedad de la Información[1] la Sociedad de la información debe estar centrada en las personas, debe ser integradora y debe estar orientada al desarrollo, basándose en una sociedad en la que se pueda crear, consultar, utilizar y compartir la información y el conocimiento con el objetivo de una mejora en la calidad de vida. El objetivo es garantizar y proteger a las personas físicas en el tratamiento de sus datos personales, las libertades públicas y los derechos fundamentales, especialmente su honor, intimidad y privacidad personal y familiar.

Podemos definir la Protección de Datos como “el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento,

[1] Ginebra, Suiza, diciembre de 2003

para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional[2]"

La Protección de Datos reconoce al ciudadano el poder de control sobre sus datos personales y su capacidad para disponer y decidir sobre los mismos.

### 3.1.1. INTIMIDAD, PRIVACIDAD Y PROTECCIÓN DE DATOS

Es muy común enlazar los principios de intimidad[3], privacidad y protección de datos y confundirlos entre sí, pero tienen un diferente alcance por lo que es necesario antes de profundizar en el tema de la Protección de Datos, tener clara su diferenciación.

La intimidad se puede entender como la "zona espiritual íntima reservada de una persona o de un grupo, especialmente de una familia[4]" mientras que la privacidad es "el ámbito de la vida privada que tiene derecho a proteger de cualquier intromisión[5]". La intimidad define la esfera de cada persona en donde se define qué es privado o qué es público (sentimientos, creencias, pensamientos etc.), por lo tanto se trata de aquellos datos que bajo ninguna circunstancia un individuo proporcionaría de manera libre.

Por otro la privacidad se refiere a la información del individuo que va más allá de lo íntimo, que puede no ser relevante, pero que analizada puede crear perfiles de los individuos (frecuencia que va al cine, tipos de novelas que lee etc.), relevando información acerca de sus gustos, preocupaciones o necesidades.

El elemento común es la información, en especial el tratamiento de la información personal, y que esta formada por la privacidad y la intimidad de un individuo. La Protección de Datos por tanto establece la libertad de cada persona de prestar sus datos personales de manera arbitraria e impone a quienes traten esa información la obligación de hacerlo con el consentimiento del afectado.

---

[2] Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal

[3] Principio recogido en el Artículo 18, apartado 1º de la Constitución Española de 1978: Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[4] Definición diccionario de la Real Academia Española

[5] Definición diccionario de la Real Academia Española

Por ejemplo, el número personal del Documento Nacional de Identidad de una persona no es un dato íntimo ni privado, pero si es un dato bajo la Protección de Datos y el individuo tiene la capacidad de decidir a quien se lo proporciona.

## 3.2. NORMATIVA

El origen de la Protección de Datos en España lo estableció la Constitución de 1978, en la que en su artículo 18, apartado 4º estableció que

"la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Justo cuando la sociedad comenzaba a informatizarse (principalmente en los seguros y la banca) ya se preveía el posterior conflicto en el manejo de la información en una sociedad informatizada. Más tarde vio la luz la primera ley sobre Protección de Datos en España, la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (conocida como la LORTAD), que se mantuvo vigente hasta el 14 de enero de 2000 y que estuvo desarrollada también por el Real Decreto 1332/94 de 20 de junio[6] y el Real Decreto 994/1999 de 11 de junio[7].

La LORTAD fue derogada por la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus Reales Decretos por el Real Decreto 1720/2007, de 21 de diciembre.
Además contamos con la normativa europea, donde la Protección de Datos viene recogida en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre.

[6] De regulación del tratamiento automatizado de los datos de carácter personal

[7] Por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal

LEGISLACIÓN ACTUAL

ESPAÑOLA

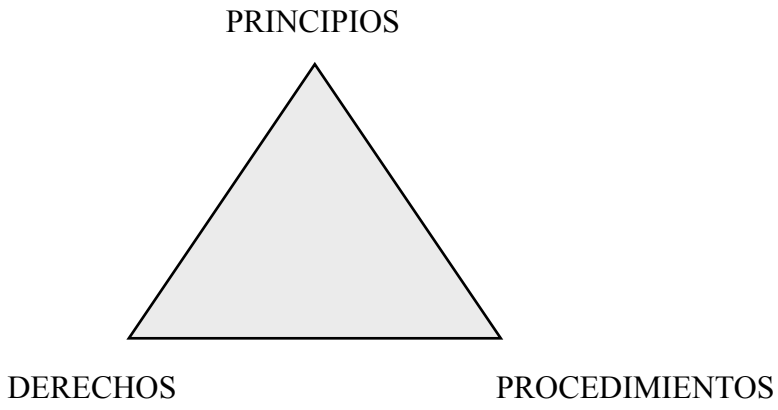
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
- Real Decreto 1720/2007, de 21 de diciembre, por lo que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

EUROPEA

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

## 3.3. ESTRUCTURA DE LA PROTECCIÓN DE DATOS

El estudio de la Protección de Datos se basa en tres elementos de igual importancia que juntos lo configuran. De acuerdo con el profesor Miguel Ángel Davara Rodríguez, se estructura en forma de un triángulo en cuyos vértices se sitúan los principios de la Protección de Datos y en la parte inferior los derechos que emanan de dichos principios y los procedimientos que garantizan el ejercicio efectivo de dichos derechos.




### 3.3.1. PRINCIPIOS

Los debe cumplir el responsable de fichero o tratamiento, que en este caso es la empresa. Los principios de la Protección de Datos son:

- Calidad de los datos - Art.4 LOPD
- Derecho de información en la recogida de datos - Art. 5 LOPD
- Consentimiento del titular de los datos - Art. 6 LOPD
- Datos especialmente protegidos - Art. 7 LOPD
- Datos relativos a la salud - Art. 8 LOPD
- Seguridad de los datos - Art. 9 LOPD
- Deber de secreto - Art. 10 LOPD
- Comunicación o cesión de datos - Art. 11 LOPD
- Acceso a los datos por terceros - Art. 12 LOPD

### 3.3.2. DERECHOS

Son los derechos reconocidos al titular de los datos, al afectado

- Derecho de impugnación de valoraciones - Art. 13 LOPD
- Derecho de consulta al Registro General de la Protección de Datos - Art. 14 LOPD
- Derecho de acceso - Art. 15 LOPD
- Derecho de rectificación y cancelación - Art. 16 LOPD
- Derecho de oposición - Art. 6.4 LOPD
- Tutela de derechos - Art. 18 LOPD
- Derecho de indemnización - Art. 19 LOPD

### 3.3.3. PROCEDIMIENTOS

Tutela al interesado cuando por el responsable del fichero o tratamiento no se cumplen los principios o se le pone algún impedimento para ejercer los derechos.

1. Recabar los datos
2. Tratamiento de los datos
3. La utilización/Comunicación a terceros de los resultados del tratamiento

Estos tres momentos tendrán incidencia al fijar los principios de la Protección de Datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer esos derechos

## 3.4 FICHEROS

### 3.4.1. DEFINICIONES

Una vez comprendido el concepto de Protección de Datos de modo general, conviene analizar diferentes conceptos clave para comprender la legislación española acerca de la Protección de Datos y su utilidad dentro de una empresa privada.

DATOS DE CARÁCTER PERSONAL

Lo primero que es necesario comprender de una manera muy clara es el concepto de datos de carácter personal. El artículo 3, apartado a) de la LOPD define dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables", mientras que el Real Decreto 1720/2007 sobre Protección de Datos en su apartado 1.f) lo define como "cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

Ambas definiciones tratan el concepto de "personas físicas" por lo que excluimos cualquier dato proveniente de personas jurídicas, es decir, no se aplica al tratamiento de datos sobre cualquier empresa u organización (en definitiva, cualquier persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, capaz de ser representada judicialmente o extrajudicialmente).

Es importante destacar que los datos de carácter personal no solamente son los datos alfabéticos, sino que también lo son los números, los gráficos, las fotos, los sonidos, video etc., siempre que esos datos conciernan a una persona identificada o identificable.

FICHERO

La LOPD lo define en su artículo 3 como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". También se puede definir de una forma más sencilla como un conjunto estructurado de datos que se recuperan por parámetros de recuperación y que están definidos por una finalidad concreta, como puede ser el fichero de clientes de una empresa, cuya finalidad principal sería el mantener el contacto con los clientes.

La nueva normativa en Protección de Datos (LOPD) ha hecho desaparecer el termino "automatizado" de su definición de fichero, por lo que engloba a ficheros automatizados y no automatizados.

- Fichero automatizado: todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados.
- Fichero no automatizado: de manera legal se definen como "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 esfuerzos desproporcionados a sus datos personales ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica[8]". Un buen ejemplo de un fichero no automatizado sería cualquier expediente de documentos archivado en archivadores corrientes, existentes en cualquier organización o empresa.

Dependiendo de la titularidad de los ficheros, se pueden diferenciar ficheros de titularidad pública (perteneciente a cualquier administración u organismo público) o ficheros de titularidad privada (perteneciente a la empresa privada).

Dependiendo del tipo de fichero que sea, pueden ser de tres tipos:

- Fichero físico: es un fichero normal, como una carpeta.
- Fichero lógico: es un fichero creado en un ordenador (Word, Excel etc.)
- Fichero jurídico: es el que hay que notificar a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

TRATAMIENTO DE DATOS

El tratamiento de datos es un termino fundamental para entender toda la estructura del tema y viene definido tanto en la LOPD, en su artículo 3 apartado c,

"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"

[8] Artículo 5.1., apartado n) del Real Decreto 1720/2007

como en su reglamento, el Real Decreto 1720/2007 en su artículo 5.1 apartado t, donde aparte de las opciones nombradas anteriormente se añaden “consulta, utilización y supresión”.

AFECTADO / INTERESADO

A efectos legislativos el afectado o interesado es la “persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo (es decir, que sean objeto de tratamiento)”, según la LOPD.

PROCEDIMIENTO DE DISOCIACIÓN

Es cuando en el tratamiento de datos los datos están disociados, es decir, no se asocian con la persona titular de los datos (afectado o interesado). La LOPD en la letra f de su artículo 3 lo define como “todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable”.

Las estadísticas por ejemplo utilizan datos disociados para obtener resultados, de tal manera que no se identifica claramente a un sujeto para dar el resultado.  Si la cesión se efectúa previo procedimiento de disociación no es necesario el consentimiento del afectado.

CONSENTIMIENTO DEL AFECTADO

La LOPD en su artículo 3 letra h, define el consentimiento del afectado como “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.

Se requiere de forma expresa cuando se trate de datos relativos a origen racial, salud o vida sexual, y además por escrito cuando sean datos relativos a la ideología, afiliación sindical, religión o creencias.

Para los demás tipos de datos de carácter personal, la norma general dicta que se requiere el consentimiento del interesado para su tratamiento, salvo que la Ley disponga lo contrario.

-Estudios de mercado: una estrategia de marketing en cualquier empresa es realizar estudios de mercado para así investigar que segmento de mercado ocupa o puede ocupar, prever ventas, lanzar nuevos productos, invertir en nuevos mercados o anticiparse a la competencia. Si ADstudio necesitara realizar cualquier estudio de mercado mediante encuestas, sondeos o entrevistas, en el procedimiento de recogida de datos, la empresa no necesitaría ningún tipo de consentimiento del afectado, siempre que en la publicación del estudio realizado no se haga referencia a una persona física identificable o identificada en concreto.

## CESIÓN DE DATOS

La cesión de datos se define como "toda revelación de datos realizada a una persona distinta del interesado" según la letra i del artículo 3 de la LOPD, mientras que el reglamento hace una definición más acertada y concreta sobre la cesión de datos, "tratamiento de datos que supone su revelación a una persona distinta del interesado".

Es recomendable de si ADstudio decide alquilar a una empresa externa datos de carácter persona accesible al público para la realización de alguna campaña publicitaria o mailing (se pueden conseguir direcciones email a través de los registros de profesionales registrados en colegios profesionales), que se firme un contrato donde la empresa externa que suministra los datos garantice que la procedencia de las direcciones sea de una fuente accesible al público. En caso de que no figuren los datos en cualquiera de las fuentes accesibles al público, la Agencia Española de Protección de Datos puede aplicar duras sanciones, que ascienden a 300.506,05 euros a la empresa que cede los

## FUENTES ACCESIBLES AL PÚBLICO

En la letra j del artículo 3 de la LOPD, las fuentes accesibles al público se definen "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".

Estas fuentes están a disposición del público en general y pueden ser consultadas por cualquier persona, aunque en ocasiones es necesario abonar una contraprestación.

Cuando una empresa hace un tratamiento de datos de carácter personal extraídos de una fuente accesible al público definida por Ley, no es necesario el consentimiento de los afectados para dicho tratamiento, aunque sí que se debe en cada comunicación que se dirija al interesado, informarle sobre el origen de los datos, identidad del responsable del tratamiento y la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos.

BLOQUEO DE DATOS

El apartado 1.b del artículo 5 del Real Decreto 1720/2007 define el bloqueo de datos como "la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades".

La definición que contempla la ley hace referencia al bloqueo de datos, en general pero no especifica en que consiste el bloqueo.

### 3.4.2. ALTA DE LOS FICHEROS EN EL REGISTRO GENERAL DE LA PROTECCIÓN DE DATOS

REGISTRO GENERAL DE LA PROTECCIÓN DE DATOS

El Registro General de la Protección de Datos es un órgano perteneciente a la Agencia Española de Protección de Datos. Su principal función es velar por la publicidad de la existencia de ficheros de datos de carácter personal, con la intención de hacer posible para el afectado o titular de los datos

el ejercicio del derecho de consulta[9] y los derechos de acceso, de rectificación, cancelación y oposición.

Ademas, de acuerdo al artículo 26 del Estatuto de la Agencia, al Registro General de la Protección de Datos corresponde también:

- Inscribir los expedientes de modificación y cancelación del contenido de los asientos
- instruir los expedientes de autorización y cancelación del contenido de los datos (TID)
- rectificar de oficio los errores materiales de los asientos
- expedir certificaciones de los asientos
- publicar una relación anual de los ficheros notificados e inscritos

El Real Decreto 1720/2007 es el que regula:

- el procedimiento de inscripción de los ficheros en el Registro General de la Protección de Datos, tanto los de titularidad pública como los de titularidad privada.
- el contenido de la inscripción
- la modificación de la inscripción
- la supresión
- las reclamaciones
- los recursos contra las resoluciones correspondientes
- demás extremos pertinentes

[9] Artículo 14 de la LOPD, "Derecho de consulta al Registro General de Protección de Datos"

CONSULTA AL REGISTRO GENERAL DE LA PROTECCIÓN DE DATOS

La consulta al Registro General de la Protección de Datos es pública y gratuita, de acuerdo al artículo 14 de la LOPD donde "El Registro General será de consulta pública y gratuita", y en caso de necesidad de consultar dicho organismo, la consulta se puede realizar de tres formas diferentes:

## I. SITIO WEB DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

En la página web de la Agencia, http://www.agpd.es y en el apartado de "Ficheros inscritos", donde podrás seleccionar entre titularidad pública o privada.

La consulta se realiza a través de un formulario de búsqueda donde se pueden introducir los datos necesarios para su búsqueda.


## II. CORREO POSTAL

Otra opción es mediante correo postal solicitando el acceso a uno o varios ficheros específicos, aportando todos los datos necesarios para su búsqueda.

La dirección postal es la siguiente:

Registro General de Protección de Datos

Agencia Española de Protección de Datos

C/ Jorge Juan, 6

28001 Madrid

III. SOPORTE CD

Por último, se puede consultar un fichero mediante la consulta del soporte CD que proporciona la Agencia Española de Protección de Datos y que contiene, entre otros documentos, los ficheros que han sido inscritos en el Registro General de Protección de Datos hasta la fecha de edición del soporte CD.

INSCRIPCIÓN DE FICHEROS

Tienen la obligación de inscribir sus ficheros de datos de carácter personal todas las personas físicas o jurídicas, sea de naturaleza pública o naturaleza privada, en el Registro General de Protección de Datos. Es decir, cualquier fichero que disponga ADstudio referente a datos únicamente de carácter personal y de los que sean titulares,

- la Administración General del Estado
- las entidades y organismos de la Seguridad Social
- los organismos autónomos del Estado
- las sociedades estatales y entes del sector público (a los que hace referencia el artículo 6 de la Ley General Presupuestaria
- las Administraciones de las Comunidades Autónomas y sus Territorios Históricos (también sus organismos y entes dependientes

- las entidades, entes y organismos que integran la Administraciones Local
- las personas jurídico-públicas
- las personas privadas, físicas o jurídicas

deberán ser inscritos en el Registro, de acuerdo al apartado 2 del artículo 39 de la LOPD:

"Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros que sean titulares las Administraciones Públicas

b) Los ficheros de titularidad privada

c) Las autorizaciones a que se refiere la presente Ley

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición"

La inscripción del fichero se podrá realizar a través de la página web de la Agencia Española de Protección de Datos (www.agpd.es), donde se encuentra disponible un formulario electrónico para efectuar el posterior registro, de manera gratuita, en el Registro General de Protección de Datos.

### 3.4.3. CREACIÓN, NOTIFICACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS

CREACIÓN Y NOTIFICACIÓN

De acuerdo al artículo 55 del Real Decreto 1720/2007, con el título de "Notificación de ficheros", la notificación de los ficheros de titularidad privada debe ser anterior a la creación de los mismos y contener toda la información solicitada a través de los formularios:

"Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de trata- miento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos"

MODIFICACIÓN

Se deberán comunicar todos los cambios que se produzcan solamente en la finalidad del fichero, en su responsable y en la dirección de la ubicación a la Agencia Española de Protección de Datos, es decir, se deberá mantener actualizado en todo momento, de acuerdo al artículo 26.3 de la LOPD:

"Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación"

SUPRESIÓN

Si la empresa decide suprimir algún fichero, deberá notificarlo inmediatamente a la Agencia Española de Protección de Datos, para que pueda llevar a cabo dicha supresión del fichero.

### 3.4.4. RESPONSABILIDAD

Se debe determinar en la empresa la persona sobre la que va a recaer la responsabilidad de los ficheros o tratamiento que se creen, así como el encargado de tu tratamiento, que actúa de acuerdo al anterior.

Es recomendable que el responsable del fichero o tratamiento sea una figura jurídica, en este caso, la empresa, en lugar de una persona física, ya que si hubieran sanciones, estas recaerían sobre la persona física concreta. Es mejor que la responsabilidad corra a cargo de la empresa.

#### 3.4.4.1. RESPONSABLE DEL FICHERO O TRATAMIENTO

La letra d del artículo 3 de la LOPD lo define al responsable del fichero o tratamiento como "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

El responsable del fichero es el encargado en la toma de decisiones sobre el objeto, utilización y fin de tratamiento, o sobre el uso que se va a dar a los datos de carácter personal resultantes del tratamiento (también si va a existir una cesión de datos o no).

En resumen, las principales tareas del responsable del fichero o tratamiento son decidir sobre:

- la finalidad
- el contenido
- y el uso del tratamiento

También, tiene la obligación de controlar el uso de los datos que trata el encargado del tratamiento, delimitando sus funciones y responsabilidades.

#### 3.4.4.2. ENCARGADO DEL TRATAMIENTO

Es importante diferenciar esta figura del responsable del tratamiento, ya que este no decide sobre la finalidad, ni el contenido ni el uso del tratamiento de los datos de carácter personal.

Según la definición dada en la letra g del artículo 3 de la LOPD, el encargado del tratamiento es "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

El encargado del tratamiento, muchas veces es una persona diferente o incluso independiente del responsable del fichero. Este es el caso cuando se realiza un servicio de tratamiento de datos para terceros.

#### 3.4.4.3. DEBER DE SECRETO

Uno de los principios más importantes que deben ser impuesto tanto al responsable de fichero como a aquellos que intervengan en cualquiera de las fases del tratamiento de datos de carácter personal es el deber de secreto profesional respecto a los datos tratados[10].

Esta obligación tiene que permanecer incluso después de finalizar sus relaciones con el titular del fichero o con su responsable.

[10] Artículo 10 de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal (LOPD)

### 3.4.5. FLUJOS DE DATOS DE LA EMPRESA

Primero tenemos que analizar que flujos de datos de la empresa ADstudio nos interesa analizar, por lo que tenemos que definir que datos van a ser objeto de estudio para la adecuación de la Ley de Protección de Datos en la empresa.

De acuerdo a la Ley, solamente nos interesa los datos:

"Datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos[11]"

Una vez analizados todos los flujos de datos de carácter personal de la empresa ADstudio se identifican

#### 3.4.5.1. PROVEEDORES

En este fichero se albergarán datos acerca de las empresas proveedoras de material/materia prima/ infraestructuras a la empresa ADstudio con el objetivo de mantener el contacto en caso de necesidad o para realizar pedidos periódicos, y así poder facturar y realizar todas las gestiones administrativas que ello conlleva a la empresa.

Otra de las finalidades por las que se crea un fichero de proveedores es para el envío de publicidad, promociones, catálogos u ofertas de los productos o servicios ofertados por ADstudio.

Primero, los tipos de datos que vamos a recoger en este fichero son datos meramente identificativos para poder contactar con el proveedor:

- Nombre empresa proveedora / nombre y apellidos proveedor
- Persona de contacto de la empresa proveedora
- Dirección
- Localidad
- Provincia, país (si se localiza fuera de España)

[11] Artículo 2 de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal (LOPD)

- Código Postal
- Teléfono 1
- Teléfono 2
- Fax
- E-mail
- Tipo de proveedor
- Fecha apunte

Y también se recogerán datos de carácter administrativo para todo tipo de gestiones administrativas entre la empresa ADstudio y el proveedor:

- Número del Documento Nacional de Identidad - DNI (si se aplica)
- Número de Identificación Fiscal - NIF
- Nombre y apellidos de la persona responsable
- Dirección
- Número de cuenta
- Nombre del banco

#### 3.4.5.2. CLIENTES

Se crea el fichero “clientes”, necesario e imprescindible en cualquier empresa, cuya finalidad es la gestión de la relación comercial y contractual con los clientes de la empresa, la gestión administrativa, la gestión contable, la gestión de cobros y pagos, y la gestión fiscal de los datos. Pero además, eso datos tienen la finalidad de servir para la fidelización de clientes, campañas publicitarias, promociones o descuentos especiales.

Dado que existe un acuerdo contractual entre la empresa y el cliente, los datos que podemos recoger son:

- Persona de contacto del cliente
- Dirección
- Localidad
- Provincia, país (si se localiza fuera de España)
- Código Postal
- Teléfono 1
- Teléfono 2
- Fax
- E-mail
- Tipo de cliente
- Tipo de producto / servicio adquirido
- Fecha apunte

#### 3.4.5.3. RELACIONES LABORALES DE LA EMPRESA: FICHERO DE SELECCIÓN Y FICHERO DE PERSONAL

En la parte laboral, se van a crear dos ficheros diferentes, uno relacionado con la selección de personal y otro con el personal de la empresa.

FICHERO DE SELECCIÓN

Este fichero contendrá los datos de las personas que aspiran a un puesto en la empresa o de las personas que han enviado un Curriculum Vitae a la empresa. En este fichero se deben recabar datos identificativos de cada candidato pero también otro tipo de datos, como educación, experiencia laboral u otros datos que los candidatos incluyan en su Curriculum Vitae, y que se pueden incluir datos relativos a la salud, origen racial, religioso, ideológico etc.

Los datos que se deberían almacenar en este fichero son:

- Nombre y apellidos del candidato

- Número del Documento Nacional de Identidad - DNI
- Número de afiliación a la Seguridad Social
- Dirección
- Localidad
- Provincia, país (si se localiza fuera de España)
- Código Postal
- Teléfono 1
- Teléfono 2
- Fax
- E-mail
- Tipo de perfil
- Fecha y lugar de nacimiento
- Educación
- Experiencia
- Otros datos de interés

FICHERO DE PERSONAL

Este fichero contendrá los datos detallados de los trabajadores de la empresa, con la finalidad de la elaboración y gestión de las nóminas o para cualquier participación activa por parte del personal de la empresa en la empresa.

Los datos a recoger serían:

- Nombre y apellidos del candidato
- Número del Documento Nacional de Identidad - DNI

- Número de afiliación a la Seguridad Social
- Sexo
- Fecha y lugar de nacimiento
- Estado Civil
- Dirección
- Localidad
- Provincia, país (si se localiza fuera de España)
- Código Postal
- Teléfono 1
- Teléfono 2
- Fax
- E-mail
- Puesto que ocupa en la empresa
- Rango
- Departamento
- Categoría
- Bajas por enfermedad
- Minusvalía
- Educación - Titulaciones
- Experiencia profesional
- Otros datos de interés

#### 3.4.5.4. VIDEOVIGILANCIA

Debido al auge de los sistemas de videovigilancia en la mayoría de las empresas mediante sistemas de circuitos cerrados de televisión, web cams o instalación de cámaras de seguridad en los puestos de trabajo, la Agencia Española de Protección de Datos en su Instrucción 1/2006, de 8 de noviembre, de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, que comprende tanto la grabación, captación, transmisión, conservación y almacenamiento de imágenes, su reproducción o emisión en tiempo real.

El fin por el que ADstudio utiliza cámaras de vigilancia es la seguridad de la empresa frente a eventuales ataques, atracos o algún otro tipo de acto delictivo, por lo tanto las cámaras deben de estar instaladas con tal fin y no violando espacios públicos innecesarios.

Las cámaras tampoco deben violar la intimidad de los trabajadores por lo que no se deberán instalar en los aseos o baños públicos de la empresa.

"las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras[12]"

"no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas[13]"

#### 3.4.5.5. FOTOGRÁFICO

Debido a que la empresa se dedica a la gestión y diseño de campañas publicitarias a otras empresas, en muchas ocasiones se utilizarán fotografías para las mismas, que podrán ser recogidas de diferentes fuentes. Una fotografía de una persona física es una imagen que contiene datos, ya que de esta manera puede identificarla, al igual que con las cámaras de videovigilancia, por lo que habrá que albergarlas en un archivo de datos de carácter personal.

[12] Artículo 4.1 de la Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos

[13] Artículo 4.3 de la Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos

La finalidad por la que ADstudio guarda fotografías no es más que para el desarrollo de su actividad empresarial.

## 3.4.6. NIVELES DE SEGURIDAD

### 3.4.6.1. MEDIDAS DE SEGURIDAD

Una de las mayores preocupaciones acerca de los datos de carácter personal en una empresa es la seguridad de los mismos, puesto que no tendría ningún sentido esos datos si no se aplica un procedimiento de seguridad adecuado y que se garantice que no sean modificados, borrados o cedidos.

Para evitar que personas no autorizadas al control y gestión de los datos tengan accesos a ellos es por lo que la seguridad es imprescindible, pero también sirve para que incluso la gente que pueda tener control sobre esos datos no se salga de la norma y trate los datos de acuerdo a la Ley de Protección de Datos vigente.

Tanto si son ficheros manuales como si son ficheros informatizados se deben tomar las medidas de seguridad pertinentes, y dependiendo de la naturaleza de los datos y el riesgo que estos tengan.

El artículo 9 de la LOPD dedicado a la seguridad de los datos así lo indica, en sus apartados uno, dos y tres:

"1.El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural

2.No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3.Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

Este artículo de la LOPD viene desarrollado en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, donde se determinan las medidas mínimas de seguridad para garantizar la

confidencialidad e integridad de la información frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Este apartado del Reglamento de la LOPD se caracteriza por:

- Ser un Reglamento de mínimos. El cumplimiento de este Título del Reglamento solamente hace que se cumplan con los mínimos exigibles por la Ley de Protección de Datos sobre seguridad de los datos, con el objetivo de evitar la pérdida, destrucción o manipulación de los mismos.
- Neutralidad tecnológica de la norma. El Reglamento no establece un sistema o herramienta tecnológica concreta para establecer estos principios de seguridad en los datos, sino que establece una neutralidad característica de este tipo de normativas en cuanto a la aplicación de las nuevas tecnologías.

Los responsables de los tratamiento o ficheros y sus encargados del tratamiento deben implantar todas las medidas de seguridad independientemente de su sistema de tratamiento, y deberán ser implantadas por ellos.

NIVELES DE SEGURIDAD

Según el tipo de dato de carácter personal, se engloba en un diferente nivel de seguridad:

NIVEL ALTO:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respeto de los que se prevea la posibilidad de adoptar el nivel básico
- recabados con fines policiales sin consentimiento de las personas afectadas
- derivados de actos de violencia de género

NIVEL MEDIO:

- sobre infracciones administrativas o penales
- sobre prestación de servicios de solvencia patrimonial y crédito [14]

[14] Artículo 29 de la Ley Orgánica 15/1999 sobre Protección de Datos, de 13 de diciembre.

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

NIVEL BÁSICO

- cualquier otro fichero que contenga datos de carácter personal
- también los ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, solamente 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 de o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guardan relación con la finalidad del fichero
    - 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

#### 3.4.6.2. DOCUMENTO DE SEGURIDAD

Toda empresa que posea ficheros de datos de carácter personal tendrá la obligación de tener un Documento de Seguridad para así poder asegurar la calidad e integridad de los datos que contienen esos archivos, así como los procedimientos que la empresa establezca para un correcto mantenimiento y tratamiento de los datos.

El documento de seguridad será de obligado cumplimiento por parte del personal de la empresa y se tendrán que detallar los ficheros protegidos, las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad, las funciones y obligaciones del personal en relación con el tratamiento de datos de carácter personal y descripción de los sistemas de información que los tratan, el procedimiento de notificación, gestión y respuesta ante las incidencias, los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos y las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de los mismos.

También en el Documento de Seguridad vendrá designado la persona Responsable de Seguridad de la empresa, que será el encargado de establecer un control periódico del Documento para verificar el cumplimiento de la normativa vigente sobre Protección de Datos y de las descripciones propuestas en el documento (ANEXO I - DOCUMENTO DE SEGURIDAD).

### 3.4.7. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

La Ley de Protección de Datos [15] establece una serie de principios básicos que se deben de tomar como pautas en todos los procesos que intervienen en la recogida, tratamiento y utilización de datos de carácter personal. Estos vienen recogidos

Es imprescindible que toda empresa tome como partida estos principios para adecuarse a la legislación vigente sobre Protección de Datos en España.

Los principios básicos de la Protección de Datos son:

- CALIDAD DE LOS DATOS - Art.4 LOPD

El principio de la calidad de datos exige que los datos que vayan a ser tratados sean pertinentes, adecuados y no excesivos en relación con la finalidad con la que han sido recogidos, de una manera legítima y expresa. Los datos deberán mantenerse exactos y puestos al día, y estos no podrán permanecer en un fichero más tiempo del que fuera necesario para la finalidad para la que han sido recabados.

- DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS - Art. 5 LOPD

Es el derecho que tienen los ciudadanos a ser informados sobre el tratamiento de los datos que se vayan a hacer. Se diferencian cuando los datos se recogen directamente del titular de los mismos o que sean recogidos de un tercero. Aunque venga expresadamente en la LOPD como un derecho, se puede tratar como un principio.

- CONSENTIMIENTO DEL TITULAR DE LOS DATOS - Art. 6 LOPD

Este principio dicta que el titular de los datos debe dar su consentimiento de manera expresa y por escrito para datos relativos a la ideología, afiliación sindical, religión y creencias (salvo para ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin animo de lucro - con finalidad política, filosófica, religiosa o sindical). Los datos que hagan referencia al origen racial, la salud y la vida sexual solo

[15] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

podrán ser recabado, tratados y cedidos cuando lo disponga la ley o el afectado lo consienta expresamente.

Para el resto de los casos, el consentimiento puede ser tácito, aunque es recomendable guardar ese consentimiento como prueba, ya sea por escrito o por soportes electrónicos.

- DATOS ESPECIALMENTE PROTEGIDOS - Art. 7 LOPD

Existen datos que la legislación considera que deben de estar especialmente protegidos, y estos son los que revelen:

- ideología, afiliación sindical, religión y creencias[16]: donde debe existir un consentimiento expreso y por escrito del afectado para tratarlos, con la excepción de los ficheros de los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, y asociaciones, fundaciones y otras entidades sin animo de lucro con finalidad política, filosófica, religiosa y sindical.

- origen racial, salud y vida sexual[17]: donde solamente podrán ser recabados, tratados y utilizados por interés general dispuesto por una ley o porque el afectado lo consienta expresamente.

La LOPD además, en el apartado 4 del artículo 7 dedicado a los datos especialmente protegidos prohibe la creación de ficheros que tengan como única finalidad la de almacenar datos sobre la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual.

Siempre que el tratamiento lo realice un profesional de la medicina o sanitario para la prevención o el diagnóstico médico, asistencia sanitaria, tratamiento médico o gestión de servicios sanitarios, estos datos especialmente protegidos, podrán ser tratados.

- DATOS RELATIVOS A SALUD - Art. 8 LOPD

[16] Artículo 7.2 de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos

[17] Artículo 7.3 de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos

Las instituciones y centros sanitarios (tanto públicos como privados) así como los profesionales correspondientes, podrán acceder al tratamiento de datos relativos a la salud del afectado cuando estos requieran ser tratados por los mismos.

- SEGURIDAD DE LOS DATOS - Art. 9 LOPD

Para garantizar un tratamiento de los datos cumpliendo con todos los apartados legislativos vigentes y también para impedir el acceso a loa datos de carácter personal a personas no autorizadas, evitar el desvío de información, la seguridad de estos datos debe ser extremada al máximo. Para ello se establece un reglamento de medidas de seguridad, con un niveles de seguridad particulares.

- DEBER DE SECRETO - Art. 10 LOPD

Tanto el responsable del fichero como todas las personas que intervengan en cualquier fase del tratamiento de los datos, estarán obligados a mantener el secreto profesional[18] sobre ellos y al deber de guardarlos.

Este deber permanecerá incluso cuando finalice las relaciones del titular de los datos con el titular del fichero o su responsable.

- COMUNICACION (CESIÓN) DE DATOS - Art. 11 LOPD

La LOPD define cesión de datos como "toda revelación de datos realizada a una persona distinta del interesado[19]".

Para que pueda haber una cesión de datos se tiene que cumplir:

- consentimiento previo del titular de los datos, que puede ser revocado y que será nulo cuando la información que se facilite no le permita conocer la finalidad de los datos o el tipo de actividad de aquél a quien se pretenda comunicar.
- solo se podrá llevar a cabo para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y el cesionario.

Los principales riesgos se presenta con el termino de privacidad, ya que cediendo datos a terceros:

[18] La Real Academia Española define Secreto Profesional como el "deber que tienen los miembros de ciertas profesiones, como los médicos, los abogados, los notarios etc., de no descubrir a terceros los hechos que han conocido en el ejercicio de su profesión".

[19] Artículo 3, apartado i de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

- se posibilita el cruce de los datos
- riesgo de que sean utilizado para otros fines que no sean para el que se han recabado
- el titular de los datos pierde el control sobre sus datos de carácter personal

Como excepciones generales para el consentimiento previo a la cesión o comunicación de datos de carácter personal, son:

- Que la cesión sea autorizada por ley
- Datos recogidos en fuentes accesibles al público[20]
- Por necesidad de una libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Solo será legítima la comunicación o cesión cuando se limite a la finalidad que la justifique.
- Cuando el ejercicio de las funciones del Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas lo requieran. También para las instituciones autonómicas con funciones equiparables a las del Defensor del Pueblo o al Tribunal de Cuentas.
- Cuando la cesión se produzca entre Administraciones Públicas y tengan como fin histórico, estadístico o científico el tratamiento de esos datos.
- Cuando se necesite para solucionar una urgencia media la cesión de datos relativos a salud o para realizar estudios epidemiológicos (dentro de lo establecido en la legislación sobre sanidad).

- ACCESO A LOS DATOS POR TERCEROS - Art. 12 LOPD

El acceso a los datos por terceros tiene lugar cuando se realiza un acceso a los datos de carácter personal que sea necesario para la prestación de un servicio al responsable del fichero, siempre cumpliendo con lo establecido en la LOPD.

[20] Fuentes accesibles al público (Artículo 3 “Definiciones”, apartado j Ley Orgánica 15/1999 de 13 de diciembre): “aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. 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”.

Cuando se realice un tratamiento por cuenta de terceros, la cesión deberá estar regulada en un contrato por escrito donde deberá establecerse que únicamente se tratarán los datos conforme a las instrucciones del responsable del tratamiento, que no serán usados para otro fin diferente al que figura en el contrato, ni se comunicarán a otras personas, ni siquiera para su conservación.

Las medidas de seguridad que establece la Ley de Protección de datos también serán aplicadas.

Una vez terminada la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, así como cualquier soporte o documentos que contengan algún dato de carácter personal del tratamiento.

### 3.4.8. CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS

En este apartado analizaremos las características de la empresa ADstudio para su perfecta adecuación a la normativa sobre Protección de Datos en España, aportando una visión práctica de cuanto hemos analizado sobre Protección de Datos.

Se analizaran cada una de las obligaciones de acuerdo a los tres procesos que recogen el tratamiento de datos, la recogida de datos, el tratamiento de los datos y su utilización.

#### I. RECABAR LOS DATOS

##### A. FICHERO DE DATOS DE CARÁCTER PERSONAL

El Reglamento de la LOPD desarrolla la idea inicial de fichero de datos de carácter personal que tenía la LOPD en su artículo 3.1, definiéndolo como "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización y acceso".

Al tratarse de una definición tan genérica sobre fichero es muy frecuente tener dudas acerca de que tipo de fichero se debe declarar o no ante la Agencia Española de Protección de Datos. La definición engloba a ficheros tanto de carácter informatizado como puede ser una base de datos, una tabla, un fichero o un programa, como a un fichero manual como puede ser una cajonera o un archivo. Este tipo de ficheros son los ficheros físicos, pero no son los que la Agencia Española de Protección de Datos ha establecido como necesarios de declarar. Los ficheros lógicos, que son un fichero o conjunto de ficheros físicos con el mismo tipo de datos y que son tratados con la misma finalidad, son los que hay que declarar y luego registrar en el Registro General de Protección de Datos.

Por ejemplo, si la empresa posee varios ficheros físicos acerca de datos de clientes, como puede ser uno para sus datos bancarios, otro para sus datos comerciales y otro para impagos, se tienen que agrupar en un mismo fichero que se llame "clientes" y es el único que tiene que ser declarado.

"La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos[21]"

Un fichero se crea por una necesidad de la empresa, a veces impuesta (por ejemplo para conservar documentación sobre el personal laboral para inspecciones de trabajo) o para que se permita la continuidad laboral de la empresa, como puede ser un fichero de proveedores.

Para la notificación de un fichero a la Agencia Española de Protección de Datos, hay que seguir un procedimiento formal que viene establecido en el artículo 27 de la LOPD. Es necesario cumplimentar unos formularios detallando la identificación del responsable del fichero, el nombre del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado, el colectivo de personas sobre quien se obtienen los datos, el procedimiento y la procedencia de los datos, las categorías de los datos, el servicio o unidad de acceso, la identificación del nivel de medidas de seguridad básico, medio o alto exigible y la identificación del encargado de tratamiento y los destinatarios de cesiones y transferencias internacionales de datos, además de un domicilio para notificaciones (VER ANEXO II - INSCRIPCIÓN DE FICHEROS).

Es el responsable del fichero el encargado de la inscripción del fichero en el Registro de la Protección de Datos. Su inscripción conlleva el cumplimiento de parte de la normativa sobre Protección de Datos, pero no conlleva con el total cumplimiento de las obligaciones previstas por la LOPD.

Las ventajas de la inscripción de los ficheros en el Registro, aparte de cumplir con las obligaciones que impone la Ley de Protección de Datos, son:

- Que la empresa conozca todas los ficheros sobre los que tiene obligación de cumplir con lo que dicta la LOPD
- Evitar sanciones por parte de la Agencia Española de Protección de Datos
- Mostrar el compromiso de cumplir con la ley por parte de la empresa

[21] Artículo 56 "Tratamientos de datos en distintos soportes", Real Decreto 1720/2007 de 21 de diciembre

- Facilitar a los titulares de los datos contenidos en sus ficheros el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Si se necesita o requiere un fichero de carácter temporal [22] o como intermediario para un tratamiento, no tienen porque inscribirse en el Registro de la Protección de Datos como tal, pero si que tiene que inscribirse el fichero de origen de los datos. Por ejemplo, si se crea un fichero temporal para las personas asistentes a la cena de Navidad de la empresa, no es necesario inscribirlo en el Registro, pero si que tendrá que estar inscrito el fichero de origen. En este caso el fichero de origen sería el fichero de "Personal" de la empresa, donde están los datos de cada empleado.

### B. LA CALIDAD DE LOS DATOS

El principio de calidad de los datos regirá en todos los procedimientos del tratamiento de datos de carácter personal de la empresa, desde el momento previo a recabar los datos hasta el fin del tratamiento.

Antes de la recogida de datos por parte del Responsable del Fichero, se debe tomar en consideración que únicamente podrán ser recabados datos que sean adecuados, pertinentes y no sean excesivos en relación con el ámbito y las finalidades del fichero, y que la forma en que se recaben los datos sea explícita y legítima. Se prohibe totalmente la recogida de datos por medios fraudulentos, desleales o ilícitos.

Por ejemplo, si se van a recabar datos de un cliente para la empresa ADstudio sobre algún proyecto de diseño, solamente se tomarán los datos adecuados y pertinentes para el fin que no es más que una relación contractual entre la empresa y el cliente. De este modo, recabar datos relativos con el estado civil del cliente por ejemplo sería excesivo para la finalidad del tratamiento.

### C. EL DEBER DE INFORMAR

[22] Definido en el Artículo 5.2, apartado g del Real Decreto 1720/2007 de 21 de diciembre, como "ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento"

Otros de los principios fundamentales que recoge la LOPD en su artículo 5, es el "Derecho de información en la recogida de datos".

Al ser un derecho aunque sea también considerado un principio, en este caso existe la obligación de informar al titular de los datos que se recaben para el tratamiento de datos. Con esto se pretende conseguir que el titular de los datos este lo suficientemente informado como para poder decidir y consentir el tratamiento de sus datos de forma consciente y libre. Para ello, es necesario informar sobre:

- La existencia de un fichero o tratamiento de datos de carácter personal
- La finalidad de la recogida de datos
- Los destinatarios de la información
- El carácter obligatorio de respuesta a las preguntas planteadas al afectado
- La posibilidad del afectado de ejercitar sus derechos de acceso, rectificación, cancelación y oposición
- La identidad y dirección del responsable del tratamiento o su representante

En muchas ocasiones al Responsable del Fichero le interesa recabar datos para otras finalidades diferentes a la que se plantea inicialmente. Aunque en un principio no sea un problema plantear al titular de los datos la finalidad con la que se recogen, puede encontrárselo a la hora de que el titular se disponga a firmar al ver todas las finalidades para las que se recopilan los datos. Es necesario igualmente informar de forma correcta sobre el posterior uso de los datos. La solución en este caso sería incluir cláusulas que permitan ampliar las finalidades de la recogida de datos.

En el caso de que se produzca una modificación en el cambio de Responsable de Fichero[23], se tendrá que informar al titular de los datos sobre los nuevos destinatarios de la información. También se deberá aclarar que la finalidad para la que se requieren los datos del titular sigue siendo la

[23] Artículo 19 del Real Decreto 1720/2007 de 21 de diciembre, de Protección

misma, y en el caso de que se quiera cambiar o ampliar, se tendrá que solicitar el aprobado por parte del titular del cese de sus datos para las nuevas finalidades del Responsable del Fichero.

Si no se obligara a informar al titular de los datos sobre el destino de estos, podría darse el caso de que estos fueran cedidos a multitud de empresas sin el consentimiento del mismo. Si la empresa requiere que esos datos sean cedidos a otras empresas de similar categorías y con la misma finalidad por la que la empresa los recoge, se tendría que añadir una cláusula o informar acerca de esta posible cesión a empresas de similar categoría y con misma finalidad.

La LOPD no establece una forma fija para que el Responsable del Fichero facilite una forma concreta de informar al titular de los datos la información necesaria para el tratamiento de los mismos. Lo más habitual es que se utilice el mismo medio que se utiliza para la recogida de datos para informar al afectado:

- Oralmente: puede ser una opción válida. También mediante carteles informativos colocados en lugares visibles.
- A través de formularios: cuando se utilice un impreso o formulario para la recogida de los datos, la información tiene que figurar de forma claramente legible.
- Contratos: si el titular firma un contrato con la empresa, se deben incluir en el mismo la información sobre el tratamiento de sus datos.
- Telefónicamente: se podrían proporcionar por teléfono, pero sería conveniente también entregar la información por escrito cuando se envíe la entrega o mismamente por corre postal.

Es recomendable utilizar medios en los que se pueda disponer de una prueba a posteriori sobre el perfecto cumplimiento de informar al titular de los datos.

Los datos no siempre son recabados del titular de los mismos, sino que existen varias vías por las que recabar datos:

- DEL PROPIO INTERESADO

Cuando los datos son recabados del propio interesado habrá que facilitarle la información de una forma directa y detallada al titular de los mismos.

La Protección de Dato juega un papel fundamental en el proceso de selección y contratación de personal para la empresa. A la hora de recabar datos de carácter personal hay una serie de obligaciones que la empresa tiene que cumplir. En el artículo 11 de la LOPD se detallan las condiciones por las que unos datos pueden ser cedidos y es donde entra en conflicto la denominada privacidad del individuo.

Solamente se podrán ceder datos del candidato al trabajo o del futuro trabajador "para el cumplimiento de fines relacionados con las funciones legítimas del cedente y del cesionario", que en este caso es la contratación de personal.

SELECCIÓN DE CANDIDATOS

Aún cuando solamente hay una relación entre la empresa y un simple candidato a un puesto de trabajo (que este o no ofertado/vacante) tiene que existir un protocolo para el correcto cumplimiento de la LOPD.

En el caso de la recepción de Curriculums Vitae en la empresa aunque no se haya solicitado la entrega de esa información, ya sea por medio de correo electrónico o convencional, debe remitirse una respuesta al afectado con la confirmación de recepción del Curriculum Vitae y el condicionando del tratamiento de los datos al acuse de recibo.

CARTA INFORMATIVA EN RESPUESTA A LOS CANDIDATOS

Sr. D. / Sra. Dña. _____

(Cuerpo de la carta notificando la recepción del CV en la empresa)

De acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, Real Decreto 1720/2007 de 21 de diciembre, los datos recabados en su "Curriculum Vitae" serán incluidos en un fichero de datos de carácter personal, cuyo responsable de tratamiento es ADstudio, con domicilio en Plaza del Rey nº2 en Burgos, cuya finalidad es la gestión de los aspectos relacionados con la selección de personal en la empresa, que se dedica exclusivamente al diseño gráfico profesional y la publicidad, respetando la confidencialidad en todo momento de la información contenida en dicho documento.

Adicionalmente, mediante la presente notificación le informamos que sus datos de carácter personal no serán cedidos a ninguna otra empresa.

Asimismo, le informamos que en todo momento se garantizará el ejercicio por su parte, mediante carta dirigida a la dirección de la empresa o por correo electrónico a la dirección arco@adstudio.com, de sus derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la citada Ley Orgánica y su normativa de desarrollo.

Los datos que usted nos ha facilitado permanecerán en el fichero por un plazo máximo de 1 año, tras el cual se procederá a su destrucción.

Aprovechamos la ocasión para mandarle un cordial salud,

ADstudio

CARTA DE SOLICITUD DE ACTUALIZACIÓN DE DATOS EN LOS C.V.

(Cuando se va a cumplir el plazo determinado por la ley para la conservación de Curriculums, se puede enviar un mensaje para que se actualice. En caso de no recibir respuesta alguna, el Currículum se elimina de la base de datos)

Sr. D. / Sra. Dña. _____

(Cuerpo de la carta)

De acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, Real Decreto 1720/2007 de 21 de diciembre, nos dirigimos a usted para solicitar la actualización de sus datos de carácter personal recabados en su "Curriculum Vitae" y que se encuentran incluidos en un fichero de datos de carácter personal, cuyo responsable es ADstudio, con domicilio en Plaza del Rey nº2, en Burgos, cuya finalidad es la gestión de los aspectos relacionados con la selección de personal de la empresa, respetando la confidencialidad en todo momento de la información contenida en dicho documento.

Adicionalmente, mediante la presente notificación le informamos que sus datos de carácter personal no serán cedidos a ninguna otra empresa.

Asimismo, le informamos que en todo momento se garantizará el ejercicio por su parte, mediante carta dirigida a la dirección de la empresa o por correo electrónico a la dirección arco@adstudio.com, de sus derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la citada Ley Orgánica y su normativa de desarrollo.

Los datos que usted nos ha facilitado permanecerán en el fichero por un plazo máximo de 1 año, tras el cual se procederá a su destrucción.

Aprovechamos la ocasión para mandarle un cordial salud,

ADstudio

## CONTRATO DE TRABAJO DE LA EMPRESA

En cada contrato laboral que efectúe la empresa, debe acompañar una cláusula obligatoria de acuerdo a la Ley 15/1999 de Protección de Datos de Carácter Personal. De esta manera, el acuerdo contractual es más transparente y el trabajador se siente seguro al aportar datos a la empresa, ya que el empresario tiene que cumplir una serie de obligaciones.

La Agencia Española de Protección de Datos ya ha sancionado a varias empresas que no han incluido una cláusula de Protección de Datos en este tipo de actividades contractuales.

También es necesario realizar este procedimiento con el personal que se incorpore en prácticas en la empresa o con una beca procedente de alguna institución educativa.

CLÁUSULA INFORMATIVA A NUEVOS EMPLEADOS

De acuerdo a lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, el Real Decreto 1720/2007 de 21 de diciembre, el trabajador manifiesta que se le ha informado que sus datos personales, incluso los relativos a su salud e imagen, así como el resto de la información facilitada por el mismo y que se recoge en este contrato u otros cuestionarios, podrá ser incorporada y tratada en un fichero de datos de carácter personal, cuyo responsable es ADstudio, con domicilio en Plaza del Rey nº 2, en Burgos, y cuyas finalidades son el desarrollo, cumplimiento y control de la relación jurídico-laboral de conformidad con la legislación vigente, así como el cumplimiento de la normativa vigente en materia laboral, tributaria, seguridad social y prevención de riesgos laborales.

Asimismo se le informa, que de acuerdo a lo previsto en el artículo 11 de la LOPD, que el responsable del fichero, podrá ceder sus datos personales a las Autoridades Tributarias, Laborales y de Seguridad Social, así como a proveedores de servicios externos vinculados al desarrollo de las funciones propias del puesto de trabajo, como aseguradoras y financieras, alquiler de vehículos, formación profesional etc., respetando en todo momento la finalidad para la que fueron recogidos sus datos de carácter personal.

Asimismo, le informamos que en todo momento se garantizará el ejercicio por su parte, mediante carta dirigida a la dirección de la empresa o por correo electrónico a la dirección arco@adstudio.com, de sus derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la citada Ley Orgánica y su normativa de desarrollo.

CLÁUSULA INFORMATIVA A PERSONAL YA CONTRATADO

De acuerdo a lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, el Real Decreto 1720/2007 de 21 de diciembre, el trabajador manifiesta que se le ha informado que sus datos personales, incluso los relativos a su salud e imagen, así como el resto de la información facilitada por el mismo y que se recoge en este contrato u otros cuestionarios, podrá ser incorporada y tratada en un fichero de datos de carácter personal, cuyo responsable es ADstudio, con domicilio en Plaza del Rey nº2, en Burgos, y cuyas finalidades son el desarrollo, cumplimiento y control de la relación jurídico-laboral de conformidad con la legislación vigente, así como el cumplimiento de la normativa vigente en materia laboral, tributaria, seguridad social y prevención de riesgos laborales.

Asimismo se le informa, que de acuerdo a lo previsto en el artículo 11 de la LOPD, que el responsable del fichero, podrá ceder sus datos personales a las Autoridades Tributarias, Laborales y de Seguridad Social, así como a proveedores de servicios externos vinculados al desarrollo de las funciones propias del puesto de trabajo, como aseguradoras y financieras, alquiler de vehículos, formación profesional etc, respetando en todo momento la finalidad para la que fueron recogidos sus datos de carácter personal.

Asimismo, le informamos que en todo momento se garantizará el ejercicio por su parte, mediante carta dirigida a la dirección de la empresa o por correo electrónico a la dirección arco@adstudio.com, de sus derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la citada Ley Orgánica y su normativa de desarrollo.

ANEXO INFORMATIVO PARA PERSONAL EN PRÁCTICAS

De acuerdo a lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, el Real Decreto 1720/2007 de 21 de diciembre, D./ Dña_____ manifiesta que se le ha informado de que los datos personales, incluso los relativos a su salud, recogida en este contrato u otros cuestionarios, podrá ser incorporada y tratada en un fichero, cuyo responsable es ADstudio, con domicilio en Plaza del Rey nº2, en Burgos, y cuyas finalidades es el desarrollo, cumplimiento y control de la relación jurídico-laboral de conformidad con la legislación vigente, así como el cumplimiento de la normativa vigente en materia laboral, tributaria, de seguridad social y de prevención de riesgos laborales.

Según lo previsto en el artículo 11 de la LOPD, la empresa informa en el presente documento que se podrá realizar una cesión de sus datos personales con la finalidad de gestionar adecuadamente su relación a favor de entidades aseguradoras y financieras.

Asimismo, le informamos que en todo momento se garantizará el ejercicio por su parte, mediante carta dirigida a la dirección de la empresa o por correo electrónico a la dirección arco@adstudio.com, de sus derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la citada Ley Orgánica y su normativa de desarrollo.

- DE TERCEROS

Cuando los datos sean facilitados por una persona diferente al titular de los datos, el responsable del fichero tendrá un plazo de 3 meses desde que se registran los datos para facilitarle la información que le permita consentir el tratamiento de los datos del afectado de una forma libre y consciente.

Se deberá informar de la procedencia de los datos, la existencia de un fichero o tratamiento, la finalidad para la que se ha recabado los datos, los destinatarios de la información, la posibilidad de ejercer los derechos de acceso, rectificación y oposición, y la identidad del responsable del tratamiento o su presentante.

La LOPD establece excepciones:

- Cuando el interesado ya ha sido informado anteriormente
- Cuando la Ley lo exprese directamente
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos
- La información del interesado resulte imposible o exija esfuerzos desproporcionados.

- DE FUENTES DE ACCESO PÚBLICO

El artículo 3 de la LOPD, en su apartado j, define las fuentes de acceso público como aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en casos determinados, el abano de una contraprestación. Son exclusivamente:

- El censo promocional
- Las guías de teléfonos
- Las listas de colegios profesionales (únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional - domicilio postal, número telefónico y de fax, dirección electrónica - e indicación de pertenencia al grupo - número de colegiado, fecha incorporación y situación de ejercicio profesional)

- Los diarios y boletines oficiales
- Los medios de comunicación

Una de las dudas más frecuentes puede ser si incluir a Internet como un medio de comunicación más y por tanto, una fuente de acceso público. La Agencia Española de Protección de Datos ha establecido que "Internet no es, a los efectos de protección de datos, un medio de comunicación social, sino un canal de comunicación, por lo que no es fuente accesible al público[24]". Los únicos medios de comunicación recogidos como tal son la televisión, la radio y la prensa.

Cuando se recaben datos en un fichero procedente de fuentes accesibles al público, también se tiene que informar al titular de los mismos de la procedencia de sus datos, la identidad y dirección del responsable de fichero o tratamiento y de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

## D. EL CONSENTIMIENTO

"Toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen" es como define la LOPD el principio del consentimiento, un principio imprescindible en la Protección de Datos.

Este principio se encuentra ligado al principio de información en la recogida de datos, ya que para que se cumpla el principio del consentimiento, se tiene que haber informado previamente sobre la existencia de un fichero de datos de carácter personal y la finalidad por la que se recaban los datos. Por ello, la solicitud de consentimiento tiene que ser requerida para cada tratamiento específico.

Solamente para algunos tratamientos de datos específicos donde puede existir un consentimiento tácito, el consentimiento tiene que manifestarse de forma expresa y por escrito:

- Tácito: suficiente para el tratamiento de todos los datos salvo los especialmente protegidos (ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual).

[24] "El nuevo reglamento de desarrollo de la ley orgánica de protección de datos: problemática, interpretación y aplicación", Madrid, 22 de abril de 2008

- Expreso y por escrito: para los datos especialmente protegidos

DERECHO DE REVOCACIÓN DEL CONSENTIMIENTO

El titular de los datos tiene el derecho a revocar[25] el consentimiento que ha prestado anteriormente al Responsable de un Fichero para el tratamiento de sus datos de carácter personal y el Responsable del Fichero, tiene la obligación de hacer efectivo ese derecho[26] cancelando los datos del titular de los mismos y parar el tratamiento de sus datos que se estuviera realizando en ese momento.

También podrá ser revocado el consentimiento que se haya autorizado para la cesión de los datos del titular [27].

El artículo 17 del Real Decreto 1720/2007 propone que no es necesario ningún tipo de forma especial para llevar a cabo la revocación del consentimiento al Responsable del Fichero, por lo que se puede realizar a través de algún medio gratuito, sencillo y que no implique desembolso alguno por parte del afectado, no teniendo porque enviar cartas certificadas, utilizar teléfonos con tarificación especial o cualquier otro medio que implique un coste.

TRATAMIENTO DE DATOS DE MENORES DE EDAD

Para recabar datos de carácter personal se necesita que el titular de los mismos tenga al menos 14 años de edad. Si se necesitasen datos de personas menores de esa edad, se requerirá el consentimiento de los padres o tutores a cargo del menor.

En ningún caso cuando se obtengan datos del menor, se podrá utilizar la ocasión para recabar datos de familiares como la actividad profesional de sus progenitores, información económica u otros datos sin el consentimiento de cada titular de ellos.

[25] Artículo 6.3 de la Ley Orgánica 15/1999 de Protección de Datos - "El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos"

[26] Artículo 16.1 de la Ley Orgánica 15/1999 de Protección de Datos

[27] Artículo 11.4 de la Ley Orgánica 15/1999 de Protección de Datos - "El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter revocable"

## II. TRATAMIENTO DE LOS DATOS

### A. LA CALIDAD DE LOS DATOS

El principio de Calidad de los datos sigue presente en este procedimiento, para los datos de carácter personal que han sido cedidos a la empresa para su tratamiento y utilización.

De acuerdo a este principio, los datos no pueden ser usado para otro fin que no sea para el que se han recabado, además de tener que ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual de su titular y que tienen que ser almacenados de forma que se permita el acceso a los mismos si el titular ejerciese su derecho de acceso.

En el caso de que se descubra durante el tratamiento que los datos resulten inexactos o incompletos, el Responsable del Fichero se verá obligado a cancelarlos y sustituirlos por los correspondientes datos actualizados y puestos al día.

### B. EL DEBER DE SECRETO

Viene establecido en el Artículo 10 de la LOPD y afecta no solamente al Responsable del Fichero, sino a todas las personas que intervienen en el proceso del tratamiento de datos de carácter personal. Se establece por tanto el secreto profesional respecto a los datos de carácter personal y al deber de guardar esos datos.

Es importante señalar que en caso de vulneración de este principio, aparte de la correspondiente sanción por parte de la Agencia Española de Protección de Datos, la revelación de secretos esta tipificada como delito por el Código Penal [28] . Se castiga el apoderamiento, utilización o modificación de datos de carácter personal o familiar de un tercero que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, sin autorización y en perjuicio de tercero. También se castiga a quien acceda a los mimos por cualquier otro medio, los altere o los utilice en perjuicio del titular sin autorización.

[28] Artículos 197 a 201 del Código Penal, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”.

## C. LA SEGURIDAD DE LOS DATOS

Este principio impone al Responsable del Fichero y a todas las personas que intervienen en el tratamiento una serie de medidas de seguridad de índole técnica y organizativa para garantizar la seguridad de los datos en la empresa.

Para ello, la empresa establece tres niveles de seguridad (básico, medio y alto) donde distribuye los datos de acuerdo a la seguridad requerida.

El Responsable del Fichero deberá designar a un Responsable de Seguridad, que será el encargado de coordinar y controlar todas las medidas del documento.

La empresa tendrá que realizar obligatoriamente un documento de seguridad donde se detallarán todos los aspectos relativos a la seguridad en el tratamiento de datos de carácter personal recogidos por la empresa (ANEXO I - DOCUMENTO DE SEGURIDAD).

## D. LA CESIÓN DE LOS DATOS

El artículo 3 de la LOPD, en su apartado i, define la cesión de datos como "toda revelación de datos realizada a una persona distinta del interesado". Solamente se podrán ceder los datos de carácter personal de un fichero si:

- la finalidad de la cesión para la que se realice esta directamente relacionada con las funciones legítimas del cedente y el cesionario
- y también que exista consentimiento previo del titular de los datos.

También se podrán ceder los datos si lo autoriza una Ley.

## E. EL ACCESO A DATOS POR TERCEROS

El encargado de tratamiento es "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento[29].

Se entiende que una empresa se encarga del tratamiento cuando no puede decidir sobre el contenido, finalidad y uso del tratamiento y siempre que su actividad no reporte otro beneficio que la prestación de servicios, sin utilizar ficheros generados en su provecho, puesto que en ese caso pasaría a ser responsable del fichero.

En caso de que el encargado del tratamiento utilice los datos con otra finalidad, los comunique o ceda, incumpliendo lo que establezca en el contrato, deberá responder a todas las infracciones como si se considerase el responsable del tratamiento.

[29] Artículo 3.g de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos

## III. FINALIZACIÓN DEL TRATAMIENTO

### A. CANCELACIÓN Y BLOQUEO DE DATOS

Según lo establecido en el artículo 4.5 de la LOPD, el Responsable de Ficheros tendrá la obligación de cancelar los datos de carácter personal cuando hayan dejado de ser necesarios para la finalidad para la que fueron recabados en su momento. La norma impide que la empresa pueda conservarlos durante un periodo mayor al que se necesita para la finalidad buscada en el momento del registro de los datos.

Solamente podrán ser conservados durante un tiempo mayor cuando puedan estos ser exigidos por algún tipo de responsabilidad derivada de una obligación jurídica o contractual.

### B. SUPRESIÓN DE FICHEROS

Cuando un fichero de datos de carácter personal ya no sea necesario para la empresa y se decida su supresión, se deberá notificar a la Agencia Española de Protección de Datos la supresión del mismo.

### C. EL DEBER DE SECRETO

La obligación del deber del secreto permanecerá en todos los que han intervenido en el tratamiento de datos incluso después de finalizar sus relaciones con el responsable del fichero.

### 3.4.9. DERECHOS DE LA PROTECCIÓN DE DATOS

La normativa española de Protección de Datos ofrece al titular de los datos unos derechos en materia de Protección de Datos que pueden ejercer en cualquier momento durante el tratamiento de los datos de carácter personal. Estos derechos están recogidos en los artículos que van desde el 13 al 19 de la LOPD.

Los derechos que se recogen son:

- Derecho de impugnación de valores - Art. 13 LOPD
- Derecho de consulta al Registro General de la Protección de Datos - Art. 14 LOPD
- Derecho de acceso - Art. 15 LOPD
- Derecho de rectificación y cancelación - Art. 16 LOPD
- Derecho de oposición - Art. 6.4 LOPD
- Derecho de indemnización - Art. 19 LOPD

El ejercicio de estos derechos los podrán ejercer:

- el afectado acreditando su identidad
- su representante legal que tendrá que acreditar su identidad igualmente, cuando el titular de los datos se encuentre en situación de incapacidad o minoría de edad.
- El representante voluntario designado para el ejercicio del derecho, junto con una copia del Documento Nacional de Identidad o equivalente, y una representación realizada por el titular. No es necesario poder notarial en este caso.

Las solicitudes de acceso, rectificación, cancelación y oposición deberán atenderse siempre que la solicitud contenga lo siguiente:

- Nombre y apellidos del interesado, fotocopia de su Documento Nacional de Identidad u otro documento identificativo (pasaporte, documento electrónico etc.), o una persona que lo represente.
- Petición en que se concreta la solicitud
- Dirección del titular o representante para notificaciones
- Fecha y firma del solicitante
- Documentos acreditativos

(ANEXO III - EJERCICIO DE DERECHOS)

Si la solicitud no reúne todo los requisitos, el responsable del fichero pedirá que se envíe toda la documentación correctamente en un plazo de 10 días. Cuando todo este en orden, comenzará el plazo para contestar por parte del Responsable de Fichero, que es quien tiene la obligación de contestar la petición.

Todas las personas en la empresa que manipulen datos de carácter personal tendrán que recibir formación acerca del procedimiento a realizar en caso de que el titular de los datos quiera ejercer alguno de sus derechos.

DERECHO DE IMPUGNACIÓN DE VALORES

Con el derecho de impugnación, el titular de los datos puede limitar el uso de técnicas que faciliten una información o perfil a través de la recogida de sus datos de carácter personal y que vaya más allá de los datos facilitados por el afectado. El texto de la LOPD lo define en su artículo 13 como el derecho a "impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad".

DERECHO DE CONSULTA AL REGISTRO GENERAL DE LA PROTECCIÓN DE DATOS

El afectado podrá ejercer su derecho de consulta de forma gratuita al Registro General de la Protección de Datos de la Agencia Española de Protección de Datos para conocer los tratamientos que se están realizando con sus datos de carácter personal la empresa, la finalidad de los mismos y la identidad del responsable del fichero. Se trata de una consulta pública y no existe limitación alguna por el número de consultas que se realicen.

DERECHO DE ACCESO

El titular de los datos podrá en todo momento dirigirse al Responsable del Fichero con la intención de conocer que datos de carácter personal figuran en el fichero, cual es el origen de los datos y las comunicaciones que se hubieran realizado o que se prevean realizar.

Este derecho también se tendrá que realizar de forma gratuita a intervalos no superiores a doce meses, salvo que el interesado acredite interés legítimo.

La empresa no puede negarse a dar a conocer los datos que figuran en el fichero, su origen y las comunicaciones que se hayan realizado a alguien que ejercite este derecho, además de no poder poner ningún impedimento, tiene que ser de forma gratuita.

El Responsable del Fichero deberá responder la solicitud de acceso en un plazo máximo de un mes desde la recepción de la solicitud. Si pasado el plazo, no ha habido respuesta, el interesado podrá interponer una reclamación ante la Agencia Española de Protección de Datos. Si los datos de la

persona que solicita su derecho de acceso no se encuentran en el fichero de la empresa, existe la obligación de comunicárselo al titular en el mismo plazo.

La información que se debe proporcionar al titular de los datos son todos los datos de base del afectado, los resultantes de cualquier tratamiento informático, la información sobre el origen de los datos, los cesionarios y la finalidad para la que fueron recogidos.

### DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

Son dos derechos independientes y que se ejercitan de manera independientes también.

El derecho de rectificación se utiliza para instar al Responsable del Fichero la modificación de datos cuyo tratamiento no se ajuste a lo que dicta la Ley o porque los datos son inexactos o incompletos.

La solicitud debe indicar a qué datos se refiere el titular y la corrección o cambios en los datos que quiere que se efectúen. El Responsable de Fichero resolverá la solicitud en un plazo máximo de 10 días desde la recepción de la solicitud, se disponga de los datos del titular que lo solicita o no.

Si los datos hubieran sido cedidos, el Responsable del Fichero deberá comunicar las modificaciones al cesionario para que pueda realizar también los cambios en el plazo de días contados desde la recepción de la solicitud.

El derecho de cancelación confiere al titular de los datos el poder cancelar sus datos del fichero de una empresa cuando el tratamiento no se ajusta a las precisiones de la Ley o cuando hayan dejado de ser necesarios para la finalidad para la que fueron recogidos.

El Responsable del Fichero dispondrá de un plazo máximo de 10 días tras la recepción de la solicitud para resolverla, se dispongan o no datos sobre el titular de los datos.

Si los datos hubieran sido cedidos, se notificará la cancelación al cesionario para que en un plazo igualmente de 10 días tras la recepción pueda cancelar los datos.

DERECHO DE OPOSICIÓN

Si para la recogida de los datos no fue necesario el consentimiento del interesado, y siempre que una Ley no disponga lo contrario, el titular podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

Cuando el fichero tenga por finalidad actividades de publicidad y prospección comercial, o por otro lado, tenga como finalidad evaluar al afectado en diferentes aspectos de su personalidad, el titular podrá ejercer su derecho de oposición igualmente.

El Responsable del Fichero tendrá que resolver la solicitud de oposición en el plazo máximo de 10 días tras recibir la solicitud, disponga o no de datos el afectado.

Se podrán conservar los mínimos datos imprescindibles para identificar a las personas que han solicitado el derecho de oposición cuando la finalidad es el envío de publicidad.

DERECHO A INDEMNIZACIÓN

Para aquellos afectados que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de las obligaciones que tienen el responsable o encargado del tratamiento, puede ser indemnizado, debiendo acudir ante los órganos de la jurisdicción ordinario, ya que la Agencia Española de Protección de Datos no tiene competencia para fijar indemnización sobre posibles daños y perjuicios.

### 3.4.10. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Quién recoge los principios y derechos de la normativa sobre Protección de Datos y el lugar donde el afectado debe recurrir en caso de vulneración de algunos de sus derechos es la Agencia Española de Protección de Datos. Se trata del órgano de vigilancia y control de la norma, independiente e interpoderes, y que esta contemplado en la ley[30].

Actúa con plena independencia de la Administración Pública para ejercer sus funciones, es un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada.

Las funciones más importantes de la Agencia son:

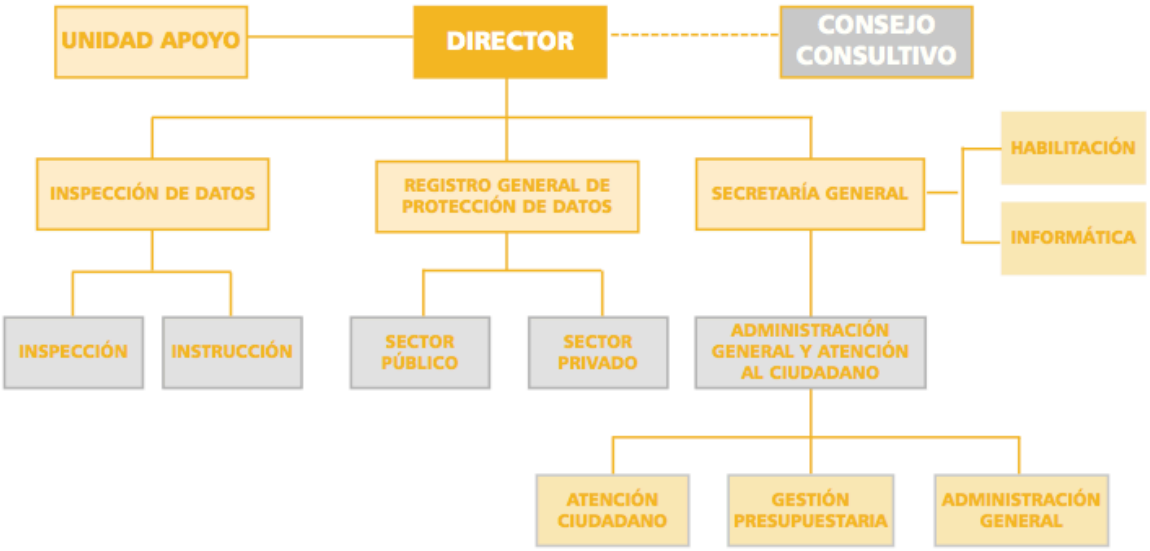
- atender las peticiones y reclamaciones realizadas por las personas correspondientes
- proporcionar información sobre los derechos en Protección de Datos
- ejercer la potestad inspectora y sancionadora
- velar por el cumplimiento de la normativa sobre Protección de Datos
- controlar la aplicación de la normativa

La Agencia Española de Protección de Datos es quien controla el Registro de Protección de Datos, donde deben ser inscritos todos los ficheros que contengan datos de carácter personal de la empresa.

Además, a la Agencia es donde debe acudir cualquier ciudadano para poder consultar sobre la existencia de cualquier fichero o tratamiento sobre sus datos, su estructura y finalidad, nombre del titular del fichero y la dirección para que el ciudadano pueda ejercer sus derechos.

[30] Viene contemplado en el Título VI de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos

El esquema organizativo de la Agencia Española de Protección de Datos.




3.4.10.1. SANCIONES

En caso de que se incumpla la normativa sobre Protección de Datos española, podrían recaer sobre la empresa una serie de sanciones económicas . En el siguiente cuadro se muestran las posibles sanciones aplicables por la Agencia Española de Protección de Datos.

| TIPO DE SANCIÓN | MULTA | PRESCRIPCIÓN |
|---|---|---|
| LEVE | 601,01 € a 60.101,21 € | 1 año |
| GRAVE | 60.101,21 € a 300.506,05 € | 2 años |
| MUY GRAVE | 300.506,05 € a 601.012,10 € | 3 años |

Dependiendo del tipo de principio o derecho que se infrinja, se requiere un tipo interpone un diferente tipo de sanción u otro:

| PRINCIPIO | DESCRIPCIÓN | SANCIÓN |
|---|---|---|
| CALIDAD DE LOS DATOS | QUE LOS DATOS SEAN PERTINENTES, ADECUADOS Y NO EXCESIVOS, ADEMÁS DE NO PODER PERMANECER EN EL FICHERO MÁS TIEMPO DEL NECESARIO | GRAVE |
| PRINCIPIO DE INFORMACIÓN | INFORMAR CON CARÁCTER PREVIO Y DE MODO EXPRESO, PRECISO E INEQUÍVOCO | MUY GRAVE |
| PRINCIPIO DEL CONSENTIMIENTO | NECESIDAD DE CONSENTIMIENTO EN LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL | GRAVE |
| DATOS ESPECIALMENTE PROTEGIDOS | RECABAR Y TRATAR DATOS ESPECIALMENTE PROTEGIDOS | MUY GRAVE |
| SEGURIDAD DE LOS DATOS | MANTENER LOS FICHEROS DE DATOS DE CARÁCTER PERSONAL CON LOS NIVELES DE SEGURIDAD APROPIADOS | GRAVE |
| DEBER DE SECRETO | SECRETO PROFESIONAL RESPECTO A LOS DATOS TRATADOS | LEVE / GRAVE |
| CESIÓN O COMUNICACIÓN DE DATOS | CESIÓN DE DATOS DE CARÁCTER PERSONAL | MUY GRAVE |

Dependiendo del tipo de derecho que se infrinja, también se pondrá la correspondiente sanción según la gravedad:

| DERECHO | DESCRIPCIÓN | SANCIÓN |
|---|---|---|
| DERECHO DE IMPUGNACIÓN DE VALORES | EVITAR QUE CON LOS DATOS DE CARÁCTER PERSONAL SE CREEN PERFILES O PERSONALIDADES PARA EVALUAR A LAS PERSONAS | GRAVE |
| | ATENDER EL DERECHO DE ACCESO DE LAS PERSONAS PARA CONOCER LOS CRITERIOS QUE SE UTILIZAN PARA LAS VALORACIONES Y EL PROGRAMA UTILIZADO | MUY GRAVE |
| DERECHO DE CONSULTA AL REGISTRO GENERAL DE LA PROTECCIÓN DE DATOS | REGISTRAR TODOS LOS ARCHIVOS EN EL REGISTRO PARA QUE PUEDAN SER REGISTRADOS | LEVE |
| DERECHO DE ACCESO | PERMITIR AL TITULAR DE LOS DATOS ACCEDER A LOS MISMOS | MUY GRAVE |
| DERECHO DE RECTIFICACIÓN Y CANCELACIÓN | ATENDER TODAS LAS SOLICITUDES DE MODIFICACIÓN EN LOS DATOS DE CARÁCTER PERSONAL | LEVE |
| | MANTENER LOS DATOS EXACTOS Y PUESTOS AL DÍA / NO REALIZAR LAS RECTIFICACIONES O CANCELACIONES SOLICITADAS | GRAVE |
| | NO ATENDER EL EJERCICIO DE RECTIFICACIÓN | MUY GRAVE |
| DERECHO DE OPOSICIÓN | IMPEDIMENTO O OBSTACULIZACIÓN DEL DERECHO DE OPOSICIÓN | GRAVE |
| | NO ATENDER EL EJERCICIO DEL DERECHO DE OPOSICIÓN | MUY GRAVE |

### 3.4.11. PUBLICIDAD: FICHEROS CON FINES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL

Uno de los temas más importantes acerca de la Protección de Datos es el principio de consentimiento, que deriva del artículo 6 de la LOPD.

Será necesario el consentimiento del titular de los datos de carácter personal siempre, salvo que la Ley dicte lo contrario. Todo ciudadano es el único con la capacidad para poder decidir cuándo, dónde y cómo son presentados y tratados sus datos. El titular tiene el control absoluto sobre sus datos y su utilización, por lo que tiene que otorgar su consentimiento para que se pueda realizar un tratamiento sobre ellos.

Este principio, el principio de consentimiento, tiene varias excepciones que vienen planteadas en el apartado 2 del artículo 6 y en el artículo 30 de la LOPD (que hace referencia a los ficheros con fines de publicidad y prospección comercial).

El artículo 30 de la LOPD dice así:

"1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud."

De este artículo se entiende que los ficheros con fines de publicidad y prospección comercial pueden albergar datos recogidos de fuentes accesibles al público o del titular de los datos directamente o con su consentimiento.

En el supuesto que los datos sean recogidos de fuentes accesibles al público, se tendrá que informar al titular de los datos en cada comunicación que se le dirija del origen de los datos, de la entidad del responsable del tratamiento y sus derechos.

El titular de los datos que figuren en un fichero con fines de publicidad y prospección comercial que ejercite su derecho de acceso tiene derecho a conocer el origen de sus datos, además que este podrá oponerse a su tratamiento sin tener una causa justificada.

El apartado primero del artículo dicta que estos ficheros se refieren a aquellas empresas que tengan como su actividad:

- recopilación de direcciones
- reparto de documentos
- publicidad
- venta a distancia
- prospección comercial
- otras actividades semejantes

Como en nuestro caso se trata de una empresa que también realiza trabajos publicitarios es muy importante tener este punto en cuenta, para la elaboración de campañas publicitarias a clientes, aunque cualquier empresa que necesite de publicidad para el tratamiento sea cual sea la actividad que desarrolle.

#### 3.4.11.1. CAMPAÑAS PUBLICITARIAS

ADstudio entre sus actividades esta la creación de campañas de publicidad que sus clientes encargan. Es muy importante cuidar este apartado para no infringir con la normativa sobre Protección de Datos.

Cuando se quiere realizar una campaña publicitaria entre los clientes, en un principio será necesario el consentimiento de los mismos para recibir este tipo de comunicaciones. Las campañas publicitarias pueden ser realizadas por la propia empresa pero si estas son encargadas a ADstudio, esta será considerada como un tercero a quien se le encomienda el proyecto, por la tanto, el tratamiento de determinados datos.

En este caso se pueden dar varias situaciones:

- cuando los datos sobre los destinatarios de la campaña publicitaria sean obtenidos y fijados por la empresa que requiere los servicios de ADstudio, esta será la Responsable del tratamiento de los datos de carácter personal de sus clientes.
- cuando los datos sobre los destinatarios de la campaña publicitaria sean obtenidos por la empresa encargada de elaborar la campaña publicitaria, esta será únicamente la Responsable del tratamiento de los datos.
- cuando intervengan ambas entidades en determinar los datos de los clientes, ambas entidades figurarán como Responsable del tratamiento de datos.

Para quienes hayan manifestado su negativa a recibir publicidad y se lo hayan comunicado a la empresa, se debería conservar los mínimos datos imprescindibles para poder identificarlos y así no volver a enviarles ningún tipo de publicidad.

También se permite la creación de las listas Robinson o ficheros comunes, que pueden ser de carácter general o sectorial, en los que figurarán los datos de las personas que quieren evitar el envío de comunicaciones comerciales que hayan manifestado su oposición anteriormente.

#### 3.4.11.2. EJERCICIO DE DERECHOS

El Reglamento de la LOPD ha establecido algunas particularidades en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

De forma inmediata, si el titular de los datos lo solicitase, se tendría dar de baja del tratamiento sus datos y se cancelarían todas las informaciones que figuren sobre ellos. La empresa deberá establecer un medio sencillo y gratuito para poder oponerse al tratamiento de sus datos con fines comerciales, como habilitar un número de teléfono gratuito, una dirección email o mismamente un servicio de atención al cliente.

En el caso que la campaña de publicidad sea realizada por ADstudio para otra empresa como parte de su ejercicio profesional, la empresa que encargo la campaña deberá de forma obligada en un plazo de diez desde la recepción de la comunicación de la solicitud de ejercicio de derechos (acceso, rectificación, cancelación y oposición) del titular de los datos, a comunicar la solicitud al responsable del fichero para que así se pueda otorgar al afectado su derecho en el plazo de diez días desde la recepción de la solicitud, notificando al afectado.

# Comercio Electrónico

## 4.1. INTRODUCCIÓN

Desde su orígenes, el comercio es la actividad que se basa en el intercambio de bienes y servicios por un valor aproximadamente equivalente. Actualmente, esta actividad sigue siendo la base de la economía y se desarrolla a través de nuevas y mejores formas para convertirla en una herramienta más eficaz. Este avance se produce gracias al desarrollo y uso de las nuevas tecnologías de la comunicación y la información, en todos los procesos comerciales y empresariales - marketing, ventas, logística, pagos, administración, fiscalidad.

Por lo tanto, el comercio a través de estas tecnologías, y principalmente a través de Internet, se ha convertido en un importante elemento para la creación de valor en las empresas, fundamental en una sociedad y un mercado cada vez más competitivos. Internet a pasado de ser una oportunidad a convertirse en una necesidad para las empresas.

Cualquier empresa que no quiera quedarse fuera de esta carrera por optimizar todos sus procesos empresariales, debe tener su presencia en este mundo electrónico para tener una mayor ventaja competitiva, ya que llegar tarde, equivale a no llegar, ya que otro ocupará tu lugar. El comercio electrónico ha eliminado todas las barreras que impedían un mercado global en el pasado, los impedimentos geográficos y logísticos, lo que ha supuesto la creación de un entorno mundial basado en la competencia, los precios y la reducción de los márgenes.

## 4.2. COMERCIO ELECTRÓNICO

Podríamos definir comercio electrónico como

"un modelo que permite a las empresas intercambiar, de forma electrónica, información y servicios esenciales para sus negocios y que involucra, necesariamente, transacciones económicas. Incluye la creación de un mercado abierto, por lo que puede considerarse como una extensión del mercado actual[31]"

El comercio electrónico supone la oportunidad de acercarse a millones de potenciales clientes en la red, ofreciendo un servicio permanente y de forma global, accesible e informativo. Supone una oportunidad para cualquier empresa que quiera ampliar sus barreras de una forma fácil y barata.

El comercio electrónico ha destruido barreras que no existían en el comercio tradicional:

- Barreras geográficas
- Barreras de información: el cliente puede informarse acerca del producto, leer opiniones y comparar en tiempo real
- Barreras de tiempo: servicio permanente, las 24 horas, 365 días al año
- Barreras de cambio: los compradores pueden cambiar de empresa continuamente

Los cuatro pilares en los que el comercio electrónico se basa son una buena estrategia de marketing y comercial, los contenidos del sitio, administración del mismo y la tecnología empleada.

[31] Definición de la "Asociación Española de Comercio Electrónico"

Los nueve elementos para la implantación de un sistema de comercio electrónico[32] son:

- Análisis de productos
- Determinar el cliente objetivo
- Plan de marketing y publicidad
- Gestión técnica del comercio electrónico
- Definición de las formas de pago
- Definición de los aspectos logísticos
- Definición y establecimiento de un servicio de atención al cliente
- Gestión del cambio: adaptación de los Recursos Humanos
- Adaptación de los procesos de la empresa, reingeniería de procesos

También es importante conocer el termino contratación electrónica, que podríamos definirla como "aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación fuera del acuerdo[33]".

[32] *The Big E-commerce Bang*. Jesse Berst, Director Editorial. 2 de Septiembre de 1999

[33] Definición de la Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Correo Electrónico

## 4.3. NORMATIVA

Es importante conocer la normativa aplicable que regula el Comercio Electrónico en España:

- Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
- Ley Orgánica 32/2003, de 3 de noviembre, General de Telecomunicaciones
- Ley Orgánica 59/2003, de 19 de diciembre, de Firma Electrónica
- Ley Orgánica 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
- Ley Orgánica 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información

En lo relativo al Comercio Electrónico, debemos basarnos principalmente en la Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

## 4.4. SERVICIO DE LA SOCIEDAD DE LA INFORMACIÓN

La Ley de Servicio de la Sociedad de la Información y de Comercio Electrónico (LSSI) entró en vigor el 12 de octubre de 2002, cuyo objetivo es impulsar la utilización de Internet como medio para realizar negocios y garantizar un marco de seguridad jurídica para las transacciones comerciales que se realicen a través de este medio.

Esta Ley también detalla las obligaciones y responsabilidades de los prestadores de servicios, comunicaciones comerciales por vía electrónica, validez y eficacia de los contratos en Internet y sanciones, entre otros temas.

La Ley debe ser de aplicación para todos los responsables de los sitios web en los que se efectúen de algún modo, actividades comerciales o de promoción de productos o servicios, regulando sus servicios. Los requisitos que una empresa ha de cumplir para considerar un servicio de la sociedad de la información, se deben cumplir una serie de características:

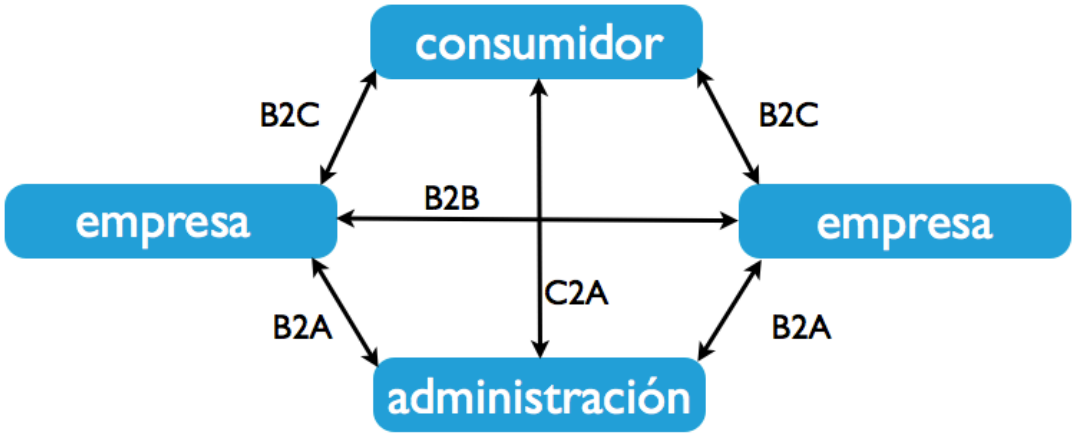
- Oneroso
- A distancia
- A petición individual del destinatario

Dependiendo de las relaciones que se establezcan entre los agentes que intervienen en el comercio electrónico (administración, empresa y consumidor), pueden existir diferentes tipos:

- Business to Consumer - B2C: en esta modalidad de negocio electrónico se determinan las transacciones entre una empresa y el consumidor final. Se trata de vender a un particular a través de internet, ocupándose de todo lo que ello requiere, forma de envío, plazos de entrega, devoluciones, medios de pago, impuestos, garantía, servicio postventa, atención al cliente, protección de datos etc.
- Business to Business - B2B: en esta modalidad de negocio electrónico se determinan las transacciones comerciales entre compañías. Normalmente en este tipo de transacciones, tanto el

comprador como vendedor se conocen. Se utiliza principalmente para mandar ordenes de compra a los proveedores, recibir facturas y realizar pagos.

- Consumer to Consumer - C2C: en esta modalidad de negocio electrónico se determinan las transacciones comerciales entre consumidores. Se utiliza para el intercambio de productos o servicios entre usuarios consumidores de Internet. El ejemplo típico es la subasta online.
- Consumer to Business - C2B: esta modalidad implica solicitudes de los compradores a las compañías para negociar un precio mejor del producto o servicio. Los consumidores llevan la iniciativa.
- Business to Administration - (B2A): abarca las transacciones entre las empresas y las administraciones públicas.
- Consumer to Administration - (C2A): son las transacciones electrónicas entre los ciudadanos y las administraciones públicas a través de Internet, como el pago de pensiones, devolución de impuestos, pago de multas etc.



También, debemos tener en cuenta el tipo de presencia que una empresa tiene en Internet. Se distinguen dos tipos:

- Estática: no existe interrelación entre el prestador del servicio y los destinatarios del servicio, que en caso, son los clientes. Suelen ser portales de información relacionados con la tarea o actividad de la empresa. El cliente no interactúa directamente con el destinatario.
- Dinámica: por otro lado, cuando existe un cierto dinamismo en la página o sitio, se produce una comunicación o relación bidireccional entre las dos partes, pudiendo llegar a la contratación electrónica. Existen dos subtipos dentro de este tipo de presencia en Internet.

    a) Conversacional: presta un servicio mayor que una página estática (que se limita a ofrecer información) pero sin llegar a la contratación electrónica, solamente un diálogo con el usuario de servicio.

    b) Contractual: se realizan contratos por vía electrónica, cuando la oferta y aceptación se transmiten por la web.

Por lo tanto, son servicios de la Sociedad de la Información:

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión por medios electrónicos o de mercados y centros comerciales virtuales
- La gestión de compras en la red por grupos de personas
- El envío de comunicaciones comerciales
- El suministro de información por vía telemática
- El video bajo demanda. Se trata de un servicio por el cual el usuario puede seleccionar a través de la red tanto el programa deseado como el momento para su suministro y recepción, así como la distribución de contenidos previa petición individual.

Todos los que no cumplan con las características anteriores no serán considerados servicios de la Sociedad de la Información, así como tampoco los que cumplan lo siguiente:

- Los servicios prestados por medio de telefonía vocal, fax o télex.
- El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
- Los servicios de radiodifusión televisiva.
- Los servicios de radiodifusión sonora
- El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

ADstudio

ADstudio dispone de un portal en Internet donde los consumidores o potenciales clientes pueden acceder para la compra de varios productos que ofrece, que son templates o plantillas de modelo sobre varios tipos de diseños gráficos que pueden ser personalizables por los consumidores. También, desde la página web se podrán realizar encargos a través de un menú donde se deberá ir eligiendo las características de un producto gráfico que luego se personalizará a gusto del cliente, así como otros servicios publicitarios y marketing.

De esta manera, analizaremos si ADstudio se trata de un prestador de servicio de la sociedad de la información y de que tipo es.

Requisitos para ser un prestador de servicio de la sociedad de la información:

- Oneroso:
- A distancia: a prestarse el servicio a través de la red, no existe un lugar geográfico específico donde poder realizar actividades comerciales electrónicas.
- Por vía electrónica: a través de redes de telecomunicaciones ofrecidas por prestadores de servicio de acceso a Internet (ISP).

- A petición individual del destinatario: el destinatario es el que decide participar o no en las transacciones comerciales.

Los agentes que intervienen en el servicio son por un lado la empresa ADstudio y por otro, los clientes, que serán los consumidores. Se tratará entonces de un modelo de relación de B2C (Business to Consumer), es decir, transacciones entre la empresa y los consumidores).

El tipo de presencia que ADstudio tendrá en internet es contractual, que se engloba dentro del modelo de negocio dinámico en comercio electrónico, ya que se podrán celebrar contratos de manera electrónica. En este caso se celebrarán contratos de compraventa entre la empresa y el consumidor.

Una vez que una empresa cumple con los requisitos mínimos para ser considerada un prestador de servicios de la Sociedad de la Información, será necesario aplicar la LSSI.

Para ello también se deberá considerar el ámbito de aplicación de la Ley, dependiendo del lugar donde este establecida la empresa. En el artículo 2 de la LSSI, en sus tres apartados, viene reflejado así:

"1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica"

Como ADstudio se encuentra establecido en España, con domicilio social en territorio español así como su gestión administrativa y dirección, se considera un prestador de servicio establecido en España.

Además, ADstudio tiene personalidad jurídica, ya que se encuentra inscrita en el Registro Mercantil.

La prestación del servicio de la sociedad de la información esta regido por el principio de libre prestación de servicios[34], por lo que no se pueden establecer ningún tipo de restricciones al comercio electrónico.

Tampoco la prestación de servicios estará sujeta a ningún tipo de autorización previa[35].

[34] Artículo 7 de la Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

[35] Artículo 6 de la Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

## 4.5. PRESTADOR DE SERVICIO DE INTERMEDIACIÓN

La Ley de Comercio Electrónico no solamente afecta a los prestador de servicios, sino también a los prestadores de servicios de intermediación. En el anexo de definiciones que trae consigo la LSSI, se define Servicio de Intermediación como:

"servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet"

ADstudio

ADstudio no realiza ningún servicio de intermediación en la Sociedad de la Información, por lo que no se podrá considerar como prestador de servicio de intermediación.

Por lo tanto, ADstudio queda libre de cumplir todos los artículos relacionados con los Prestadores de Intermediación que hagan referencia a los mismos en la normativa española sobre Comercio Electrónico.

ADstudio no realiza entre sus actividades comerciales en Internet:

- facilitar el servicio de acceso a Internet
- trasmitir datos por redes de telecomunicaciones
- copiar temporalmente paginas de Internet solicitadas por los usuarios, servicios también conocidos como Proxy-Caché
- alojar en sus propios servidores de datos, aplicaciones o servicios suministrados por otros
- instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet

## 4.5. OBLIGACIONES Y RESPONSABILIDADES

### 4.5.1. OBLIGACIONES

Los artículos que van del 9 al 12 de la Ley sobre Comercio Electrónico (LSSI) tratan de las obligaciones que impone la normativa:

CONSTANCIA REGISTRAL DEL NOMBRE DE DOMINIO - ART. 9

Este artículo queda sin contenido por la Ley 56/2007 de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, en su Artículo 4, sobre modificaciones de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

INFORMACIÓN GENERAL - ART. 10

Un prestador de servicios de la Sociedad de la Información deberá tener tanto para destinatarios como para los órganos competentes y de una forma permanente, visible, fácil, directa y gratuita, la siguiente información[36]:

a. Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b. Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c. En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

[36] Extraído del Artículo 10 de la Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico

d. Si ejerce una profesión regulada deberá indicar:

    1. Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

    2. El título académico oficial o profesional con el que cuente.

    3. El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

    4. Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e. El número de identificación fiscal que le corresponda.

f. Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.

g. Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

ADstudio en su sitio web deberá informar acerca de todos los apartados que exige la Ley de Comercio Electrónico. Al final de la página se colocará de forma visible y fácil de localizar la siguiente información:

En virtud de lo establecido en la Ley Orgánica 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico, se ofrece la siguiente información:

Responsable de la web: ADstudio
Domicilio de contacto: Plaza del Rey nº 2, 09005 Burgos
E-mail de contacto: info@adstudio.com
Teléfono: + 34 651 68 59 59
Fax: 952 68 59 59
Datos Fiscales: A92509748
Datos de Inscripción Registral: inscrito en el Registro Mercantil de Burgos, Tomo 374, Libro 2351, Folio 54, Hoja BU-68721

ADstudio va a ser la encargada de alojar su página web en un servidor privado. En caso de que un órgano competente, dentro de sus funciones, ordene que se interrumpa su presencia total en Internet o solamente de algunos contenidos, la empresa será la encargada de hacerlo según haya sido ordenado. En caso de no cumplir con la orden de cese o retirada de los contenidos, se podrían adoptar medidas pertinentes.

En caso de que la empresa decidiese usar en un futuro servicios de tarificación adicional que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario. Se informará de forma clara, visible e identificable de:

a. Las características del servicio que se va a proporcionar

b. El número que se marcará

c. El procedimiento para dar fin a la conexión de tarificación y restablecer la conexión.

DEBER DE COLABORACIÓN DE LOS PRESTADORES DE SERVICIOS DE INTERMEDIACIÓN - ART. 11

No afecta a ADstudio ya que no se trata de un prestador de servicios de intermediación.

DEBER DE RETENCIÓN DE DATOS DE TRÁFICO RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS - ART. 12

Este Artículo ha quedado derogado por la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

OBLIGACIONES DE INFORMACIÓN SOBRE SEGURIDAD - ART. 12 BIS

Este Artículo lo incluye la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, para prestador de servicio de acceso a Internet y prestador de servicio de correo electrónico o servicios similares. No afecta a ADstudio, ya que entre sus actividades no se encuentran estos servicios.

### 4.5.2. RESPONSABILIDADES

Entre las responsabilidades que los prestadores de servicios en la Sociedad de la Información debe tener en cuenta son[37]:

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN - ART. 13

Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa que se establece en el ordenamiento jurídico español, sin perjuicio de lo dispuesto en la Ley 32/2002.

RESPONSABILIDAD DE LOS OPERADORES DE REDES Y PROVEEDORES DE ACCESO - ART. 14

No afecta a ADstudio ya que no se trata de un prestador de servicios de intermediación.

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS QUE REALIZAN COPIA TEMPORAL DE LOS DATOS SOLICITADOS POR LOS USUARIOS - ART. 15

No afecta a ADstudio ya que no se trata de un prestador de servicios de intermediación.

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE ALOJAMIENTO O ALMACENAMIENTO DE DATOS - ART. 16

No afecta a ADstudio ya que no se trata de un prestador de servicios de intermediación.

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS QUE FACILITEN ENLACES A CONTENIDOS O INSTRUMENTOS DE BÚSQUEDA - ART. 17

No afecta a ADstudio ya que no se trata de un prestador de servicios de intermediación.

[37] Comprenden los Artículos 13 a 17 de la Ley Orgánica 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico

### 4.5.3. COMUNICACIONES COMERCIALES POR VIA ELECTRÓNICA

La Ley de Comercio Electrónico define como comunicación comercial:

"toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional".

Partiendo de este concepto, está prohibido el envío de comunicaciones publicitarias por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido expresamente autorizadas[38]. Esto se refiere principalmente al envío de SPAM [39].

La forma en la que ADstudio envía publicidad a sus clientes es a través de correos electrónicos - envió de catálogos sobre productos y servicios de la empresa o promociones específicas para campañas específicas como pueden ser Navidad o verano, pero siempre relacionado con la actividad que desarrolla la empresa.

El Título III[40] de la Ley sobre Comercio Electrónico se centra en lo dispuesto en cuanto a comunicaciones comerciales de las empresas a través de medios electrónicos.

RÉGIMEN JURÍDICO - ART. 19

Este Artículo establece que las comunicaciones comerciales y ofertas promocionales estarán regidas no solamente por la Ley de Comercio Electrónico, sino por su normativa propia y la que se encuentre vigente sobre los aspectos comerciales y de publicidad de las empresas.

Hace referencia también a que se debe aplicar en todo momento la Ley Orgánica 15/!999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como la normativa que la

[38] De acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos.

[39] La Ley esta intentando regular el Spam Mail, pero aún no se regulan otros tipos de Spam, como puede ser el Spam mediante pop-ups.

[40] Comprende los Artículos del 19 al 22

desarrolla[41] para la obtención de datos personales, información al titular de los mismos y todo lo relacionado sobre los ficheros de datos de carácter personal. Se debe tener en consideración de acuerdo a esta Ley:

- se debe pedir siempre el consentimiento del titular de los datos para poder obtener sus datos personales
- se debe informar al titular el envío de publicidad relacionada con la actividad de la empresa
- se debe crear un fichero de datos de carácter personal, con los datos estrictamente necesarios para la finalidad para la que se recaban, que es la de comunicaciones comerciales y promociones.
- se debe inscribir el fichero de datos en el Registro General de Protección de Datos.
- se deben tomar las medidas de seguridad oportunas que garanticen la integridad de los dtaos
- se debe mantener el deber de secreto profesional

INFORMACIÓN EXIGIDA SOBRE LAS COMUNICACIONES COMERCIALES, OFERTAS PROMOCIONALES Y CONCURSOS - ART.20

Toda información comercial que la empresa realice vía email, es decir, comunicaciones comerciales electrónicas, deberán ser identificables como tal, indicando la persona física o jurídica en nombre de quien se realiza.

Para un fácil identificación de que es una comunicación comercial, la Ley obliga a que se incluya al comienzo del mensaje la palabra "*publicidad*" o la abreviatura "*publi*".

En todas las comunicaciones comerciales que realiza ADstudio entonces se deberá notificar claramente que se trata de una comunicación comercial como parte de su estrategia publicitaria y que debe indicarse claramente el nombre de la persona jurídica en este caso (ADstudio).

PROHIBICIÓN DE COMUNICACIONES COMERCIALES NO SOLICITADAS REALIZADAS A TRAVÉS DE CORREO ELECTRÓNICO O MEDIOS DE COMUNICACIÓN ELECTRÓNICA EQUIVALENTES - ART. 21

[41] Real Decreto 1720/2007, de 21 de diciembre, de Protección de Datos

No se deberán enviar comunicaciones comerciales o publicidad por correo electrónico u otro medio de comunicación electrónica que no hayan sido previamente y de forma expresa, autorizadas por los destinatarios.

En caso de que existe una relación contractual entre la ADstudio y el destinatario donde este ubicada una cláusula aceptando el envío de comunicaciones comerciales relacionadas exclusivamente con las actividades de la empresa, no será necesario el consentimiento específico sobre el envío de comunicaciones comerciales.

ADstudio debe ofrecer al destinatario de la comunicación la opción de oponerse al tratamiento de sus datos con fines comerciales, tanto cuando se recaban los datos como en cada comunicación comercial que se realice. Esto tiene que realizarse mediante un procedimiento sencillo y gratuito.

### DERECHOS DE LOS DESTINATARIOS DE COMUNICACIONES COMERCIALES - ART. 22

El destinatario de las comunicaciones comerciales de una empresa podrá revocar en cualquier momento el consentimiento prestado en la recepción de comunicaciones comerciales con una simple notificación de la voluntad de hacerlo.

Se deberá facilitar información accesible por medios electrónicos sobre dichos procedimientos.

Una opción sencilla para ADstudio sería colocar toda la información relativa al ejercicio de los derechos por parte de los titulares de los datos/destinatarios de las comunicaciones comerciales en un enlace en la página web que se llame "*Aviso Legal*".

### 4.5.4. CONTRATACIÓN VIA ELECTRÓNICA

La Ley de Comercio Electrónico asegura la validez y eficacia de los contratos que tengan lugar por vía electrónica, aunque no consten en soporte papel, como prueba de validez ante los Tribunales, con igual valor que los contratos de formato papel.

Como la mayoría de las empresas hoy en día, ADstudio ha sufrido una gran serie de transformaciones, principalmente debido al desarrollo e implantación de las tecnologías de la información y las comunicaciones. Ha pasado de ser una empresa pequeña y localizada en la ciudad de Burgos a poder permitirse tener presencia global gracias a red.

ADstudio quiere ir más allá y lo que pretende es dar una nueva facilidad a sus clientes, poder contratar los servicios y productos de la empresa de forma telemática, lo que supondrá la presencia global de la empresa, un abaratamiento de los costes y facilidad para el cliente.

El único problema que la contratación electrónica plantea a priori es el no poder ver el producto de una manera física, de no haber un contacto físico entre empresa y cliente. Aunque aparezcan catálogos y fotos de pedidos acabados en la página web, siempre se realizará la compra sin apreciar con todo detalle el producto/servicio final.

El Título IV[42] de la Ley de Comercio Electrónico plantea todo lo relacionado con la contratación vía electrónica.

VALIDEZ Y EFICACIA DE LOS CONTRATOS CELEBRADOS POR VÍA ELECTRÓNICA - ART. 23

Los contratos electrónicos tendrán todos los efectos y validez de los contratos previstos por el ordenamiento jurídico, siempre que exista un consentimiento y demás requisitos de un contrato para su validez. También, estos serán regidos por los Códigos Civil y de Comercio y por las demás normas civiles o mercantiles sobre contratos, poniendo especial atención a las normativa en protección de los consumidores y usuarios.

No será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

[42] Comprende los artículos del 23 al 29

Si la Ley exige que el contrato o cualquier información relacionada con el mismo conste por escrito y la información queda en un soporte electrónico, se cumple con el requisito.

Pueden celebrarse por vía electrónica todo tipo de contratos, salvo los que son relativos al Derecho de Familia y sucesiones (como puede ser matrimonio, adopciones o testamento). Como ADstudio no realiza ningún actividad relacionada con el Derecho de Familia, no influye este apartado.

### PRUEBA DE LOS CONTRATOS CELEBRADOS POR VÍA ELECTRÓNICA - ART. 24

En caso de que se decida firmar el contrato electrónicamente, se tendrá que considerar la Ley Orgánica 59/2003 sobre Firma Electrónica, como medio de identificación de ADstudio para ratificar el contrato.

El soporte electrónico en que conste un contrato celebrado por vía electrónica podrá ser adjuntado como prueba documental en caso de juicio.

### INTERVENCIÓN DE TERCEROS DE CONFIANZA - ART. 25

En caso de que ambas partes que firman un contrato deseen pactar que un tercero archive las declaraciones de voluntad que los integran, así como la fecha y hora en que han tenido lugar, podrán hacerlo a través de un tercero de confianza.

El tercero de confianza deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía electrónica entre ambas partes integrantes del contrato, por un periodo de tiempo nunca menor a cinco años.

Los terceros de confianza vienen representados por los Prestadores de Servicios de Certificación, que también son los encargados de expedir los certificados electrónicos.

### LEY APLICABLE - ART. 26

Este Artículo indica que en la Ley aplicable a los contratos electrónicos se tendrá en cuenta las normas de Derecho Internacional Privado del ordenamiento jurídico español, tomando en consideración los artículos 2 y 3 de la Ley de Comercio Electrónico.

ADstudio deberá tener presente que la idea del contrato electrónico tendrá la misma validez que cualquier contrato que se encuentre en formato papel, por lo que podrá servir como prueba judicial y deberá mantenerlo almacenado mientras no prescriba. Es recomendable que se genere un PDF con el contenido del contrato. Las ventajas de que se realice en formato PDF es que es fiable, estándar y seguro, además de que puede ser protegido por una contraseña para poder abrirse, imprimirse o modificarse.

También, se deberá tener en cuenta el uso de firma electrónica para poder firmar dichos contratos y así reconocer de manera oficial la adhesión al contrato. Los archivos en formato PDF además, podrán firmarse digitalmente.

En caso de que así lo decidan, ADstudio tendrá la opción de contratar a un tercero de confianza que almacenará el contrato por un mínimo de cinco años, así como fecha y hora de celebración. Los Prestadores de Servicios de Certificación puede ejercer esta función. La función de un tercero de confianza es equiparable (pero no igual) a la de un notario.

### OBLIGACIONES PREVIAS AL INICIO DEL PROCEDIMIENTO DE CONTRATACIÓN - ART. 27

De manera previa al procedimiento de contratación, el prestador de servicios de la sociedad de la información no solamente tendrá que cumplir con los requisitos de información que establece la normativa sobre Comercio Electrónico, sino que también tendrá la obligación de informar al destinatario de manera clara, comprensible e inequívoca antes de iniciar el procedimiento de los siguientes apartados:

- Los distintos trámites que deben seguirse para celebrar el contrato. Todos estos trámites podrán ser detallados en un apartado que ADstudio dispondrá en su página web llamado "*Términos y condiciones generales*". Es recomendable además, que se incluya algún tipo de guía o video explicativo acerca del proceso de compra o contratación de productos y servicios a través de la página web de la empresa.

- el prestador de servicios archivará el documento electrónico del contrato en formato PDF y además, ADstudio enviará una copia al cliente por correo electrónico.
- Los medios técnicos que el prestador pone a disposición para identificar y corregir errores en la introducción de los datos. En este sentido, ADstudio deberá por ejemplo notificar que campos son obligatorios, que campos solo admiten un determinado número de caracteres o solamente números. Además, sería recomendable que los clientes puedan modificar sus datos una vez introducidos por cambio de domicilio por ejemplo.
- La lengua o lenguas en que podrá formalizarse el contrato. Sería recomendable que la página no solamente estuviera en idioma castellano, sino que pinchando en un enlace (normalmente una bandera que identifica la nación con el idioma) cambie a otro idioma. El idioma inglés es el recomendable para Internet, teniendo al idioma chino ganando posiciones como principal mercado emergente mundial.

Si el contrato se realizase por vía email directamente entre la empresa y el interesado, no sería necesario cumplir con todas las características anteriores que exige la Ley.

Las contrataciones por vía electrónica serán validas por el periodo que la empresa oferente así lo decida, o en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.

### INFORMACIÓN POSTERIOR A LA CELEBRACIÓN DEL CONTRATO - ART. 28

Cuando se produzca un contrato electrónico, la empresa oferente, en este caso ADstudio, estará obligado a confirmar la recepción de la aceptación del contrato por alguno de los siguientes medios:

- Envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en un plazo de 24 horas desde la recepción de la aceptación
- Por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la aceptación pueda ser almacenada por el destinatario.

Cuando ambas partes tengan constancia de confirmación del contrato, se entenderá que se ha recibido la aceptación por ambas partes.

### LUGAR DE CELEBRACIÓN DEL CONTRATO - ART. 29

Los contratos que se celebren vía electrónica podrán ser considerados que han sido celebrados en lugares diferentes dependiendo de:

- si el contrato electrónico tiene lugar entre la empresa y un consumidor, el contrato se considerará celebrado en el lugar que el consumidor tenga residencia habitual.
- si el contrato electrónico es entre empresarios o profesionales, se presumirá celebrado en el lugar en el que este establecido el prestador de servicios.

### 4.5.5. SOLUCIÓN JUDICIAL Y EXTRAJUDICIAL DE CONFLICTOS

La empresa prestadora de servicios tiene dos posibilidades diferentes para poder resolver cualquier conflicto que surja de sus relaciones comerciales, la solución judicial y la solución extrajudicial.

SOLUCIÓN JUDICIAL

Los usuarios tienen a su disposición una serie de acciones civiles y penales para reclamar las obligaciones del acuerdo contractual entre la empresa y el consumidor, igualando los contratos electrónicos con los demás. También existen medidas para la reparación de daños y perjuicios.

La Ley de Comercio Electrónico añade a estas otra acción, la acción de cesación [43], que se dirige a obtener el cese inmediato de toda conducta que sea contraria a la Ley y que lesione intereses colectivos de los consumidores y usuarios y a prohibir su reiteración en el futuro.

La acción de cesación podrá ser ejercida por personas, asociaciones o grupos de consumidores que hayan sido perjudicados, así como por el Ministerio Fiscal, el Instituto Nacional del Consumo y los órganos correspondientes de las Comunidades Autónomas y Entidades Locales.

La tramitación de esta acción viene regulada por la Ley de Enjuiciamiento Civil.

SOLUCIÓN EXTRAJUDICIAL

Existen multitud de procedimientos de resolución extrajudicial de conflictos,, como puede ser un defensor de cliente o un servicio de reclamaciones de una empresa, así como los órganos creados en la propia industria para ello, como los Códigos de Conducta (normas deontológicas).

Cualquier conflicto entre ADstudio y un cliente podrá someterse a los arbitrajes previstos en la legislación de arbitraje[44] y de defensa de los consumidores y usuarios.

[43] Artículo 30 de la Ley Orgánica 34/2002 de Servicios de la Sociedad de la Información

[44] Regulado por la Ley Orgánica 36/1988, de 5 de diciembre, de Arbitraje. El arbitraje de consumo esta regulado a su vez por el Real Decreto 636/1993, de 3 de mayo y desarrollado por la Ley Orgánica 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios

El sistema arbitral de consumo tiene la ventaja de que los conflictos se resuelven con rapidez (en menos de cuatro meses desde que se designan los árbitros) y de forma gratuita por ambas partes (salvo si se solicitan la práctica de determinadas pruebas). Además se evitan cargas y trámites burocráticos, se puede llevar a cabo un seguimiento de la resolución y son llevadas a cabo por especialistas en el tema.

Por lo tanto, es aconsejable la vía extrajudicial para la resolución de los conflictos ocasionados por la contratación electrónica.

En caso de que ADstudio decidiese unirse al sistema arbitral de consumo, debería alojar en su página web el siguiente distintivo:


Además se deberá incluir en el contrato una cláusula acerca del arbitraje, para informar al usuario acerca de la existencia de un sistema arbitral para poder resolver todas las controversias que se puedan originar.

### 4.5.6. DEBER DE COLABORACIÓN

El Artículo 36, titulado como Deber de Colaboración, hace referencia a que todos los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Industria, Turismo y Comercio y a los órganos que correspondan en las Comunidades Autónomas, toda información y colaboración precisa para el ejercicio de sus funciones como órganos competentes.

Si en una inspección, se dieran a conocer hechos que pudiera ser considerado como una infracción tipificada en otras leyes, ya sean estatales como autonómicas, se dará cuenta de ello a los organismos u órganos competentes para su supervisión y sanción.

### 4.5.7. SANCIONES

Los prestadores de servicios de la Sociedad de la Información están sujetos al régimen sancionador que se establece en el Título VII de la Ley de Comercio Electrónico, siempre que esta Ley sea de aplicación. La Ley tipifica las sanciones como muy graves, graves y leves:

| SANCIÓN | INFRACCIÓN |
|---|---|
| MUY GRAVE | Incumplir con la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene. |
| GRAVE | Cuando los datos del prestador de servicios no estén claramente visibles en la página web. |
| | El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica a destinatarios que no hayan autorizado o solicitado su remisión. |
| | No poner a disposición del destinatarios las condiciones generales del contrato |
| | Incumplimiento de la obligación de confirmar la recepción de una aceptación |
| | La resistencia, excusa o negativa a la actuación inspectora de los órganos competentes para llevarlas a cabo. |
| LEVES | No incluir en cada comunicación comercial con el cliente la denominación social de la empresa, así como la palabra “publicidad” o “publi” |
| | El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica a los destinatarios que no hayan solicitado su remisión, cuando no constituya infracción grave. |
| | El incumplimiento de la obligación de confirmar la recepción de la petición en los términos del artículo 28 |

| SANCIÓN | INFRACCIÓN |
|---|---|
| | No incluir un procedimiento para revocar el consentimiento para recibir comunicaciones comerciales que no constituya una infracción grave. |
| | En el caso de utilizar un servicio de tarificación o descarga de programas, no pedir el consentimiento inequívoco del afectado cuando no constituya infracción grave. |
| | No facilitar información a la que se refiere el artículo 27.1, de trámites que deben seguirse para tramitarse un contrato, formar de archivar y accesibilidad al contrato electrónico, medios técnicos que deben ponerse a disposición para identificar y corregir errores en la introducción de datos y lenguas en las que se podrá formalizar el contrato. |

En el siguiente cuadro se muestran las diferentes multas aplicables para los diferentes tipos de sanción, así como su prescripción:

| SANCIÓN | MULTA | PRESCRIPCIÓN |
|---|---|---|
| LEVE | HASTA 30.000 EUROS | 1 AÑO |
| GRAVE | 30.001 A 150.000 EUROS | 2 AÑOS |
| MUY GRAVE | 150.001 A 600.000 EUROS | 3 AÑOS |

# Firma Electrónica

## 5.1. INTRODUCCIÓN

Para que un documento firmado sea único se utiliza la rúbrica, que es algo que solamente el que ratifica el documento sabe hacer y solo un experto en grafología puede identificar. En las comunicaciones electrónicas, en muchas ocasiones, se necesita de una firma para que el documento goce de cierta oficialidad y las comunicaciones se realicen en un entorno seguro. Las comunicaciones electrónicas también permiten un sistema de firma, que además, es mucho más seguro que nuestra propia firma manuscrita.

El sistema de firma electrónica no solamente garantiza nuestra identidad, sino que ejerce una función de protección y seguridad en el documento, garantizando que el texto no ha sido modificado en ninguna de sus formas.

Las características más importantes que debe cumplir un sistema de firma digital son:

- No puede ser generada más que por el emisor del documento, debe ser infalsificable e inimitable.
- Debe permitir la identificación del firmante (autoría electrónica), para asegurar que la persona es quien dice ser
- La firma va unida indisociablemente al documento al que se refiere.
- Las informaciones que se generen a partir de la firma electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.

## 5.2. NORMATIVA

Es importante primero conocer y tener presente para cualquier consulta la normativa que regula la Firma Digital en España, y que se basa en la siguiente Ley:

- Ley Orgánica 59/2003, de 19 de diciembre, de Firma Electrónica

que define en su artículo 2 la Firma Electrónica como:

"el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".

También cabe destacar otra normativa como:

- Real Decreto 1533/2005, de 23 de diciembre, por el que se regula la Expedición del Documento Nacional de Identidad y sus Certificados de Firma Electrónica
- Ley Orgánica 44/2002, de 22 de noviembre, de Reforma del Sistema Financiero

## 5.3. CRIPTOGRAFÍA

La Firma Electrónica se basa en un método técnico ya empleado en la Antigüedad para ocultar mensajes clave en situaciones importantes, la criptografía.

Se trata de una ciencia usada desde hace miles y que hoy en día guarda su carácter original, simplemente se han cambiado la utilización de novedosos medios tecnológicos. Los métodos criptográficos que se utilizan para la creación de Firmas Electrónicas se basan en algoritmos matemáticos de cierta complejidad.

El sistema utilizado es convertir una serie de datos legibles en ilegibles, de tal manera que estos no puedan ser descifrados por un tercero que desconoce la clave necesaria para descifrarlo y tener acceso a la información.

Existen dos tipos de cifrado posibles, la criptografía de clave única o simétrica y la criptografía de clave asimétrica o pública.


Fuente: www.cert.fnmt.es

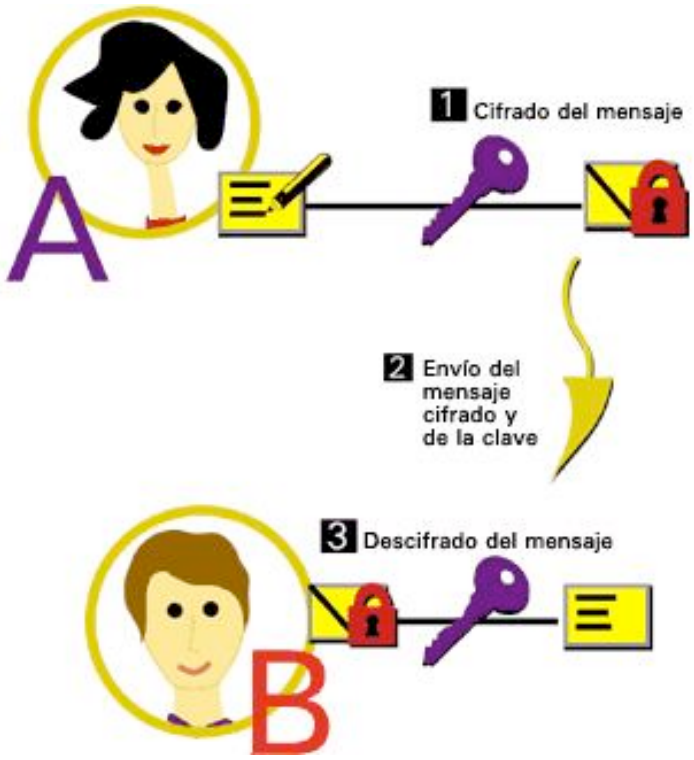
### 5.3.1. CRIPTOGRAFÍA DE CLAVE ÚNICA O SIMÉTRICA O PRIVADA O SECRETA

Es el método que ha sido utilizado a lo largo de la historia para cifrar los mensajes secretos. En este sistema, se utiliza la misma clave para cifrar y descifrar los datos, por lo que la clave deberá ser conocida por el emisor y el receptor del mensaje cifrado.

Este método requiere la confianza por ambas partes para poner en conocimiento la clave utilizada al otro, además de disponer de un canal seguro para poder transmitir la clave. Por lo tanto, el principal inconveniente es la falta de seguridad a la hora de transmitir el mensaje, aunque este vaya cifrado.

El algoritmo cifrado simétrico más conocido es el DES (Data Encryption Standard).

Si la clave secreta es interceptada por un tercero, peligrarían la seguridad de los mensajes que se envían encriptados con esa clave. Otro problema puede ser que el destinatario ceda la clave a un tercero, peligrando así también la confidencialidad de los mensajes.




Fuente: www.cert.fnmt.es

### 5.3.2. CRIPTOGRAFÍA DE CLAVE PÚBLICA O ASIMÉTRICA

Se trata de un método de cifrado de mensajes para su intercambio más seguro y fiable, que se basa en la asignación de dos claves complementarias, que son, una pública y otro privada. Este método se basa en la ciencia de la encriptación y en algoritmos matemáticos de cifrado y descifrado de mensajes.

Se basa en el sistema de dos claves:

- Clave privada: utilizada para cifrar los datos
- Clave pública: utilizada para descifrar los datos

De esta manera, el receptor de una determinada información conocerá la clave pública del emisor con la que descifraría unos datos que solo podrán haber sido cifrados con la clave privada del emisor. La información que es cifrada con la clave privada es descifrada con la clave pública.

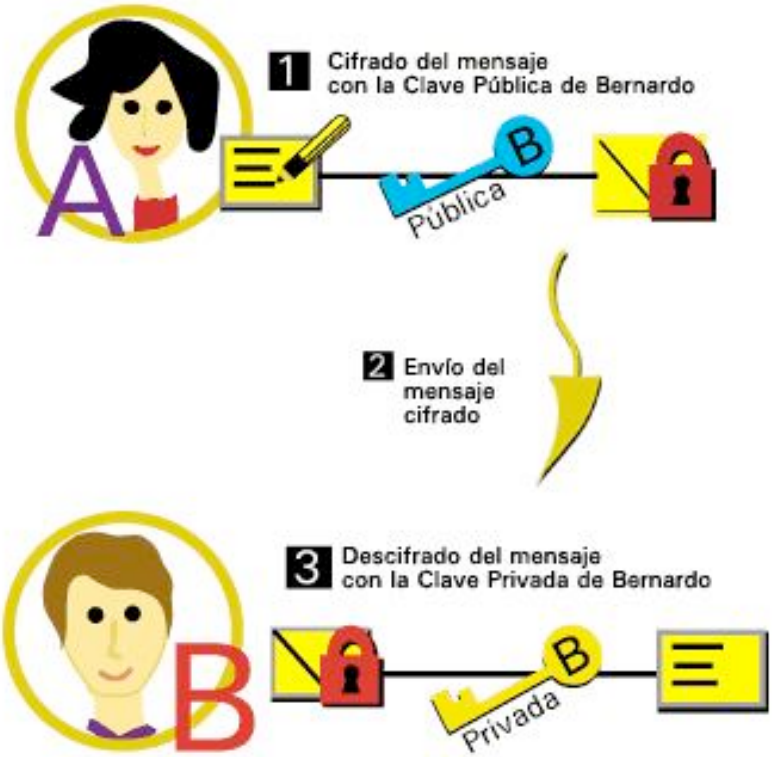
La Clave Pública se basa en una infraestructura llamada PKI - Public Key Infraestructure y RSA - Rivest, Shamir y Adleman.

La Criptografía de Clave Pública suple la mayoría de las carencias que tiene la criptografía de Clave Única. En esta, un particular o una empresa tiene dos claves complementarias (la privada y la pública). Cualquier información que haya sido cifrada por la clave privada, solamente podrá ser descifrada por la clave pública, y viceversa, cualquier información cifrada utilizando la clave pública sólo puede ser descifrada usando la clave privada.

De esta forma, el destinatario no tiene porque preocuparse al enviar la clave pública con el mensaje, porque si un tercero la averigua, lo único que podrá hacer es enviar un mensaje privado al destinatario, no pudiendo descifrar mensajes enviados al destinatario ni tampoco puede imitarle. El destinatario puede firmar los mensajes, porque el destinatario es la única persona con su clave privada, si cifra un mensaje con su clave privada, es equivalente a utilizar una firma electrónica.

Con este tipo de cifrado de mensajes se pueden obtener las siguientes características:

- Confidencialidad: el mensaje se mantiene en secreto durante todo el envío, solamente el emisor y el receptor pueden acceder a la información. La única manera de descifrarlo una vez enviado es a través de la clave privada del receptor, que es la única persona que la posee.
- Identificación y autenticación: el receptor tiene la seguridad de que el mensaje ha sido enviado por el emisor si este lo cifra con su clave privada, ya que es el único que la conoce. Lo único que debe hacer el receptor es descifrar el mensaje con su clave pública.
- Confidencialidad y autenticación:
- Integridad: se garantiza con este método que el mensaje no haya sido modificado, ya que aunque este sea interceptado en el envío, no conoce la clave privada del emisor para descifrar el mensaje real ni la clave privada del receptor para cifrar el mensaje falso.
- No repudio: este sistema utiliza marcas de tiempo, de manera que unidas al mensaje, se cifran con la clave privada del emisor. Esto garantiza la hora del envío del mensaje.




Fuente: www.cert.fnmt.es

LA FUNCIÓN HASH

La función Hash es un algoritmo matemático que, cuando se aplica a un texto en claro, nos permite obtener un resumen del mismo y que se utiliza para comprobar si durante el envío de los datos se ha producido alguna alteración por la intervención de un tercero sin autorización. Esto garantiza la integridad del mensaje, y la firma electrónica está basada en este sistema.

## 5.4. AMBITO DE APLICACIÓN DE LA LEY

Para evitar que los clientes eviten la desconfianza de comprar y contratar servicios o productos a través de la red, es necesario encontrar soluciones fiables y seguras. Para ello se utiliza la Firma Electrónica, para identificar, autenticar, integrar y producir no repudio.

La Ley de Firma Electrónica en su artículo primero determina su ámbito de aplicación, que es "regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación".

Los tres conceptos sobre los que se basa la Ley son entonces la firma electrónica, su eficacia jurídica y los prestadores de servicios de certificación.

El artículo segundo define a los denominados prestadores de servicios de certificación así:

"Se denomina prestador de servicios de certificación a la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica"

Además, la Ley solamente es aplicable a "los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España".

Por la definición que da la Ley sobre los prestadores de servicios de certificación, ADstudio no se puede considerar una ya que entre su actividad no esta la de emitir certificados electrónicos. Pero si que ADstudio necesita un certificado electrónico que le permita identificarse en Internet, para que las operaciones comerciales con sus clientes tengan mayor seguridad. Por lo tanto, se deberá contratar los servicios de un prestador de servicios de certificación.

El artículo 3 de la Ley sobre Firma Electrónica define firma electrónica como:

"La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".

Además, en este artículo se definen los tipos de firma electrónica que existen.

## 5.5. CLASES DE FIRMA ELECTRÓNICA

Aparte de la firma electrónica simple, que viene definida en el primer apartado del artículo 3, en los apartados posteriores de definen otras dos clases de firmas, la firma electrónica avanzada (Artículo 3.2) y la firma electrónica reconocida (Artículo 3.3).

FIRMA ELECTRÓNICA AVANZADA - ART. 3.2

La Ley define firma electrónica avanzada como:

“la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control”.

FIRMA ELECTRÓNICA RECONOCIDA - ART. 3.3

Define el concepto de firma electrónica reconocida como:

“la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”

Este tipo de firma añada a la firma electrónica avanzada la necesidad de estar basada en un certificado reconocido y haber sido generada mediante un dispositivo seguro de creación de firma.

Solamente la firma reconocida será equiparable a la firma manuscrita y así viene expuesto en el apartado cuarto del artículo tercero:

“la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel”

| FUNCIONES | FIRMA ELECTRÓNICA SIMPLE | FIRMA ELECTRÓNICA AVANZADA | FIRMA ELECTRÓNICA RECONOCIDA |
|---|---|---|---|
| IDENTIFICACIÓN DE LAS PARTES | ✗ | ✓ | ✓ |
| AUTENTICACIÓN DEL CONTENIDO | ✗ | ✓ | ✓ |
| INTEGRIDAD DEL CONTENIDO | ✗ | ✓ | ✓ |
| CONFIDENCIALIDAD | ✗ | ✗ | ✗ |
| NO REPUDIO | ✗ | ✗ | ✓ |

Del cuadro anterior se deduce que para ofrecer una mayor seguridad a la hora de realizar transacciones comerciales entre diferentes partes en Internet, se deberá utilizar una firma electrónica avanzada o reconocida.

La diferencia entre ambas y la firma electrónica simple, es que esta utiliza criptografía de clave simétrica, mientras que las que ofrecen mayor seguridad utilizan criptografía de clave asimétrica o de clave pública.

DOCUMENTO ELECTRÓNICO

"Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tramitación diferenciado[45]"

Sería recomendable, tal y como hemos explicado anteriormente, que ADstudio utilice todos sus documentos electrónicos en formato PDF.

En cuanto a la validez probatoria de la firma electrónica, podemos deducir el siguiente cuadro resumen sobre firma electrónica de acuerdo a la Ley 59/2003[46]:

| FIRMA ELECTRÓNICA SIMPLE | FIRMA ELECTRÓNICA AVANZADA | FIRMA ELECTRÓNICA RECONOCIDA |
|---|---|---|
| Conjunto de datos en forma electrónica consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante<br><br>La firma electrónica que no reúna los requisitos de firma electrónica reconocida no se le negarán los efectos jurídicos con relación a los datos que esté asociada por el mero hecho de presentarse en forma electrónica | La firma electrónica que: permita identificar al firmante y detectar cualquier cambio ulterior en los datos firmados<br><br>Está vinculada al firmante y a los datos firmados de manera única y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control<br><br>La firma electrónica que no reúna los requisitos de una firma electrónica reconocida no se le negarán los efectos jurídicos en relación con los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica | La firma electrónica avanzada basada en un certificado reconocido generada mediante un dispositivo seguro de creación de firma<br><br>Tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en soporte papel |

[45] De acuerdo con el Artículo 3 de la Ley Orgánica 59/2003 de Firma Electrónica

[46] Cuadro extraído del "Factbook Comercio Electrónico". Miguel Ángel Davara Rodriguez. 3ª Edición, Editorial Aranzadi.

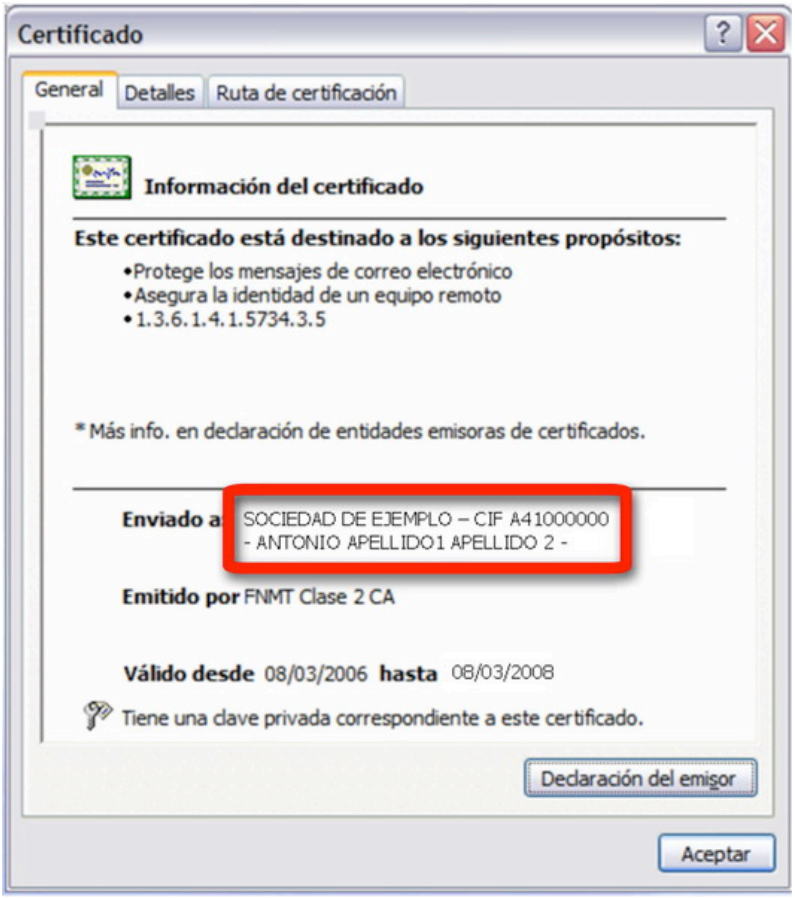
## 5.6. CERTIFICADOS ELECTRÓNICOS

El Artículo 2.2 de la Ley sobre Firma Electrónica define a los Prestadores de Servicios de Certificación como “la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica”.

La solución para los problemas de autenticación en las transacciones comerciales en una empresa es utilizar un certificado digital o electrónico, que se trata de un documento electrónico que contendrá los datos identificativos de la empresa (emisor) y su clave pública, haciéndose responsable de los datos que figuran en el certificado un tercero de confianza, que se conoce como Prestador de Servicios de Certificación.

El tercero de confianza es el que se encarga de emitir el certificado electrónico, llevando a cabo una serie de procedimientos para asegurarse de que quien lo solicita dice ser quien es y que la clave pública realmente le pertenece.

El formato de los certificados digitales es estándar, siendo el X.509 v3 el recomendando por la Unión Internacional de Comunicaciones (ITU). Actualmente se encuentra en vigor.




Los datos más comunes que se incluyen en un certificado son:

- Versión: que normalmente suele ser una versión estándar del X.509.
- Número de serie: identifica el certificado y es único para cada certificado, lo emite la Autoridad Certificadora.
- Algoritmo de firma: algoritmo que se utiliza para la firma digital.
- Autoridad Certificadora: la autoridad que emite el certificado
- Fechas de inicio y fin de la validez del certificado: marcan el periodo de validez del certificado. Generalmente es un año.
- Propietario: persona o entidad vinculada al certificado.
- Clave Pública: representación en hexadecimal de la clave pública vinculada a su propietario, junto con el algoritmo criptográfico que es aplicable.

- Algoritmo: usado para utilizar la firma digital
- Firma de la Autoridad Certificadora: asegura la autenticidad
- Información adicional

Para cualquier transacción comercial que emplee ADstudio con un cliente por ejemplo, en el que se necesite asegurar la confidencialidad se utilizará un certificado de seguridad. ADstudio emitirá uno al cliente que tendrá que validar (este viene encriptado con clave privada de la empresa). Si el cliente lo valida, es decir, lo considera de confianza, a través de su clave pública, le permitirá conocer si el certificado es legítimo o no.

Una vez que el certificado haya sido aceptado por el cliente, las comunicaciones entre ambos serán confidenciales ya que los mensajes estarán cifrados y solamente podrán ser descifrados con las claves que poseen.

De esta manera solo hay validación y confidencialidad por parte de la empresa y no por la del cliente, quien podría utilizar un sistema parecido, como puede ser el DNI electrónico.

El Título II de la Ley sobre Firma Electrónica es el que dedica la Ley para certificados electrónicos, del artículo 6 al 16:

CONCEPTO DE CERTIFICADO ELECTRÓNICO Y DE FIRMANTE - ART. 6

Realiza una definición de certificado electrónico (definido anteriormente) y de firmante, que lo define como:

“la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa”.

CERTIFICADOS ELECTRÓNICOS DE PERSONAS JURÍDICAS - ART. 7

Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios, que serán los responsables de los datos de creación de firma asociados a cada certificado electrónico de cada persona jurídica.

Un representante legal o administrador de ADstudio será quien deberá solicitar un certificado electrónico, que podría recaer sobre el Responsable de Seguridad por ejemplo.

Los datos de creación de firma de ADstudio solamente podrán ser utilizados con dos fines:

- Relaciones con la Administración Pública
- Actividades relacionadas con la actividad de la empresa.

EXTINCIÓN DE LA VIGENCIA DE LOS CERTIFICADOS ELECTRÓNICOS - ART. 8

Las causas por las que se puede extinguir la vigencia de un certificado electrónico son:

- Expiración del periodo de validez. Este periodo figura en el certificado.
- Revocación formulada por el firmante. En el caso de ADstudio sería la persona física que haya solicitado el certificado electrónico como representante de la misma.
- Cuando haya peligro del secreto de los datos de creación de firma o haya una utilización indebida de los mismos.
- Cuando una resolución judicial o administrativa lo ordene.
- Extinción de la personalidad jurídica de la empresa, en este caso, la extinción de la personalidad jurídica de ADstudio.
- Cese en la actividad del prestador de servicios de certificación, salvo que a petición del firmante los datos y la gestión del certificado electrónico sea transferido a otro prestador de servicios de certificación.
- Modificación de los datos aportados cuando se obtuvo el certificado.
- Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

Cuando un certificado expira, se incluye en el servicio de consulta sobre la vigencia de los certificados del Prestador de Servicios de Certificación, informando previamente a la empresa de

este hecho, aunque se mantiene accesible el servicio de consulta hasta al menos la fecha en la que hubiera finalizado su periodo inicial de validez.

Cuando un certificado expira, pierde toda su validez. Es recomendable que toda empresa tenga especial cuidado con la fecha de expiración, ya que en este caso no tendría ningún valor.

A su vez, tampoco es recomendable que ADstudio acepte instalar o aceptar un certificado que haya expirado o que haya sido generado por una entidad emisora de no confianza.

## CERTIFICADOS ELECTRÓNICOS

El Capítulo II del Título II de la Ley sobre Firma Electrónica esta dedicado a los certificados reconocidos, que son los que más garantías de seguridad ofrecen y los que son más recomendables utilizar en el sector privado.

## CONCEPTO Y CONTENIDO DE LOS CERTIFICADOS RECONOCIDOS - ART. 11

La Ley los define como “los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten”.

También establece los datos mínimos que deben incluir:

- La indicación que se expiren como tales
- El código identificativo del certificado
- La identificación del prestador de servicios de certificación que expire el certificado y su domicilio
- La firma electrónica avanzada del prestador de servicios de certificación

- La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número nacional de identidad, o a través de un seudónimo que conste como tal de manera inequívoca, y en el caso de que se traten de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- El comienzo y el fin del período de validez del certificado.
- Los límites de uso del certificado, si se establecen.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

OBLIGACIONES PREVIAS A LA EXPEDICIÓN DE CERTIFICADOS RECONOCIDOS - ART. 12

En este artículo se establecen las obligaciones previas a la expedición de los certificados reconocidos que se deben de cumplir, para que a la hora de que una empresa, en este caso ADstudio, vaya a escoger el Prestador de Servicios de Certificación lo haga con uno que preste su servicio de acuerdo a la Ley de Firma Electrónica:

- Comprobar la identidad y circunstancias de la empresa
- Verificar que la información del certificado es exacta
- Asegurarse de que la empresa está en posesión de los datos de creación de firma
- Garantizar la complementariedad de los datos de creación y verificación de firma

## 5.7. CLIENTES: DNI ELECTRÓNICO

El Artículo 25 de la Ley de Firma Electrónica da una definición del DNI electrónico:

"El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos"

El DNI lo emite la Dirección General de la Policía, que a su vez pertenece al Ministerio del Interior y es el documento, que acredita desde ha más de 50 años:

- Identidad
- Datos personales del titular
- Nacionalidad del titular

Con las nuevas tecnologías de la información y las comunicaciones, ha sido necesario adecuar este documento a las realidades actuales, teniendo que trasladar ese mecanismo de acreditación a la red para poder así operar con la misma certeza con la que operamos en la vida cotidiana.

Para ello se crea el DNI electrónico (DNIe), que incorpora un pequeño circuito integrado (chip), donde almacena información de una forma segura y es capaz de procesarla internamente.

Con el DNI electrónico, se podrán realizar[47]:

- compras firmadas a través de Internet
- tramites con las Administraciones Públicas, a cualquier hora sin tener que adecuarse a los horarios administrativos
- transacciones seguras con entidades bancarias y financieras
- acceder al edificio donde trabajamos
- utilizar de forma segura nuestro ordenador persona

[47] Características extraídas del sitio web "www.dnielectronico.es"

- participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser

El DNI electrónico tiene un chip criptográfico que contiene la siguiente información en formato digital:

- un certificado electrónico para autenticar la personalidad del ciudadano
- un certificado electrónico para firmar electrónicamente, con la misma validez jurídica que la firma manuscrita
- certificado de autoridad de certificación emisora
- claves para su utilización
- la plantilla biométrica de la impresión dactilar
- la fotografía digitalizada del ciudadano
- la imagen digitalizada de la firma manuscrita
- datos de la filiación del ciudadano, correspondientes con el contenido personalizado en la tarjeta

El DNI electrónico puede ser el mecanismo que utilicen los clientes de ADstudio como firma electrónica reconocida para realizar los pedidos a la empresa, de tal manera que son identificados claramente.

Para que una persona pueda utilizar su DNIe necesitará aparte de un ordenador con conexión a Internet, un dispositivo lector de DNI electrónico, como el que se muestra en la imagen:

## 5.8. PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

El Título III de la Ley de Firma Electrónica trata sobre las obligaciones y responsabilidades de los Prestadores de Servicios de Certificación:

"la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica[48]

OBLIGACIONES

En el Capítulo I se detallan las obligaciones sobre los Prestadores de Servicios de Certificación.

En el primer artículo, el Artículo 17, se puede extraer la obligación por parte de los Prestadores de Servicios de Certificación de cumplir con la normativa vigente sobre Protección de Datos, la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su desarrollo.

En el artículo 19, citan varias obligaciones que se tienen que comprometer a cumplir, que son:

- la gestión de los datos de creación y verificación de firma y de los certificados electrónicos
- las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados
- las medidas de seguridad técnicas y organizativas
- los perfiles y los mecanismos de información sobre la vigencia de los certificados
- en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

[48] Artículo 2.2 de la Ley Orgánica 59/2003, de 19 de diciembre, de Firma Electrónica

En los Artículos del 17 al 21 de la Ley se detallan otras obligaciones que todos los Prestadores de Servicios de Certificación deben cumplir:

- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios
- Informar al solicitante antes de la expedición del certificado sobre:
    - Obligaciones del firmante
    - Los mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo
    - El método utilizado para comprobar la identidad del firmante
    - Las certificaciones que haya obtenido el prestador
    - Los procedimientos para la resolución extrajudicial de conflictos
    - Las demás informaciones contenidas en la declaración de prácticas de certificación
- Mantener un directorio actualizado de certificados
- Disponer de un servicio de consulta sobre la vigencia de los certificados rápido y seguro
- Declaración de prácticas de certificación, que este disponible al público de una manera fácilmente accesible, por vía electrónica al menos y de forma gratuita. Contendrá las obligaciones que se comprometen a cumplir, las condiciones aplicables a los certificados, así como los perfiles y mecanismos de información sobre vigencia de los certificados.

Por otra parte, en los Artículos 12 al 20 de la Ley 59/2003 se detallan las obligaciones que tienen que tener los que expidan certificados reconocidos solamente:

- Comprobar la identidad y circunstancias personales, verificar, asegurarse y garantizar la complementariedad de los datos de creación y verificación de firma de forma previa a la expedición del certificado.
- Demostrar la fiabilidad necesaria

- Garantizar con determinación precisa la hora y la fecha en la que se expidió, extinguió o suspendió el certificado
- Emplear personal con cualificación, conocimientos y experiencia necesaria para la prestación de servicios de certificación, los procedimientos de seguridad y los procedimientos de gestión adecuados en el ámbito de la firma electrónica.
- Utilizar sistemas y productos fiables
- Tomar medidas contra la falsificación de certificados
- Conservar registrada toda la información relativa a un certificado reconocido al menos durante 15 años desde que es expedido.
- Utilizar sistemas fiables para almacenar los certificados reconocidos.
- Constituir un seguro de responsabilidad civil o aval bancario por importe de 3.000.000 de euros.

Si un Prestador de Servicios de Certificación procede al cese de su actividad[49], deberá comunicarlo a los firmantes con una antelación mínima de dos meses, pudiendo transferir su gestión a otro Prestador con su consentimiento, y al Ministerio de Industria, Turismo y Comercio.

RESPONSABILIDADES

En el Capítulo II del Título III de la Ley sobre Firma Electrónica vienen las responsabilidades que deben tener los Prestadores de Servicios de Certificación. Estos tendrán que responder cuando:

- cuando causen algún daño o perjuicio a cualquier persona en el ejercicio de su actividad. Si causase algún tipo de perjuicio a la empresa, en este caso a ADstudio, el Prestador sería el responsable tendría que asumir con todo.

[49] Artículo 21, de la Ley Orgánica 59/2003, de 19 de diciembre, de Firma Electrónica

- cuando por falta o retraso en la inclusión del servicio de consulta sobre la vigencia del certificado, cause perjuicios al firmante o a los terceros de buena fe.

En cambio, el Prestador de Servicios de Certificación no será responsable por los daños y perjuicios causados, cuando ADstudio incumpla alguno de los siguientes supuestos:

- no proporcionar información veraz, completa y exacto sobre los datos que constan en el certificado electrónico al Prestador de Servicios de Certificación
- la no comunicación al Prestador de cualquier modificación de los datos
- actuar de forma negligente en la conservación de los datos de creación de firma, en la confidencialidad y en la protección de todo acceso o revelación.
- no solicitar la suspensión o revocación del certificado en caso de duda sobre el mantenimiento de la confidencialidad
- utilizar los datos de creación de firma cuando haya expirado la validez del certificado
- superar los límites que figuren en el certificado en usos e importe de las transacciones que puedan realizarse con él

Por tanto, ADstudio deberá tomar toda clase de medidas para que no incumpla cualquiera de los supuestos anteriormente mencionados, ya que la empresa sería la responsable. Por lo tanto es muy importante fijarse en el periodo de validez del certificado, sus usos y limites en el uso, comprobar si el certificado es seguro y si ha sido expedido por una entidad certificadora de confianza.

En la página web del Ministerio de Industria, Turismo y Comercio pueden consultarse un listado de empresas que ofrecen servicios de certificación seguros y de confianza. Además puede consultarse que Prestadores de Servicios de Certificación han comunicado su cede de actividad.

## RELACIÓN PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

| Prestadores |
|---|
| AC ABOGACÍA |
| ANCERT - Agencia Notarial de Certificación |
| ANF AC |
| Autoritat de Certificació de la Comunitat Valenciana - ACCV |
| BANESTO CA |
| CAMERFIRMA |
| CATCert |
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| CICCP |
| Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía |
| EDICOM |
| Firmaprofesional, S.A. |
| Gerencia de Informática de la Seguridad Social |
| HEALTHSIGN, S.L. |
| Izenpe, S.A |
| Ministerio de Defensa de España |
| REGISTRADORES DE ESPAÑA |
| Santander |

Fuente: Ministerio de Industria, Turismo y Comercio

## RELACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN QUE HAN COMUNICADO SU CESE DE ACTIVIDAD

- Nombre o Razón Social: **Hewlett-Packard Española Sociedad Limitada**

  Nombre Comercial: **NETFOCUS**

  Fecha de resolución por la que se acepta la comunicación de cese: 03 de abril de 2009

Fuente: Ministerio de Industria, Turismo y Comercio

ADstudio

# Propiedad Intelectual

## 6.1. INTRODUCCIÓN

La red ha creado un mundo con más competencia que anteriormente, con un mayor mercado donde poder ofertar bienes y servicios. Por ello surge la necesidad de invertir en el diseño estético y funcional del sitio web y que este este protegido jurídicamente, ya que forma parte de una estrategia comercial más de las empresas que puede ser fácilmente copiada o imitada por otras.

Este nuevo entorno de mercado fomenta la posibilidad de utilizar de forma ilegal las composiciones comerciales en formato digital de otras empresas, aún estando amparadas por los derechos de propiedad intelectual. Esto se debe a que cualquier contenido en formato digital, como pueden ser imágenes, datos, vídeos, programas o diseños son accesibles mediante cualquier ordenador o dispositivo electrónico.

Aunque el termino de propiedad intelectual es más fácil atribuírselo a objetos u obras de arte, que es un bien material, también debe abarcar cualquier creación de bienes inmateriales, como los programas informáticos.

Entre los bienes inmateriales que protege la Propiedad Intelectual, en la sociedad de la información destacan:

- Nombres de dominio: tienen gran importancia como identificadores comerciales de las empresas.
- Creaciones del intelecto: creaciones fomentadas por proyectos de I+D+I que permiten un ahorro en los costes de la empresa

Estos bienes son protegidos por la normativa española, dependiendo de que producto se trate, de dos maneras diferentes, por la Propiedad Intelectual y por la Propiedad Industrial.

En todos los casos, para que exista una protección jurídica sobre las creaciones, esta se tiene que llevar a cabo a priori, es decir, debe registrarse las creaciones con anterioridad en un Registro para así poder ejercer los derechos en caso de necesitarlo.

## 6.2. NORMATIVA

La normativa vigente en España sobre Propiedad Intelectual se basa en la Ley de Propiedad Intelectual:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia

Esta Ley ha sido actualizada por otra basándose en una Directiva Europea:

- Ley 5/1998, de 6 de marzo, de incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos
- Directiva 96/9/CE, Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos

## 6.3. PROPIEDAD INTELECTUAL Y PROPIEDAD INDUSTRIAL

Los derechos de la Propiedad Intelectual protegen todas aquellas creaciones del ser humano con un carácter literario, científico o artístico, expresadas en un soporte tangible o intangible. Los derechos que las protegen pueden ser de carácter moral o patrimonial.

Por otro lado, los derechos de la Propiedad Industrial protegen el ejercicio de la actividad empresarial en general, principalmente todo lo que haga referencia a patentes, marcas, identificadores comerciales, etc.

En todos los casos, para que exista una protección jurídica sobre las creaciones, esta se tiene que llevar a cabo a priori, es decir, debe registrarse las creaciones con anterioridad para así poder ejercer los derechos en caso de necesitarlo.

Todo lo relacionado con el software no se incluye en la Propiedad Industrial, ya que la legislación española no lo considera invenciones, como viene reflejado en el artículo 4.4.c de la Ley 11/1986, de 20 de marzo, de Patentes de Invención y Modelos de Utilidad:

“No se considerarán invenciones en el sentido de los apartados anteriores, en particular:

a. Los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, así como los programas de ordenadores”

En cambio, en otros países como en Estados Unidos, si que se permite patentar los programas de ordenador, algo que hubiera evitado muchos casos de plagio en nuestro país.

### PROPIEDAD INTELECTUAL

La legislación española centra el hecho de la intangibilidad del objeto sobre el que se desarrolla con Propiedad Intelectual. Estos objetos, por ser intangibles, pueden ser igualmente vendidos, cedidos o intercambiados, pero por el hecho de serlo así, necesitan una protección especial.

La persona que gozará la protección de la obra será el autor, que de forma general, será una persona física, aunque la ley también contempla casos en los que la Ley podría beneficiar a una persona jurídica también.

La Ley[50] enumera los diferentes objetos o creaciones que son objeto de la Propiedad Intelectual y que se acogen a su normativa y derechos:

"Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:

a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza.
b) Las composiciones musicales, con o sin letra.
c) Las obras dramáticas y dramático-musicales, las coreográficas, las pantomimas y, en general, las obras teatrales.
d) Las obras cinematográficas y cualesquiera otras obras audiovisuales.
e) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o comics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas.
f) Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.
g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.
h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía.
i) **Los programas de ordenador**"

Existen sin embargo una serie de ventajas el incluir al software dentro de la Propiedad Intelectual y en particular en los derechos de autor, que es recomendable prestar atención no solamente como desarrolladores de productos de software (no es el caso de ADstudio), sino como consumidores del mismo:

- Plazo de protección: tiene un plazo mayor que la propiedad industrial, por lo que el autor puede sacar mayor beneficio y adaptar las peculiaridades del programa al usuario, para así poder recuperar la inversión en un tiempo de protección lo suficientemente amplio para comercializar la obra.

[50] En su Artículo 10

- Copias no autorizadas: un desarrollar de software se puede encontrar con el problema de copia del programa, o de su utilización para crear un programa más potente y mejor, así como para poder comercializarlo con otra identidad. Los derechos de autor protegen en gran medida y solventan parcialmente el problema.
- Nacimiento de la protección de forma automática: la protección jurídica de los derechos de autor nace desde el mismo momento en que la idea es expresada en un soporte, de forma que con solamente el comienzo de la creación de un programa de ordenador y expresarlo en un soporte magnético, óptico o en papel, siendo susceptible de tratamiento automatizado, ya esta protegido jurídicamente sin necesidad de cumplir con más formalismos.
- Pocas obligaciones para el titular: no se necesita ningún procedimiento para que el autor goce de los derechos que le otorgan la propiedad intelectual.

## 6.4. AUTORES

El Artículo 5 de la Ley sobre Propiedad Intelectual define a la figura del autor de una obra susceptible de ser protegida bajo la Propiedad Intelectual:

"1. Se considera autor a la persona natural que crea alguna obra literaria, artística o científica.

2. No obstante, de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella".

Se considera autor de la obra a la persona natural que crea una obra literaria, artística o científica, aunque en determinados casos las personas jurídicas también pueden ser titulares de derechos de autor, aunque nunca se les puede considerar creadores.

El autor de una obra protegida por la Propiedad Intelectual goza de dos tipos de derechos, los derechos morales y los derechos patrimoniales.

### 6.4.1. DERECHOS MORALES

Los derechos morales son derechos irrenunciables e inalienables, no pueden ser cedidos y tampoco se puede renunciar a ellos.

Si por ejemplo, un informático de ADstudio desarrolla un programa de ordenador para facilitar la gestión de la empresa, poseería los siguientes derechos morales:

- Decidir si su obra va a ser divulgada y de que forma
- Determinar si la obra se va a divulgar con su nombre, con un seudónimo o signo, o de forma anónima
- Exigir la paternidad de la obra, reconocimiento de su condición como autor

- Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a los legítimos intereses del autor o menoscabando su reputación
- Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural
- Poder retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación.
- Poder acceder al ejemplar único o raro de la obra, en caso de que se halle en poder de otro, con el fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.

### 6.4.1. DERECHOS PATRIMONIALES

El autor puede decidir sobre el uso de la obra creada, que no se podrá utilizar sin su autorización (salvo en determinados casos que prevé la vigente ley de Propiedad Intelectual española [51]). Estos derechos facultan sobre la explotación de la obra, y pueden cederse a terceros para:

- Reproducción: fijación de la obra en un medio que permita su comunicación y obtención de copias de todo o parte de la obra
- Distribución: puesta a disposición del público del original o copias de la obra por venta, alquiler, préstamo o cualquier otra forma.
- Comunicación pública: cuando un conjunto de personas tiene acceso a la obra sin previa distribución de ejemplares.
- Transformación: acto de traducción, adaptación y cualquier otra modificación de una obra y que derive en otra obra diferente. Para el ejemplo de las bases de datos, se considera transformación su reordenación.

[51] Recogidos en el Artículo 100, "Límites a los derechos de explotación", del Real Decreto 1/1996, de 12 de abril

Como normal general, los derechos de explotación de una obra duran toda la vida del autor más 70 años después de su muerte o declaración de fallecimiento. Una vez transcurrido este tiempo, la obra pasa a dominio público y podrá ser utilizada sin autorización, siempre que se respete la autoría e integridad de la obra.

Los derechos patrimoniales pueden ser transmitidos, ya sea de forma mortis causa[52] o inter vivos[53].

El Artículo 100 recoge ciertas limitaciones sobre los derechos de explotación:

- No se necesitará autorización del titular del programa para la reproducción o transformación del programa cuando sea necesario para la utilización del mismo, salvo que se disponga lo contrario en el acuerdo contractual.
- No se podrá impedir la copia de seguridad por parte de quien tiene derecho a utilizar el programa.
- El usuario del programa podrá observar, estudiar o verificar el funcionamiento del programa siempre que lo haga durante las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que tiene derecho a hacer.
- Salvo que se indique lo contrario, el autor no se podrá oponer a que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo. De este modo, si ADstudio cede los derechos de explotación de un programa creado a una tercera empresa, salvo que se indique lo contrario en el acuerdo contractual, esta podrá modificar y crear versiones diferentes del mismo.
- No se necesitará la autorización del titular del derecho cuando la reproducción del código y la traducción de su forma sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente con otros programas, siempre que se cumplan los siguientes requisitos.

[52] "Por causa de muerte": expresión latina utilizada en Derecho para hacer referencia a los actos jurídicos que se producen o tienen efecto tras el fallecimiento de una persona. Ejemplo: el testamento

[53] "Entre vivos": expresión latina utilizada en Derecho para hacer referencia a los actos jurídicos que se producen entre personas vivas, en contraposición a los actos mortis causa.

a. Que dichos actos sean realizados por el usuario legítimo u otra persona que pueda utilizar una copia del programa, o autorizada en su nombre.

b. Que la información para conseguir la interoperabilidad no haya sido dada de manera fácil y rápida a disposición del usuario legítimo u otra persona que pueda utilizar una copia del programa, o autorizada en su nombre.

c. Que los actos sólo se aplicarán a las partes del programa necesarias para obtener la interoperabilidad.

- La excepción contemplada en el apartado 5 será aplicable siempre que la información así obtenida:

a. se utilice únicamente para conseguir la interoperabilidad del programa creado de forma independiente

b. solo se comunicará a terceros cuando sea necesario para la interoperabilidad del programa creado de forma independiente

c. no se utilizará para el desarrollo o comercialización de un programa sustancialmente similar en su expresión

## 6.5. TIPOS DE OBRAS

Existen diferentes tipos de obras, que también pueden clasificar a los programas de ordenador, así como a cualquier tipo de creación susceptible de protección como obra del intelecto, y son:

### 6.5.1. OBRA EN COLABORACIÓN

El Artículo 7 de la Ley sobre Propiedad Intelectual las define como aquellas que son resultado unitario de la colaboración de varios autores. En este tipo de obras, los derechos de autor corresponden a todos los autores que han participado en la creación de la obra.

Para la divulgación o modificación de la obra se necesita el consentimiento de todos los coautores. En cambio, una vez que la obra este publicada, ningún coautor podrá rehusar injustificadamente su consentimiento para la forma en que se divulgó la explotación, salvo que lo haga de forma justificada.

Los coautores podrán explotar de forma separada sus aportaciones a la obra, salvo que esto cause perjuicio a la explotación común. Esto se podrá ver modificado por lo que los autores decidan al respecto

La proporción sobre los derechos de propiedad intelectual de la obra en colaboración que a cada uno corresponde, deberá ser determinada por los mismos. En el supuesto que no hayan previsto nada, se les aplicarán las normas del Código Civil respecto a la comunidad de bienes.

Si la creación se tratase de un programa de ordenador, habría que hacer referencia a la definición que la Ley de Propiedad Intelectual hace de programa de ordenador:

“toda secuencia de instrumentos o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador”.

De este modo se entiende que el autor del programa de ordenador como obra unitaria no solamente es la persona que haya realizado su programación, sino también la persona que haya elaborado la documentación técnica o los manuales de uso o consulta, salvo que se pueda diferenciar el trabajo de cada uno.

### 6.5.2. OBRA COLECTIVA

El Artículo 8 de la Ley de Propiedad Intelectual considera obra colectiva la obra:

"creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una contribución única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada".

Se entiende de que aunque la obra sea de varios autores, se presume que se ha producido una transmisión desde el comienzo de la misma de los derechos a la persona que edita o divulga bajo su nombre la obra.

### 6.5.3. OBRA COMPUESTA

El Artículo 9 de la Ley de Propiedad Intelectual define la obra compuesta como aquella:

"obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última, sin perjuicio de los derechos que a éste correspondan y de su necesaria autorización".

Se entiende que pervive junto a los derechos de propiedad intelectual del autor de la obra compuesta los derechos de los autores de las obras originales que constituyan cada una de las partes de esa obra compuesta.

### 6.5.4. OBRA INDEPENDIENTE

El Artículo 9 de la Ley de Propiedad Intelectual también define la obra independiente, y lo hace como toda obra que:

“constituya creación autónoma se considerará independiente, aunque se publique conjuntamente con otras”

Los autores de cada obra independiente tendrán derechos sobre su obra original.

## 6.6. LOS PROGRAMAS DE ORDENADOR

La Ley de Propiedad Intelectual incluye a los programas de ordenador como objetos de protección junto a los demás tipos de obras que protege. El Título VII de la Ley lo dedica por completo a los programas de ordenador, que es importante tener en cuenta para que cualquier empresa, en este caso ADstudio, no infrinja la ley en materia de derechos de autor, tanto en un desarrollo de algún trabajador de la empresa como en un desarrollo de una tercera empresa.

La Ley ofrece la misma protección a los programas como a las versiones sucesivas y a los programas derivados, así como a los manuales de uso y documentación preparatoria.

La Ley marca el objeto de análisis de los programas de ordenador en su artículo 96, titulado como "Objeto de la protección":

"1. A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.
A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La **documentación técnica y los manuales de uso de un programa gozarán de la misma protección** que este Título dispensa a los programas de ordenador.
2. El programa de ordenador **será protegido únicamente si fuese original**, en el sentido de ser una creación intelectual propia de su autor.
3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección **se extiende a cualesquiera versiones sucesivas** del programa así como a los **programas derivados**, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.
Cuando los programas de ordenador **formen parte de una patente o un modelo de utilidad gozarán**, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la **propiedad industrial.**

4. **No estarán protegidos** mediante los derechos de autor con arreglo a la presente Ley **las ideas y principios** en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces."

Por lo tanto, para la empresa ADstudio no solamente serán de protección por la Propiedad Intelectual el software que haya creado por sus propios informáticos, sino también los desarrollos de terceros que haya adquirido, así como toda la documentación preparatoria, técnica y los manuales de uso.

El apartado segundo hace referencia claramente a que las obras que gozan de protección tienen que ser obras originales, que se entiende que es aquella producida directamente por su autor, sin que sea copia ni imitación de ninguna otra obra. Para que se proteja un programa de ordenador desarrollado por ADstudio tiene que haber sido creado de forma original, sin plagiar ninguno que ya existiera.

También será ámbito de protección las versiones sucesivas sobre el programa creado así como los programas derivados. La Ley aparta de la protección a los programas que puedan ocasionar efectos nocivos a un sistema informático como pueden ser los virus.

Si el programa que se desarrolle forma parte de una patente o de un modelo de utilidad de la empresa, no gozará de los derechos de la Propiedad Intelectual, sino de los de la Propiedad Industrial.

La Ley no protege mediante los derechos de autor las ideas y principios en los que se basa cualquiera de los elementos de un programa de ordenador. Para que se proteja, es necesario que la idea haya sido expresada anteriormente en algún tipo de soporte.

### 6.6.1. LOS AUTORES

El Artículo 97 de la Ley de Propiedad Intelectual centra en las personas naturales la consideración de autores de las obras del intelecto que gozan de protección. En el caso de ADstudio, sería la persona responsable de los desarrollos informáticos.

Como se ha indicado previamente, en caso de que se trate de una obra colectiva, se considerará al autor la persona natural o jurídica que la edite y divulgue bajo su nombre.

En el caso de los programas de ordenador que se creen dentro de una empresa por uno de los empleados, la Ley ha dispuesto el apartado 4 del Artículo 97:

"Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario".

Este supuesto es el que puede afectar a ADstudio como empresa que pueda realizar un desarrollo de software y que sea algún asalariado (empleado de la empresa) quien lo realice.

Si por ejemplo un trabajador de la empresa realiza un programa sin la coordinación de ADstudio, los derechos de explotación corresponderán exclusivamente al trabajador, ya que no se ha realizado conforme a las instrucciones de la empresa.

ADstudio obtendrá todos los beneficios económicos de la explotación de todos los programas de ordenador que se creen en su empresa por sus asalariados. Sin embargo, los derechos morales resultantes de la creación de un programa de ordenador serán propiedad del trabajador asalariado.

Es importante tener en cuenta que para que los derechos de uso de un programa de ordenador puedan ser cedidos, se puede realizar con un contrato de licencia de uso, en el que el titular del derecho de explotación autoriza a otro a utilizar el programa, conservando el cedente la propiedad del mismo.

Salvo que se establezca lo contrario, es de carácter no exclusivo e intransferible, es decir, que el programa podrá usarlo otras personas y que el cesionario no podrá cederlo a su vez a otros, ya que esta cesión tiene el objetivo de satisfacer únicamente las necesidades del usuario.

En los contratos de licencia se tienen que establecer diversas cláusulas limitando el uso del programa sobre el que se establece la licencia, además de las limitaciones.

ADstudio con las licencias de uso de los programas informáticos que adquiera, como pueden ser de un paquete ofimático, programas de gestión o de programas de diseño publicitario, no podrá venderlo, alquilarlo o prestarlo a algún tercero.

## 6.7. REGISTRO DE LA PROPIEDAD INTELECTUAL

Los derechos sobre los programas de ordenador que se creen, así como sucesivas versiones y programas derivados podrán ser objeto de inscripción en el Registro de la Propiedad Intelectual. De esta forma se notifica que los derechos sobre una obra existen y pertenecen a un determinado titular.

El problema que se presenta con el registro de un programa de ordenador en el Registro es su carácter público, ya que estaría expuesto a ser consultado públicamente, ya que además se tendría que depositar el código fuente y este podría estar expuesto a copia. Esto no resultaría una vía segura de protección.

Como alternativa a la inscripción en el Registro, se propone realizar un depósito notarial del programa, ya que se protegería con mayor garantía de secreto los derechos de autor. En caso de que ADstudio creara un programa de ordenador, esta sería la mejor alternativa para su registro.

# Nombres de Dominio

## 7.1. INTRODUCCIÓN

Con el progreso de las nuevas tecnologías y el avance de Internet y su acceso, resulta indispensable un sistema para poder reconocer a cada integrante y poder transmitir la información de un ordenador a otro mediante una dirección unívoca en cada uno de ellos.

En un principio, las direcciones que se utilizaban para las comunicaciones entre ordenadores conectados eran las direcciones IP, que funcionaban con un sistema parecido al de los números de teléfono. El principal inconveniente de este sistema era la dificultad que tenía memorizar un dirección IP, ya que esta formada por cuatro números separados por un punto que comprenden entre el 0 y el 255. Un ejemplo de dirección IP puede ser 198.329.13.64.

El sistema de nombres de dominio (DNS, Domain Name System) es una forma de identificación en la red, de forma que se puede identificar una máquina conectada. Las empresas u organismos habitualmente registran su nombre de domino con su marca o nombre con el que son reconocidos en el mercado. De esta manera para realizar cualquier comunicación con una empresa a través de Internet, solamente es necesario conocer la denominación de la misma. De aquí la importancia de hoy en día en tener un nombre de dominio conocido o deducible para las empresas u organizaciones que quieran extender su actividad en Internet.

## 7.2. CLASES DE NOMBRE DE DOMINIO

Un nombre de dominio por tanto se puede traducir como un nombre base que agrupa a un conjunto de equipos o dispositivos para así poder asignar un nombre que pueda ser recordado más fácilmente , en lugar de las IP numéricas que se utilizaban en un principio para ello.

En un nombre de dominio se deben tener en cuenta otras consideraciones como puede ser el ámbito de actuación de la empresa, ya que esta compuesto por el nombre que elige la empresa pero además con una terminación que se asocia o bien a un país (.es, .pt, .uk) o a una actividad (.org, .biz).

Por ello, los nombres de dominio se clasifican en dos clases diferentes (los de primer y segundo nivel), además de un tercero que ha creado el Plan Nacional:

### 7.2.1. NOMBRES DE DOMINIO DE PRIMER NIVEL

También son conocidos por las siglas TLD( Top Level Domain) y son los que se sitúan al final de la dirección, después del último punto. Estos se dividen en dos grupos a su vez, los genéricos y los de código de país:

NOMBRES DE DOMINIO DE PRIMER NIVEL GENÉRICO

Estos también son conocidos como gTLD (generic Top Level Domain) y eran siete en un principio, pero debido a problemas de saturación con los nombres de dominio, se han creado siete más, que aunque ya están creados, aún no se encuentran activos:

| gTLD | ACTIVO | DESCRIPCIÓN |
|---|---|---|
| .com | ✓ | Es el nombre de dominio de primer nivel genérico más utilizado en Internet y el que más conflictos genera. En un principio se pensó para las compañías que querían tener presencia en Internet. Es un dominio de acceso libre, por lo que no será necesario demostrar nada para poder registrar con este nombre de dominio. |

| gTLD | ACTIVO | DESCRIPCIÓN |
|---|---|---|
| .net | ✓ | Se trata de otro nombre de dominio de primer nivel genérico de libre acceso, que solamente requiere su solicitud, pero ha sido utilizado en menor medida que el .com. En un principio se creo para las empresas que tuvieran su actividad solamente en Internet. |
| .org | ✓ | Es el tercer nombre de dominio de primer nivel genérico de libre acceso, aunque el menos utilizado de los tres. Se creo en un principio para que las organizaciones tuvieran cabida en Internet. |
| .mil | ✓ | Se trata de un nombre de dominio de primer nivel genérico de uso restringido para la utilización por parte del ejercito de los Estados Unidos. |
| .int | ✓ | Se creo para las organizaciones internacionales sin ánimo de lucro. |
| .edu | ✓ | Es un nombre de dominio que se creó para las organizaciones superiores y solamente este tipo de organizaciones puede usarlo, por lo que se trata de un nombre de dominio de primer nivel genérico restringido. |
| .gov | ✓ | Es un nombre de dominio de primer nivel genérico de uso restringido para solamente los organismos del Gobierno de los Estados Unidos. |
| .biz | ✗ | Se ha pensado como un registro abierto pero que se utilice para fines comerciales. Es el que más se aproxima por semejanza al .com, por lo que se espera que sea el nuevo gTLD con mayor número de solicitudes de registro. Se pretende que sea también para las empresas que se quedaron sin poder registrarse en .com. Su definición corresponde con la abreviatura de la pronunciación del termino anglosajón *business.* |
| .info | ✗ | Se trata de otro nombre de dominio de primer nivel genérico de acceso libre, que no prevé que se exija ningún requisito para su registro. Se prevé que pase por un período por el cual solamente se permita que utilicen este registro los titulares de una marca con igual denominación. |

| gTLD | ACTIVO | DESCRIPCIÓN |
|---|---|---|
| .pro |  | Se trata de un nombre de dominio de primer nivel genérico que hace referencia a la palabra profesionales y que solamente estará disponible para las personas que sean profesionales de determinadas categorías, que a su vez se subdividirán en subcategorías (médicos, abogados etc). Para poder utilizar este nombre de dominio se deberá acreditar la pertenencia a un colegio profesional u organización similar. |
| .name |  | Este dominio será de libre adquisición pero con el único requisito de que el titular sea una persona física. Este tipo de nombre de dominio se denomina de doble punto, es decir, que delante del TLD habrá un nombre de dominio de segundo nivel (SLD) y otro de tercer nivel, que pertenecerán ambos a lo que se haya registrado. El nombre de dominio de segundo nivel equivaldrá al apellido y el de tercer nivel al nombre. Un ejemplo sería: ivan.ramos.name |
| .coop |  | Este nombre de domino de primer nivel genérico esta reservado únicamente para las cooperativas, por lo que tendrán que demostrarlo para que puedan registrarlo. |
| .aero |  | Es un nombre de dominio de primer nivel genérico de uso exclusivo y restringido a la industria aeronáutica. |
| .museum |  | Se trata de un dominio de primer nivel genérico de uso restringido para los museos que quieran tener presencia en Internet. |

Debido a que existen numerosos nombres de dominio que imponen ciertos criterios de uso que no cumple ADstudio, sería recomendable que registrase los nombres de dominio:

www.adstudio.com

www.adstudio.es

De esta forma la empresa se aseguraría tener los nombres de dominio .com y .net para ella. Ya que gestionar diferentes portales web requiere recursos, se recomienda que solamente se utilice el

dominio .com como dominio principal y que los demás que se vayan creado estén reedireccionados automáticamente a este.

NOMBRES DE DOMINIO DE PRIMER NIVEL DE CÓDIGO DE PAÍS

Son conocidos también como ccTLD (Country-code Top Level Domain) y están compuestos por dos caracteres, de acuerdo con las normas ISO-3166.

El ccTLD que utiliza España es el .es, registrado por la entidad registradora Red Española de Televisión, organismo que depende del Ministerio de Industria, Turismo y Comercio.

Ya que el ámbito de aplicación inicial y donde se asienta la empresa ADstudio es España, también es recomendable que la empresa registre el dominio .es (que sería www.adstudio.es), y que esté redireccionado al dominio principal, www.adstudio.com.

NOMBRE DE DOMINIO DE PRIMER NIVEL DE CÓDIGO EUROPEO

El 22 de abril de 2002, el Parlamento Europeo y el Consejo aprobaron el Reglamento por el cual se regula la aplicación del dominio de primer nivel .eu.

El objetivo principal es la aceleración del comercio electrónico definido en la iniciativa eEurope.

Este nombre de dominio podría ser una opción para ADstudio si decidiese comprar otro nombre de dominio, pero no sería necesario a priori.

### 7.2.2. NOMBRES DE DOMINIO DE SEGUNDO NIVEL

También son conocidos con las siglas SLD (Second Level Domain) y son los que habitualmente se equiparán a la marca o al nombre comercial de la empresa que los define, y por ello, son los que más conflictos sobre propiedad intelectual e industrial causan.

ADstudio tomará como nombre de dominio de segundo nivel el nombre de la empresa, que sería “adstudio”.

### 7.2.3. NOMBRES DE DOMINIO DE TERCER NIVEL

El Plan Nacional ha creado los indicativos .com.es, nom.es, org.es, gob.es y edu.es, bajo los que se pueden registrar nombres de dominio de tercer nivel. Esto permitirá a los solicitantes ubicarse en un espacio adecuado a su actividad o al tipo de entidad que constituyan.

Un ejemplo de este tipo de dominio sería: www.adstudio.com.es

## 7.3. REGISTRO DE UN NOMBRE DE DOMINIO

Antes de registrar un nombre de dominio específico para cualquier empresa es necesario tener claro que el nombre de dominio a registrar será de segundo nivel, bajo un nombre de dominio de primer nivel, y que, se debe diferenciar el nombre de dominio de primer nivel, bajo el que se quiere registrar el de segundo nivel, si se trata de un nombre genérico o territorial.

### 7.3.1. REGISTRO DE UN NOMBRE DE DOMINIO BAJO UN gTLD

Si se quiere registrar un nombre de dominio genérico gTLD, en este caso el .com y el .net para la empresa ADstudio, se deben seguir los siguientes pasos:

1. Seleccionar algún registrador acreditado por la ICANN (Internet Corporation for Assigned Names and Numbers), que es la entidad encargada de la gestión de los gTLD. Para visualizar los registradores acreditados por la ICANN, se puede acceder desde su página web (www.icann.org) y a su vez, en el apartado que indica *Registrars*, que nos llevará a otra pantalla donde podremos acceder al link *Listing Registrars*, con un listado sobre los registradores, descripción y país en el que esta establecido.
2. Si se accede a la página web de uno de los registradores acreditados, se tendrá que rellenar un impreso de solicitud de registro del nombre de dominio, además de abonar las tasas del mismo. En un principio, no se controlan los datos del solicitante del registrador, por lo que se establece el principio de *First come, first served*.
3. El registro del nombre de dominio estaría listo ya y habría que esperar confirmación de la solicitud por parte de la entidad.

Bastaría con seguir este procedimiento para registrar el dominio de la empresa ADstudio, donde habría que consultar si este dominio esta ya registrado por alguna otra empresa. Si esta libre, se procedería al registro.

### 7.3.2. REGISTRO DE UN NOMBRE DE DOMINIO BAJO EL ccTLD <<.es>>

El registro de los nombres de dominio ccTLD se debe hacer a través del órgano asignado para cada país por parte del InterNIC. En España, dicho órgano es la entidad ES-NIC para la designación de nombres de dominio .es.

Mediante la Resolución de la Secretaría General de Telecomunicaciones de 10 de febrero de 200, se le traspaso a la entidad pública empresarial Red.es la actividad de registro de nombres de dominio ccTLD para .es.

También existen los agentes registradores acreditados que actúan en nombre de Red.es y que desarrollan su actividad en régimen de libre competencia y la asignación de nombres de dominio se realizan por orden cronológico desde su recepción. Al igual que con la ICANN, desde la página web de ES-NIC se puede visualizar el listado de registradores.

REGISTRO DE NOMBRES DE DOMINIO DE SEGUNDO NIVEL BAJO <<.es>>

A. Se asignan por orden cronológico, después de ser validada la sintaxis y que no este incluida en la lista de términos prohibidos o reservados.

B. Podrán solicitar un nombre de dominio

- Personas físicas
- Personas jurídicas
- Entidades sin personalidad

Podrán registrar un dominio .es los que tengan intereses o mantengan vínculos con España como residentes o establecidos en España, quieran dirigir sus servicios al mercado español u ofrecer información, productos o servicios que estén vinculados cultural, histórica o socialmente con España.

C. Limitaciones que hay que tener en cuenta para la asignación del nombre de dominio:

• Cuando coincide el nombre de dominio de segundo nivel con alguno del primero y esto pueda crear confusión, como por ejemplo “com.org”.

•No se podrán utilizar los términos que se incluyan en la lista de términos prohibidos.

•Además existe una lista de términos reservados que no podrán ser utilizados libremente.

REGISTRO DE NOMBRES DE DOMINIO DE TERCER NIVEL BAJO <<.es>>

También se realiza por orden cronológico de solicitud y dependiendo del nombre de dominio que se utilice, tendrá unas características especiales:

- .com.es: personas físicas, jurídicas o entidades sin personalidad que tengan intereses o mantengan vínculos con España.
- .nom.es: personas físicas que tengan intereses o mantengan vínculos con España.
- .org.es: entidades sin ánimo de lucro que tengan intereses o mantengan vínculos con España.
- gob.es: administraciones públicas españolas y entidades de Derecho Público.
- .edu.es: entidades con reconocimiento oficial que realicen funciones relacionadas con la enseñanza o investigación en España.

NORMAS DE SINTAXIS

Existen establecidas unas normas de sintaxis que se comprobarán de forma previa a la asignación del nombre de dominio.

- Los únicos caracteres que son válidos para un nombre de dominio son las letras de los alfabetos de las lenguas españolas, los dígitos del 0 al 9 y el guión (-).
- El primer y el último carácter del nombre de dominio no podrá ser un guión.

- Los cuatro primeros caracteres no podrán ser xn--
- Longitud mínima de un nombre de dominio de segundo nivel son tres caracteres.
- Longitud mínima de un nombre de dominio de tercer nivel son dos caracteres.
- La longitud máxima para los nombres de dominio de segundo y tercer nivel es 63 caracteres.
- No se pueden incluir términos o expresiones que resulten contrarios a la Ley, a la moral y al orden público.
- Tampoco se pueden incluir los que vulneren los derechos de las personas físicas, propiedad industrial, honor, intimidad y buen nombre.
- Los nombres de dominio compuestos por un nombre y apellido deberán tener relación directa con el beneficiario del nombre de dominio.

El nombre de dominio de la empresa ADstudio cumple con todas las normas de sintaxis que se exigen para su registro.

DERECHOS Y OBLIGACIONES

Los derechos que la posesión de un nombre de dominio .es establecen a sus titulares son:

- Derecho a utilizar el nombre de dominio a efectos de direccionamiento en el sistema de nombres de dominio.
- Derecho a la continuidad y calidad del servicio que presta la autoridad de asignación.

Los deberes que han de cumplir los que posean un nombre de dominio .es, son:

- Facilitar sus datos identificativos siendo responsables de su veracidad y exactitud.
- Respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del dominio.

- Informar a la autoridad de asignación de las modificaciones que se produzcan en los datos del registro del nombre de dominio.

### TRANSMISIÓN DE LOS NOMBRES DE DOMINIO

El Plan Nacional permite que se realice una transmisión voluntario del derecho de utilización de un nombre de dominio, siempre que se cumplan las normas previstas. Para ello se necesita contar con la aprobación del antiguo titular del nombre dominio y que sea comunicada a la autoridad de asignación con carácter previo a la correspondiente modificación de los datos de registro del nombre de dominio.

Por lo tanto, si llegase el momento en el que ADstudio desee transmitir su nombre de dominio, lo podrá realizar.

## 7.4. NOMBRES DE DOMINIO Y PROPIEDAD INDUSTRIAL: CONFLICTOS

Los nombres de dominio tienen una doble función, ser la dirección en la red (la forma de localizar un sitio) y también ser el identificativo en Internet para la identificación de la empresa o marcas de sus productos o servicios. Es normal que las empresas elijan una denominación y la protejan como marca, nombre comercial, denominación social o nombre de dominio para utilizarlos como imagen y donde apoyar sus inversiones publicitarias. Pero el registro de nombres de dominio, a diferencia de las marcas, no es competencia de la Oficina Española de Patentes y Marcas (reguladora de la Propiedad Industrial), sino que se rige por su propia legislación nacional e internacional y todos los conflictos que pudieran surgir tienen que presentarse ante organismos internacionales de arbitraje como la OMPI-WIPO o los tribunales.

Uno de los principales problemas es la utilización como propio de un nombre de dominio de una marca ajena que este registrada. una marca notoria sería la conocida por el sector del público al que se destinan sus productos o servicios. Si la marca esta registrada se protege por encima del principio de especialidad según su grado de notoriedad, y en el caso de no estarlo, se faculta a su titular no sólo a ejercitar la correspondiente acción de nulidad, sino además a presentar oposición al registro en la vía administrativa.

La fama o importancia de las marcas puede ocasionar estos problemas, el deseo de lucrarse de un nombre de una marca comercial o servicio mediante la imitación o simplemente utilizando su nombre, beneficiándose de la reputación adquirida.

Según el Informe Final sobre nombres de dominio de la OMPI, muchas personas han llevado a cabo prácticas “predatorias y parasitarias” sin ningún tipo de derechos y propone, para terminar con este tipo de problema, que las marcas prohiban a terceros registrar su marca como nombre de dominio. Otro problema radica en que los “ciberocupadores” suelen registrar marcas con nombres parecidos a los de la empresa.

Debido a la dificultad al aplicar la legislación en cada caso de conflicto, la ICANN estableció un procedimiento a seguir para poder resolver todo tipo de controversias, por el que si una marca se viese afectada por este problema tendría que sostener que:

- El demandado tiene un nombre de dominio idéntico o similar que lleva a la confusión con respeto a la marca del demandante.
- El demandado no tiene derechos o intereses legítimos sobre el nombre de dominio
- El demandado utiliza el nombre de dominio a mala fe

Si el demandante no es capaz de demostrar ni uno solo de estos tres aspectos, el problema no podría ser resuelto y el demandado seguiría utilizando su nombre de dominio.

## 7.5. PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

Debido a los problemas entre nombres de dominio y determinados derechos y las dificultades de aplicar las legislaciones nacionales en este ámbito, la entidad reguladora de nombres de dominio ICANN ha promulgado una serie de normas y procedimientos para la resolución de conflictos.

### 7.5.1. PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS DE LA ICANN

La ICANN aprobó el 26 de agosto de 1999 una Política Uniforme de Solución de Controversias en materia de nombres de dominio, que se puede encontrar en la pagina web en inglés y una traducción al español en la página web de la OMPI. Se trata de procedimientos de solución de controversias relacionadas con los nombres de dominio de primer nivel genéricos.

Esto será necesario para si por ejemplo ADstudio necesitase ocupar un nombre de dominio que esta ocupado ya por otra empresa.

INICIACIÓN DEL PROCEDIMIENTO

Para iniciar un procedimiento de recuperación de nombre de dominio, se deberá presentar una demanda a cualquiera de los siguientes proveedores aprobados por la ICANN:

- Centro de Meditación y Arbitraje de la OMPI. Es el que mayor resolución de conflictos resuelve y que además se recomienda utilizar a ADstudio.
- Foro Nacional de Arbitraje - FNA
- Asian Domain Name Dispute Resolution Centre - ADNDRC
- Instituto para la Resolución de Disputas - IRD

La manera de presentar las solicitudes es electrónica y se deberá especificar la forma preferida para efectuar las comunicaciones con la empresa demandante.

El demandado tendrá que someterse a un procedimiento administrativo en caso de que el demandante sostenga ante el proveedor competente que:

- El demandado posee un nombre de dominio idéntico o similar hasta el punto de crear confusión con respecto a una marca de productos o servicios sobre la que la empresa demandante tiene derechos.
- El demandado no tiene derechos o intereses legítimos respecto del nombre de dominio.
- El demandado posee un nombre de dominio que ha sido registrado y se utiliza de mala fe.

### LEGISLACIÓN ADICIONAL

Si las dos partes son del mismo país se puede aplicar por parte del árbitro que lleva la controversia las normas del país para resolverla.

### PRUEBAS

La carga de las pruebas estará siempre del lado del demandante, y tendrá que demostrar todos y cada uno de los tres puntos mencionados anteriormente. Si no es capaz de probar uno solo de ellos, el dominio seguirá perteneciendo al demandado.

### PRUEBAS DEL REGISTRO Y UTILIZACIÓN DE MALA FE

Para probar el registro y utilización de un nombre de dominio de mala fe, se deberán probar las siguientes circunstancias (sola de ellas es suficiente, pero se deberán de mostrar tanto el momento del registro como de la utilización del nombre de dominio):

- El demandado ha registrado el nombre de dominio por el que ha tenido lugar la controversia con el fin de venderlo, alquilarlo o cederlo a la empresa que es el titular de la marca de servicios o a un competidor de la empresa, por un valor que es mayor que los costes relacionados directamente con el nombre de dominio.
- El demandado ha registrado el nombre de dominio por el que ha tenido lugar la controversia con el objetivo de impedir que la empresa demandante refleje su marca en un nombre de dominio.

- El demandado ha registrado el nombre de dominio por el que ha tenido lugar la controversia con el fin de perturbar la actividad comercial de la empresa demandante.
- El demandado utiliza el nombre de dominio registrado con el fin de intentar de manera intencionada atraer, con ánimo de lucro a usuarios de Internet creando la posibilidad de que exista confusión con la marca de la empresa demandante.

### CÓMO DEMOSTRAR SUS DERECHOS Y SUS LEGÍTIMOS INTERESES SOBRE EL NOMBRE DE DOMINIO AL RESPONDER UNA DEMANDA

El demandado podrá mostrar no obstante su interés legítimo sobre el nombre de dominio por el que ha sido demandado. Con probar solamente uno de los siguientes supuestos, se probará como que el demandado demuestra su interés legítimo sobre el nombre de dominio y no habrá posibilidad de traspaso al demandante.

- Antes de haber recibido cualquier aviso de la controversia, el demandado ha utilizado el nombre de dominio, o ha efectuado preparativos demostrables para su utilización, en relación con una oferta de buena fe de productos o servicios.
- El demandado ha sido conocido corrientemente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios.
- El demandado hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera inequívoca o de empeñar el buen nombre de la marca de productos o servicios en cuestión.

### RESOLUCIÓN Y COSTES DE PROCEDIMIENTO

Los costes del procedimiento siempre serán por parte del demandante. Los únicas tres costes que pueden ser de parte del demandado es cuando quiera que se amplíe el número de árbitros a tres, por lo que pagará la diferencia.

El órgano administrativo será quien decida acerca del nombre de dominio:

- Que siga utilizando el demandado, cuando entienda que no se han cumplido los tres puntos señalados
- Que pase al demandante, cuando entienda que el demandado no tiene derecho a ello y que lo registró y utilizó de mala fe
- Que se cancele el nombre de dominio, cuando pueda resultar ofensivo para el demandante

RECURSOS

Contra la resolución del órgano administrativo se pueden interponer recursos antes de iniciar el procedimiento administrativo o después de la conclusión, de forma que el registrador esperará diez días hábiles a conocer si se ha iniciado alguna vía judicial de resolución de esa controversia antes de ejecutar la decisión que hayan tomado los expertos.

ADSTUDIO

Este será el procedimiento que la empresa ADstudio tendría que llevar a cabo en el caso de que al intentar registrar su nombre de dominio de primer nivel genérico (ha registrado .com y .net) hubiera tenido problemas con alguna otra empresa o particular. Como al intentar registrar su dominio no ha tenido problemas, no es necesario a priori llevar a cabo un procedimiento parecido.

### 7.5.2. PROCEDIMIENTO DE RESOLUCIÓN DE CONTROVERSIAS EN UN DOMINIO <<.es>>

En caso de que surgieran problemas acerca de los intereses legítimos de un nombre de dominio .es, como por ejemplo que al intentar registrar una empresa, en este caso ADstudio, su nombre de dominio ya estuviera registrado por una tercera persona pero esta desea recuperarlo, se debería llevar a cabo un procedimiento extrajudicial. La autoridad encargada de ello es Red.es, la Autoridad de Asignación de nombres de dominio bajo .es. Este sistema de resolución de controversias viene reflejado en la Instrucción del Director General de la entidad pública empresarial Red.es por la que

se establece el Reglamento del procedimiento de resolución extrajudicial de conflictos para nombres de dominio bajo el código de país correspondiente a España .es.

El procedimiento se llevará a cabo castellano si ambas partes están de acuerdo, aunque pueden realizarse en otro idioma, y la empresa demandante será la responsable del pago de tarifas y honorarios del procedimiento de resolución de la OMPI (en torno a unos 1400 euros).

DEMANDA

Primero quien quiera recuperar su nombre de dominio bajo .es deberá enviar tres copias en formato impreso o electrónico de la demanda a la OMPI y también una copia a Red.es.

En la demanda se deberá incluir la siguiente información:

- Nombre de dominio
- Datos del demandante
    - Nombre
    - Dirección postal
    - Correo electrónico
    - Número de teléfono
    - FAX
- Forma de comunicación
- Datos del demandado
    - Nombre
    - Información conocida del demandante (como dirección posta, correo electrónico, teléfono etc)
- Agente registrador del demandado
- Derechos previos del demandante (como marca registrada o seudónimo notorio)
- Pruebas de registro o uso del nombre de dominio de mala fe

- Cuando el demandado haya registrado el nombre o adquirido el nombre de dominio con el fin de vender, alquilar o ceder por cualquier título el registro del nombre de dominio al demandante que posee los derechos previos sobre el nombre de dominio o a un competidor de este, por un valor mayor que el adecuado para el registro del nombre de dominio.

- Cuando el demandado haya registrado el nombre de dominio a fin de impedir que el que posee los derechos legítimos utilice los mismos a través del nombre de dominio, siempre y cuando el demandado haya desarrollado una actividad de esa índole.

- Cuando el demandando haya registrado el nombre de dominio con el objetivo de perturbar la actividad comercial de un competidor.

- Cuando el demandado al utilizar el nombre de dominio ha intentado atraer con ánimo de lucro usuario de Internet a su pagina web o a cualquier otra creando la posibilidad que exista confusión con la identidad del Demandante en cuanto a la fuente, patrocinio, afiliación o promoción de su página web o de un producto o servicio que figure en su pagina web.

- El demandado haya realizado actos similares a los anteriores en perjuicio del demandante.

- Argumentación registro abusivo (tiene que tener una extensión menor a 5000 palabras).

- Objeto de la demanda:

    - Transmisión del nombre de dominio

    - Cancelación

- Procedimientos judiciales que se hayan comenzado sobre el nombre de dominio

- Declaración responsable de información leal

- Declaración de no reclamación

BLOQUEO DEL NOMBRE DE DOMINIO

Una vez recibida la demanda y verificada, se inhabilita el nombre de dominio para realizar la trasferencia de la titularidad del nombre de dominio a un tercero, para dar de baja al nombre de dominio o para la modificación de datos de registro.

NOTIFICACIÓN DE LA DEMANDAD AL DEMANDADO

Al demandado se le notificará la demandada al inicio del procedimiento. La notificación de la demandad al demandado inicia el procedimiento.

El proveedor, que puede ser la OMPI, envía una demanda al demandado en un plazo máximo de 5 días después del bloqueo y el pago.

En caso de que existan defectos subsanables en la demanda, se dispondrán 5 días para poder arreglarlos, para que no se desestime la demanda.

CONTESTACIÓN A LA DEMANDA

En un plazo de 20 días el demandado enviará un escrito de contestación en formato impreso o electrónico a la OMPI y al demandante, que deberá incluir la siguiente información:

- Respuesta de las declaraciones y alegaciones de la demanda, incluyendo las razones así como pruebas documentales por las que se deben mantener el nombre de dominio. Tiene que tener una extensión máxima de 5000 palabras
- Datos del demandado
- Forma de comunicación
- Procedimientos judiciales que se hayan comenzado o terminado sobre el nombre de dominio
- Declaración responsable de información leal

Si el demandado no respondiera, la OMPI resolverá la controversia basándose exclusivamente en la demanda.

### NOMBRAMIENTO DEL EXPERTO Y PLAZO DE RESOLUCIÓN

La OMPI nombra a un experto en un plazo de 5 días desde la recepción de la contestación de la demanda, le remitirá el expediente y notificará el nombre y la dirección electrónica de contacto del experto al demandante, al demandado y a Red.es.

En caso de que la OMPI tenga dudas justificables sobre la incapacidad e independencia del experto, o si el demandante y demandado lo solicitan en el plazo de 5 días desde su nombramiento, se sustituirá el experto.

### RESOLUCIÓN

El experto enviará a la OMPI tres ejemplares firmados y una versión electrónica de la resolución en el plazo de 15 días desde la recepción del escrito de contestación.

La OMPI enviará una copia firmada de la decisión al demandado y al demandante y una copia a Red.es y a los agentes registradores de cada una de las partes.

Red.es publicará la resolución del experto en la página web.

Red.es en un plazo de 15 días ejecuta la decisión, a no ser que alguna de las partes inicie un procedimiento judicial y se lo notifique a Red.es, que suspenderá la ejecución de la decisión.

# Contratación Informática

## 8.1. INTRODUCCIÓN A LOS CONTRATOS INFORMÁTICOS

Ante el desconocimiento general por parte de los usuarios del negocio en el ámbito de Internet, deben existir unas medidas para la gestión de los recursos y las actividades de manera que no solamente se rija por el principio de la autonomía de la voluntad de los contratantes.

Los contratos informáticos están compuestos por elementos dispares de varios tipos de contratos y voluntades de las partes por llegar a un justo acuerdo y tener éxito en la Sociedad de la Información en la que estamos inmersos.

En la sociedad actual la gran mayoría de las empresas precisan de ciertos elementos que las obligan a realizar contratación informática, como puede ser una página web, aplicaciones o programas informáticos para la gestión de la empresa, licencias de uso de programas o bases de datos.

Todas estas necesidades también las tiene ADstudio para la labor de su actividad. Además de necesitar programas o aplicaciones informáticas, también se necesitan equipos y otros elementos físicos y el mantenimiento tanto del hardware como del software.

CONTRATACIÓN INFORMÁTICA

Podemos decir que un contrato existe “desde que una o varias personas consienten en obligarse respecto de otra u otras, a dar alguna cosa o prestar algún servicio[54]”. El problema que caracteriza a un contrato informático es que son atípicos y carecen de regularización específica, por lo que no es válido solamente con la voluntad de las partes que la integran, sino que se suelen establecer pactos, cláusulas y condiciones, siempre que no sean contrarias a las leyes, la moral o el orden público.

Los sujetos de un contrato informático serán el proveedor del bien o del servicio informático prestado y por otro lado el usuario, que sería en este caso ADstudio. Uno de los principales problemas que un contrato informático es que ambos sujetos no se encuentran en la misma posición de conocimiento, por lo que puede existir por parte del usuario de cierta inseguridad jurídica. Si el

[54] Definición extraída del Código Civil

usuario es un gran desconocedor de la informática, se encuentra en una situación de desventaja. Es frecuente que se firmen contratos con grandes empresas del sector informático sin que el usuario conozca realmente que esta contratando, en que condiciones y no saber siquiera si es lo más apropiado para su empresa. Además como los contratos informáticos poseen una gran pluralidad de prestaciones, los hacen de carácter técnico.

Es necesario y recomendable tener en cuenta la normativa sobre Protección de los Consumidores, en particular el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios[55], así como otras leyes complementarias.

[55] Publicado en el Boletín Oficial del Estado número 287, del 30 de noviembre

## 8.2. TIPOS DE CONTRATO

Dentro de la contratación informática existen diferentes tipos de contratos que serán necesario estudiar para poder elegir cual es el más adecuado para las exigencias de la empresa. Los contratos informáticos pueden clasificarse por el objeto y también por el negocio jurídico que les confiere.

| TIPO DE CONTRATO | OBJETO DEL CONTRATO |
|---|---|
| VENTA | HARDWARE |
| ARRENDAMIENTO FINANCIERO - LEASING | HARDWARE |
| ALQUILER | HARDWARE Y MANTENIMIENTO |
| OPCIÓN A COMPRA | HARDWARE |
| MANTENIMIENTO | MANTENIMIENTO HARDWARE Y SOFTWARE |
| PRESTACIÓN DE SERVICIOS | SOFTWARE Y MANTENIMIENTO |
| ARRENDAMIENTO DE OBRA | SOFTWARE E INSTALACIÓN LLAVE EN MANO |
| PRÉSTAMO | HARDWARE |
| DEPÓSITO | HARDWARE |

### 8.2.1. POR EL OBJETO

Atendiendo al objeto del contrato, se pueden obtener cuatro tipos de contratos a su vez:

- Contratos de hardware: es el tipo de contrato por el que se contrata al proveedor informático todo aquello que forma parte del equipo físico, de comunicaciones u otros elementos auxiliares necesarios para el funcionamiento del sistema, es decir, de hardware.
- Contratos de software: aquí podemos diferenciar a su vez si se trata de:

  - Software de base o de sistema, o software de utilidad: responden a unas características generales que son las del propio sistema o utilidad para la que sirve. El producto ya esta conformado de antemano.
  - Software de aplicación o usuario: responde a las necesidades particulares del propio usuario que lo contrato, de acuerdo a esas necesidades. Estas necesidades quedan reflejadas en el contrato.
- Contratos de instalación llave en mano: incluyen tanto el hardware como el software, así como el mantenimiento y la formación a usuarios.
- Contratos de servicios auxiliares o complementarios: son contratos de servicios, y aquí se puede incluir por ejemplo el mantenimiento de equipos o la formación al personal de la empresa.

Lo más apropiado para una empresa que no esta especializada en productos o servicios informáticos es efectuar un contrato de instalación llave en mano con un proveedor informático, donde se fije claramente el resultado que la empresa quiere obtener, de forma que la responsabilidad y riesgo son del proveedor. Este se compromete a entregar tanto el hardware necesario (equipos informáticos, impresoras, escáneres etc.) como los programas y documentación.

Es el tipo de contrato que se recomienda para una empresa como ADstudio, que no esta especializada en productos o servicios informáticos y no tiene un departamento informático capaz de hacerlo de forma independiente. Con este tipo de contrato, se abaratarían los costes ya que no se contrata todo de forma independiente a varios suministradores, sino que se realiza en paquete con un único proveedor.

### LICENCIAS DE USO

Entre los tipos de software, podemos diferenciar software de medida y software de masas:

- Software de medida: el desarrollo se encarga y se realiza específicamente para la empresa usuaria, de acuerdo a su modelo de negocio, actividad y necesidades. El problema de este tipo de software es el elevado precio que supone que realicen software a medida del usuario.

- Software de masas: es el software ya desarrollado y existente en el mercado, aunque es más difícil que se ajusten por completo a las necesidades específicas de una empresa o usuario. Estos se basan en las licencias de uso.

Cuando se adquiere software de masas se tiene que firmar un contrato de licencia de uso por lo que el titular de los derechos del programa los cede al usuario conservando la propiedad del software. Este tipo de contratos existen para los dos tipos de software, tanto para los que pueden ser personalizados (software a medida) como los que no (software de masas), que guardan las mismas características y condiciones para todos los usuarios.

Existirán requerimientos específicos por parte de ADstudio para la adquisición de software a medida, como para la gestión de la empresa o la página web, pero se tendrán que adquirir licencias de uso de programas ofimáticos y de diseño publicitario, ya que es la principal actividad de la empresa.

### 8.2.1. POR EL NEGOCIO JURÍDICO

Los contratos informáticos pueden ser clasificados de acuerdo con el objeto, pero también de acuerdo con el negocio jurídico, que pueden ser:

- De venta: el proveedor entrega un producto al usuario por un precio cierto.
- De arrendamiento financiero o leasing: se trata de un contrato mercantil por el que una de las partes, que va a ser la que preste el servicio o producto, se obliga a adquirirlo en concreto y ceder su uso a la otra parte por un período de tiempo y precio fijado, basado en cuotas tasadas para la amortización del bien. Una vez finalizado el contrato, el usuario deberá devolver el bien a la empresa suministradora o bien comprarlo por un precio fijado.
- De arrendamiento: el arrendamiento de bienes informáticos esta regulado por el Código Civil y esta caracterizado porque el proveedor se obliga a dar al usuario el uso de un bien determinado durante un tiempo y por un precio fijado.

- De opción a compra: es un contrato atípico en el que se deben cumplir tres requisitos:
    - la decisión del optante debe ser unilateral de la realización de la opción a compra
    - el precio de la compraventa debe quedar perfectamente señalado para el caso de que el optante decida acceder
    - el plazo del ejercicio de la opción de compra debe quedar determinado con claridad en el acuerdo.
- De mantenimiento: se puede aplicar tanto para equipos como para programas, e incluso para de mantenimiento integral en el que se puede incluir un servicio de información, asesoramiento o consulta.
- De prestación de servicios: una parte se obliga a prestarle unos determinados servicios a la otra y estos pueden ser de análisis, especificaciones, horas máquina, tiempo compartido, programas etc., con independencia del resultado que se obtenga mediante esta prestación.
- De arrendamiento de obra: una parte se compromete a ejecutar una obra (el prestador/ suministrador) mientras que la otra a realizar una contraprestación en pago por la obra realizada. El contrato obliga a terminar una obra determinada, independientemente del trabajo o medios empleados.
- De préstamo: la parte usuaria utiliza un bien por un tiempo determinado y lo devuelve al propietario pasado el tiempo fijado en el contrato.
- De depósito: consistente cuando una persona recibe un bien informático con la obligación de guardarlo y restituirlo, en el que el depositario tendrá derecho a exigir retribución por el depósito, al tratarse de un depósito mercantil, salvo pacto en contrario, con las obligaciones para el depositario de conservación del bien informático.

Debido a que el contrato atendiendo al objeto más apropiado para ADstudio es el contrato de llave en mano, se recomienda utilizar el contrato de arrendamiento de obra, por lo que la parte contratada

se compromete a realizar una obra concreta, que es la instalación de los equipos y programas necesarios, así como toda la documentación y formación necesaria en la empresa, independientemente del coste que esto requiera para la empresa contratada.

## 8.3. FASES DE UN CONTRATO

En el caso de que una empresa realice un contrato de software, es necesario tener presente las distintas fases que marcan un tipo de contrato de estas características, por lo que lo analizaremos para que ADstudio tenga presente el modelo. Lo podemos dividir en tres fases, la fase precontractual, la fase contractual y el desarrollo y ejecución del contrato.

### 8.3.1. FASE PRECONTRACTUAL

Es muy importante que en esta fase, por muchos conocimientos informáticos que se tengan, la empresa que vaya a proveer a la empresa usuaria realice un asesoramiento e informe acerca de sus productos, servicios y sus utilidades.

Esta fase puede implicar que la negociación requiera de la intervención de abogados y técnicos informáticos para la redacción del contrato.

Otra de las obligaciones que tiene la empresa proveedora es la del cumplimiento del plazo, que no consiste solamente en la entrega de un programa informático, sino que dependiendo del tipo de prestación que se este realizando, también la implementación total de la aplicación, pruebas de aceptación y depuraciones que garanticen su funcionamiento (todo debe estar perfectamente especificado en el contrato).

El proveedor tendrá que proporcionar todos los conocimientos técnicos y operativos necesarios, la documentación precisa y formación si fuese requerida para la perfecta utilización del programa contratado.

En el contrato también se deberán fijar las responsabilidades de cada una de las partes y su interrelación en la consecución del cumplimiento del contrato.

Si se trata de un contrato en la que se esperan resultados, el incumplimiento por parte del proveedor significará que no obtendrá ningún beneficio de ello.

### 8.3.2. FASE CONTRACTUAL

En esta fase nos encontramos con diferentes partes, la parte expositiva, las cláusulas o pactos y los anexos:

PARTE EXPOSITIVA

En el contrato se deberán fijar los intereses de ambas partes, con las necesidades de la parte contratante y la oferta de la parte contractual, dejando de manera clara lo que ofrece una parte y lo que acepta la otra. Debe existir un compromiso de colaboración entre ambas partes, para que se pueda respetar el contrato y se sigan unas directrices.

CLÁUSULAS O PACTOS

Puesto que los contratos hacen que dos partes cedan por el beneficio de ambas, es necesario que todo se realice en un entorno de seguridad, por lo que es necesario establecer unas cláusulas o pactos como las siguientes:

- Objeto del contrato
- Precio y forma de pago: se deben especificar las fases de entrega y el precio a pagar por la parte usuaria, así como la moneda utilizada para ello.
- Entrega: puede ser entrega única o parcial. Es el lugar donde se deben incluir penalizaciones en caso de incumplir con lo establecido en el contrato en cuento a las entregas en tiempo pactado.
- Calidad:
    - Batería de pruebas
    - Plazo para que el cliente verifique el software
    - Plazo para que el programador realice las correcciones
    - El programador no puede garantizar que el programa esté exento de errores

- Garantía: periodo de tiempo por el que la empresa que ha realizado la programación de un programa específico por ejemplo tiene para poder subsanar los errores que se produzcan en el funcionamiento normal del programa. Se debe especificar el inicio de la garantía, el plazo de duración de la garantía y los límites de la misma. También es recomendable establecer unas garantías de compatibilidad y de modularidad y posibilidad de ampliación, que entran dentro de los derechos de explotación del programa creado.

- Mantenimiento: duración pactada del mantenimiento del producto, lugar en el que se presta ese servicio, la forma de pago del mismo (puede ir o no incluido en el precio), el tiempo de respuesta estipulado y el responsable del servicio de mantenimiento.

- Propiedad del programa: si no se establece lo contrario, tanto los derechos morales como los patrimoniales del programa creado serán del creador. Es recomendable para ello que se pacte un cláusula para la cesión de los derechos patrimoniales, que deberá ir acompañada del código fuente del programa creado, por si en un futuro se decidiera modificar el programa.

- Pacto de confidencialidad: el proveedor se compromete a guardar de manera confidencial la información que se le comunica para que pueda prestar el servicio. También se puede pactar por ejemplo la destrucción por parte del proveedor de los documentos que contengan información confidencial sobre el usuario.

- Pacto de exclusividad: esta cláusula puede ser pactada con el objetivo de que el programador no realice programas similares para otros.

- Resolución anticipada: este apartado sirve para recoger las causas por las que puede tener lugar una resolución anticipada y puede ser por incumplimiento de las obligaciones asumidas en virtud del contrato o por otras causas de resolución anticipada que las partes establezcan en el contrato.

- Prohibición de subarrendar: de acuerdo al Código Civil[56], el arrendatario podrá subarrendar en todo o en parte la cosa arrendada. Lo más seguro es que el proveedor establezca una cláusula de subarrendar.

[56] Artículo 1550 del Código Civil

- Sustitución del programa: modularidad lógica para poder adaptar cambios al programa que vayan apareciendo. Es frecuente que en muy poco plazo de tiempo el software que se adquiere quede obsoleto.
- Definición de términos o conceptos oscuros: en este apartado se pueden aclarar las partes o expresiones informáticas utilizadas que puedan resultar difíciles de entender a quien contrata los servicios de un proveedor y que puede llevar a diferentes interpretaciones.

Es frecuente que al adquirir programas informáticos se incluyan diferentes cláusulas en los contratos donde las empresas proveedores recortar responsabilidades perjudicando al usuario final, por lo que es necesario realizar bien una redacción del contrato de forma que no pueda uno perjudicar a otro en su beneficio.

ANEXOS

Es importante que los contratos informáticos vayan acompañados igualmente de anexos que contengan diferentes desarrollos de los elementos que contienen el contrato, que pueden ser por ejemplo:

- Especificaciones del sistema a contratar
- Especificaciones de los programas a desarrollar
- Pruebas de aceptación
- Resultados a obtener y como en este caso, formarán parte del propio objeto de contrato
- Análisis

## 8.4. EL OUTSOURCING INFORMÁTICO

Se trata de un proceso económico que ocurre cuando una empresa o entidad tiene una necesidad sobre un campo en especial, en este caso relacionado con los sistemas de información y comunicación, y contrata a otra empresa para esa gestión. Esta empresa esta especializada en ese área, y que se integra en la toma de decisiones y desarrollo de aplicaciones de la empresa contratante. El objetivo es la optimización de los resultados de la empresa, además del acceso a estos recursos y tecnologías.

Además, con esto la empresa reparte los costes y responsabilidades entre la entidad contratante y el proveedor de servicios de outsourcing.

El outsourcing se puede realizar de diferentes maneras, como en los locales de la propia entidad contratante (se conoce como "in-house") o en las instalaciones del proveedor (se denomina "off-site"). Es común que la externalización del contrato de outsourcing llegue hasta la transferencia de personas de una entidad a otra[57].

Es una de las posibilidades que se le podría presentar a ADstudio en caso de que necesitase que una empresa profesional gestionase sus servicios de información y comunicación.

[57] Sobre cuestiones de Derecho Laboral, esta contemplado Artículo 42 y 44 del Estatuto de Trabajadores, sobre la responsabilidad empresarial en caso de subcontrata de obras o servicios y sobre la sucesión de empresas.

# Pago Electrónico

## 9.1. INTRODUCCIÓN

El proceso de pago de una tienda virtual es un proceso complejo que va desde que el cliente va en busca del producto que desea, completa su pedido a través de la figura del "carrito de compra" que suelen tener las páginas web, solicita el pago y envío de los productos adquiridos, se hace la gestión del cobro por parte de la empresa y se efectúa el envío correspondiente.

Como la empresa ADstudio también esta enfocada al ámbito del negocio por Internet, se debe implementar un mecanismo de pago electrónico, ya que no sería adecuado proporcionar un mecanismo de contratación electrónica por Internet y que los clientes tuvieran que realizar un pago mediante un sistema no electrónico.

Este ámbito del Comercio Electrónico plantea un problema propio de un sistema de compra que no es presencial, el comprador debe tener garantía sobre calidad, cantidad y características de los bienes que adquiere, mientras que el vendedor debe tener garantía de pago, y la transacción debe tener un aceptable nivel de confidencialidad. Además es importante que tras la realización de un pago, nadie pueda suplantar la identidad del cliente para realizar otras compras en su nombre y a su cargo.

El Comercio Electrónico implica una operación de compra que esta estructurada en una serie de etapas, que siempre tienen lugar en una transacción de compra-venta por Internet.

## 9.2. SISTEMAS DE PAGO ELECTRÓNICO

Es frecuente que en el Comercio Electrónico se utilicen diferentes estrategias en torno a la forma de pago que se permite realizar. El pago electrónico es una de las barreras de éxito en el comercio electrónico, una barrera tanto tecnológica como psicológica. La desconfianza de los compradores a los sistemas de pago empleados a través de Internet, además del temor al fraude y su fiabilidad, retrasan el despegue del comercio electrónico.

Es importante que los sistemas de pago cumplan cinco requisitos básicos, que son:

- Autenticación: tanto el comprador y el vendedor, como el intermediario, deben poder comprobar mutuamente que son quienes dicen ser.
- Autorización: los agentes deben poder demostrar la autoridad para ofrecer, transferir o aceptar el pago.
- No repudio
- Integridad de los datos y protección de datos
- Atomicidad: si en cualquier momento cualquiera de los sistemas, tanto del comprador como del vendedor, detectasen cualquier anomalía, la transacción se cierra y no se realiza.

Los sistemas de pago más extendidos hoy en día para el intercambio electrónico son:

### 9.2.1. TARJETAS

El funcionamiento de las tarjetas como método de pago se basa en la autonomía de la voluntad y en la teoría general de obligaciones y contratos, ya que no existe legislación alguna relacionada. Las tarjetas electrónicas podrían definirse como el "documento mercantil, instrumental y electrónico, que permite a su titular, mediante compromiso contractual con el emisor, servir como documento de pago a la vez que beneficiarse de una línea de crédito limitada, que podrá utilizar en la compra de bienes o servicios en establecimientos adheridos al sistema, o en el acceso a cantidades limitadas de dinero en bancos o entidades financieras que hayan concertado el servicio[58]".

[58] Definición recogida del "Factbook Comercio Electrónico". Miguel Ángel Davara Rodriguez. 3ª Edición, Editorial Aranzadi.

Las características más importantes que presentan las tarjetas son:

- La tarjeta no pertenece al titular de la misma, sino a la entidad emisora que la emitió.
- Es un dispositivo de pago, prepago, disposición de efectivo o de identificación del titular.
- Se expide a favor del titular que es una persona física en todo momento.
- Posee un título impropio o título legitimación.

También, las tarjetas tienen una serie de funciones:

- Función identificativa
- Función de instrumento de pago
- Función de instrumento de crédito al consumo

### 9.2.2. MICROPAGOS

El micropago consiste en la utilización de cupones electrónicos que son proporcionados por el comerciante y que un intermediario de alguna forma hace llegar al cliente para que los utilice en los servicios que proporciona el vendedor, que normalmente son orientadas a transacciones comerciales repetitivas y de pequeño valor.

El objetivo de este pago es el de rentabilizar el pago electrónico realizado cuando el pago que se va a realizar tiene un valor muy pequeño con respecto a los gastos para realizar dicho pago.

### 9.2.3. CHEQUES ELECTRÓNICOS

Los cheques electrónicos son la transcripción de los cheques convencionales al ciberespacio. Normalmente deben ir acompañados de una firma electrónica. El consumidor envía una orden de pago al vendedor, que la presentará al banco emisor para autenticarla y cobrarla. Son utilizados para pagos de cantidades importantes y tienen un coste muy bajo. Deben incorporar al menos un número de serie único, fecha y hora de emisión, cantidad a pagar, información bancaria del portador y su firma.

### 9.2.4. MONEDEROS ELECTRÓNICOS

Los monederos electrónicos son tarjetas prepago que contienen un fondo de pago materializado en un chip que tienen incorporado y en el que se almacenan elementos o unidades de valor previamente añadidas con cargo a nuestra propia cuenta bancaria. El importe siempre es determinado, pudiendo su propietario ir gastando hasta que se agota.

No se trata de una tarjeta tradicional de plástico con banda magnética, sino que puede ser utilizada por canales que no requieran una presencia física, como Internet.

Las ventajas de este sistema es su accesibilidad a todos los públicos, además de que es importante para mantener el anonimato.

### 9.2.5. SERVICIOS INTERMEDIOS

La empresa que vaya a realizar una "tienda virtual", como ADstudio, puede implantar un sistema de pago basado en la confianza de un tercero que es el encargado de almacenar los datos de carácter personal del cliente y del prestador de servicios.

De este modo, el prestador de servicios no tiene el conocimiento de los datos bancarios de sus clientes, lo cuál presenta ventajas, ya que mejora la imagen de la empresa, como seria y fiable, y da confianza a los clientes.

### 9.2.6. OTROS SISTEMAS DE PAGO-E

Otros sistemas de pago electrónico que son empleados actualmente son:

- Contra reembolso: es el único en pago-e que implica la utilización de dinero en efectivo y que garantiza al cliente la entrega del producto antes del pago. Para el vendedor, las principales desventajas son la necesidad de recolectar el dinero físicamente y el retraso en el pago.
- Transferencia bancaria: consiste en pagar a la tienda efectuando un ingreso en su cuenta bancaria.
- Pagos a través del teléfono móvil: un ejemplo de pagos a través del móvil es la plataforma creada por 90 entidades financieras, tres operadoras de telefonía móvil y tres sociedades de pago de

España la plataforma Mobipay, con el objetivo de impulsar un mecanismo único de pago seguro mediante el teléfono.

- Cobro de servicios web por acceso: es uno de los modelos de cobro más directo en Internet, el sistema de pago de servicios prestados con cargo a cuentas telefónicas. Pueden ser con cuentas de valor añadido (número de teléfono que generan un ingreso para quien recibe la llamada), mediante modem o dialers o con mensajes SMS.

ADSTUDIO

Para ADstudio y su modelo de negocio, el sistema de pago más recomendado serían o bien el uso de tarjetas de crédito o débito en las transacciones que se realicen o bien utilizando algún servicio intermediario entre la empresa y el cliente, como puede ser empresas como Paypal. Este último sistema dará más confianza a los clientes al utilizar a un tercero de confianza para que guarde sus datos de carácter personal.

Además de decidir el método de pago, es importante garantizar un conjunto de medidas de seguridad que permitan una fiabilidad y seguridad a la hora de realizar tanto las transacciones comerciales por Internet, como en el almacenamiento de los datos bancarios de los clientes en el caso de usarse también el sistema de tarjetas de crédito o débito.

## 9.3. SEGURIDAD EN EL PAGO ELECTRÓNICO

Es evidente que Internet como un sistema para conectar unos servidores con otros y así poder compartir la información para los usuarios que lo deseen, puede por otra parte convertirse en una gran amenaza en seguridad a la hora de transferir los datos. Esto genera una gran desconfianza al usuario, además que otro de los vínculos comerciales tradicionales es conocer a la otra parte con la que se esta realizando un trato, y en muchas ocasiones en Internet se desconoce completamente.

Se pueden diferenciar tres etapas en la seguridad en Internet:

- Seguridad en la conexión: asegurarnos que la dirección a la que nos dirigimos corresponde realmente con la empresa a la que deseamos hacer el pedido.
- Seguridad en la transacción: no debe ser posible interceptar los datos que estemos transmitiendo durante la comunicación por la Red entre nuestro ordenador y el servidor de la tienda.
- Seguridad permanente: puesto que los datos personales quedan almacenados en las bases de datos de la empresa, se deben evitar los ataques o accesos no permitidos a estas bases de datos.

Para asegurar la transferencia de datos se utilizan algunos estándares o protocolos en Internet, además de la utilización de la firma electrónica. Los dos protocolos de seguridad más generalizados que existen son el protocolo SSL y el SET.

### 9.3.1. SSL - SECURE SOCKETS LAYERS

El protocolo de seguridad SSL fue creado por Marc Andreessen, el diseñador de Mosaic y Netscape. Actualmente todos los ordenadores están preparados para comunicarse con estos protocolos, y en especial, con el SSL, a través del protocolo https.

El protocolo SSL utiliza el método de cifrado asimétrico RSA. Su funcionamiento se basa en encriptar los datos que el usuario rellena en un formulario de una página web, y transferirlos por la red hasta el servidor de comercio electrónico, lo que imposibilita interceptarlos por un tercero.

Las empresas que acepten pagos mediante estos sistemas deben tener instalados un software de servidor seguro SSL, que puede ser obtenido en entidades como VeriSign. Además, deberá disponer de un par asimétrico de claves, certificadas por una autoridad. El comprador no necesitará ni claves ni certificados.

Cuando el usuario accede a una tienda virtual con SSL, se inicia automáticamente una fase de reconocimiento. El servidor envía su clave pública y su certificación, y el navegador del cliente recibe estos datos y se prepara para la comunicación con sistema de seguridad.

El usuario de forma totalmente transparente introduce los datos y los envía. El navegador codifica estos datos mediante clave simétrica. La función resumen de los datos y la clave simétrica son codificadas con la clave pública que acaba de recibir el vendedor. El resultado de estas operaciones realizadas es enviado al vendedor. De esta forma, los datos que ha proporcionado el cliente viajan a través de Internet encriptados, de forma que solamente el vendedor podrá desencriptarlos.

### 9.3.2. SET - SECURE ELECTRÓNIC TRANSACTION

SET es un protocolo de seguridad elaborado por iniciativa de VISA y MasterCard, al que se adhirieron un gran número de bancos y empresas de software de todo el mundo. Se preveía que en poco tiempo se generalizaría el uso de este tipo de protocolo, pero varios años después se puede observar que sigue sin generalizarse y los expertos ven poco futuro como principal sistema de seguridad.

Surgió con el objetivo de garantizar la autenticación de todas las partes implicadas en una transacción comercial, así como la confidencialidad e integridad ya que utiliza una infraestructura de clave pública (PKI). El proceso que utiliza sería:

- Se obtienen los certificados de cada entidad (emisora y adquiriente), del titular y del comerciante.
- Se instalan las aplicaciones.
- El titular recibe el certificado y la clave pública del comerciante, lo verifica y paga con la tarjeta para que lo que recibe la clave pública de la entidad adquiriente.

- El cliente envía un mensaje electrónico con su certificado al comercio en el que incluye la orden de pago firmado electrónicamente y cifrada.
- Al recibir la empresa el mensaje, verifica el certificado del titular y el pedido, para posteriormente expedir la petición de autorización al cliente.
- La entidad adquiriente recibe la transacción electrónica del comercio, descifra la orden de pago, y envía la entidad emisora, la solicitud de autorización de la operación, cuyo resultado reenvía al comerciante, que confirma la operación al titular y envía la mercancía.

### 9.3.3. DIFERENCIAS ENTRE SSL Y SET

Las principales diferencias entre ambos protocolos las podemos observar en el siguiente cuadro[59]:

| SET | SSL |
|---|---|
| Protocolo de seguridad | Protocolo de seguridad |
| Se trata de un protocolo multiparte | No es un protocolo multiparte |
| Autentica el servidor al que se conecta el usuario para efectuar la transacción | Autentica el servidor |
| Autentica la identidad del comprador | No se produce la autenticación del comprador |
| Autentica a otros terceros que intervienen en la transacción, como los bancos de las partes | No autentica al banco del comerciante, al no ser un producto multiparte |
| Hace uso de firmas electrónicas | No hace uso de firmas electrónicas |
| Garantiza el no repudio del envío entre las partes | No garantiza el repudio del envío del mensaje |
| Proporciona confidencialidad en la transmisión de datos mediante encriptación, entre todas las partes | Proporciona confidencialidad en la transmisión de datos mediante encriptación, pero sólo entre el usuario y el comerciante |

[59] Cuadro extraído del "Factbook Comercio Electrónico". Miguel Ángel Davara Rodriguez. 3ª Edición, Editorial Aranzadi.

| SET | SSL |
|---|---|
| La integridad queda garantizada a través de la firma electrónica | La integridad no queda garantizada, debido a que no se hace uso de firmas electrónicas |
| Resulta inadecuado para realizar un gran número de transacciones de poco valor | Es más apropiado para realizar diversas operaciones que impliquen pagos de poco valor, si bien debe considerarse la seguridad que proporciona el mismo |

ADSTUDIO

El sistema SSL tiene la gran ventaja de la absoluta transparencia para el usuario, que no necesita ningún tipo de software instalado ni conocimientos previos sobre el tema. Queda garantizada plenamente la identidad del vendedor y sólo él recibirá los datos, aunque presenta el inconveniente que no se puede garantizar la identidad del comprador, por lo que puede producirse el repudio en la transacción.

Se recomienda a ADstudio la utilización del protocolo de seguridad SSL en lugar del SET tanto para vender en Internet como para la realización de todas sus transacciones, de una manera segura y fiable.

Para que ADstudio pueda instalar un sistema SSL en un servidor, puede acudir a los servicios de empresas como VeriSign por ejemplo. Además de facilitar el certificado de seguridad SSL, estas empresas facilitan:

- el dominio al que se ha concedido el certificado de seguridad SSL. Además a través de ellos, los visitantes de un sitio web pueden comprobar que el dominio tiene realmente un certificado de seguridad y si esta en vigor.
- saber quién es el propietario del certificado. Esta comprobación aumenta la confianza del usuario en la web, ya que se puede conocer en cualquier momento que empresa real esta detrás de cada transacción comercial en Internet

- conocer la situación geográfica del propietario del dominio y el sitio web, factor también de importancia a la hora de dar confianza al usuario y potencial cliente.

Hoy por hoy, el protocolo SSL es el protocolo más utilizado por las empresas que venden en Internet y a pesar de todas sus deficiencias, es el más recomendable para todas las empresas que como ADstudio necesiten un sistema de seguridad a la hora de realizar sus transacciones comerciales por Internet.

# Fiscalidad Electrónica

## 10.1. INTRODUCCIÓN

El surgimiento de comercio electrónico ha ocasionado una nueva manera de llevar a cabo transacciones comerciales en un entorno internacional, y uno de los principales problemas observados por los Estados es la disminución de la recaudación de la factura fiscal por parte de los mismos.

Por ello, diversas organizaciones internacionales, conscientes de la relevancia del comercio electrónico y su desarrollo, han estado investigando de que forma regular la tributación. Entre estas destaca los elaborados por la Organización para la Cooperación y el Desarrollo Económico (OCDE).

Entre los principales factores sobre fiscalidad electrónica se plantea el problema de la localización de la actividad comercial, los inconvenientes a la hora de calificar las rentas logradas a través de este tipo de operaciones y la dificultad de control por parte de la administración tributaria[60].

[60] *La Fiscalidad del Comercio Electrónico*. Mireia García. VI Congreso Nacional de Usuarios de Internet. Madrid, Febrero de 2001.

## 10.2. PROBLEMAS Y PRINCIPIOS EN FISCALIDAD ELECTRÓNICA

Dependiendo del tipo de impuesto que se utilice, en el comercio electrónico se plantean diversos problemas, que se recogen en la siguiente tabla[61]:

| IMPOSICIÓN INDIRECTA | IMPOSICIÓN DIRECTA |
|---|---|
| Identificación y localización del sujeto pasivo | Calificación de la renta |
| Distinción entre entrega de bienes y prestación de servicios | Identificación y localización del perceptor de la renta |
| Localización del hecho imponible | Control de la renta (paraísos informáticos) |
| Gestión del impuesto y control de las transacciones | Jurisdicción competente: doble imposición o desimposición |

Ante este tipo de problemas planteados se necesitaba una reacción internacional con el desarrollo del comercio electrónico para adaptar los impuestos y no estrangular las nuevas formas de actuación empresarial. El punto de partida lo tomo la OCDE en Turku, Finlandia en 1997, y más tarde, en 1998, en la Conferencia Ministerial de Ottawa, donde se aprobó una Resolución conjunta en relación con las condiciones del sistema tributario del comercio electrónico.

La OCDE estableció unos principios básicos de la tributación del comercio electrónico:

- Neutralidad: la fiscalidad debe aspirar a asegurar la neutralidad fiscal entre las diferentes formas de comercio electrónico y las formas de correo convencional.
- Internacionalización: mínimo consenso internacional.
- Certeza, claridad y simplicidad: las reglas fiscales han de ser de fácil comprensión y sencilla aplicación, permitiendo a los contribuyentes conocer por anticipado las consecuencias fiscales de una transacción.
- Eficiencia: costes de cumplimentación y gestión deben ser mínimos tanto para el contribuyente como la Administración Tributaria.

[61] Extraída de la conferencia “Aproximación a la fiscalidad del comercio electrónico”, Borja López Pol y Diego Montoya Esteban, MAC TIC, Burgos, 27 de marzo de 2010.

- Efectividad y fidelidad
- Flexibilidad.

## 10.3. NORMATIVA

El 17 de enero de 2002 se publicó en el diario de las Comunidades Europeas (D.O.C.E.) la Directiva 2001/115/CE, aprobada el 20 de diciembre de 2001, por la que se modifica la Directiva 77/388/CEE con el fin de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido. Esta Directiva es conocida como la Directiva de Facturación y establece que las facturas transmitidas a través de medios electrónicos han de ser aceptadas por los Estados miembros en condición de que se garantice la autenticidad de su origen y la integridad de su contenido, mediante firma electrónica avanzada o mediante un intercambio de datos (EDI).

En España, tras la Directiva de Facturación de la Unión Europea, se desarrollo paralelamente la Ley de Servicios de la Sociedad de la Información (LSSI) y la normativa sobre la e-Factura, que determinarían que servicios estarían grabados físicamente y los formatos electrónicos para las facturas telemáticas.

De acuerdo con la LSSI, los servicios más relevantes que están grabados fiscalmente son:

- La contratación de bienes o servicios por vía electrónica que impliquen transacción comercial directa, tarjetas, transferencias etc.
- La organización y gestión de subastas por medio electrónicos o centros comerciales virtuales.
- La gestión de compras en red por grupos de personas.
- El suministro de información por vía telemática.
- El video bajo demanda, como servicio en el que el usuario puede seleccionar a través de la red tanto el programa deseado como el momento de su suministro y recepción.
- Los servicios prestados por medio de telefonía vocal, fax o télex.
- Los servicios que utilizan telefonía IP.
- El intercambio de información por medio de correo electrónico u otro medio de comunicación equivalente para fines de la actividad económica de quien lo utilizan, cuando suponga la venta de una información.

## 10.4. IMPOSICIÓN DIRECTA

Los impuestos que gravan el comercio electrónico son los mismos que gravan el comercio tradicional. Los impuestos de imposición directa para las empresas que realicen alguna actividad comercial en Internet serían:

- Impuesto sobre la Renta de las Personas Físicas (IRPF)
- Impuesto sobre Sociedades
- Impuesto sobre la renta de no residentes

De acuerdo con la Agencia Tributaria, las personas jurídicas que tengan residencia en territorio español como es el caso de ADstudio serán contribuyentes por el IRPF y el Impuesto sobre Sociedades, por lo que el Impuesto sobre la renta de no residentes no sería de aplicación.

De esta manera, los aspectos fiscales del comercio electrónico por ADstudio no tienen ninguna diferencia respecto a los que se derivan de su forma de comercio tradicional, por lo que estos impuestos deberán gravarse independientemente de la forma de comercio que realice ADstudio.

## 10.5. IMPOSICIÓN INDIRECTA

Los impuestos que recaen sobre las transacciones comerciales de bienes o servicios, ya sean electrónicas o mediante comercio tradicional, se ven afectadas por los impuesto de imposición indirecta, que son los que gravan el consumo.

El impuesto de imposición indirecta más importante que existe es el Impuesto sobre el Valor Añadido - IVA. El tipo impositivo actual es desde el 1 de julio de 2010 del 18% para tasas normales (anteriormente era del 16%).

Las reglas generales sobre la imposición del IVA dependiendo de la localización de las operaciones difieren de:

- Entrega de bienes: IVA del lugar de puesta a disposición del bien del adquiriente o de inicio del transporte.
- Prestaciones de servicios:
    - Business to Business (B2B): el IVA que se grava es el del país donde el receptor tiene su sede
    - Business to Consumer (B2C): el IVA que se grava es el del lugar donde el prestador de servicios tenga la sede de su actividad económica. En este caso, ADstudio deberá fijar el IVA de España para la venta de sus servicios y productos en el extranjero por comercio electrónico.

De acuerdo a la localización de los servicios prestados por vía electrónica, tendremos los siguientes supuestos, suponiendo que se trata de una empresa que esta establecida en España y que vende sus productos también a través de Internet, como realiza ADstudio:

- Si proporciona un servicio a un empresario o consumidor español, se grava el IVA español correspondiente
- Si proporciona un servicio a un empresario de la Unión Europea, no se grava el IVA español, sino que se grava el IVA del país de destino.

- Si proporciona un servicio a un empresario fuera de la Unión Europea, no se grava el IVA español, salvo que el servicio se use efectivamente en España.
- Si proporciona un servicio a un empresario de Canarias, Ceuta o Melilla, no se grava el IVA.
- Si proporciona un servicio a un particular fuera de la Unión Europea, tampoco se grava el IVA.

ADstudio deberá declarar todos los servicios prestados por vía electrónica a particulares en todos y cada uno de los estados miembros de la Unión Europea. Lo podrá hacer cumpliendo las siguientes obligaciones:

- Declarar vía electrónica el inicio, la modificación y el cese de las operaciones incluidas en este régimen especial.
- Presentar vía electrónica, una declaración-liquidación trimestral del IVA, aún cuando en el correspondiente período trimestral no se hayan prestado servicios por vía electrónica. El plazo establecido es de 20 días a partir del final del período a que se refiere la declaración, es decir, hasta el 20 de abril en caso del primer trimestre, el 20 de julio del segundo, el 20 de octubre del tercero y el 20 de enero del último.
- Ingresar el IVA a la Agencia Tributaria en el momento de presentar la declaración o liquidación.
- Mantener un registro de las operaciones incluidas en este régimen especial.
- Expedir y entregar factura por las operaciones que se acojan a este régimen especial.

## 10.6. LA E-FACTURA

ADstudio tiene la obligación de expedir y entregar facturas a sus clientes, además de conservar una copia de las mismas durante un periodo de tiempo correspondiente al plazo de prescripción. La factura electrónica tiene la misma validez que la factura tradicional.

Una factura electrónica es la representación informática de una factura, generado y mantenido electrónicamente, que reemplaza al documento físico pero que tiene un valor idéntico.

Cuando entra en vigor el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento que regula las obligaciones de facturación, que modifica el Reglamento de Impuesto sobre Valor Añadido, se abre la posibilidad de enviar facturas por medios electrónicos de una forma normalizada.

Las obligaciones que tienen que tener en cuenta las empresas que emiten facturas electrónicas, como puede hacerlo ADstudio son:

- Conservar los datos de las facturas. No es necesario conservar las facturas físicamente, sino los propios datos en una base de datos que permitan generarlas.
- Asegurar que en el futuro podrán ser leídas en su formato original.
- Garantizar el acceso completo a las facturas: visualización, búsqueda selectiva, copia o descarga en línea o impresión.
- Están obligadas a firmar electrónicamente la factura o delegar esta acción a un tercero (subfacturación), o en el Receptor (autofacturación). Se debe contar con la autorización del receptor el uso de la modalidad de facturación.

Por otro lado, las obligaciones que tienen que cumplir las empresas que reciban facturas electrónicas son:

- Conservar las facturas recibidas en su formato original (electrónico), incluso aunque hayan sido necesarias transformaciones de datos internas.

- Puede conservar la factura impresa con marcas gráficas tipo PDF o almacenarla en otro tipo de soportes como un CD por ejemplo.
- Se debe asegurar la legibilidad en el formato original.
- Se debe garantizar el acceso completo a las facturas, visualización, búsqueda selectiva, copia o descarga en línea e impresión.
- Disponer de software necesario que permita verificar la firma e identidad del emisor, así como la vigencia del certificado digital.

Para que la Agencia Tributaria pueda controlar la fiscalidad de todas las transacciones comerciales vía electrónica, deberán incorporar firma electrónica reconocida, utilizando cualquiera de los certificados de firma electrónica, para el cumplimento de las obligaciones tributarias formales por medios telemáticos.

# Administración Electrónica

## 11.1. INTRODUCCIÓN

Desde el 1 de enero de 2010 las Administraciones Públicas están obligadas a proporcionar el acceso electrónico para las gestiones publicas a los ciudadanos. Esta fecha marca el establecimiento de la Ley de Acceso Electrónico con el objetivo de proporcionar la comunicación electrónica entre el ciudadano y las administraciones y la obligación de las Administraciones de dotarse de los medios y sistemas electrónicos suficientes y necesarios para que se pueda ejercer el derecho.

Anteriormente se pretendía que las Administraciones se dotasen de todos los equipos técnicos necesarios, pero hasta esta Ley no tiene carácter de obligación. De esta manera, todos los documentos que emita la Administración Pública o sus copias, gozarán de la misma validez que en formato papel, siempre que la autenticidad, integridad y conservación estén garantizadas.

Para las empresas, se trata de una oportunidad para la facilitación de las tramitaciones y gestiones necesarias con las Administraciones, lo que supondrá un importante ahorro de tiempo y dinero en desplazamientos. De esta forma, no será necesaria la presencia física en cualquiera de las Administraciones como algún Ministerio, el Ayuntamiento de tu ciudad o el gobierno de la región.

## 11.2. LEY DE ACCESO

La Ley de Acceso esta compuesta por cuatro títulos, más el Título Preliminar (Artículos 1 al 5) titulado “del ámbito de aplicación y los principios generales”, donde se recogen las finalidades de la Ley y un anexo sobre definiciones. Los demás cuatro títulos son “Los derechos de los ciudadanos”, “Régimen jurídico de la Administración electrónica”, “Gestión electrónica de los procedimientos” y “Cooperación entre Administraciones para el impulso de la Administración electrónica”.

### 11.2.1. TÍTULO I

El Título I de la Ley viene titulado como “Los derechos de los ciudadanos” y es donde se establece la obligación a la Administración de habilitar todos los medios necesarios para el cumplimiento de los derechos de los ciudadanos en sus relaciones con la Administración Pública.

Entre los servicios electrónicos de calidad que debe prestar se encuentran:

- El ejercicio de los derechos
- Obtener informaciones
- Realizar consultas y alegaciones
- Formular solicitudes
- Manifestar consentimiento
- Establecer pretensiones
- Efectuar pagos
- Realizar transacciones
- Oponerse a resoluciones y actos administrativos

El ciudadano o empresa, en este caso ADstudio, podrá escoger el canal de comunicación más adecuado para sus relaciones con las Administraciones Públicas, ya sea físico, es decir, de manera presencial, o electrónico, como podría ser mediante Internet, SMS, TDT etc.

También, se contempla que cada Administración tiene la obligación de facilitar datos y documentos que hayan sido aportados a otras Administraciones, con el consentimiento del titular (en cumplimiento con la Ley de Protección de Datos). De esta manera, la empresa ADstudio no tendrá que presentar los mismos datos varias veces para las diferentes administraciones.

Existe una entidad que vela por la defensa de los ciudadanos que se relacionan con la Administración Pública vía electrónicamente, que se denomina "Defensor del usuario de la Administración Electrónica".

### 11.2.2. TÍTULO II

Este Título aparece titulado como "El régimen jurídico de la Administración Electrónica" y se divide a su vez en varios capítulos.

El primer capítulo recoge las características de la sede electrónica, que se entiende como la dirección electrónica que cada Administración debe poner a disposición de los ciudadanos a través de las redes electrónica, cuya gestión y administración debe correr a cargo de la Administración Pública. Debe funcionar con plena responsabilidad respecto de la integridad, veracidad y actualización de la información y los servicios a los que puede accederse a través de ella.

En el capítulo segundo, titulado como "identificación y autenticación", se recogen las formas en las que se deberán realizar la identificación y autenticación del ciudadano que se relaciona con la Administración. Esta potencia el uso del Documento Nacional de Identidad Electrónico (DNIe) y el uso de las firmas electrónicas que llevan incorporadas.

En el capítulo tercero se regulan los registros electrónicos, las comunicaciones y las notificaciones electrónicas.

El capítulo cuarto, “De los documentos y archivos electrónicos”, regula las condiciones de validez de un documento electrónico y las copias electrónicas.

### 11.2.3. TÍTULO III

Se titula “Gestión electrónica de los procedimientos” y hace referencia a la posibilidad que tiene un ciudadano, o una empresa como ADstudio para consultar electrónicamente la información del estado de tramitación de los procedimientos (iniciación, instrucción o terminación), tanto gestionados en su totalidad por medios electrónicos como para el resto de ellos.

ADstudio también tiene la posibilidad de obtener copias electrónicas de los documentos electrónicos que formen parte de sus procedimientos.

### 11.2.4. TÍTULO IV

En este título, que se titula “Cooperación entre Administraciones para el impulso de la Administración electrónica”, se determinan los principios para garantizar la interoperabilidad de los sistemas de información entre Administraciones.

Por ejemplo, una de esas medidas es la publicación exclusivamente electrónicamente del BOE desde el 1 de enero de 2009, desapareciendo su edición en papel.

### 11.2.5. FINES DE LA LEY DE ACCESO

De acuerdo con lo que se contempla en el artículo 3 de la Ley de Acceso, los fines de la misma son:

1. Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.

2. Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso, como:

    a. Barreras temporales: se podrá acceder las 24 horas del día a la Administración.

    b. Barreras espaciales: se evitarán los desplazamientos.

    c. Barreras funcionales: facilita el acceso a todas las personas, independientemente de su situación física.

    d. Barreras operativas: se evitarán largas colas de espera.

3. Se crean las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.

5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las Tecnologías de la Información, con las debidas garantías en la realización de sus funciones.

6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.

7. Contribuir al desarrollo de la Sociedad de la Información en el ámbito de las Administraciones Públicas y en sociedad en general.

Para ADstudio esta Ley supone una ventaja a la hora de resolver cualquier cuestión con las Administraciones Públicas, ya sean locales, regionales o nacionales. De esta manera, la empresa

podrá pagar impuestos a través de la sede electrónica de la Agencia Tributaria, presentarse a cualquier concurso público o solicitar subvenciones. Con esto la empresa gana en tiempo y ahorra en costes, ya que no tiene que desplazar a un empleado durante un determinado tiempo a una administración para realizar todas las gestiones administrativas. Todo ello de una forma segura y manteniendo la integridad de las comunicaciones entre ambas partes en todo momento.

# ANEXO I - Documento de Seguridad

## OBJETO DEL DOCUMENTO

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

El desarrollo reglamentario de este artículo se encuentra en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre.

El presente documento responde a la obligación establecida en la Normativa española sobre Protección de Datos, donde se recogerán las medidas de índole técnica y organizativa que establece la Ley.

Este documento es de carácter interno en la empresa.

## AMBITO DE APLICACIÓN

El documento de seguridad ha sido elaborado por el Responsable de Seguridad, responsable de la implantación de la normativa sobre seguridad en los datos de carácter personal en la empresa y que es de obligado cumplimento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso a los datos.

El Responsable de Seguridad a su vez se encargará de mantener en todo momento el documento actualizado y revisado siempre que se produzcan cambios importantes en el sistema de información, sistema de tratamiento que se emplea, organización, contenido de la información de los ficheros o tratamientos o como consecuencia de los controles periódicos realizados. [62]

El Responsable también adecuará el contenido del documento de seguridad a normativa vigente en materia de seguridad de datos de carácter personal.

La persona nombrada como Responsable de Seguridad en materia de datos de carácter personal en ADstudio es .....

Según el tipo de dato de carácter personal, se engloba en un diferente nivel de seguridad:

NIVEL ALTO:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respeto de los que se prevea la posibilidad de adoptar el nivel básico
- recabados con fines policiales sin consentimiento de las personas afectadas
- derivados de actos de violencia de género

NIVEL MEDIO:

- sobre infracciones administrativas o penales

[62] Artículo 88, apartado 7 de la Ley Orgánica 15/1999 sobre Protección de Datos, de 13 de diciembre

- sobre prestación de servicios de solvencia patrimonial y crédito [63]
- sobre administraciones tributarias
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros
- de Entidades Gestoras y Servicios Comunes de Seguridad Social
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
- que ofrezcan una definición de personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización

NIVEL BÁSICO

- cualquier otro fichero que contenga datos de carácter personal
- también los ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, solamente 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 de o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guardan relación con la finalidad del fichero
    - 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

[63] Artículo 29 de la Ley Orgánica 15/1999 sobre Protección de Datos, de 13 de diciembre.

## RELACIÓN DE FICHEROS DECLARADOS

Según la relación de ficheros que son responsabilidad de la empresa, se han notificado a la Agencia Española de Protección de Datos los siguientes ficheros:

- PROVEEDORES

▸ Descripción: gestión de proveedores

▸ Finalidad: gestión administrativa, fiscal y contable con los proveedores, contacto, publicidad, promociones, catálogos y otras ofertas.

▸ Nivel de Seguridad: Básico (nombre y apellidos, dirección, localidad, provincia, código postal, teléfono, fax, e-mail, tipo de proveedor, datos económicos)

▸ Encargado del Tratamiento: ADstudio

- CLIENTES

▸Descripción: datos de contactos de clientes, personas físicas y jurídicas, de la empresa

▸ Finalidad: gestión de clientes, relación comercial y contractual, administrativa, contable y fiscal, fidelización de clientes, campañas publicitarias, promociones y descuentos especiales

▸ Nivel de Seguridad: básico (nombre, apellidos, dirección, teléfono, tipo de cliente, datos económicos)

▸ Encargado del Tratamiento: ADstudio

- FICHERO DE SELECCIÓN

▸Descripción: gestión de los procesos de selección de recursos humanos

▸ Finalidad: selección de candidatos para cubrir los puestos vacantes en la empresa

- Nivel de Seguridad: medio (nombre, apellidos, DNI, dirección, teléfono, imagen, firma, email, características personales, datos académicos y profesionales, detalles del empleo)

- Encargado del Tratamiento: ADstudio

## FICHERO DE PERSONAL

- Descripción: gestión de los datos del personal de la empresa

- Finalidad: gestión de nóminas y demás funciones del departamento de Recursos Humanos

- Nivel de Seguridad: medio (nombre y apellidos, DNI, dirección, teléfono, Número de la Seguridad Social, imagen, características personales, datos académicos y profesionales, datos económicos, financieros, seguros)

- Encargado del Tratamiento: ADstudio

## VIDEOVIGILANCIA

- Descripción: imágenes obtenidas en las cámaras de seguridad

- Finalidad: seguridad de las instalaciones

- Nivel de Seguridad: básico (imágenes obtenidas para la seguridad de la empresa)

- Encargado del Tratamiento: ADstudio

## FOTOGRÁFICO

- Descripción: imágenes para el desarrollo de la actividad publicitaria de la empresa

- Finalidad: fines comerciales de la empresa

- Nivel de Seguridad: básico

- Encargado del Tratamiento: ADstudio

Periódicamente, y siempre que haya alguna modificación, tanto en la legislación vigente como en alguno de los datos de la declaración de ficheros a la Agencia, el Responsable de Seguridad revisará los ficheros declarados y realizará las modificaciones o cancelaciones para cada caso.

## FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todas los empleados de la empresa que accedan a datos de carácter personal están obligados a conocer y observar las medidas, normas, procedimientos, reglas y estándares establecidos por la normativa vigente sobre Protección de Datos. Será obligación del Responsable del Fichero establecer todas las medidas oportunas así como mecanismos para evitar que una persona que no esta autorizada pueda acceder a datos con un nivel de seguridad más alto.

Es obligación del personal de la empresa que toda clase de incidencia sobre seguridad debe ser notificada al Responsable de Seguridad de la empresa.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos de carácter personal en el transcurso de su rutina laboral, haciendo uso de ellos exclusivamente para los fines para los cuales esos datos han sido recabados y no cediendo información confidencial, salvo excepciones en los que esté autorizado. También deberá cumplir los procedimientos y normas de seguridad que contiene este documento.

El personal de ADstudio se clasifica de este modo en tres categorías:

- Responsable de Seguridad: será el responsable de la difusión del documento de seguridad entre todo el personal de la empresa que vaya a utilizar el fichero y el responsable de la implantación de medidas establecidas en este documento.
- Administradores del sistema: encargados de administrar los sistemas operativos de la empresa, donde se encuentra el entorno operativo de los ficheros. Por las funciones de su trabajo rutinario en la empresa utilizan las herramientas de administración que permiten el acceso a los datos de carácter personal protegidos por la empresa, pudiéndose saltar las barreras de acceso de las aplicaciones y acceder a los mismos.
- Usuarios del fichero: personal que para el desarrollo de su trabajo rutinario en la empresa utilizan o consultan los ficheros con los datos de carácter personal.

| PERFIL | PUESTO | FUNCIONES | OBLIGACIONES | FICHEROS |
|---|---|---|---|---|
| Responsable de Seguridad | Responsable de seguridad | - Acceso a ficheros<br>- Inventario de ficheros<br>- Comprobar cumplimiento de la normativa vigente | Velar por la seguridad de los datos | - Todos |
| Informático | Administrador de red | - Acceso a ficheros<br>- Crear usuarios y perfiles<br>- Copias de seguridad | Velar por la seguridad de los datos en los sistemas de información | - Todos |
| Recursos Humanos | Gestión de personal | - Nóminas<br>- Empleados<br>- Selección de curriculums | Gestión de personal en la empresa | - Fichero de selección<br>- Fichero de personal |
| Administración | Gestión administrativa | - Contabilidad<br>- Fiscalidad<br>- Administración | Gestión administrativa en la empresa | - Clientes<br>- Proveedores |
| Comercial y Marketing | Gestión comercial y Marketing | - Publicidad<br>- Marketing<br>- Clientes<br>- Proveedores | Gestión comercial y marketing comercial y publicitario de la empresa | - Clientes<br>- Proveedores<br>- Fotográfico |
| Dirección | Dirección de la empresa | - Dirección | Dirección | - Todos |

El incumplimiento de la normativa y todas las obligaciones que esta conlleva puede llevar a la empresa a ser sancionada económicamente por la Agencia Española de Protección de Datos, que según su gravedad pueden ser:

LEVES

- Las sanciones van de 601 a 60.101 euros
- Puedes ser sancionado por no cumplir las instrucciones de la Agencia Española de Protección de Datos, poseer datos obsoletos, no rectificar inexactitudes

GRAVES

- Las sanciones pueden ser de 60.101 a 300.506 euros
- Crear ficheros con finalidades distintas al objeto legítimo de la entidad, no declarar ficheros sobre Protección de Datos a la Agencia.

MUY GRAVES

- Las sanciones pueden ser de 300.506 a 601.012 euros
- Cesión no permitida de datos personales, vulnerar principios para datos especialmente protegidos.

## NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Para que no exista un acceso no autorizado a ficheros de datos de carácter personal se realiza mediante el control de todos los procedimientos que pueden dar acceso a esa información.

Los recursos que pueden servir de medio directo o indirecto para tener acceso a al fichero son:

- Instalaciones de la empresa donde se encuentren ubicados los ficheros o se almacenan los soportes que los contengan
- Los puestos de trabajo desde donde se pueda tener acceso a los datos
- Los servidores y el entorno donde este situado el fichero
- Los sistemas informáticos establecidos para acceder al fichero

### INSTALACIONES DE LA EMPRESA

Las instalaciones de la empresa donde estén ubicados los ordenadores que contengan los ficheros de datos de carácter personal deben ser objeto de especial protección, especialmente en el caso que el fichero esté ubicado en un servidor accedido a través de una web.

- El local debe contar con las medidas de seguridad apropiadas destinadas a evitar riesgos fortuitos o intencionados.
- El acceso al local donde se encuentran los ficheros debe estar restringido solamente a los administradores del sistema.
- En caso de que el fichero sea de documentación no automatizada con nivel de seguridad medio y alto, debe encontrarse ubicada en armarios protegidos con puertas con llave. Las personas que sean responsables del tratamiento de los datos que albergan estos ficheros serán los responsables de la custodia de dichos documentos.

## PUESTOS DE TRABAJO

Se refiere a todos los dispositivos a través de los cuales se puede acceder a los datos de un ficheros, como por ejemplo, ordenadores de trabajo.

- Las personas con derecho de acceso a los ficheros de datos de carácter personal están detalladas en el apartado “Funciones y obligaciones del personal”
- Implica que tanto los monitores como impresoras u otros dispositivos este ubicados en sitios que ofrezcan cierta confidencialidad.
- Cuando el responsable de un puesto de trabajo abandone su puesto temporalmente o fin de jornada laboral, deberá dejarlo de tal modo que se garantice una confidencialidad en la información que contiene los ficheros. Se debe impedir la visualización de los datos protegidos mediante contraseña.
- En el caso de las impresoras, el empleado debe asegurarse que no quedan documentos impresos relacionados con información de carácter personal en la bandeja de la misma cuando las impresoras sean compartidas para varios empleados. Los responsables deberán ir retirando los documentos de la impresora según vayan saliendo impresos.
- Queda prohibido la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero.
- Los puestos desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones y no podrá ser modificada o cambiada si no es bajo supervisión y autorización del responsable de seguridad.

## ENTORNO DE SISTEMA OPERATIVO Y DE COMUNICACIONES

Es necesario regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, de forma que se impida el acceso no autorizado a los datos de fichero.

- El sistema operativo tiene que tener al menos un responsable en la empresa

- Si un fichero se encuentra ubicado solamente en un ordenador personal, el administrador del sistema operativo podrá ser el mismo usuario que accede al fichero en el desempeño de su trabajo.
- Ninguna herramienta que permita el acceso a un fichero deberá ser accesible a ningún usuario.
- El administrador es el responsable de guardar en un lugar protegido las copias de seguridad y respaldo del fichero, de forma que ninguna persona sin autorización tenga acceso a ellas.

## SISTEMAS INFORMÁTICOS O APLICACIONES

Son todos aquellos sistemas informáticos o aplicaciones con las que se puede acceder a los datos del fichero y que suelen ser utilizados por los usuarios para acceder a los mismos, como puede ser el sistema de gestión empresarial SAP.

- El acceso a los ficheros dentro de estos sistemas informáticos o aplicaciones tienen acceso restringido mediante nombre de usuario y contraseña, con una caducidad periódica.
- Si la aplicación no cuenta con un control de acceso predefinido por el mismo, deberá ser el sistema operativo el que ejecute esa restricción de acceso, mediante un nombre de usuario y contraseña igualmente.
- Se controlará los intentos de acceso inválidos al fichero, de tal manera que se limitará el número máximo de intentos fallidos.

## PROTECCIÓN DE CONTRASEÑAS PERSONALES

Uno de los elementos más importantes en cuanto a la seguridad informática son las contraseñas personales, que vienen asociadas a un nombre de usuario individual. Se utilizan como llave de acceso al sistema y tienen que ser estrictamente confidenciales y personales.

- Cada indicio que haga suponer que se esta atentando contra la confidencialidad de las contraseñas, debe ser inmediatamente comunicado al administrador del sistema.

- Cada usuario es responsable de la confidencialidad de su contraseña. En caso de que sea conocida fortuitamente o fraudulentamente, deberá abrirse una incidencia al Responsable de Seguridad de la empresa.
- Las contraseñas deben ser cambiadas y asignadas mediante un cierto mecanismo y periodicidad que será establecido por el Responsable de Seguridad junto con los administradores.
- El mecanismo donde se almacenen las contraseñas deberá estar protegido y bajo responsabilidad del administrador del sistema.

## GESTIÓN DE INCIDENCIAS

Una incidencia es cualquier circunstancia que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del fichero, en cuanto a su confidencialidad, integridad y disponibilidad de datos, como por ejemplo:

- Acceso no autorizado a datos y recursos
- No bloqueo del usuario por contraseña errónea
- Incidencias en los tratamientos informatizados de datos
- Perdida o deterioro de los soportes magnéticos
- Recuperación de los datos
- Accesos de personas no autorizadas a instalaciones donde se ubiquen los ficheros

Cuando una persona solicite ejercitar su derecho de acceso, rectificación, cancelación y oposición a los datos de carácter personal que posea la empresa será considerado una incidencia.

Las comunicaciones de las incidencias deberán realizarse directamente a la persona responsable, en este caso al Responsable de Seguridad de la empresa.

Se debe mantener un registro de incidencias para así poder prevenir posibles o futuros ataques a esa seguridad. El Responsable de Seguridad en este caso debe abrir un Libro de Incidencias donde deben ser registradas, que deberá estar bajo su responsabilidad.

## GESTIÓN DE SOPORTES

Un soporte informático es un medio de grabación y recuperación de datos que se utiliza para realizar copias y que pueden ser utilizados en los procesos de la aplicación que gestiona un fichero.

Como estos tipos de soportes son fácilmente transportables, reproducibles y copiables, es evidente que la seguridad en estos dispositivos es esencial para un correcto y adecuado flujo de datos de carácter personal en la empresa.

- Los soportes que contengan datos de algún fichero de datos de carácter personal debe ser almacenado en algún lugar en los que no tenga acceso ninguna persona no autorizada para el uso de esa información.
- Solamente se podrán realizar copias o podrán ser reproducidos estos soportes con contenido acerca de los ficheros bajo control del Responsable de Seguridad.
- Las copias desechadas deberán ser destruidas para que se impida el acceso a la información. En el caso que se trate de medios reutilizables, se deberá destruir toda la información que contienen (formatear) antes de volver a ser reutilizados.
- Es importante y necesario identificar aquellos soportes que contengan datos de algún fichero para su identificación y localización en la empresa.
- Para una mayor seguridad, no esta permitida la salida de este tipo de soportes que contengan datos de carácter personal fuera de las instalaciones de la empresa.

## GESTIÓN DE FICHEROS TEMPORALES

Se debe establecer un procedimiento adecuado para la creación, mantenimiento y cancelación de un fichero de carácter temporal, para que, aunque sea temporal, se garantice seguridad de los datos personales que estos contengan.

Cuando la empresa necesite crear un fichero para una finalidad específica, por lo que pasado un periodo de tiempo deja de ser útil para la empresa, se pueden llevar a cabo uno de los siguientes procedimientos:

- Registrar el fichero en la Agencia Española de Protección de Datos. Esto supone un mayor coste administrativo y de tiempo, ya que supone la inscripción del fichero y la adopción de las medidas de seguridad oportunas de acuerdo a la normativa vigente así como su mantenimiento actualizado, y la obligación de cancelarlo cuando la información este desfasada. Si se elige este procedimiento es porque a la empresa le interesa su mantenimiento principalmente, así que dejaría de ser un fichero temporal.
- Eliminarlo

## PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN

Para garantizar la integridad y la disponibilidad de los datos de carácter personal de los ficheros de una empresa, existen unos procesos de respaldo y recuperación que permite que en caso de fallo informático y correspondiente pérdida de la información, se recuperen o reconstruyan los datos.

- El administrado del sistema es responsable de realizar una copia de seguridad del fichero de forma periódica.
- En caso de que el fallo en el sistema llegue a pérdida total o parcial de los datos albergados en el sistema, existen unos procedimientos informáticos concretos para su reconstrucción en el estado en el que se encontraban en el momento del fallo.

## CONTROLES PERIÓDICOS DE VERIFICACIÓN DEL CUMPLIMIENTO

Tanto la veracidad como la adecuación del documento al cumplimiento de la legislación vigente en cada momento debe ser periódicamente comprobada, para así poder detectar posibles fallos, carencias o desuso en la información del documento.

- El Responsable de Seguridad de la empresa debe comprobar de forma periódica la lista de usuarios con acceso a ficheros de datos de carácter personal.
- El administrador de redes debe comunicar al Responsable de Seguridad cualquier alta o baja de usuarios con acceso a algún fichero de datos.
- Se debe comprobar de forma regular también la existencia de copias de respaldo para una posible recuperación de los datos.
- Se establece que cada año se realice una auditoría, que puede ser externa o interna para que asegure un correcto cumplimiento de la normativa vigente en cada momento y la correcta adecuación de las medidas presentes en este Documento de Seguridad.
- Tanto los controles periódicos como las auditorías deben quedar reflejadas en el Libro de Incidencias que el Responsable de Seguridad ha dispuesto a la empresa.

# ANEXO II - Registro de Ficheros

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN

NOTIFICACIONES TELEMATICAS A LA AEPD

No válida para presentación

1 Responsable del fichero — Validar — Borrar — ?

Denominación social del responsable del fichero | Actividad

CIF/NIF | Domicilio Social

Localidad | Código Postal | Provincia | País

Teléfono | Fax | Correo electrónico

2 Derechos de oposición, acceso, rectificación y cancelación — Validar — Borrar — ?

Nombre de la oficina o dependencia

CIF/NIF | Dirección postal / Apdo. de Correos

Localidad | Código Postal | Provincia | País

Teléfono | Fax | Correo electrónico

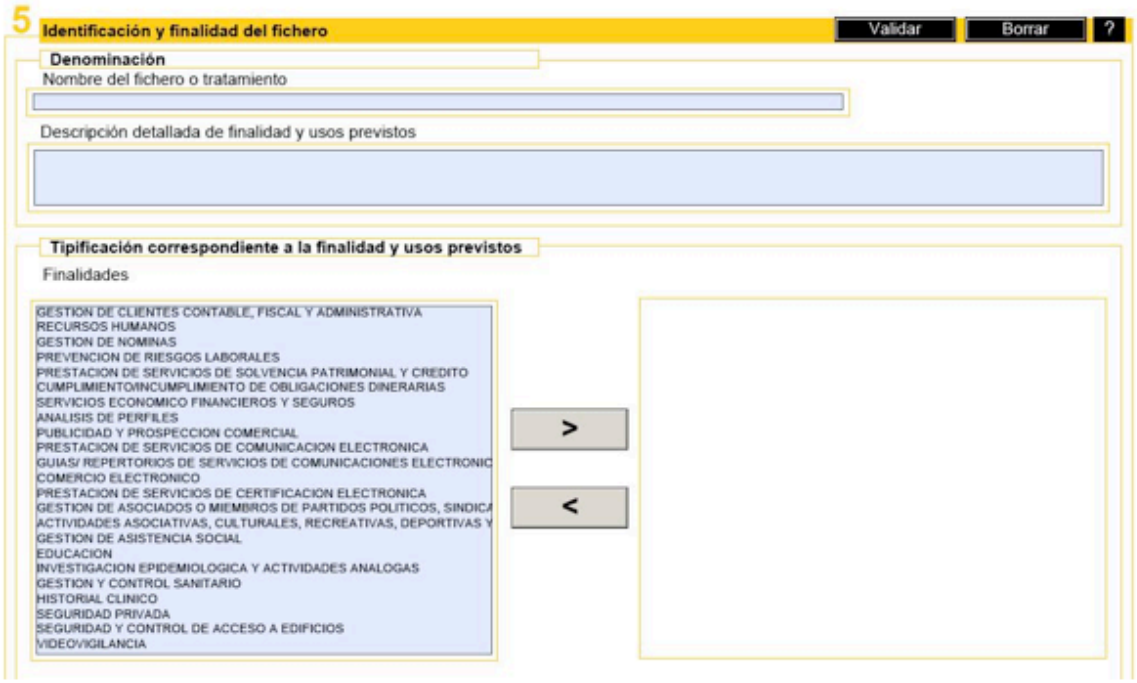
4 Encargado del tratamiento — Validar — Borrar — ?

Denominación social del encargado del tratamiento

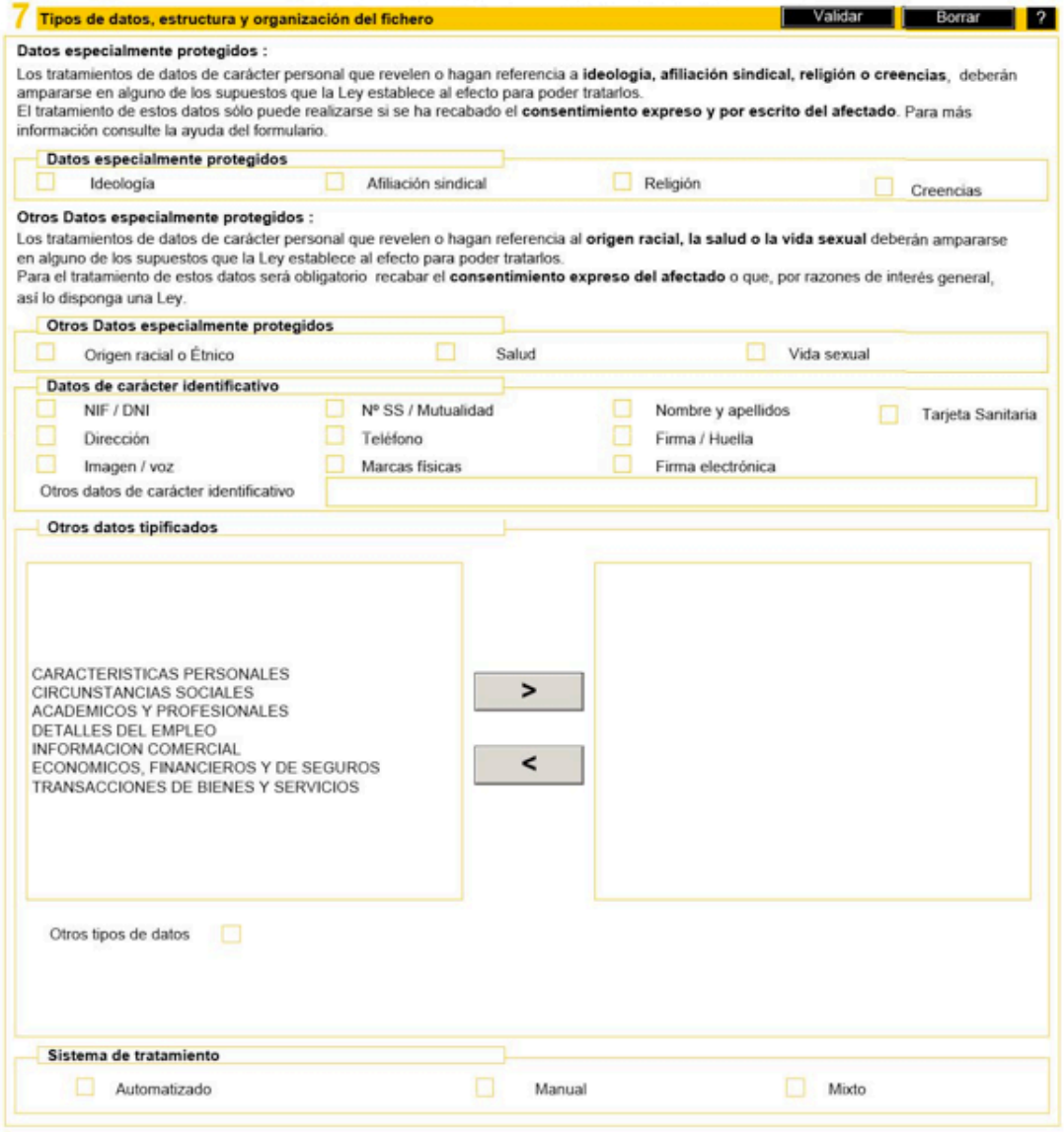
CIF/NIF | Dirección postal

Localidad | Código Postal | Provincia | País

Teléfono | Fax | Correo electrónico


5
Identificación y finalidad del fichero
Validar
Borrar
?
Denominación
Nombre del fichero o tratamiento
Descripción detallada de finalidad y usos previstos
Tipificación correspondiente a la finalidad y usos previstos
Finalidades
GESTION DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA
RECURSOS HUMANOS
GESTION DE NOMINAS
PREVENCION DE RIESGOS LABORALES
PRESTACION DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CREDITO
CUMPLIMIENTO/INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS
SERVICIOS ECONOMICO FINANCIEROS Y SEGUROS
ANALISIS DE PERFILES
PUBLICIDAD Y PROSPECCION COMERCIAL
PRESTACION DE SERVICIOS DE COMUNICACION ELECTRONICA
GUIAS/ REPERTORIOS DE SERVICIOS DE COMUNICACIONES ELECTRONIC
COMERCIO ELECTRONICO
PRESTACION DE SERVICIOS DE CERTIFICACION ELECTRONICA
GESTION DE ASOCIADOS O MIEMBROS DE PARTIDOS POLITICOS, SINDICA
ACTIVIDADES ASOCIATIVAS, CULTURALES, RECREATIVAS, DEPORTIVAS Y
GESTION DE ASISTENCIA SOCIAL
EDUCACION
INVESTIGACION EPIDEMIOLOGICA Y ACTIVIDADES ANALOGAS
GESTION Y CONTROL SANITARIO
HISTORIAL CLINICO
SEGURIDAD PRIVADA
SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS
VIDEOVIGILANCIA
>
<


6
Origen y procedencia de los datos
Validar
Borrar
?
Origen
El propio interesado o su representante legal
Otras personas físicas
Fuentes accesibles al público
Registros públicos
Entidad privada
Administraciones Públicas
Colectivos o categorías de interesados
EMPLEADOS
CLIENTES Y USUARIOS
PROVEEDORES
ASOCIADOS O MIEMBROS
PROPIETARIOS O ARRENDATARIOS
PACIENTES
ESTUDIANTES
PERSONAS DE CONTACTO
PADRES O TUTORES
REPRESENTANTE LEGAL
SOLICITANTES
BENEFICIARIOS
CARGOS PUBLICOS
>
<


7 Tipos de datos, estructura y organización del fichero
Validar
Borrar
?
Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia a ideología, afiliación sindical, religión o creencias, deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
El tratamiento de estos datos sólo puede realizarse si se ha recabado el consentimiento expreso y por escrito del afectado. Para más información consulte la ayuda del formulario.
Datos especialmente protegidos
Ideología
Afiliación sindical
Religión
Creencias
Otros Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia al origen racial, la salud o la vida sexual deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
Para el tratamiento de estos datos será obligatorio recabar el consentimiento expreso del afectado o que, por razones de interés general, así lo disponga una Ley.
Otros Datos especialmente protegidos
Origen racial o Étnico
Salud
Vida sexual
Datos de carácter identificativo
NIF / DNI
Nº SS / Mutualidad
Nombre y apellidos
Tarjeta Sanitaria
Dirección
Teléfono
Firma / Huella
Imagen / voz
Marcas físicas
Firma electrónica
Otros datos de carácter identificativo
Otros datos tipificados
CARACTERISTICAS PERSONALES
CIRCUNSTANCIAS SOCIALES
ACADEMICOS Y PROFESIONALES
DETALLES DEL EMPLEO
INFORMACION COMERCIAL
ECONOMICOS, FINANCIEROS Y DE SEGUROS
TRANSACCIONES DE BIENES Y SERVICIOS
>
<
Otros tipos de datos
Sistema de tratamiento
Automatizado
Manual
Mixto


8 Medidas de seguridad
Validar
Borrar
?
Nivel básico
Nivel Medio
Nivel Alto
9 Cesión o comunicación de datos
Validar
Borrar
?
Este apartado únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. No se considerará cesión de datos la prestación de un servicio al responsable del fichero por parte del encargado del tratamiento. La comunicación de los datos ha de ampararse en alguno de los supuestos legales establecidos en la LOPD. Para mayor información consulte la ayuda de este formulario.
Categorías de destinatarios de cesiones
ORGANIZACIONES O PERSONAS DIRECTAMENTE RELA
ORGANISMOS DE LA SEGURIDAD SOCIAL
REGISTROS PUBLICOS
COLEGIOS PROFESIONALES
ADMINISTRACION TRIBUTARIA
OTROS ORGANOS DE LA ADMINISTRACION PUBLICA
COMISION NACIONAL DEL MERCADO DE VALORES
COMISION NACIONAL DEL JUEGO
NOTARIOS Y PROCURADORES
FUERZAS Y CUERPOS DE SEGURIDAD
ORGANISMOS DE LA UNION EUROPEA
ENTIDADES DEDICADAS AL CUMPLIMIENTO/INCUMPLIM
BANCOS, CAJAS DE AHORRO Y CAJAS RURALES
ENTIDADES ASEGURADORAS
OTRAS ENTIDADES FINANCIERAS
ENTIDADES SANITARIAS
PRESTACIONES DE SERVICIOS DE TELECOMUNICACIO
>
<
10 Transferencias internacionales
Validar
Borrar
?
Este apartado únicamente ha de cumplimentarse en el caso de que se realice o esté previsto realizar un tratamiento de datos fuera del territorio del Espacio Económico Europeo. En el caso de que la transferencia internacional tenga como destino un país que no preste un nivel de protección adecuado al que presta la LOPD, deberá tener en cuenta que la LOPD establece que las previsiones para realizar transferencias internacionales son diferentes, dependiendo de que los países destinatarios tengan un nivel de protección adecuado o no. Para más información consulte la ayuda de este formulario.
Países y destinatarios de la transferencia
Países
Categoría de destinatarios
País
Otras categorías de destinatarios
Guardar
Imprimir
Limpiar
Validar
Volver a Preguntas iniciales
Cumplimentar Hoja de Solicitud

# ANEXO III - Ejercicio de Derechos

## SOLICITUD DEL EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL FICHERO Y RESPONSABLE DE FICHERO

Nombre del fichero o ficheros:

Responsable:

Dirección:

Localidad: Provincia: Código Postal:

Si Vd. desconoce el nombre del fichero o el responsable del mismo, puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información. La Agencia no dispone de la información contenida en el fichero, sino tan sólo de los nombres de los ficheros, responsables y direcciones de los mismos.

DATOS DEL SOLICITANTE[64]

D./Dña._____

Domicilio_____CP_____

Localidad/Provincia_____Teléfono_____

e-mail _____

DNI_____, del que acompaño fotocopia por medio de la presente solicitud manifiesto el deseo de ejercer mi Derecho de ACCESO respecto mis datos de carácter personal.

[64] Los datos personales recogidos serán incorporados y tratados en el fichero Clientes, cuya finalidad es la gestión y administración de los clientes, inscrito en el Registro de Ficheros de Datos Personales de la Agencia de protección de Datos, y no serán cedidos salvo en los casos previstos por la Ley. El órgano responsable del fichero es ADstudio, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es Plaza del Rey nº2, 09005 Burgos, España, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

SOLICITA:

Que se le faciliten sus datos de carácter personal contenidos en el fichero indicado, así como la información relacionada con el tratamiento de los mismos, de conformidad con el derecho de acceso regulado en el artículo 15 de la Ley Orgánica 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94, así como lo dispuesto en la Instrucción 1/2006, de 8 de noviembre, ( para el caso de tratamiento de imágenes), e Instrucción 1/1998, ambas de la Agencia Española de Protección de Datos.

INSTRUCCIONES:

Es necesario el nombre, apellidos y fotocopia del DNI o cualquier otro modo de identificación válido. Los mismos datos serán necesarios referidos al representante legal en caso de que el interesado sea menor o esté incapacitado, debiendo presentar la documentación que acredite la representación legal.Es necesario también que se acredite un domicilio para notificaciones, fecha y firma del interesado.El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo causa justificada.

El responsable deberá responder al solicitante en un plazo máximo de un mes, a contar desde la recepción de la solicitud. Si transcurrido este plazo sin que se conteste a la petición de acceso, está solicitud será entendida como denegada.

REQUISITOS:

Si la solicitud del derecho de acceso fuese desestimada, el responsable deberá informar al interesado, en la forma elegida por éste, en el plazo de 10 días desde la fecha de la estimación.

La información solicitada deberá contener los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y los fines para los que fueron recabados.

Este proceso es gratuito.

TUTELA DE DERECHOS: si transcurre un mes desde la solicitud de acceso y el solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus datos, puede reclamar ante la Agencia Española de Protección de Datos para que inicie el procedimiento de tutela de sus derechos.

Esta solicitud debe ser enviada a través de los siguientes medios:

- E-mail: arco@adstudio.com
- Correo postal: Plaza del Rey, nº2, 09005 Burgos
- Fax: 947685959

En....., a.....de.....de 201..

(Nombre y firma del solicitante)

## SOLICITUD DEL EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DEL FICHERO Y RESPONSABLE DE FICHERO

Nombre del fichero o ficheros:

Responsable:

Dirección:

Localidad: Provincia: Código Postal:

Si Vd. desconoce el nombre del fichero o el responsable del mismo, puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información. La Agencia no dispone de la información contenida en el fichero, sino tan sólo de los nombres de los ficheros, responsables y direcciones de los mismos.

DATOS DEL SOLICITANTE[65]

D./Dña._____

Domicilio_____CP_____

Localidad/Provincia_____Teléfono_____

e-mail _____

DNI_____, del que acompaño fotocopia por medio de la presente solicitud manifiesto el deseo de ejercer mi Derecho de RECTIFICACIÓN respecto mis datos de carácter personal.

[65] Los datos personales recogidos serán incorporados y tratados en el fichero Clientes, cuya finalidad es la gestión y administración de los clientes, inscrito en el Registro de Ficheros de Datos Personales de la Agencia de protección de Datos, y no serán cedidos salvo en los casos previstos por la Ley. El órgano responsable del fichero es ADstudio, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es Plaza del Rey nº2, 09005 Burgos, España, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

SOLICITA:

Que se proceda a la rectificación de los datos erróneos relativos a mi persona que se encuentran en el fichero, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, el artículo 15 del Real Decreto 1332/94, así como con la Instrucción 1/1998, de la Agencia de Protección de Datos.

Los datos a rectificar serían los siguientes:

INSTRUCCIONES:

Es necesario el nombre, apellidos y fotocopia del DNI o cualquier otro modo de identificación válido. Los mismos datos serán necesarios referidos al representante legal en caso de que el interesado sea menor o esté incapacitado, debiendo presentar la documentación que acredite la representación legal.Es necesario también que se acredite un domicilio para notificaciones, fecha y firma del interesado.El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo causa justificada.

El responsable deberá responder al solicitante en un plazo máximo de un mes, a contar desde la recepción de la solicitud. Si transcurrido este plazo sin que se conteste a la petición de acceso, está solicitud será entendida como denegada.

REQUISITOS:

Si la solicitud del derecho de acceso fuese desestimada, el responsable deberá informar al interesado, en la forma elegida por éste, en el plazo de 10 días desde la fecha de la estimación.

La información solicitada deberá contener los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y los fines para los que fueron recabados.
Este proceso es gratuito.

TUTELA DE DERECHOS: si transcurre un mes desde la solicitud de acceso y el solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus datos, puede reclamar ante la Agencia Española de Protección de Datos para que inicie el procedimiento de tutela de sus derechos.

Esta solicitud debe ser enviada a través de los siguientes medios:

- E-mail: arco@adstudio.com
- Correo postal: Plaza del Rey, nº2, 09005 Burgos
- Fax: 947685959

En....., a.....de.....de 201..

(Nombre y firma del solicitante)

## SOLICITUD DEL EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL FICHERO Y RESPONSABLE DE FICHERO

Nombre del fichero o ficheros:

Responsable:

Dirección:

Localidad: Provincia: Código Postal:

Si Vd. desconoce el nombre del fichero o el responsable del mismo, puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información. La Agencia no dispone de la información contenida en el fichero, sino tan sólo de los nombres de los ficheros, responsables y direcciones de los mismos.

DATOS DEL SOLICITANTE[66]

D./Dña._____

Domicilio_____CP_____

Localidad/Provincia_____Teléfono_____

e-mail _____

DNI_____, del que acompaño fotocopia por medio de la presente solicitud manifiesto el deseo de ejercer mi Derecho de CANCELACIÓN respecto mis datos de carácter personal.

[66] Los datos personales recogidos serán incorporados y tratados en el fichero Clientes, cuya finalidad es la gestión y administración de los clientes, inscrito en el Registro de Ficheros de Datos Personales de la Agencia de protección de Datos, y no serán cedidos salvo en los casos previstos por la Ley. El órgano responsable del fichero es ADstudio, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es Plaza del Rey nº2, 09005 Burgos, España, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

SOLICITA:

Que se proceda a la cancelación de cualquier dato relativo a mi persona que se encuentre en el fichero, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94, así como con la Instrucción 1/1998, de la Agencia de Protección de Datos.

INSTRUCCIONES:

Es necesario el nombre, apellidos y fotocopia del DNI o cualquier otro modo de identificación válido. Los mismos datos serán necesarios referidos al representante legal en caso de que el interesado sea menor o esté incapacitado, debiendo presentar la documentación que acredite la representación legal.Es necesario también que se acredite un domicilio para notificaciones, fecha y firma del interesado.El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo causa justificada.

El responsable deberá responder al solicitante en un plazo máximo de un mes, a contar desde la recepción de la solicitud. Si transcurrido este plazo sin que se conteste a la petición de acceso, está solicitud será entendida como denegada.

REQUISITOS:

Si la solicitud del derecho de acceso fuese desestimada, el responsable deberá informar al interesado, en la forma elegida por éste, en el plazo de 10 días desde la fecha de la estimación.

La información solicitada deberá contener los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y los fines para los que fueron recabados.

Este proceso es gratuito.

TUTELA DE DERECHOS: si transcurre un mes desde la solicitud de acceso y el solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus datos, puede reclamar ante la Agencia Española de Protección de Datos para que inicie el procedimiento de tutela de sus derechos.

Esta solicitud debe ser enviada a través de los siguientes medios:

- E-mail: arco@adstudio.com
- Correo postal: Plaza del Rey, nº2, 09005 Burgos
- Fax: 947685959

En....., a.....de.....de 201..

(Nombre y firma del solicitante)

## SOLICITUD DEL EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL FICHERO Y RESPONSABLE DE FICHERO

Nombre del fichero o ficheros:

Responsable:

Dirección:

Localidad: Provincia: Código Postal:

Si Vd. desconoce el nombre del fichero o el responsable del mismo, puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información. La Agencia no dispone de la información contenida en el fichero, sino tan sólo de los nombres de los ficheros, responsables y direcciones de los mismos.

DATOS DEL SOLICITANTE[67]

D./Dña._____

Domicilio_____CP_____

Localidad/Provincia_____Teléfono_____

e-mail _____

DNI_____, del que acompaño fotocopia por medio de la presente solicitud manifiesto el deseo de ejercer mi Derecho de CANCELACIÓN respecto mis datos de carácter personal.

[67] Los datos personales recogidos serán incorporados y tratados en el fichero Clientes, cuya finalidad es la gestión y administración de los clientes, inscrito en el Registro de Ficheros de Datos Personales de la Agencia de protección de Datos, y no serán cedidos salvo en los casos previstos por la Ley. El órgano responsable del fichero es ADstudio, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es Plaza del Rey nº2, 09005 Burgos, España, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

SOLICITA:

Que se proceda a excluir el tratamiento de cualquier dato relativo a mi persona que se encuentre en el fichero indicado, de conformidad con el derecho de oposición al tratamiento regulado en los artículos 6 y 17 de la Ley Orgánica 15/1999 y el Capítulo IV, del Título III, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Se adjunta además documentación justificativa de los motivos fundados y legítimos, relativos a una concreta situación personal del afectado.

INSTRUCCIONES:
Es necesario el nombre, apellidos y fotocopia del DNI o cualquier otro modo de identificación válido. Los mismos datos serán necesarios referidos al representante legal en caso de que el interesado sea menor o esté incapacitado, debiendo presentar la documentación que acredite la representación legal.Es necesario también que se acredite un domicilio para notificaciones, fecha y firma del interesado.El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo causa justificada.
El responsable deberá responder al solicitante en un plazo máximo de un mes, a contar desde la recepción de la solicitud. Si transcurrido este plazo sin que se conteste a la petición de acceso, está solicitud será entendida como denegada.

REQUISITOS:
Si la solicitud del derecho de acceso fuese desestimada, el responsable deberá informar al interesado, en la forma elegida por éste, en el plazo de 10 días desde la fecha de la estimación.
La información solicitada deberá contener los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y los fines para los que fueron recabados.
Este proceso es gratuito.

TUTELA DE DERECHOS: si transcurre un mes desde la solicitud de acceso y el solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus datos, puede reclamar ante la

Agencia Española de Protección de Datos para que inicie el procedimiento de tutela de sus derechos.

Esta solicitud debe ser enviada a través de los siguientes medios:

- E-mail: arco@adstudio.com
- Correo postal: Plaza del Rey, nº2, 09005 Burgos
- Fax: 947685959

En....., a.....de.....de 201..

(Nombre y firma del solicitante)

# ANEXO IV - Glosario de términos

- **Accesos autorizados**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

- **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento.

- **ARPANET (Advanced Research Projects Agency Network):** Agencia de Proyectos de Investigación para la Defensa, nacida en 1972 como resultado de las investigaciones que desde 1965 se llevaban a cabo desde la DARPA (U.S. Defense Advanced Research Projects Agency). Es la predecesora de Internet.

- **Autenticación:** procedimiento de comprobación de la identidad de un usuario.

- **B2B: (Business to business),** o b-to-b, engloba a las relaciones mercantiles y comerciales entre empresas. Conjunto de tecnologías basadas en los estándares internet que permiten conducir diferentes procesos de negocio que se desarrollan entre las empresas sobre una plataforma electrónica.

- **B2C: (Business to consumer),** o b-to-c. Comercio desde las empresas hacia el cliente final, al consumidor.

- **B2E (Business to employees),** o b-to-e. Comercio hacia los empleados. Venta a través del website corporativo, o desde las páginas de la intranet de acceso restringido, a los empleados de una empresa o conjunto de las mismas.

- **Banner:** Espacio publicitario en una web. Normalmente creado en Flash o como un Gif animado.

- **Cancelación**: procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

- **Certificado electrónico:** Certificado que proporciona una tercera entidad (Autoridad Certificadora) confiable, la cual verifica que las claves de encriptación pertenecen a las partes.

- **Cesión o comunicación de datos:** tratamiento de datos que supone su revelación a una persona distinta del interesado.

- **Comunidad Virtual:** Grupo de personas con intereses similares que hacen uso de un espacio en Internet para comunicarse y colaborar. Su gestión puede realizarse mediante grupos de noticias, foros de debate, chats, listas de distribución, etc.

- **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.

- **Contraseña**: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

- **Contrato Electrónico:** Contrato realizado on-line por las partes.

- **Control de acceso:** mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

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

- **Dato disociado:** aquél que no permite la identificación de un afectado o interesado.

- **Datos de carácter personal relacionados con la salud:** las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

- **Datos de carácter personal**: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- **Destinatario o cesionario:** la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

- **Dominio:** Nombre mediante el cual nos damos a conocer en internet. Es la dirección electrónica. Puede basarse en el nombre de la empresa o en una de sus marcar.

- **EDI (Electronic Data Interchange**): Intercambio Electrónico de datos. Sistema mediante el cual, de modo seguro, las empresas realizan transacciones entre ellas.

- **E-Marketing:** Técnicas de marketing aplicadas a la red para mejorar la visibilidad y posiciones en los buscadores.

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

- **Encriptación:** Proceso de codificar una información para evitar que sea accesible a todo aquel que no disponga del código de descodificación. Sirve para evitar que el contenido de mensajes pueda estar al alcance de cualquiera manteniendo de este modo un determinado nivel de seguridad y/o privacidad.

- **Exportador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

- **Extranet:** Prolongación de la intranet de una compañía para integrar compañías externas con las que se relaciona normalmente (clientes, proveedores, partners, etc).

- **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 esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

- **Fichero:** todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **Ficheros de titularidad privada**: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se

encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

- **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 los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

- **Ficheros temporales**: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

- **Firma Electrónica:** Sistema que permite a un usuario verificar su identidad en los medios digitales. Jurídicamente requiere equiparar a a la firma manuscrita, estableciéndose los requisitos que debe cumplir las actuales Agencias de Certificación.

- **FTP (File Transfer Protocol**): Sistema según el cual un ordenador almacena archivos o programas que el usuario puede descargarse accediendo a él a través de internet.

- **HTML:** Hypertext Markup Language. Lenguaje informático para crear páginas web. Conjunto de etiquetas o instrucciones que permiten estructurar el contenido de una web e incluir los hipervínculos o enlaces a otras páginas.

- **HTTP:** Hypertext Transfer Protocol. Protocolo estándar de transferencias de hipertextos. Es el protocolo de comunicaciones en el que es basado la Word Wide Web.
  identificación de un usuario físico.

- **Identificación**: procedimiento de reconocimiento de la identidad de un usuario.

- **Importador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Intranet:** Visualización interna de la red corporativa de una empresa o de algunas de sus funciones o informaciones mediante internet y sus estándares, destinada a ser usada por los empleados o directivos de la misma.

- **M-Commerce** (Mobile Commerce): Comercio electrónico desde el teléfono móvil.

- **Perfil de usuario:** accesos autorizados a un grupo de usuarios.

- **Persona identificable**: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

  Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

  Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

  Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Procedimiento de disociación**: todo tratamiento de datos personales que permita la obtención de datos disociados.

- **Protocolo**: Conjunto de normas que especifican como se comunican dos ordenadores entre si y como intercambian información.

- **Recurso:** cualquier parte componente de un sistema de información.

- **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.

- **Responsable del fichero o del tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

- **SET: (Secure Electronic Transaction**) Sistema que garantiza la seguridad en las transacciones electrónicas, defendiendo las especificaciones técnicas y los procesos.

- **Sistema de información**: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

- **Sistema de tratamiento**: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

- **Soporte**: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

- **SQL (Structured Query Language**): Lenguaje estructurado de petición. Es el sistema estándar utilizado para realizar solicitudes a la base de datos.

- **SSL: (Secure Socket Layer).** Sistema que permite qe la información entre el servidor y el cliente se transmita encriptado, evitándose que puede ser intervenida por terceras partes.

- **TCP/IP (Transmission Control Protocol/internet Protocol):** Sistema de Protocolos de comunicaciones entre ordenadores en el que se basa internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que

el segundo se responsabiliza de dirigirla adecuadamente a través de la red, seleccionando el camino óptimo para cada uno de los paquetes.

- **Tercero:** la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

- **Transferencia internacional de datos**: tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

- **Transmisión de documentos**: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

- **Tratamiento de datos:** cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
  Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

- **World Wide Web**: Sistema basado en hipertextos cuya función es buscar y tener acceso a documentos a través de la red. Se considera a Tim Berners-Lee el padre de la WWW.

ADstudio

# Bibliografía

## MONOGRAFÍAS / LIBROS


UNIVERSIDAD DE BURGOS / DAVARA&DAVARA. *Documentación Master MAC- TIC*. 2009-2010.

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Factbook Comercio Electrónico*. 3ª Edición, 2004, Pamplona. Editorial Aranzadi. 1497 p.

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Manual de Derecho Informático*. 10ª Edición, 2008, Pamplona. Editorial Aranzadi. 528 p.

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Análisis del Real Decreto 1720/2007: El Reglamento de la LOPD*. 1ª Edición, 2008, Madrid. Editorial DaFeMa. 256 p.

DAVARA RODRIGUEZ, MIGUEL ÁNGEL. *La protección de datos en la empresa*. 2003. Madrid. Edita Madrid Excelente. 65 p.

PABLO REDONDO, ROSANA. *Negocio Electrónico*. 2009. Madrid. Editorial UNED, Colección Aula Abierta. 280 p.

REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española*. Vigésima segunda edición, 2001, Madrid. Editorial RAE.

## PUBLICACIONES EN LÍNEA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Documentación* [en línea]

https://www.agpd.es/portalwebAGPD/index-ides-idphp.php.

CEDRO CENTRO ESPAÑOL DE DERECHOS REPROGRÁFICOS. *Derechos de autor* [en línea]. http://www.cedro.org/tipos_derechos.asp.

CERES. *Firma electrónica* [en línea].

http://www.cert.fnmt.es.

CUIDA TUS DATOS. *Introducción a la Ley de Protección de Datos* [en línea].

http://www.cuidatusdatos.com/lopd/index.html.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS ICANN. Nombres de dominio [en línea].

http://www.icann.org/tr/spanish.html